Zdravotně sociální fakulta
Faculty of Health and Social Sciences

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Analýza zranitelnosti elektrizační soustavy České republiky

DIPLOMOVÁ PRÁCE

Studijní program:

OCHRANA OBYVATELSTVA

Autor: Bc. Jan Michalec

Vedoucí práce: Ing. Lenka Brehovská, Ph.D.

České Budějovice 2017

Prohlášení

Prohlašuji, že svoji diplomovou práci s názvem *„Analýza zranitelnosti elektrizační soustavy České republiky“* jsem vypracoval samostatně pouze s použitím pramenů v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby diplomové práce. Rovněž souhlasím s porovnáním textu mé diplomové práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 15. května 2017

……

Bc. Jan Michalec

Poděkování

V první řadě bych chtěl poděkovat vedoucí práce Ing. Lence Brehovské Ph.D. za odborné vedení a trpělivost, dále všem expertům, kteří mi poskytli cenné rady a informace. V neposlední řadě rovněž Mgr. Ladislavu Louženskému a celé své rodině za podporu, nejvíce však svojí manželce Ing. Karolíně Michalcové, bez jejíž pomoci bych se neobešel.

Analýza zranitelnosti elektrizační soustavy České republiky

Abstrakt

Terorismem se někteří jedinci, skupiny nebo nadnárodní sítě snaží šířit pomocí násilí svoje politické názory, myšlenky a ideologii ve společnosti. Svými útoky mohou ohrozit zdraví a životy, životní prostředí a kritickou infrastrukturu jednotlivých států. V poslední době pro Evropu představují riziko primárně takzvaní zahraniční bojovníci pocházející ze států severní Afriky a Blízkého východu, jež jsou poškozeny rozsáhlou destabilizací a válečnými konflikty. Tomu všemu napomáhá neřešená otázka ilegální migrace z těchto zemí na území Evropské unie. Schengenský prostor umožňuje volný pohyb lidí na vnitřních hranicích členských států, což je obrovská výhoda pro volný pohyb občanů a obchodu, na druhou stranu však představuje velké bezpečnostní riziko z hlediska terorismu. Proto by měl být kladen mnohem větší důraz na ochranu vnějších hranic. Dalším obrovským problémem je radikalizace jednotlivců a skupin minorit na území členských států Evropské unie. Ta může být způsobena frustrací ze společnosti, kdy nebyla úspěšná jejich asimilace a zůstali vyloučeni na jejím okraji. Cílem práce bylo analyticky zhodnotit možné teroristické ohrožení elektrizační soustavy České republiky. Toho bylo dosaženo rozčleněním elektrizační soustavy na jednotlivé sektory a prvky a dále stanovením jednotlivých rizikových faktorů terorismu s pomocí expertů elektrizačních společností, následně byla provedena analýza pomocí checklistu. Poté proběhla komparace a vyhodnocení dat, čímž došlo k definování nejvíce ohrožených prvků elektrizační soustavy České republiky teroristickými útoky. Tato diplomová práce má sloužit pro navržení možných zlepšení v rámci elektrizační soustavy České republiky a pro výuku v rámci Zdravotně sociální fakulty Jihočeské univerzity v Českých Budějovicích.

Klíčová slova

kritická infrastruktura, elektrizační soustava, výrobny elektřiny, přenosová soustava, distribuční soustava, terorismus

Czech electricity grid vulnerability analysis

Abstract

Acts of terrorism are used by various individuals, groups and transnational networks to push forward own political views, ideas and ideology on society whilst using multiple forms of violence. Their acts of violence are able to jeopardize and endanger health and safety of peoples, environment and the vitality of critical infrastructure as well. Nowadays the most spelled threat comes from so called foreign fighters whose destabilized and war-torn countries of origin are located in Northern Africa and Middle East. In combination with inefficient management of illegal migration phenomenon and unsatisfactory EU policies on that matter the problem becomes even more amplified. Schengen Area provides EU-members with non-restrictive border regime which fosters migration and trade by a great deal but on the other hand it creates an enormous security risk in terms of terrorism and its prevention. For that matter there should be much more emphasis added to the management of EU outside borders. The second most problematic issue are the matters of radicalization of individuals and minority groups in the EU. There might be a causal relationship between growing rates of frustration between peoples and social marginalization of noted societal groups which might be caused by unsatisfactory assimilation policies of respective EU member states. The goal of this given thesis was to analyze risks to Czech electrical grid which might be posed by an act of terrorism. The analysis was done by breaking down the electrical grid safety measures into respective sectors and parts. Risk for each particular category were analyzed and final risk assessment whilst using help of security professionals. A questionnaire method was used to complete this particular task. The questionnaire dataset was later used to identification of most vulnerable weak-points in the electricity transmission system of the Czech Republic in respect to acts of terrorism. This diploma thesis might be used as a blueprint for improvements in the security management of the Czech electricity transmission system and for educatory purposes at the University of South Bohemia, at the Faculty of Health and Social Sciences.

Key words

critical infrastructure, electricity grid, power plants, electricity transmission system, electricity distribution system, terorism

Obsah

ÚVOD ***9***

1 TEORETICKÁ ČÁST ***10***

1.1 KRITICKÁ INFRASTRUKTURA *10*

1.1.1 Členění kritické infrastruktury *13*

1.1.2 Ochrana kritické infrastruktury *16*

1.1.3 Vlastnosti síťové kritické infrastruktury *20*

1.2 ELEKTRIZAČNÍ SOUSTAVA *21*

1.2.1 Výrobny elektřiny *21*

1.2.2 Přenosová soustava *24*

1.2.3 Prvky evropské kritické infrastruktury *27*

1.2.4 Distribuční soustava *27*

1.2.5 Stav a rozvoj elektroenergetiky *29*

1.2.6 Energetická bezpečnost *31*

1.3 BEZPEČNOSTNÍ HROZBY *31*

1.3.1 Naturogenní hrozby *32*

1.3.2 Antropogenní hrozby *34*

1.4 TERORISMUS *39*

1.4.1 Teroristická hrozba z hlediska původce útoku *41*

1.4.2 Teroristická hrozba z hlediska cíle útoku *42*

1.4.3 Teroristická hrozba z hlediska nástrojů terorismu *43*

1.4.4 Strategie ČR pro boj proti terorismu *44*

1.4.5 Systém vyhlašování stupňů ohrožení terorismem *46*

1.5 KOMPARACE SE ZAHRANIČÍM *47*

1.5.1 USA *48*

1.5.2 EU *48*

1.5.3 Slovensko *49*

1.5.4 Komparace vybraných států *50*

2 CÍL PRÁCE A VÝZKUMNÁ OTÁZKA ***51***

2.1 CÍL PRÁCE *51*

2.2 VÝZKUMNÁ OTÁZKA *51*

3 METODIKA ***52***

4 VÝSLEDKY ..... **CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.**

4.1 POLICEJNÍ STATISTIKY NAPADENÍ ELEKTRIZAČNÍ SOUSTAVY ČR .. CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

4.2 TERORISTICKÉ ÚTOKY VEDENÉ NA ELEKTRIZAČNÍ SOUSTAVU ..... CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

4.3 SPECIFIKACE JEDNOTLIVÝCH RIZIKOVÝCH FAKTORŮ TERORISMU OHROŽUJÍCÍCH ELEKTRIZAČNÍ SOUSTAVU ČR ..... CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

4.4 OBLASTI ELEKTRIZAČNÍ SOUSTAVY OHROŽENÉ TERORISMEM ..... CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

4.4.1 Výrobny elektřiny ..... Chyba! záložka není definována.

4.4.2 Přenosová soustava ..... Chyba! záložka není definována.

4.4.3 Distribuční soustava ..... Chyba! záložka není definována.

4.5 VÝSLEDKY VÝZKUMU ..... CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

4.5.1 Checklist expertů elektrizačních společností ..... Chyba! záložka není definována.

4.5.2 Checklist experta Policie ČR oddělení krizového řízení ..... Chyba! záložka není definována.

4.5.3 Hodnocení elektrizační soustavy ČR experty elektrizačních společností ... Chyba! záložka není definována.

4.5.4 Hodnocení elektrizační soustavy ČR expertem Policie ČR .... Chyba! záložka není definována.

4.5.5 Komparace hodnocení elektrizační soustavy ČR ..... Chyba! záložka není definována.

***5 DISKUSE* ..... CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.**

5.1 EXPERTI ELEKTRIZAČNÍCH SPOLEČNOSTÍ ..... CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

5.1.1 Výrobny elektřiny z pohledu expertů elektrizačních společností ..... Chyba! záložka není definována.

5.1.2 Přenosová soustava z pohledu expertů elektrizačních společností ..... Chyba! záložka není definována.

5.1.3 Distribuční soustava z pohledu expertů elektrizačních společností ..... Chyba! záložka není definována.

5.1.4 Shrnutí všech sektorů z pohledu expertů elektrizačních společností ..... Chyba! záložka není definována.

5.2 EXPERT POLICIE ČR ODDĚLENÍ KRIZOVÉHO ŘÍZENÍ ..... CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

5.2.1 Výrobny elektřiny z pohledu experta Policie ČR ..... Chyba! záložka není definována.

5.2.2 Přenosová soustava z pohledu experta Policie ČR ..... Chyba! záložka není definována.

5.2.3 Distribuční soustava z pohledu experta Policie ČR ..... Chyba! záložka není definována.

5.2.4 Shrnutí všech sektorů z pohledu experta Policie ČR ..... Chyba! záložka není definována.

5.3 KOMPARACE VÝSLEDKŮ MEZI EXPERTY ELEKTRIZAČNÍ SOUSTAVY A POLICIE ČR CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.

5.3.1 Komparace výsledků výroben elektřiny ..... Chyba! záložka není definována.

5.3.2 Komparace výsledků přenosové soustavy ..... Chyba! záložka není definována.

5.3.3 Komparace výsledků distribuční soustavy ..... Chyba! záložka není definována.

5.3.4 Komparace všech sektorů hodnocených experty elektrizačních společností a Policie ČR ..... Chyba! záložka není definována.

***ZÁVĚR* 55**

***SEZNAM POUŽITÝCH ZDROJŮ* 56**

***SEZNAM OBRÁZKŮ* 62**

***SEZNAM TABULEK* 63**

***SEZNAM PŘÍLOH* 65**

***SEZNAM ZKRATEK* 66**

Úvod

V dnešní době se stále zvyšuje riziko ohrožení teroristickými útoky jak v Evropě, tak na samotném území České republiky. Primárním cílem těchto útoků je vyvolat strach jednotlivce o svůj život, kdy k útoku může dojít kdekoliv a kdykoliv. Pro společnost jako takovou je však mnohem více nebezpečné možné ohrožení prvků kritické infrastruktury, kdy narušení jejich funkce by mělo závažný dopad na svrchovanost státu nebo územní celistvost státu anebo jeho demokratické základy, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Kritickou infrastrukturu tvoří systém prvků a spojnic, které jsou síťově uspořádané. Místa, kde se nachází více prvků spojnic, se nazývají uzly. Dané uzly mohou být strategicky významné, kdy jejich poškození, či narušení by mohlo vést ke zhroucení celé kritické infrastruktury. Tyto uzly by měly být chráněny primárně a jejich ochrana by měla směřovat k prevenci. Stupeň ochrany je závislý na investovaných finančních prostředcích. Je zřejmé, že žádná ochrana nemůže být dokonalá a nemůže pokrývat celé spektrum prvků a spojnic, proto je potřeba určit priority, jež jsou z hlediska fungování klíčové. Dalším problémem je to, že ne všechny prvky patří do vlastnictví státu, náleží také soukromým subjektům. To může v jejich ochraně způsobovat další komplikace, kdy soukromé subjekty mohou mít odlišné zájmy oproti státu.

Jeden z nejdůležitějších prvků kritické infrastruktury je elektrizační soustava, kdy její narušení by mohlo vést k obrovským sekundárním škodám. Jedná se o škody, které jsou způsobeny tím, že by nebyla dodávána elektřina ke koncovým odběratelům. To by způsobilo mnohem větší následky, než samotná škoda na poškozeném, či narušeném strategicky významném uzlu. Čím déle a čím větší by výpadek byl, tím větší by vznikly škody. Elektřinu není možné skladovat, proto je třeba zabezpečit vyváženou výrobu a spotřebu. Pokud by došlo k nevyvážení výroby a spotřeby, nastane výpadek elektrické energie. To by mohlo mít nedozírné následky, protože bez elektrické energie se v moderní společnosti už téměř nic neobejde.

1 Teoretická část

1.1 Kritická infrastruktura

Tato kapitola si klade za cíl definovat kritickou infrastrukturu, evropskou kritickou infrastrukturu a s tím spojené pojmy, následně rozčlenit jednotlivá kritéria a oblasti kritické infrastruktury. Poté popsat problematiku její ochrany a nakonec se věnovat síťové kritické infrastruktuře a jejímu určování.

a) krizové řízení - *„souhrn řídících činností orgánů krizového řízení, zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s*

1. přípravou na krizové situace a jejich řešením, nebo

2. ochranou kritické infrastruktury" (Zákon č. 240/2000 Sb.)

b) krizová situace - *„mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu"* (Zákon č. 240/2000 Sb.)

c) mimořádná událost - *„škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací"* (Zákon č. 239/2000 Sb.)

d) stav nouze - *„Stavem nouze je stav, který vznikl v elektrizační soustavě v důsledku*

1. živelních událostí,

2. opatření státních orgánů za nouzového stavu, stavu ohrožení státu nebo válečného stavu,

3. havárií nebo kumulace poruch na zařízeních pro výrobu, přenos a distribuci elektřiny,

4. smogové situace podle zvláštních předpisů,

5. teroristického činu,

6. nevyrovnané bilance elektrizační soustavy nebo její části,

7. přenosu poruchy ze zahraničí elektrizační soustavy, nebo

8. je-li ohrožena fyzická bezpečnost nebo ochrana osob a způsobuje významný a náhlý nedostatek elektřiny nebo ohrožení celistvosti elektrizační soustavy, její bezpečnosti a spolehlivosti provozu na celém území státu, vymezeném území nebo jeho části. *"* (Zákon č. 458/2000 Sb.)

e) záchranné práce - *„činnost k odvrácení nebo omezení bezprostředního působení rizik vzniklých mimořádnou událostí, zejména ve vztahu k ohrožení života, zdraví, majetku nebo životního prostředí, a vedoucí k přerušení jejich příčin"* (Zákon č. 239/2000 Sb.)

f) likvidační práce - *„činnost k odstranění následků způsobených mimořádnou událostí"* (Zákon č. 239/2000 Sb.)

g) krizové opatření - *„organizační nebo technické opatření určené k řešení krizové situace a odstranění jejich následků, včetně opatření, jimiž se zasahuje do práv a povinností osob"* (Zákon č. 240/2000 Sb.)

h) kritická infrastruktura - *„prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu"* (Zákon č. 240/2000 Sb.)

i) evropská kritická infrastruktura - kritická infrastruktura na území České republiky (dále jen „ČR"), jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie (dále jen „EU") (Zákon č. 240/2000 Sb.)

j) prvek kritické infrastruktury - *„zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury"* (Zákon č. 240/2000 Sb.)

k) ochrana kritické infrastruktury - *„opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury"* (Zákon č. 240/2000 Sb.)

l) subjekt kritické infrastruktury - *„provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt*

evropské kritické infrastruktury" (Zákon č. 240/2000 Sb.)

Kritická infrastruktura je klíčovým systémem prvků, jejichž narušení nebo nefunkčnost by měla závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva nebo ekonomiku státu. Pro vysoký stupeň vzájemného propojení jednotlivých odvětví je kritická infrastruktura ohrožena komplexně, a to jak naturogenními, tak antropogenními hrozbami. Zvláště funkčnost energetické infrastruktury je ohrožována jak politickými tlaky, tak hrozbami s kriminální podstatou. Ukázkou těchto ohrožení jsou politicky motivované manipulace s dodávkami strategických surovin, vstup cizího kapitálu s potenciálně rizikovým původem a cíli do kritické infrastruktury ČR, sabotáže, kybernetické útoky či hospodářská kriminalita. (Bezpečnostní strategie ČR, 2015)

Základním principem ochrany kritické infrastruktury je zajištění fungování klíčových a strategických infrastruktur s cílem zabezpečit ochranu obyvatelstva. Jednotlivé prvky kritické infrastruktury na sebe navzájem navazují a jsou nezbytné pro chod státu. Základní potřeby společnosti jsou zabezpečovány životně důležitými funkcemi společnosti, které závisí na infrastrukturách. Ty jsou posuzovány podle kritérií závislostí, alternativ a těsného propojení, jež tvoří základ rozhodování o tom, zda jsou nebo nejsou životně důležité pro obyvatelstvo a stát. (Komplexní strategie ČR k řešení problematiky kritické infrastruktury, 2010)

Základní povinností státu je zajištění svrchovanosti a územní celistvosti ČR, ochrana demokratických základů a ochrana životů, zdraví a majetkových hodnot. (Ústavní zákon č. 110/1998 Sb.)

Mezi zásady určování odvětvových prvků kritické infrastruktury patří základní kritéria, těmi jsou nenahraditelnost a nahraditelnost. Nenahraditelností se rozumí skutečnost, že při jejím narušení nebo zničení je nutná oprava, rekonstrukce nebo výstavba prvku nebo jeho části, nelze nahradit v krátkém období, náhrada pouze provizorně s významným ovlivněním života obyvatelstva a fungování veřejné správy. Omezené nebo znemožněné naplňování některých základních potřeb obyvatelstva jako například dodávky elektřiny, plynu, služeb, fungování komunikačních prostředků. Může být vyhlášen krizový stav. Bude nutné vyhlásit regulační stupně, stavy nouze nebo omezení, ta mohou dosáhnout celostátní úrovně. Nahraditelností se rozumí fakt, že při narušení

nebo zničení jsou potřeba opravy, rekonstrukce nebo výstavba prvku nebo jeho části, činnost však lze nahradit jiným subjektem nebo provizorním způsobem v dostačujícím rozsahu a úrovni. (Národní program ochrany kritické infrastruktury, 2010)

Jednotlivá odvětvová a průřezová kriteria pro určení prvku kritické infrastruktury jsou uvedena v Nařízení vlády č. 432/2010 Sb., které vychází ze Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (dále jen „Směrnice o EKI“). Ta dodržuje základní práva a ctí zásady uznávané zejména Listinou základních práv EU. Dále se podle ní zavádí postup pro určování a označování evropských kritických infrastruktur a společný přístup k posouzení potřeby zvýšit jejich ochranu s cílem přispět k ochraně obyvatel.

Průřezovými kriterii se rozumí soubor obecných hledisek pro posuzování závažnosti vlivu narušení nebo zničení prvku kritické infrastruktury s mezními hodnotami, která zahrnují počet obětí, ekonomický dopad a dopad na veřejnost. Dále odvětvovými kritérii, kterými se rozumí technické nebo provozní hodnoty k určování prvků kritické infrastruktury v konkrétních odvětvích kritické infrastruktury. Klíčoví nositelé úkolů problematiky kritické infrastruktury jsou současně realizátory programu ochrany kritické infrastruktury, jsou to: Vláda ČR, ministerstva a ústřední správní úřady, v jejichž gesci jsou jednotlivé oblasti kritické infrastruktury, Ministerstvo vnitra a subjekty kritické infrastruktury. (Národní program ochrany kritické infrastruktury, 2010)

1.1.1 Členění kritické infrastruktury

Základní členění prvků kritické infrastruktury je na průřezová a odvětvová kritéria. Průřezová kritéria definuje jako soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvku kritické infrastruktury s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života. Odvětvová kritéria jako technické nebo provozní hodnoty k určování prvku kritické infrastruktury v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby

a veřejná správa. (Zákon č. 240/2000 Sb.)

Hlediska průřezových a odvětvových kritérií se dají přesně definovat. (Nařízení vlády č. 432/2010 Sb.)

a) Průřezová kritéria

1. hledisko obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin

2. hledisko ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu

3. hledisko dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob

b) Odvětvová kritéria

Jednotlivá odvětvová kritéria jsou uvedena v tabulce 1, dělí se na 9 oblastí kritické infrastruktury, které se ještě dále dělí do podoblastí. (Nařízení vlády č. 432/2010 Sb.,)

Tabulka 1 Odvětvová kritéria

I. Energetika
A. Elektřina
B. Zemní plyn
C. Ropa a ropné produkty
D. Centrální zásobování teplem
II. Vodní hospodářství
III. Potravinářství a zemědělství
A. Rostlinná výroba
B. Živočišná výroba
C. Potravinářská výroba
IV. Zdravotnictví
V. Doprava
A. Silniční doprava
B. Železniční doprava
C. Letecká doprava
D. Vnitrozemská vodní doprava
VI. Komunikační a informační systémy
A. Technologické prvky pevné sítě elektronických komunikací
B. Technologické prvky mobilní sítě elektronických komunikací
C. Technologické prvky sítí pro rozhlasové a televizní vysílání
D. Technologické prvky pro satelitní komunikaci
E. Technologické prvky pro poštovní služby
F. Technologické prvky informačních systémů
G. Oblast kybernetické bezpečnosti
VII. Finanční trh a měna
VIII. Nouzové služby
A. Integrovaný záchranný systém
B. Radiační monitorování
C. Předpovědní, varovná a hlásná služba
IX. Veřejná správa
A. Veřejné finance
B. Sociální ochrana a zaměstnanost
C. Ostatní státní správa
D. Zpravodajské služby

Zdroj: vlastní výzkum

Z důvodu zaměření této práce na elektrizační soustavu je podrobněji uvedeno v tabulce 2 jen odvětví energetiky, konkrétně elektřina, kde jsou vypsány jednotlivé podoblasti.

Tabulka 2 Podoblast Elektřina

A. ELEKTŘINA
A. 1 Výrobna elektřiny
a) výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW
b) výrobna poskytující podpůrné služby s celkovým instalovaným elektrickým výkonem nejméně 100 MW
c) vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny
d) dispečink výrobce elektřiny
A. 2 Přenosová soustava
a) vedení přenosové soustavy o napětí nejméně 110 kV
b) elektrická stanice přenosové soustavy o napětí nejméně 110 kV
c) technický dispečink provozovatele přenosové soustavy
A. 3 Distribuční soustava
a) elektrická stanice distribuční soustavy a vedení o napětí 110 kV (stanice typu 110/10 kV, 110/22 kV a 110/35 kV a k nim patřící vedení se posuzují podle jejich strategického významu v distribuční soustavě)
b) technický dispečink provozovatele distribuční soustavy

Zdroj: vlastní výzkum

1.1.2 Ochrana kritické infrastruktury

Ochrana kritické infrastruktury jsou činnosti, které jsou zaměřené na zajištění funkčnosti, nepřetržitosti a celistvosti kritické infrastruktury, jež mají zabránit hrozbě, riziku nebo zranitelnosti, zmírnit je a neutralizovat. (Směrnice o EKI, 2008)

Úkolem společnosti je ochránit kritickou infrastrukturu v každé situaci. Tím se rozumí proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování subjektů kritické infrastruktury a vazeb mezi nimi. Kritická infrastruktura je svázána s územím a obyvatelstvem, které obývá dané území. To celé lze označovat jako systém. Ten je prostorově a časově vymezen. Jeho prvky mohou být dále nedělitelné nebo vytvářet systém samy o sobě. To samé platí o kritické infrastruktuře, jež každá část tvoří sama o sobě systém. Vstupy a výstupy ze systému se realizují na hranicích a to buď bodově jako liniové stavby nebo kontinuálně jako například hraniční řeky a lesní masivy. Tyto vstupy a výstupy na hranicích systému mohou být například energetického, finančního nebo surovinového charakteru. ČR se ochranou kritické infrastruktury zabývá dlouhodobě. Od 80. let 20. století byl hlavním úkolem zvyšovat odolnost objektů národního hospodářství proti účinkům zbraní hromadného ničení, bral se v úvahu však i vliv živelních pohrom a provozních havárií. Konec tisíciletí zaznamenal rozsáhlé povodně, což přineslo požadavek na ochranu kritické infrastruktury před následky živelních pohrom. V roce 2001 nastala další změna v podobě teroristických útoků. (Šenovský, 2007)

Teroristické útoky ve Spojených státech amerických (dále jen „USA“) z 11. září 2001 změnily pohled na to, jak organizace definují kritickou infrastrukturu a jaké strategie využít pro její ochranu. Kritickou infrastrukturu ohrožuje mnoho hrozeb, které se dají rozdělit do 5 kategorií podle Severoatlantické aliance (dále jen „NATO“): vojenské akce, přírodní pohromy, průmyslové havárie, kybernetické útoky a terorismus. Vojenské akce lze definovat jako záměrné útoky na kritickou infrastrukturu vojenskou silou jiného státu pro podporu vlastních vojenských a politických cílů. Přírodní pohromy jsou vyvolány počasím nebo dalšími přírodními fenomény včetně zemětřesení, tornád, hurikánů a tsunami. S ohledem na kritickou infrastrukturu nejsou znepokojující ztráty životů spojené s katastrofou samotnou, ale spíše fyzické účinky na kritickou infrastrukturu vyplývající z přírodní katastrofy. Příkladem z nedávné doby je radiační kontaminace a druhotné účinky jaderné katastrofy ve Fukušimě v Japonsku následující vlnu tsunami v březnu 2011. Průmyslové havárie jsou způsobeny pochybením samotného systému kritické infrastruktury, chybou operátora nebo obojím dohromady, nejsou spuštěny přírodní pohromou. Jako příklad je jaderná katastrofa v Černobylu v roce 1986. Kybernetické útoky jsou záměrné útoky na informační systémy kritické infrastruktury. Příklad je počítačový virus objevený v červnu 2010, který útočil na průmyslové řídící systémy Siemensu, jež byl pravděpodobně vytvořen pro konkrétní útok na íránský jaderný program. Zatímco teroristické útoky jsou tradičně definovány jako překvapivý útok zahrnující záměrné použití násilí proti civilistům v naději dosažení politických či náboženských cílů, v posledních letech teroristé využili útoky na kritickou infrastrukturu proto, aby zvětšili následky poškození společnosti i přes jejich asymetrické schopnosti. Příklady zahrnují madridské vlakové bombové útoky z roku 2004 a londýnské vlakové a autobusové bombové útoky z roku 2005. (Edwards et al., 2014)

Klíčoví nositelé úkolů ochrany kritické infrastruktury mají tyto úkoly:

a) Vláda ČR

Při zajišťování připravenosti ČR na krizové situace, při jejich řešení nebo k ochraně kritické infrastruktury ukládá úkoly ostatním orgánům krizového řízení, řídí a kontroluje jejich činnost. Určuje ministerstvo nebo jiný ústřední správní úřad pro koordinaci přípravy na řešení konkrétní krizové situace. Zřizuje Ústřední krizový štáb jako svůj pracovní orgán k řešení krizových situací. Rozhoduje na základě seznamu

předloženého Ministerstvem vnitra o prvcích kritické infrastruktury. (Zákon č. 240/2000 Sb.)

b) ministerstva a jiné ústřední správní úřady

K zajištění připravenosti na řešení krizových situací v jejich působnosti zřizují pracoviště krizového řízení. Zpracovávají krizový plán. Zřizují krizový štáb jako pracovní orgán. Zajišťují na základě vyžádání jiného ministerstva nebo jiného ústředního správního úřadu provedení odborných prací vyplývajících z jejich působnosti. Poskytují na požádání podklady ministerstvům, krajským úřadům a obecním úřadům obcí s rozšířenou působností. Vyžadují potřebné podklady od krajských úřadů a obecních úřadů obcí s rozšířenou působností. Stanovují podřízeným územním správním úřadům povinnost poskytovat na vyžádání podklady pro zpracování krizových plánů krajů. (Zákon č. 240/2000 Sb.)

K ochraně kritické infrastruktury náležející do jejich působnosti navrhují odvětvová kritéria a předkládají je Ministerstvu vnitra. Vyžadují od právnické nebo podnikající fyzické osoby, jako provozovatele stavby, zařízení, prostředku nebo veřejné infrastruktury, o kterých lze oprávněně předpokládat, že splňují kritéria pro určení prvku kritické infrastruktury nebo prvku evropské kritické infrastruktury, informace nezbytné k určení těchto prvků. Určí opatřením obecné povahy prvky kritické infrastruktury a prvky evropské kritické infrastruktury. Zašlou návrhy prvků kritické infrastruktury a prvků evropské kritické infrastruktury Ministerstvu vnitra. Kontrolují plány krizové připravenosti subjektů kritické infrastruktury a ochranu prvků kritické infrastruktury a ukládají opatření k nápravě nedostatků zjištěných při kontrole. Poskytují Ministerstvu vnitra jednou ročně informaci o ochraně evropské kritické infrastruktury včetně údajů o typech zranitelnosti, hrozbách a zjištěných rizicích. Poskytují Ministerstvu vnitra každé dva roky informaci o provedených kontrolách subjektů evropské kritické infrastruktury včetně informací o závažných zjištěních a nařízených opatřeních. (Zákon č. 240/2000 Sb.)

Dále vedou přehled možných zdrojů rizik, provádějí analýzy ohrožení a odstraňují nedostatky, které by mohly vést ke vzniku krizové situace. Rozhodují o činnostech k řešení krizových situací a ke zmírnění jejich následků. Organizují okamžité opravy nezbytných veřejných zařízení pro přežití obyvatelstva a k zajištění funkčnosti veřejné

správy. Vytvářejí podmínky pro nouzovou komunikaci. Poskytují si bezplatně a bez zbytečného odkladu údaje z informačních systémů veřejné správy. (Zákon č. 240/2000 Sb.)

c) Ministerstvo vnitra

Za účelem koordinace výkonu státní správy v oblasti krizového řízení sjednocuje postupy v oblasti krizového řízení. Organizuje instruktáže a školení a podílí se na přípravě k získání zvláštní odborné způsobilosti zaměstnanců orgánů krizového řízení. Provádí kontrolu zajištění připravenosti ostatních ministerstev a jiných ústředních správních úřadů na řešení krizových situací a ve spolupráci s příslušným ministerstvem provádí kontrolu krizových plánů krajů. V době nouzového stavu nebo stavu ohrožení státu vede ústřední evidenci údajů o přechodných změnách pobytu osob. Navrhuje průřezová kritéria. Zpracovává seznam, který je podkladem pro určení prvků kritické infrastruktury a prvků evropské kritické infrastruktury. Plní úkoly v oblasti kritické infrastruktury vyplývající z členství ČR v EU, zabezpečuje mezinárodní výměnu informací v této oblasti, plní funkci kontaktního místa ČR a podává Evropské komisi zprávy o plnění úkolů vyplývajících z právních předpisů EU v této oblasti. Každoročně informuje Evropskou komisi o počtu prvků evropské kritické infrastruktury podle odvětví a o počtu členských států EU, které jsou závislé na jednotlivých prvcích evropské kritické infrastruktury. Každé dva roky předkládá Evropské komisi souhrnnou zprávu se všeobecnými údaji o typech zranitelnosti, hrozbách a rizicích zjištěných v jednotlivých odvětvích evropské kritické infrastruktury. Zpracovává ve spolupráci s jiným ústředním správním úřadem plán cvičení orgánů krizového řízení. Předává ministerstvům a jiným ústředním správním úřadům na jejich žádost údaje. V rozsahu potřebném pro zajištění připravenosti na řešení krizových situací koordinuje další úkoly. Dále odpovídá za přípravu a řešení krizových situací souvisejících s vnitřní bezpečností a veřejným pořádkem a přitom určuje a kontroluje postupy Policie ČR. (Zákon č. 240/2000 Sb.)

d) subjekty kritické infrastruktury

V rámci příslušných programů zabezpečují ochranu kritické infrastruktury a zvyšují jejich odolnost, například technickými zabezpečovacími prostředky, kybernetickou ochranou, fyzickou ochranou, režimovými a organizačními opatřeními a jejich

vzájemnou kombinací. Základním dokumentem ochrany kritické infrastruktury je plán krizové připravenosti zpracovaný subjektem kritické infrastruktury. Programy pro ochranu kritické infrastruktury v jednotlivých oblastech kritické infrastruktury představují hloubkové řešení její ochrany s ohledem na konkrétní účastníky procesu. Prakticky zahrnuje zpracování materiálů, ze kterých vyplyne potřeba aktualizace nebo přijetí nových opatření zacílených na bezproblémový chod životně důležitých infrastruktur. To v sobě skrývá jak horizontální tak vertikální spolupráci zástupců veřejné správy a soukromého sektoru v celém spektru činností (technické, organizační, legislativní, výzkumné atd.), a to v souladu s přidělenými gesčními nebo spolugesčními působnostmi a kompetencemi. (Národní program ochrany kritické infrastruktury, 2010)

1.1.3 Vlastnosti síťové kritické infrastruktury

Síťová infrastruktura je základem moderní společnosti. Tvoří páteř pro transport materiálu, věcí, energie, vody, ale i dat. Každé narušení těchto sítí omezí uživatele, může je však i ohrozit na životě. Síťová infrastruktura je také citlivá na kaskádní selhání, kdy v důsledku selhání uzlu může následně kaskádně dojít k selhání i dalších uzlů s ním spojených. Po přesažení určité meze u zhroucených uzlů může dojít až vyřazení celé sítě. Jako příklad jsou výpadky proudu na severovýchodě USA v roce 2003 nebo v západní Evropě v roce 2006. Každým tímto výpadkem bylo postiženo několik miliónů lidí v zasažených oblastech. (Šenovský, 2007)

Určování kritičnosti prvků síťové kritické infrastruktury probíhá tak, že stupněm uzlu rozumíme počet uzlů, se kterými je posuzovaný uzel spojen. Významnost spojení mezi uzly je možné poměřovat několika způsoby, avšak nejvíce používaným je Wienerův index W. Významnost spojení nebo uzlu sítě lze poměřit porovnáním hodnoty Wienerova indexu před a po odstranění předmětného elementu. Čím vyšší číslo vyjde, tím je odstraněný element důležitější. (Šenovský, 2007)

$$W = \sum_{(u,v)} d\,(u, v)$$

W - Wienerův index

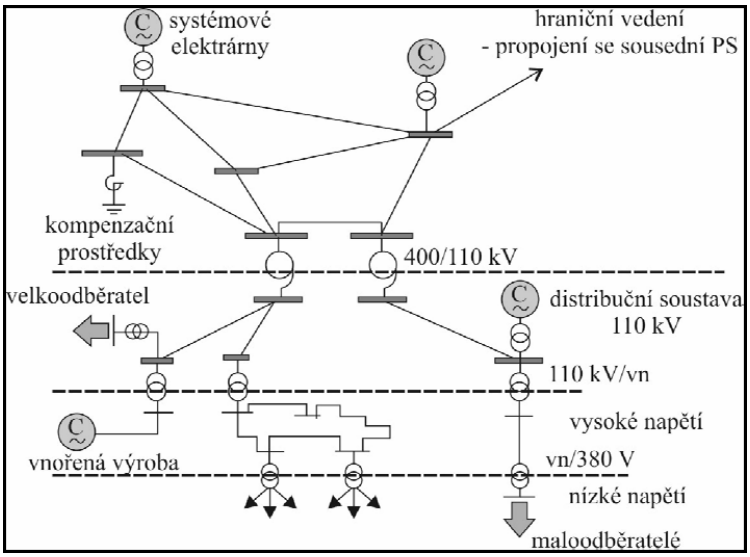
(u, v) - pro všechny dvojice propojených uzlů u a v

d - vzdálenost

1.2 Elektrizační soustava

Tato kapitola si klade za cíl rozebrat a blíže specifikovat elektrizační soustavu určením výroben elektřiny, přenosové soustavy a distribuční soustavy a dále popsat stav a rozvoj elektroenergetiky.

Elektrizační soustavou je vzájemně propojený soubor zařízení pro výrobu, přenos, transformaci a distribuci elektřiny, včetně elektrických přípojek, přímých vedení, a systémy měřící, ochranné, řídící, zabezpečovací, informační a telekomunikační techniky. Skládá se ze zdrojů, sítě a spotřebičů viz obrázek 1. Základem elektrizační soustavy je přenosová soustava, která je charakterizována sítí o napětí 400 a 220 kV, vyvedením výkonu velkých, takzvaných systémových elektráren, transformační vazbou na napětí 110 kV, propojením do soustav sousedních států pomocí hraničních vedení. Na přenosovou soustavu dále navazuje distribuční soustava, kterou vyznačuje několik napěťových úrovní od 110 kV až po sítě nízkého napětí, sítě radiální nebo okružní. Z té jsou zásobování buď velkoodběratelé (z vyšších napěťových hladin), nebo maloodběratelé (ze sítě nízkého napětí 380/220 V), vyvedeny jsou do ní zdroje nižšího výkonu (distribuovaná nebo vnořená výroba). (Hromada et al., 2014)



Obrázek 1 Zjednodušené zobrazení elektrizační soustavy
Zdroj: Hromada et al., 2014

1.2.1 Výrobny elektřiny

Jedná se o energetické zařízení pro přeměnu různých forem energie na elektřinu,

zahrnující všechna nezbytná zařízení; výrobna elektřiny o celkovém instalovaném elektrickém výkonu 100 MW a více, s možností poskytovat podpůrné služby k zajištění provozu elektrizační soustavy, je zřizována a provozována ve veřejném zájmu. (Zákon č. 458/2000 Sb., energetický zákon)

V tabulce 3 je rozepsána roční výroba elektřiny v ČR pro rok 2010. Výroba je rozdělena na jednotlivé druhy elektráren a k nim přiřazené hodnoty GWh vyrobené elektřiny. Ty se dále dělí na hrubou výrobu, vlastní spotřebu na výrobu a čistou výrobu elektřiny. Nejvíce elektrické energie se vyrobilo v parních elektrárnách (49979,7 GWh), to představuje 58 %. Následují jaderné elektrárny (27998,2 GWh), což je 33 % z celkové výroby. (Hromada et al., 2014)

Tabulka 3 Roční výroba elektřiny 2010

výroba elektřiny	druh elektrárny	celkem [GWh]
výroba elektřiny brutto	parní	47261
	jaderné	30324,2
	paroplynové a plynové	4435,1
	vodní včetně přečerpávajících vodních	2963
	fotovoltaické	2173,1
	větrné	417,3
	celkem	**87573,7**
vlastní spotřeba na výrobu elektřiny	parní	4537,7
	jaderné	1721,5
	paroplynové a plynové	182,2
	vodní	22,3
	fotovoltaické	19,8
	větrné	1,9
	celkem	**6485,4**
výroba elektřiny netto	parní	42723,3
	jaderné	28602,7
	paroplynové a plynové	4252,9
	vodní	2940,7
	z toho přečerpávající vodní	718,9
	fotovoltaické a větrné	2568,8
	celkem	**81088,4**

Zdroj: vlastní výzkum

V tabulce 4 je pro porovnání vývoje rozepsána roční výroba elektřiny v ČR pro rok 2016. Výroba je rozdělena na jednotlivé druhy elektráren a k nim přiřazené hodnoty GWh vyrobené elektřiny. Ty se dále dělí na hrubou výrobu, vlastní spotřebu na výrobu a čistou výrobu elektřiny. Nejvíce elektrické energie se vyrobilo opět v parních

elektrárnách (41520 GWh), to představuje 54 %. Následují jaderné elektrárny (22730,4 GWh), což je 29 % z celkové výroby. (Čtvrtletní zpráva o provozu elektrizační soustavy ČR IV. čtvrtletí 2016, 2017)

Tabulka 4 Roční výroba elektřiny 2016

výroba elektřiny	druh elektrárny	celkem [GWh]
výroba elektřiny brutto	parní	45704,3
	jaderné	24104,2
	paroplynové a plynové	7663,1
	vodní včetně přečerpávajících vodních	3201,7
	fotovoltaické	2128,2
	větrné	496,9
	celkem	**83298,4**
vlastní spotřeba na výrobu elektřiny	parní	4184,3
	jaderné	1373,8
	paroplynové a plynové	264,8
	vodní	17,8
	fotovoltaické	21,4
	větrné	8,7
	celkem	**5870,8**
výroba elektřiny netto	parní	41520
	jaderné	22730,4
	paroplynové a plynové	7398,3
	vodní	3167,9
	z toho přečerpávající vodní	1186
	fotovoltaické a větrné	2595
	celkem	**77411,8**

Zdroj: vlastní výzkum

Z těchto dat vyplývá, že za dané období se snížila jak výroba elektřiny, tak se snížila dominance parních a jaderných elektráren oproti dalším typům.

V tabulce 5 je uvedena struktura zdrojů elektrizační soustavy v ČR v roce 2010 podle výrobce a zdroje výroby, hodnoty jsou udávány v GWh. Z tabulky vyplývá, že primárním výrobcem je skupina ČEZ, a.s., jež pokrývá přes 70 % celkové výroby, dominantní zdroje výroby jsou u ní parní a jaderné elektrárny . (Hromada et al., 2014)

Tabulka 5 Struktura zdrojů elektrizační soustavy v ČR

výrobce	celkem [GWh]	zdroj výroby	[GWh]
ČEZ, a.s.	**61470,7**	parní elektrárny	34411,3
		jaderné elektrárny	27998,2
		vodní elektrárny	2061,1
ostatní výrobci	**24439,4**	parní elektrárny	18568,4
		paroplynové + plynové a spalovací elektrárny	3600,4
		vodní elektrárny	1319,5
		solární elektrárny	615,7
		větrné elektrárny	335,5

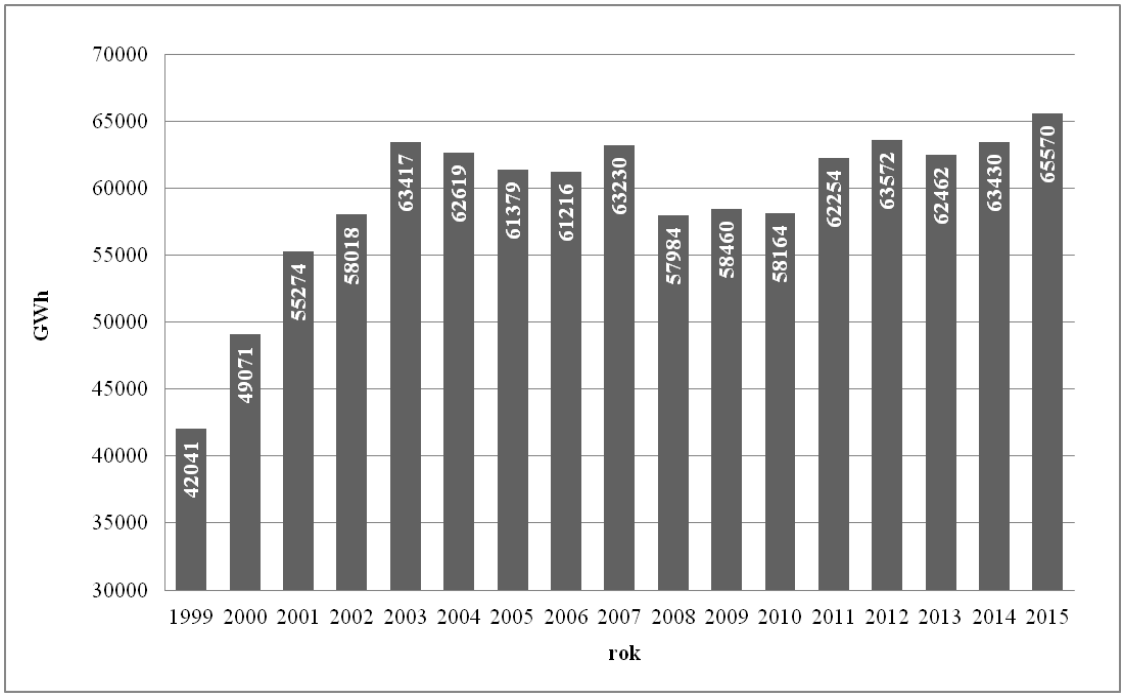
Zdroj: vlastní výzkum

1.2.2 Přenosová soustava

Je to vzájemně propojený soubor vedení a zařízení 400 kV, 220 kV a vybraných vedení a zařízení 110 kV sloužící pro zajištění přenosu elektřiny pro celé území ČR a propojení s elektrizačními soustavami sousedních států, včetně systémů měřící, ochranné, řídící, zabezpečovací, informační a telekomunikační techniky. Je zřizována a provozována ve veřejném zájmu. Službou přenosové soustavy je zajišťování přenosu elektřiny, systémových služeb a služeb souvisejících se zabezpečením spolehlivého a bezpečného provozu přenosové soustavy. (Zákon č. 458/2000 Sb.)

Jediným provozovatelem přenosové soustavy v ČR je ČEPS, a.s.. Přenosové služby spočívají v zajištění přenosu elektrické energie z míst výroby do míst spotřeby v rámci ČR i do a ze zahraničí. Dále řídí toky elektřiny v přenosové soustavě při respektování přenosů elektřiny mezi propojenými soustavami ostatních států a ve spolupráci s provozovateli distribučních soustav. Páteřní přenosová síť byla dokončena v 80. letech 20. století a v současné době ji tvoří hlavně vedení 400 kV, a dále trasy 220 kV ze 70. let, které dnes plní převážně funkci záložních a doplňkových vedení. Tato páteřní přenosová soustava slouží k rozvedení výkonu z velkých elektráren do celého území ČR a souběžně je součástí mezinárodního propojení Evropy. Napájí elektřinou distribuční soustavy, které ji dále rozvádějí ke konečným spotřebitelům. Přenosová soustava je napojena přeshraničním vedením na soustavy všech sousedních států, a tím synchronně spolupracuje s celou elektroenergetickou soustavou kontinentální Evropy. Do přenosové soustavy patří 41 rozvoden s 71 transformátory pro obě základní napěťové hladiny. Nejstarší soustavy 110 kV v 70. letech postupně převzaly úlohu uzlově napájených distribučních sítí. (ČEPS, 2017)

Na obrázku 2 jsou uvedeny přenosové služby, které ukazují množství přenesené elektřiny v přenosové soustavě v GWh mezi lety 1999 až 2015. Hodnoty mezi léty 1999 až 2012 (Hromada et al., 2014). Pro rok 2013, 2014 a 2015 (Energetický regulační věstník, 2014, 2015, 2016).



Obrázek 2 Množství přenesené elektřiny v přenosové soustavě

Zdroj: vlastní výzkum

Přenosovou soustavu ČEPS, a.s., z hlediska pohledu ochrany a odolnosti kritické infrastruktury tvoří:

a) Propojený soubor vedení a zařízení 400 kV, 220 kV a vybraných vedení a zařízení 110 kV

Tento soubor se nazývá vedení přenosové soustavy, má přiřazen kód - 11AA. V tabulce 6 jsou uvedeny délky jednotlivých vedení v km a porovnání mezi lety 2006 až 2014.

Tabulka 6 Délka vedení ČEPS, a.s. v provozu

rok	vedení 400 kV	vedení 220 kV	vedení 110 kV	celkem [km]
2006	3420	1920	94	**5434**
2010	3479	1910	83	**5472**
2014	3508	1910	83	**5501**
2017	3617	1909	84	**5610**

Zdroj: vlastní výzkum

b) Elektrické stanice

Ty jsou souborem staveb a zařízení elektrizační soustavy, který umožňuje transformaci, kompenzaci, přeměnu nebo přenos a distribuci elektřiny, včetně prostředků nezbytných pro zajištění jejich provozu. (Zákon č. 458/2000 Sb., energetický zákon)

V tabulce 7 je uvedena struktura zařízení přenosové soustavy z roku 2017, do které patří trasy vedení, délky vedení, zahraniční vedení, rozvodny, transformátory a kompenzační uzly, dále je zde uveden transformační a kompenzační výkon.

Tabulka 7 Zařízení ČEPS, a.s.

popis zařízení	celkem ČR	jednotky
trasy vedení 400 kV	3008	km
trasy vedení 220 kV	1349	km
trasy vedení 110 kV	45	km
délka vedení 400 kV	3617	km
délka vedení 220 kV	1909	km
délka vedení 110 kV	84	km
zahraniční vedení 400 kV	11	ks
zahraniční vedení 220 kV	6	ks
rozvodny 420 kV	26	ks
rozvodny 245 kV	14	ks
rozvodny 123 kV	1	ks
transformační výkon	21980	MVA
transformátory 400/220 kV	4	ks
transformátory 400/110 kV	48	ks
transformátory 220/110 kV	21	ks
kompenzační výkon 400 kV	660	MVAr
kompenzační výkon 35 kV	277,6	MVAr
kompenzační výkon 10 kV	408,6	MVAr
kompenzační uzly (tlumivky) 400 kV	4	ks
kompenzační uzly (tlumivky) 35 kV	5	ks
kompenzační uzly (tlumivky) 10 kV	9	ks

Zdroj: vlastní výzkum

c) Technický dispečink

Ten řídí elektrizační soustavu a zajišťuje rovnováhu mezi výrobou a spotřebou v každém okamžiku. Dispečink ČEPS, a.s. (hlavní technický dispečink v Praze

a záložní technický dispečink) zásadním způsobem přispívá k plnění povinností provozovatele přenosové soustavy a zodpovídá za zajištění bezpečného a spolehlivého provozu přenosové soustavy ČR v reálném čase. Technický dispečink řídí:

1. výrobny elektřiny připojené k přenosové soustavě,

2. výrobny elektřiny a odběrná elektrická zařízení zákazníků připojená k distribuční soustavě poskytující provozovateli přenosové soustavy podpůrné služby v rozsahu poskytnuté podpůrné služby,

3. odběrná elektrická zařízení zákazníků, která jsou připojena k přenosové soustavě, a

4. technické dispečinky provozovatelů regionálních distribučních soustav.

(Hromada et al., 2014)

1.2.3 Prvky evropské kritické infrastruktury

Ministerstvo průmyslu a obchodu dne 17. 2. 2011 určilo prvky evropské kritické infrastruktury na území ČR v energetice v pododvětví elektřina:

a) Přenosová soustava

1. hlavní technický dispečink,

2. záložní technický dispečink,

3. elektrická stanice přenosové soustavy Sokolnice,

4. elektrická stanice přenosové soustavy Slavětice,

5. elektrická stanice přenosové soustavy Nošovice.

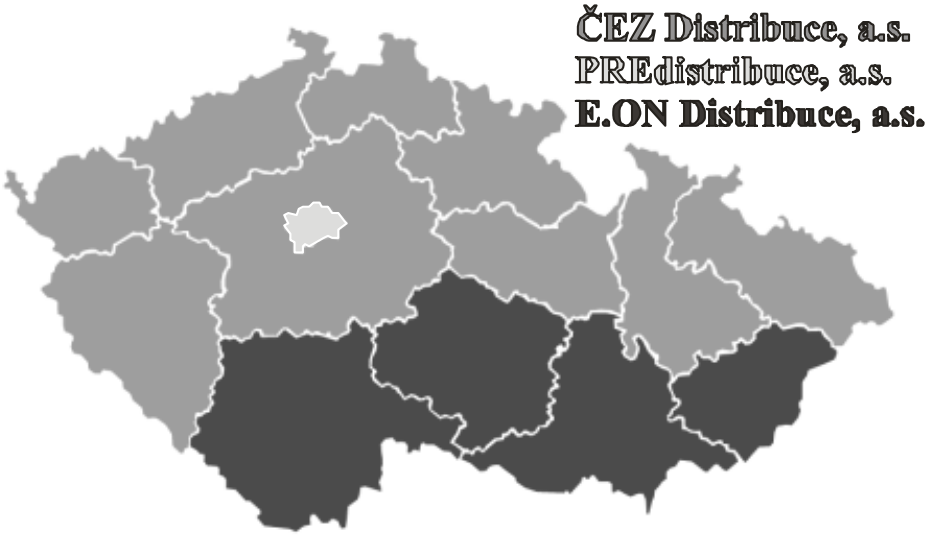
(Hromada et al., 2014)

1.2.4 Distribuční soustava

Jedná se o vzájemně propojený soubor vedení a zařízení o napětí 110 kV, s výjimkou vybraných vedení a zařízení o napětí 110 kV, která jsou součástí přenosové soustavy, a vedení a zařízení o napětí 0,4/0,23 kV 3 kV, 6 kV, 10 kV, 22 kV, 25 kV nebo 35 kV sloužící k zajištění distribuce elektřiny na vymezeném území ČR, včetně systémů

měřící, ochranné, řídící, zabezpečovací, informační a telekomunikační techniky včetně elektrických přípojek ve vlastnictví provozovatele distribuční soustavy. Je zřizována a provozována ve veřejném zájmu. Službou distribuční soustavy je zajišťování distribuce elektřiny a služeb souvisejících se zabezpečením spolehlivého a bezpečného provozu distribuční soustavy. (Zákon č. 458/2000 Sb., energetický zákon)

V ČR jsou 3 provozovatelé distribuční soustavy. Jedná se o ČEZ Distribuce, a.s, PREdistribuce, a.s. a E.ON Distribuce, a.s., jejich působnost je rozdělena na obrázku 3.



Obrázek 3 Působnost provozovatelů distribuční soustavy na území ČR
Zdroj: vlastní výzkum

V tabulce 8 jsou uvedeny základní technické informace provozovatelů distribuční soustavy na území ČR, data náleží roku 2012. Z tabulky je zřejmé, že největším provozovatelem distribuční soustavy je ČEZ Distribuce, a.s., zhruba poloviční je E.ON Distribuce, a.s., nejmenším provozovatelem je PREdistribuce, a.s., který je svou velikostí zhruba čtvrtinový a pokrývá pouze území Prahy.

Tabulka 8 Základní technické informace provozovatelů distribuční soustavy ČR 2012

	ČEZ Distribuce, a.s.	**PREdistribuce, a.s.**	**E.ON Distribuce, a.s.**	jednotka
zásobovací oblast	52001	496	26499	km2
odběrná místa	3566175	759768	1446389	počet
max. zatížení sítě	6159	2855	4575	MW
délka vedení celkem	159456	11921	64458,2	km
velmi vysoké/vysoké napětí	59962	3865	25621,1	km
nízké napětí	99494	7850	38837,1	km
distribuční stanice	57423	3274	145	počet
transformovny	233	22	78	počet

Zdroj: vlastní výzkum dle Hromada et al., 2014

a) Technické dispečinky provozovatelů distribučních soustav

1. technické dispečinky regionálních distribučních soustav (přímo připojených k přenosové soustavě) řídí:

I. výrobny elektřiny připojené k jím řízené distribuční soustavě,

II. odběrná elektrická zařízení zákazníků, která jsou připojena k jím řízené distribuční soustavě,

III. technické dispečinky provozovatelů lokálních distribučních soustav, jejichž zařízení jsou připojena k jím řízené distribuční soustavě, a

IV. přímá vedení připojená k jím řízené distribuční soustavě.

2. technické dispečinky lokálních distribučních soustav (přímo nepřipojených k přenosové soustavě) řídí:

I. výrobny elektřiny připojené k jím řízené distribuční soustavě,

II. odběrná elektrická zařízení zákazníků, která jsou připojena k jím řízené distribuční soustavě,

III. technické dispečinky provozovatelů distribučních soustav uvnitř jeho vymezeného území a

IV. přímá vedení připojená k jím řízené distribuční soustavě

(Hromada et al., 2014)

1.2.5 Stav a rozvoj elektroenergetiky

V oblasti výroby a dodávky elektřiny se musí postupně dojít k transformaci zajišťující změnu struktury výroby a obnovy dožívajících výroben s výrazně vyšší účinností, částečným přechodem z uhlí k jádru, zemnímu plynu a obnovitelným zdrojům energie, a tím zajistit zvyšující spotřebu elektřiny ve vytápění a dopravě do roku 2040. Hlavní cíl je zajištění mírně přebytkové výkonové bilance elektrické energie na dalších 20 až 30 let. Dostupnost dodávek a dovoz z okolních zemí nebude podle dnešního chování

sousedů pravděpodobně možný, proto je potřeba dosáhnout mírně přebytkové bilance pro zajištění nezbytné rezervy. Elektřina může nahrazovat v době nouze využívání ropy a jejich produktů v železniční dopravě nebo vytápění. Proto se jedná o strategické rozhodnutí. Současně se ani nedá přesně odhadnout budoucí technologický pokrok, který může vést ke zvýšené poptávce elektřiny. ČR díky své poloze ve středu Evropy může z pozice výkonové bilance, její struktury, disponibility krátkodobých a dlouhodobých dodávek jen získat. (Maule et al., 2015)

Hlavní cíle lze podle Státní energetické koncepce shrnout takto:

a) Zabezpečit výkonově přebytkovou výrobní bilanci založenou na diverzifikovaném palivovém mixu a efektivním využití disponibilních tuzemských primárních zdrojů.

b) Prostřednictvím vhodné velikosti a struktury rezervních kapacit, disponibilních regulatorních výkonů pro potřeby ČR, zásobníků energie a kapacit přenosové a distribučních sítí včetně řídících prvků a ochran, zabezpečit vysokou bezpečnost, spolehlivost a energetickou odolnost.

c) Zabezpečit rozvoj systémů a nástrojů řízení elektrizační soustavy účinné využívající jak nové technologie (inteligentní sítě), tak i rozšiřující se regionální spolupráci v oblasti řízení soustav a posílení rezerv. Podporovat rozvoj distribuovaných i centralizovaných systémů akumulace.

d) Udržet a dále posilovat vysokou tranzitní schopnost sítí a otevřenost energetiky ČR, zajistit trvalé plnění spolehlivostních kritérií a přiměřenost budoucím potřebám přenosu.

e) S ohledem na strategický význam energetického sektoru ponechat nadále společnost Česká energetická přenosová soustava, a.s. (dále jen „ČEPS“) ve výhradním vlastnictví státu a zachovat dominantní vliv státu ve společnosti České energetické závody, a.s.. (dále jen „ČEZ“).

f) Zajistit územní ochranu ploch a koridorů veřejné infrastruktury a souvisejících rozvojových záměrů prostřednictvím nástrojů územního plánování.

g) Prosazovat rychlou a plnou integraci energetických trhů ve střední Evropě a rozvoj tržních mechanismů usnadňujících přístupy na trh i změny dodavatele při současné

přiměřené kontrole tržních rizik. Zajistit otevřené a vysoce konkurenční prostředí s účinnou kontrolou tržní dominance a zneužívání trhu. Podporovat úsilí o zajištění tržního prostředí na evropském trhu s elektřinou s minimálním rozsahem tržních deformací. V případě, že se nepodaří navrátit vývoj na vnitřním trhu s elektřinou k plně liberalizovanému prostředí bez tržních distorzí, pak prosazovat celoevropskou harmonizaci kapacitních mechanismů na bázi technologické neutrality. V krajním případě, kdyby se nepodařilo prosadit ani toto harmonizované řešení, tak bude zájmem ČR implementovat takové regionální (případně národní) řešení, které umožní naplnit požadavky ČR na výrobní a systémovou přiměřenost. **(Maule et al., 2015)**

1.2.6 Energetická bezpečnost

Energetická bezpečnost má za cíl zajistit kontinuitu nezbytných dodávek energie a energetických služeb pro zajištění chráněných zájmů státu. Dělí se do 3 témat:

a) Bezpečnostní zajištění energetických zdrojů

b) Bezpečnost energetických transformací a dopravy energie

c) Energetická bezpečnost konečných uživatelů energie

Největší problém bezpečnosti energetických transformací a dopravy energie je privatizace a liberalizace, díky které dochází k rozchodu přístupu veřejného a soukromého sektoru. Odpovědnost veřejného sektoru vychází ze zajištění spolehlivého a bezpečného toku energie ke spotřebiteli, oproti tomu odpovědnost soukromého sektoru vede ke zvyšování tržní hodnoty energetických podniků, díky čemuž může docházet ke střetům. Kde jsou malé tržby, není zajištěna míra spolehlivosti dodávek z důvodu malé ekonomické motivace. Energetická bezpečnost konečných uživatelů energie je nejkritičtější, kdy přerušení dodávek energie spotřebitelům může způsobit krizové situace a ohrožovat chráněné zájmy ČR. (Beneš, 2007)

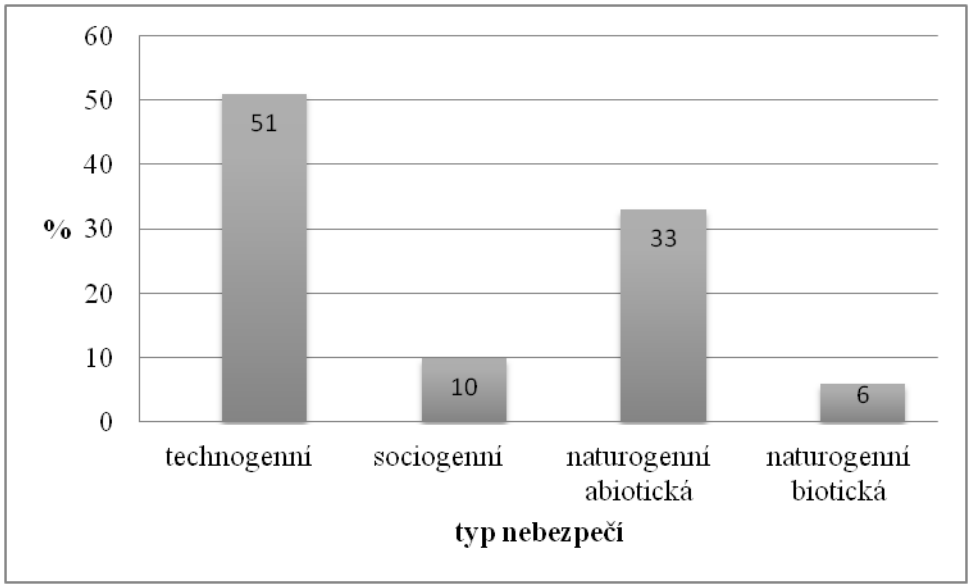
1.3 Bezpečnostní hrozby

Cílem této kapitoly je poukázat na bezpečnostní hrozby, které mohou negativně působit na kritickou infrastrukturu ČR.

ČR je zodpovědný člen mezinárodních organizací a proto řadí mezi relevantní i takové bezpečnostní hrozby, jež přímo neohrožují bezpečnost ČR, ale mohou ohrozit její

spojence. (Bezpečnostní strategie ČR, 2015)

Hrozby a z nich plynoucí rizika ovlivňují přímo nebo nepřímo zajišťování ochrany obyvatelstva. Jednotlivé hrozby na sebe mohou navazovat a tím jejich dopady násobit. To vyžaduje neustálou adaptaci schopností složek bezpečnostního systému ČR. Z důvodu neustále se zvyšujícího počtu přírodních a člověkem způsobených mimořádných událostí a závažnosti jejich následků nabývá na významu integrovaný přístup zaměřený na snižování vlivu těchto jevů. Obrázek 4 uvádí zastoupení kategorií nebezpečí na celkovém počtu nebezpečí podrobených detailní analýze. (Analýza hrozeb pro ČR, 2015)



Obrázek 4 Typy nebezpečí
Zdroj: vlastní výzkum

1.3.1 Naturogenní hrozby

Naturogenní hrozby způsobuje příroda, ty se dále dělí na způsobené živou (biotické) nebo neživou přírodou (abiotické). Vznikají působením extrémních projevů počasí, kdy ohrožují bezpečnost, zdraví a životy obyvatel, majetek a životní prostředí. Dále mohou poškozovat i kritickou infrastrukturu, zásobování surovinami a ekonomiku země. Větší nároky na ochranu veřejného zdraví a zajištění poskytování zdravotní péče klade možné šíření infekčních nemocí s pandemickým potenciálem. (Bezpečnostní strategie ČR, 2015)

a) Abiotické

1. Dlouhodobé sucho

To vzniká při déletrvajícím srážkově deficitním období, kdy bývá nadnormálně teplo a zvýšený výpar. Díky zástavbě území s rychlým odvodem vod a metodám hospodaření na zemědělské půdě dochází ke snížení infiltračních schopností, načež došlo ke snížení retenční kapacity v ČR. To může vést k ohrožení zdraví a životů, napomáhat výskytu a šíření požárů, poškozování lesních porostů a zemědělských kultur a snižovat hospodářskou produkci. (Audit národní bezpečnosti, 2016)

2. Extrémně vysoké teploty

Ty ohrožují zdraví a život obyvatel a dále funkčnost kritické infrastruktury hlavně v odvětvích energetika, vodní hospodářství, doprava, zemědělství a potravinářství. Ovlivňují výpar vody z krajiny, což může vést ke vzniku sucha a požárů. V kritické infrastruktuře je ohrožena hlavně energetika kvůli zvýšení spotřeby energie na klimatizaci a omezené možnosti chlazení a také dopravní konstrukce. (Audit národní bezpečnosti, 2016)

3. Povodeň, přívalová povodeň, vydatné srážky

Povodně způsobují přívalové nebo vytrvalé deště a tání sněhu s nepříznivými podmínkami, ty dále ohrožují zdraví, život, majetek a životní prostředí. Povodně samotné mohou způsobit další krizové stavy. Dopady na kritickou infrastrukturu mohou nastat hlavně v odvětví vodního hospodářství, energetiky, dopravy, zemědělství a potravinářství. (Audit národní bezpečnosti, 2016)

4. Extrémní vítr

Vzniká v zimě při postupu hlubokých tlakových níží k východu a v létě u intenzivních bouřek. Postihuje pouze určitou lokalitu, kde poškozuje sídla, lesní porosty, komunikace a dopravu. V kritické infrastruktuře je ohrožena zejména doprava a energetika v oblasti energetické rozvodné sítě. (Audit národní bezpečnosti, 2016)

b) Biotické

1. Epidemie - hromadné nákazy osob

Jedná se o výskyt infekčního onemocnění, jež výrazně převyšuje obvyklé hodnoty incidence v daném místě a čase. Může se jednat jak o běžně se vyskytující infekci nebo epidemii, tak o zcela nový typ infekčního onemocnění. U epidemií velkého rozsahu není možné jednoznačně stanovit dopady na kritickou infrastrukturu, může tak působit na všechna odvětví. (Audit národní bezpečnosti, 2016)

2. Epifytie - hromadné nákazy polních kultur

Jedná se o hromadnou nákazu lesních kultur a zemědělských plodin, ty jsou závislé na vývoji klimatických podmínek. (Audit národní bezpečnosti, 2016)

3. Epizootie - hromadné nákazy zvířat

Jedná se o vysoce nakažlivé virové onemocnění velkých skupin zvířat na velkém území v určitém časové období. Projevuje se rychlým nástupem, šířením a nemocností, kdy extrémní formou je panzootie zasahující celé kontinenty. V Evropě se jedná hlavně o slintavku a kulhavku, ptačí chřipku nebo mor prasat. (Audit národní bezpečnosti, 2016)

1.3.2 Antropogenní hrozby

Jedná se o hrozby způsobené lidskou činností. Lze jim předcházet pomocí preventivních opatření, dále je nezbytné zajištění připravenosti na řešení těchto situací. Mohou být způsobeny úmyslně či neúmyslně, mající vojenský nebo nevojenský charakter. Dělí se na technogenní, ekonomické a sociogenní. (Audit národní bezpečnosti, 2016)

a) Technogenní

1. Narušení dodávek potravin velkého rozsahu

Pravděpodobný výskyt hrozí spíše jako sekundární důsledek jiných krizových situací. (Audit národní bezpečnosti, 2016)

2. Narušení funkčnosti významných systémů elektronických komunikací, narušení bezpečnosti informací kritické informační infrastruktury

U narušení bezpečnosti informací kritické informační infrastruktury se vychází ze skutečnosti, že zákonné podmínky předpokládají pro tuto situaci vyhlášení krizového stavu. (Analýza hrozeb pro ČR, 2015)

Kybernetický prostor je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací. (zákon č. 181/2014, o kybernetické bezpečnosti a o změně souvisejících zákonů)

Kybernetické útoky jsou velmi nebezpečné, protože v této sféře neexistují omezení jako hranice států nebo vzdálenosti mezi nimi, kdy útočník na druhém konci světa může poškodit strategické a významné zájmy ČR. Kybernetické útoky i jejich sofistikovanost se neustále zvyšuje a primárně směřují na finanční, průmyslové, energetické, komunikační nebo dopravní systémy, jež způsobují významné hmotné škody, ale může docházet i k politické a ekonomické špionáži. Dále mohou ohrožovat obranyschopnost země, protože na informačních a komunikačních systémech jsou závislé i ozbrojené síly. Vláda se s touto hrozbou snaží vypořádat vytvořením vládního koordinačního místa pro okamžitou reakci na kybernetické bezpečnostní incidenty, které má sloužit pro zajištění bezpečnosti kritické informační infrastruktury a významných informačních systémů. (Bezpečnostní strategie ČR, 2015)

Kybernetické útoky se dále dělí na:

I. Kybernetická špionáž

Útoky jsou cíleny proti jednotlivci i skupinám v soukromém i veřejném sektoru a působí jako snaha o získání citlivých informací a dat bez souhlasu držitele. Vedou k získání osobní, ekonomické, politické nebo vojenské výhody za použití kyberprostoru. Ta je velmi sofistikovaná, obtížně rozpoznatelná, odhalitelná a těžko se identifikuje jejich původce. Bývá to jedním z prvních znaků přípravy kybernetického útoku, kdy dochází k mapování prostředí, na které může být později zaútočeno. (Audit národní bezpečnosti, 2016)

II. Narušení nebo snížení odolnosti infrastruktury informační technologie

Její odolnost je schopnost entity udržet přijatelnou úroveň služeb, rychle se adaptovat a reagovat na vzniklé problémy, kdy selhání mohou způsobit technické, lidské, přírodní nebo kybernetické faktory, proto musí ČR vytvářet zabezpečený kyberprostor, navyšovat své kapacity a odolnost IT infrastruktury. (Audit národní bezpečnosti, 2016)

III. Nepřátelské kampaně

Ty představují řadu kybernetických operací cílených na jeden konkrétní strategický cíl, kdy jsou většinou podporované nebo organizované cizím státem. Často dochází k recyklaci, protože vývoj nástrojů a postupů pro útoky je velmi časově náročný a nákladný. Není proti nim v současné době dostatečná obrana. (Audit národní bezpečnosti, 2016)

IV. Narušení nebo snížení bezpečnosti eGovernmentu

Jedná se o správu věcí veřejných pomocí moderních elektronických nástrojů jako síť kontaktních míst veřejné správy Czech POINT, je pro ně však nezbytné vytvořit robustní a bezpečnou infrastrukturu, protože systémy pracují s velkým objemem důležitých dat. (Audit národní bezpečnosti, 2016)

V. Kyberterorismus

Lze definovat jako agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, kdy je jeho prostřednictvím dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy. (Audit národní bezpečnosti, 2016)

3. Zvláštní povodeň

Ta je způsobena poruchou nebo havárií vodního díla, nebo nouzovým řešením kritické situace na vodním díle způsobeným úmyslným poškozením nebo terorismem, které způsobí vznik mimořádné události pod vodním dílem. Vodní díla jsou zařazena do I. až IV. kategorie podle výše možných škod v území pod vodním dílem při havárii kvůli dohledu nad nimi. Vlastníci nebo správci vodních děl musí zajišťovat odborný technickobezpečnostní dohled, zejména na vodních dílech I. až III. kategorie. (Audit národní bezpečnosti, 2016)

4. Únik nebezpečné chemické látky ze stacionárního zařízení

Jedná se o bezpečnostní riziko vzniku závažných havárií, které nastanou technickou závadou nebo selháním neúmyslného či úmyslného lidského faktoru s cílem vyvolat

závažné škody na zdraví člověka, majetku, životním prostředí nebo na fungování společnosti. Pro efektivní ochranu slouží stanovení jednotných pravidel pro všechny činnosti spojené s nakládáním s nebezpečnými látkami, které se stupňují v závislosti se zvyšujícím se rizikem. Při dosažení kritického množství musí subjekt plnit přísnější povinnosti. (Audit národní bezpečnosti, 2016)

5. Narušení dodávek pitné vody velkého rozsahu

To může mít vliv na obyvatelstvo, výrobu, zemědělství a zdravotnictví, ke kterému může dojít v důsledku jiných mimořádných událostí a krizových situací nebo úmyslným narušením. Když k tomuto výpadku dojde běžnou poruchou, problém řeší vlastník nebo provozovatel náhradním zásobováním. V případě narušení velkého rozsahu je potřeba provádět opatření nouzového zásobování, která jsou stanovena příslušnými havarijními a krizovými plány. (Audit národní bezpečnosti, 2016)

6. Narušení dodávek elektrické energie, plynu, ropy a ropných produktů velkého rozsahu

Význam zajištění energetické a surovinové bezpečnosti je stále větší, hlavně jedná-li se o přístup ke strategickým zdrojům, zejména energetických surovin. Díky tomu se soutěžení o ně stává součástí mezinárodních vztahů. Cílem je vytvářet nepřerušované diverzifikované dodávky těchto surovin a zajistit stabilní dodávky elektrické energie, roste i význam zajištění přístupu ke zdrojům pitné vody v oblasti potravinové bezpečnosti. (Bezpečnostní strategie ČR, 2015)

U energetické bezpečnosti ČR nejvíce hrozí narušení dodávek elektrické energie velkého rozsahu, dále dodávek plynu a ropy velkého rozsahu, které mají zásadní dopad na ostatní oblasti chodu státu a jsou tak nejdůležitějšími odvětvovými kritérii. Surovinová bezpečnost má zásadní vliv pro naprostou většinu průmyslových odvětví a ekonomik států, což si plně uvědomují a proto pro zajištění nepřerušovaných a dostatečných nerostných zdrojů kladou mimořádný důraz. (Audit národní bezpečnosti, 2016)

7. Radiační havárie

Požadavky na bezpečné nakládání s jadernými materiály, zdroji ionizujícího záření, havarijní připravenost a jadernou bezpečnost jsou stanoveny atomovým zákonem a jeho

prováděcími předpisy. Ten stanovuje pravidla radiační ochrany osob a životního prostředí, dále pak podmínky vykonávání činností souvisejících s využíváním jaderné energie a ionizujícího záření. Výkon státní správy a dozoru provádí Státní úřad pro jadernou bezpečnost, jež vydává příslušná povolení, schvaluje a kontroluje pracoviště se zdroji ionizujícího záření. (Audit národní bezpečnosti, 2016)

b) Ekonomické

1. Narušení finančního a devizového hospodářství státu velkého rozsahu

U narušení finančního a devizového hospodářství státu velkého rozsahu se vychází ze skutečnosti, že zákonné podmínky předpokládají pro tuto situaci vyhlášení krizového stavu. (Analýza hrozeb pro ČR, 2015)

c) Sociogenní

1. Migrační vlny velkého rozsahu

Mezinárodní migrace je primárně způsobena lokálními ozbrojenými konflikty, které způsobují jak legální, tak nelegální migraci, to následně způsobuje bezpečnostní problémy v dalších zemích. Pokud nedojde k integraci byť i legálních migrantů, může docházet k sociálnímu napětí, jež vede k radikalizaci přistěhovaleckých komunit. (Bezpečnostní strategie ČR, 2015)

S migrací souvisí bezpečnostní aspekty. Hrozbu mohou představovat konkrétní imigranti anebo jejich masy. To může mít podobu terorismu, organizovaného zločinu, ale i šíření infekční nákazy, kulturních zvyklostí neslučitelných s naším právním pořádkem nebo snížené ochoty k integraci. Svou roli v podobě migrační hrozby může sehrát i objem migračních toků. Bezpečnost může ohrozit masová neřízená imigrace, která by mohla vyústit ve společenské nepokoje či radikalismus, a to jak na straně minority, tak majority. (Audit národní bezpečnosti, 2016)

2. Narušování zákonností velkého rozsahu (včetně terorismu)

Organizovaný zločin v poslední době přesahuje hranice států, kdy kriminální sítě dovedou narušovat instituce a hodnoty právního státu infiltrováním orgánů státní správy díky korupci a tím ohrožovat bezpečnost. To celé může vést ke ztrátě důvěryhodnosti veřejných institucí a destabilizaci státu a dále k propojování teroristických sítí

se strukturami organizovaného zločinu. (Bezpečnostní strategie České republiky, 2015)

1.4 Terorismus

Tato kapitola slouží pro definici terorismu, zkoumá teroristické hrozby, rozebírá strategii ČR pro boj proti terorismu a nakonec se věnuje systému vyhlašování stupňů ohrožení terorismem.

Teroristický útok *- „Kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost ČR, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu ČR nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla,*

a) *provede útok ohrožující život nebo zdraví člověka s cílem způsobit smrt nebo těžkou újmu na zdraví,*

b) *zmocní se rukojmí nebo provede únos,*

c) *zničí nebo poškodí ve větší míře veřejné zařízení, dopravní nebo telekomunikační systém, včetně informačního systému, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, veřejné prostranství nebo majetek s cílem ohrozit tím lidské životy, bezpečnost uvedeného zařízení, systému nebo prostranství anebo vydat majetek v nebezpečí škody velkého rozsahu,*

d) *naruší nebo přeruší dodávku vody, elektrické energie nebo jiného základního přírodního zdroje s cílem ohrozit tím lidské životy nebo vydat majetek v nebezpečí škody velkého rozsahu,*

e) *zmocní se letadla, lodi, jiného prostředku osobní či nákladní dopravy nebo pevné plošiny na pevninské mělčině, nebo nad takovým dopravním prostředkem nebo pevnou plošinou vykonává kontrolu, anebo zničí nebo vážně poškodí navigační zařízení nebo ve větším rozsahu zasahuje do jeho provozu nebo sdělí důležitou nepravdivou informaci, čímž ohrozí život nebo zdraví lidí, bezpečnost takového dopravního prostředku anebo vydá majetek v nebezpečí škody velkého rozsahu,*

f) *vyrábí nebo jinak získá, přechovává, dováží, přepravuje, vyváží či jinak dodává nebo užije výbušninu, jaderný materiál, jadernou, biologickou, chemickou nebo jinou*

zbraň, bojový prostředek nebo materiál obdobné povahy, anebo provádí výzkum a vývoj jaderné, biologické, chemické nebo jiné zbraně nebo bojového prostředku nebo výbušniny, nebo

g) *vydá lidi v obecné nebezpečí smrti nebo těžké újmy na zdraví nebo cizí majetek v nebezpečí škody velkého rozsahu tím, že způsobí požár nebo povodeň nebo škodlivý účinek výbušnin, plynu, elektřiny nebo jiných podobně nebezpečných látek nebo sil nebo se dopustí jiného podobného nebezpečného jednání, nebo takové obecné nebezpečí zvýší nebo ztíží jeho odvrácení nebo zmírnění.“* (Zákon č. 40/2009 Sb.)

Terorismus může zásadním způsobem otřást kterýmkoli státem, včetně České republiky. Útoky nebo pokusy o útoky, ke kterým v Evropě nebo jinde ve světě dochází, musí být pro ČR varováním. (Strategie ČR pro boj proti terorismu, 2013)

Hrozba terorismu jako metody násilného prosazování politických cílů je stále vysoká. Existují nadnárodní sítě volně propojených skupin i jednotlivců, ti jsou nazýváni vlky samotáři a i bez jednotného velení sdílejí plány, cíle a ideologii. Mohou přímo ohrozit zdraví a životy, životní prostředí a kritickou infrastrukturu. V poslední době to jsou primárně takzvaní zahraniční bojovníci. (Bezpečnostní strategie ČR, 2015)

Riziko provedení teroristických útoku v Evropě zvyšují vzájemně provázané faktory způsobené rozsáhlou destabilizací některých států v severní Africe a Blízkého východu, nástup teroristických skupin, s tím spojení zahraniční bojovníci, radikalizace jednotlivců a skupin a migrační krize. (Audit národní bezpečnosti, 2016)

Terorismus je ekvivalentem válečných zločinů v období míru. To může potvrdit teroristický útok ze dne 11. září 2001, kdy došlo v USA k útoku na Světové obchodní centrum v New Yorku a na Pentagon ve Washingtonu, D. C., což vedlo k novému milníku terorismu. Díky tomu si státní krizový manažeři i prostí občané kladou řadu otázek:

a) Jak se zachovat při hrozbě teroristického útoku, v jeho průběhu, či po něm?

b) Máme dostatek znalostí a dovedností, víme jak se máme zachovat a kde se máme ukrýt?

c) Máme připraveny dostatečné akční plány a metodiky pro rychlou a kvalifikovanou

odezvu na takové útoky?

d) Jsou záchranné síly a prostředky odborně i kapacitně dostatečné pro zvládnutí a řešení situace při teroristickém útoku?

d) Je odborný personál záchranných sil dostatečně technicky vybaven, dobře připraven a vycvičen? (Mika, 2003)

Terorismus nerespektuje geografické ani politické hranice, proto proti němu musí být zakročeno celospolečensky a na mezinárodní úrovni, kdy nestačí pouze omezení na technickou stránku věci, jež má na starosti policie nebo vládní úřad. Výsledky může přinést pouze spolupráce mezi státy a jejich institucemi. Za strategický cíl musí být zvoleno odstranění jeho příčin jako vytvoření stabilizované a prosperující společnosti, kdy 100% stav nelze dosáhnout, což je důvod nikdy nekončícího boje proti terorismu. Jinak by hrozila totální dezintegrace a demoralizace lidské společnosti, včetně ohrožení samé podstaty státu a státní moci. Teroristický akt obsahuje na rozdíl od kriminálního činu především politickou motivaci a důsledky. Od konvenční a partyzánské války se terorismus liší v tom, že nerespektuje rozdíly mezi bojovníky a civilisty, kdy civilisté jsou zabíjeni z důvodu politického a psychologického nátlaku. Dalším rozdílem od válek je to, že prioritně nejde o obsazení území, ale o působení na psychiku lidí pomocí strachu. Výběr cílů probíhá tak, aby útok vyvolal masový a dlouhodobí zájem a mohlo tak dojít k účinné propagandě teroristických idejí. (Brzybohatý, 1999)

1.4.1 Teroristická hrozba z hlediska původce útoku

a) Islámský radikalismus

Relevance hrozby pro ČR je nízká. V poslední době si získal největší pozornost veřejnosti, avšak v druhé polovině 20. století se v Evropě nejvíce objevoval radikálně levicový a separatistický terorismus. Islámský radikalismus představuje pro ČR malé riziko, protože radikalismus často souvisí se sociálním vyloučením, kdy muslimové v ČR jsou dobře integrováni do společnosti. Zde by spíše hrozilo nebezpečí jednotlivců. (Audit národní bezpečnosti, 2016)

b) Politický extremismus, ostatní teroristické skupiny

Relevance hrozby pro ČR nízká. Naše země má s pravicovým a levicovým

extremismem dlouholeté zkušenosti, některé z nich mají i mezinárodní vazby. Jejich členové páchají trestnou činnost, někdy i násilného charakteru, nebezpečí teroristických útoků je ale nízké díky dobrému monitorování a roztříštěnosti těchto stran. (Audit národní bezpečnosti, 2016)

c) Teroristé jednající samostatně (osamělí vlci)

Relevance hrozby pro ČR je střední. Na našem území se ještě neobjevil takový teroristický útok, ale střelba v Uherském Brodě v roce 2015 psychicky narušenou osobou měla stejný průběh i následky, proto lze na obě skupiny reagovat podobně. Teroristický útok jednotlivce či malé skupiny může být inspirován jak islámským radikalismem, tak jinou ideologií jako Breivik v Norsku, jež byl pravicový extremista. K radikalizaci může dojít i pomocí internetu, proto musí být prioritou boj proti internetové propagandě. (Audit národní bezpečnosti, 2016)

d) Zahraniční bojovníci

Relevance hrozby pro ČR je střední. Konflikty na Ukrajině, Sýrii a Iráku způsobují značné riziko pro Evropu, konkrétně pro západní Evropu, protože díky propagandě a radikalizaci do těchto konfliktů odcházejí bojovat občané EU, kteří získávají bojové zkušenosti a po návratu do vlasti mohou představovat vysokou bezpečnostní hrozbu. ČR pro ně představuje tranzitní zemi. (Audit národní bezpečnosti, 2016)

1.4.2 Teroristická hrozba z hlediska cíle útoku

a) Útok na kritickou infrastrukturu

Relevance hrozby pro ČR je střední. Ochrana kritické infrastruktury je primárním úkolem každého státu. Pro teroristické organizace naštěstí představuje druhořadý cíl, i když její narušení může způsobit závažné škody, ohrozit zdraví a život osob. Jejich primárním cílem jsou psychologické dopady útoků než objektivní následky, které by mohl představovat rozsáhlý výpadek energie, jenž by způsobil daleko větší škody na majetku a životech, než například traumatizující střelba v metru. Útoky cílené na kritickou infrastrukturu dokážou způsobit značnou škodu s malými náklady a prostředky a jejich ochrana je navíc velmi nákladná a obtížná. Další bezpečnostní riziko představují tzv. insideři, tedy zaměstnanci nebo bývalý zaměstnanci ohrožených objektů, případně osoby se znalostí bezpečnostních opatření. (Audit národní

bezpečnosti, 2016)

b) Útok na měkké cíle

Relevance hrozby pro ČR je střední. Měkké cíle (soft targets) představují místa s vysokou koncentrací osob, což bývají obchodní centra, sportovní, kulturní a společenské instituce a události, prostředky hromadné dopravy, školy, nemocnice a další, které nejsou téměř nijak chráněné. Útok teroristů s pomocí minimálních sil a prostředků dosáhne maximálních psychologických následků na rozdíl od dobře zabezpečených takzvaných tvrdých cílů (hard targets), mezi které patří jaderné elektrárny, letiště a další. Z toho důvodu se na ně skutečně soustředí. V poslední době i sebevražední útočníci nejen pomocí výbušných systémů, ale i automatickými střelnými zbraněmi pomocí mnohonásobných útoků ve stejný čas, což bývá mnohem náročnější pro bezpečnostní složky. Měkké cíle představují zřejmě nejpravděpodobnější terč teroristického útoku v ČR. (Audit národní bezpečnosti, 2016)

c) Zvlášť ohrožené objekty a osoby

Relevance hrozby pro ČR je střední. Mezi další kategorii spadají objekty, které mají pro teroristy vysokou symbolickou hodnotu, ty představují například policejní a vojenské objekty, sídla úřadů veřejné správy, politických stran, sídla médií či výstavy, budovy zastupitelských úřadů, místa spojená s náboženskou symbolikou atd. Zvýšené riziko platí i pro osoby, jež reprezentují postoje či instituce, na které mohou teroristé cílit, mezi ně patří aktivní osoby ve veřejném životě, politici a diplomaté. (Audit národní bezpečnosti, 2016)

d) Ohrožení českých občanů či objektů v zahraničí

Relevance hrozby pro ČR je střední. Hrozba ohrožení českých občanů a objektů v zahraničí je větší než na území ČR, protože útoky tam jsou snazší. Primárně se jedná o únosy osob západní kultury, není cílen na občany ČR. Mezi ohrožené objekty patří zastupitelské úřady v místě válečných konfliktů. (Audit národní bezpečnosti, 2016)

1.4.3 Teroristická hrozba z hlediska nástrojů terorismu

a) Zneužití zbraní hromadného ničení, konvenčních zbraní, výbušnin a položek dvojího užití

Relevance hrozby pro ČR je střední. Jejich praktické využití je velmi nepravděpodobné, avšak následky by byly velmi rozsáhlé, naposledy se stal tento případ v roce 1995 v tokijském metru. Získání i manipulace s těmito prostředky je velmi složitá, proto použití konvenčních forem útoků. Tato problematika vyžaduje mezinárodní spolupráci států v boji proti snahám teroristů. Velké riziko představuje ilegální šíření konvenčních zbraní, kdy se stávají stále využívanějším nástrojem teroristických útoků. (Audit národní bezpečnosti, 2016)

b) Financování terorismu a ostatní podpůrné aktivity

Relevance hrozby pro ČR je střední. I samotná pasivita státu může zvyšovat ohrožení terorismem nejen u sebe, ale i v zahraničí, kdy teroristé mohou získávat či převádět finanční prostředky v ČR, využívat jí jako tranzitní zemi nebo místo úkrytu. (Audit národní bezpečnosti, 2016)

1.4.4 Strategie ČR pro boj proti terorismu

Byla sestavena roku 2013 a navazuje na Strategii boje proti terorismu 2010 - 2012, kdy se opírá o principy Bezpečnostní strategie ČR. Obsahuje opatření zaměřená na minimalizaci rizik a dopadů potenciálních teroristických útoků na území ČR a proti zájmům ČR v zahraničí. Je rozčleněna na pět stěžejních oblastí:

a) Spolupráce zainteresovaných subjektů v boji proti terorismu

Úsilí bezpečnostních složek má hlavně preventivní roli. Spolupráce mezi policejními a zpravodajskými složkami je přitom naprosto zásadní, kdy se obě složky doplňují a spolupracují. (Strategie ČR pro boj proti terorismu, 2013)

b) Ochrana obyvatelstva a dalších potenciálních cílů

Je nezbytné věnovat zvýšenou pozornost prevenci teroristických útoků na místech s vysokou koncentrací obyvatelstva (například významné dopravní uzly, místa sportovních utkání, nákupní centra) a dále pak prvkům kritické infrastruktury (například přenosové soustavy, elektrárny, zdroje pitné vody), kdy je vyžadována nezbytná spolupráce se soukromými subjekty. (Strategie ČR pro boj proti terorismu, 2013)

c) Bezpečnostní výzkum a komunikace s veřejností

Musí pokračovat dosavadní koordinace národních priorit bezpečnostního výzkumu s EU a čerpat národní i unijní zdroje s důrazem na ochranu kritické infrastruktury, boj proti zneužití chemických, biologických, radioaktivních látek, jaderných materiálů a výbušnin (dále jen „CBRNE“) a ochranu před kybernetickými útoky. Dále pak vzdělávání členů všech složek integrovaného záchranného systému (dále jen „IZS“), protože jedině metodicky připravení zdravotníci, hasiči a policisté mohou poskytovat relevantní informace široké veřejnosti. Nakonec je potřeba efektivně využívat prostředků pro zajištění činnosti IZS nebo krizového řízení pro potřeby boje proti terorismu. (Strategie ČR pro boj proti terorismu, 2013)

d) Prevence radikalizace a rekrutování do teroristických skupin

Mělo by docházet k prohlubování komunikace orgánů veřejné správy s představiteli konkrétních náboženských nebo přistěhovaleckých komunit na lokální, regionální i celostátní úrovni. Všechny opatření v prevenci radikalizace těchto členů a jejich příklonu k terorismu je potřeba vytvářet společně s kroky proti domácímu extremismu, rasismu a xenofobii pomocí vzdělávacích a osvětových aktivit pro širokou veřejnost. (Strategie ČR pro boj proti terorismu, 2013)

e) Legislativní ukotvení problematiky boje proti terorismu

Bylo nezbytné provést úpravy odpovědnosti právnických osob v českém právním systému. Přijetím zákona o trestní odpovědnosti právnických osob a řízení proti nim je důležitým prvkem trestní politiky státu, který má vést k dlouhodobě pozitivním důsledkům vnitřní bezpečnosti země. (Strategie ČR pro boj proti terorismu, 2013)

Základní principy v boji proti terorismu v ČR jsou: Soulad boje s terorismem s Bezpečnostní strategií ČR a dalšími klíčovými dokumenty. Respektování principů demokracie a ochrany lidských práv. Spolupráce a sdílení informací mezi zainteresovanými institucemi. Prohlubování zapojení ČR do mezinárodních aktivit. Budování a prohlubování důvěry mezi stejně smýšlejícími zahraničními partnery. Prověřování (cvičení) schopnosti čelit hrozbě terorismu. Vzdělávání. Aktivní přístup při prevenci hrozeb. Informování veřejnosti v účelném a přiměřeném rozsahu. Maximální pomoc, podpora a ochrana subjektům, které poskytnou informace o připravovaných

teroristických akcích. (Strategie ČR pro boj proti terorismu, 2013)

V boji proti terorismu je nezbytná celosvětová spolupráce na úrovni EU a NATO, kdy by mělo dojít k eliminaci hrozeb ještě před hranicemi EU a ČR, to vyžaduje aktivní přístup ČR. Proto jsou využívány klíčové unijní dokumenty, jako Evropská protiteroristická strategie a s ní spojený Akční plán EU pro boj s terorismem a jiné. ČR se vydává směrem zavádění v zahraničí osvědčených a v podmínkách ČR využitelných myšlenek do praxe, není potřebné hledat řešení od píky, která již fungují v řadě dalších států, to samé má platit i u spolupráce domácích subjektů. (Strategie ČR pro boj proti terorismu, 2013)

1.4.5 Systém vyhlašování stupňů ohrožení terorismem

Doporučení vyplývající z jednotlivých stupňů budou určena pro širokou veřejnost i pro bezpečnostní složky, kdy budou platit celostátně nebo budou omezeny na určité území dle rozhodnutí. Ohrožení terorismem lze rozdělit na čtyři stupně, přičemž základním je nulový stav, který není nijak znázorněn a není samostatně vyhlašován. Zvýšené stupně ohrožení terorismem lze vidět na obrázku 5. Ty se označují jako první, druhý a třetí stupeň ohrožení terorismem. Již se barevně rozlišují, první stupeň je znázorněn žlutým trojúhelníkem, druhý oranžovým a třetí je označen červeným. (Systém vyhlašování stupňů ohrožení terorismem, 2016)

Obrázek 5 Stupně ohrožení terorismem
Zdroj: vlastní výzkum

a) Základní nulový stav

V tomto stavu není známa žádná konkrétní, ani obecná hrozba teroristického či obdobného útoku na území ČR. Díky situaci ve světě a náležitosti ČR do euroatlantických struktur se jedná o naprosto ideální stav, který může být těžce dosažitelný. Nejsou zde vydávána žádná zvláštní doporučení nebo varování a nejsou přijímána žádná opatření. (Systém vyhlašování stupňů ohrožení terorismem, 2016)

b) První stupeň (žlutý trojúhelník)

Ten upozorňuje na existenci obecného ohrožení terorismem, podle situace v zahraničí nebo z mezinárodních aktivit ČR, zároveň však není známa konkrétní hrozba teroristických aktivit na území ČR. Vyžaduje obecnou všímavost a dlouhodobě platí vytipovaná zvýšená bezpečnostní opatření. (Systém vyhlašování stupňů ohrožení terorismem, 2016)

c) Druhý stupeň (oranžový trojúhelník)

Existuje zvýšená pravděpodobnost ohrožení terorismem, kdy bližší okolnosti hrozby nelze předpovědět. Dochází k vyhlášení díky předchozím událostem nebo informacím o hrozbě projevů terorismu. (Systém vyhlašování stupňů ohrožení terorismem, 2016)

d) Třetí stupeň (červený trojúhelník)

U tohoto stupně se zavádí vysoká bdělost a pohotovost, kdy je teroristický útok s vysokou pravděpodobností očekáván nebo již nastal a je nezbytné přijmout opatření k zamezení opakování nebo pokračování útoku a minimalizovat následné škody. (Systém vyhlašování stupňů ohrožení terorismem, 2016)

Zvýšený stupeň ohrožení terorismem se vyhlašuje vláda ČR na návrh ministra vnitra (ten vychází z návrhu Společné zpravodajské skupiny) pomocí jednotlivých stupňů. V případě nebezpečí z prodlení může vyhlásit ministr vnitra na návrh Společné zpravodajské skupiny (ta vychází ze společného vyhodnocení hrozeb jejími členy), vláda následně zvýšený stupeň potvrdí nebo zruší, to samé platí u snižování stupňů. Doporučená opatření po vyhlášení jednotlivých stupňů ohrožení terorismem vydává vláda ČR nebo ministr vnitra ve vztahu k veřejnosti. Rozhodnutí o opatřeních směrem k bezpečnostním složkám státu přijímá vláda a věcně příslušní členové vlády v rámci jejich resortů. Finanční nároky, jež by mohli vyvstat v souvislosti se zvýšenými stupni ohrožení terorismem budou řešeny ad-hoc na úrovni vlády. (Systém vyhlašování stupňů ohrožení terorismem, 2016)

1.5 Komparace se zahraničím

Tato kapitola si klade za cíl stanovit a porovnat mezi sebou strukturu kritické infrastruktury USA a EU. Směrnice o EKI konkrétně u Slovenské republiky (dále jen

„SR“) s ČR a dále pak popsat jejich historický vývoj.

1.5.1 USA

Moderní původ vnitřní bezpečnosti a jeden z jejich pilířů, ochrana kritické infrastruktury, se řadí k roku 1995, kdy prezident Clinton vydal nařízení 39 (Presidential Decision Directive 39), které připravilo půdu pro to, co mělo přijít, v podstatě vyhlásil válku terorismu. Důležitou otázkou se stala kritičnost národní infrastruktury a souvisejících klíčových aktiv díky zákonu O-13010, který vydal v roce 1996. Založil tak Prezidentskou komisi pro ochranu kritické infrastruktury, jejíž předsedou byl Marsh. Ten vydal Marshovu zprávu, která poprvé definovala kritickou infrastrukturu jako sítě nezávislých, většinou soukromých, umělých systémů, které spolupracují a distribuují nepřetržitý tok základního zboží a služeb. Kritická infrastruktura je tak zásadní, že její narušení nebo zničení může mít oslabující vliv na obranu a národní bezpečnost. (Lewis, 2015)

Tato komise dále modernizovala kritickou infrastrukturu nařízením 63 (PDD-63), jež definovala kritickou infrastrukturu více podrobně do 8 základních sektorů. Toto nařízení se dále rapidně vyvinulo díky útokům z 11. září, kdy kancelář prezidenta vydala Národní strategii pro vnitřní bezpečnost v roce 2002. Dále pak vydáním Národní strategie pro fyzickou ochranu kritické infrastruktury a klíčových aktiv rychle navázala na rozšíření definice odvětví kritické infrastruktury v únoru 2003. Ochranu infrastruktury má na starosti ministerstvo vnitřní bezpečnosti, které vzniklo v reakci na tragédii z 11. září sloučením 22 samostatných agentur. Zodpovědnost za ochranu kritické infrastruktury je rozložena do několika ředitelství v rámci ministerstva vnitřní bezpečnosti. Kritická infrastruktura USA nyní obsahuje 16 sektorů, které naposledy upravil prezident Obama v roce 2013. (Lewis, 2015)

1.5.2 EU

V červnu 2004 požádala Evropská rada o přípravu celkové strategie pro ochranu evropských kritických infrastruktur. V říjnu 2004 Evropská rada přijala Evropskou strategii pro ochranu kritické infrastruktury před teroristickými útoky, to předložilo návrhy na téma, jak zvýšit evropskou prevenci, připravenost a odezvu na teroristické útoky zahrnující kritické infrastruktury. Po přípravné fázi, kdy došlo k jednání se subjekty soukromého a veřejného sektoru a vydání Zelené knihy, byly návrhy

převedeny do souboru strategických opatření pod názvem Evropský program na ochranu kritické infrastruktury, jež byl schválen v roce 2006 (dále jen „EPCIP“). Ten dále poskytuje trvalé a dynamické národní partnerství mezi institucemi EU, provozovateli kritické infrastruktury a členskými státy EU pro zabezpečení trvalého fungování kritické infrastruktury Evropy. (Edwards et al., 2014)

EPCIP si klade za cíl zlepšení ochrany kritických infrastruktur v EU, kdy by měla být zajištěna adekvátní úroveň ochrany, minimalizovat jednotlivé body výpadků a zajistit rychlá opatření obnovy. To má být zajištěno Směrnicí o EKI, akčním plánem EPCIP, Výstražnými informačními sítěmi kritické infrastruktury (dále jen „CIWIN“), využívání skupin odborníků, procesů sdílení informací o ochraně a určení a analýzy vzájemných závislostí. Dále poskytování podpory členským státům v oblasti vnitrostátních kritických infrastruktur, vnější prostředí, pohotovostní plánování a doprovodná finanční opatření. Vzorová kritická infrastruktura EU obsahuje 11 sektorů, z níž si každý členský stát EU implementuje vybrané sektory dle svých vlastních národních potřeb. (Edwards et al., 2014)

1.5.3 Slovensko

Ochrana kritické infrastruktury v SR se dříve vztahovala na obrannou infrastrukturu podle zákona č. 319/2002 Z. z. o obraně SR ve znění pozdějších předpisů. Novodobý vývoj začal schválením dokumentu Koncepce kritické infrastruktury SR a způsob její ochrany a obrany, jež byl schválený usnesením vlády SR č. 120 ze dne 14. 2. 2007, to uložilo ministrovi vnitra SR spolupráci s ministry a předsedy dalších ústředních orgánů státní správy SR připravit a předložit na zasedání vlády SR návrh zákona o kritické infrastruktuře. (Ministerstvo vnútra SR, 2017)

Pokračováním procesu bylo vypracování Národního programu pro ochranu kritické infrastruktury SR, který vláda SR schválila usnesením č. 185 z 26. 3. 2008. Jednotlivé rezorty a ostatní ústřední orgány státní správy v tomto dokumentu připravili první identifikaci nejdůležitějších sektorů a podsektorů národní infrastruktury a zhodnotili současný stav. Zákon č. 45/2011 Z. z. o kritické infrastruktuře byl přijat 8. 2. 2011. Cílem je v souladu se Směrnicí o EKI zkvalitnit dosavadní ochranu nejdůležitější infrastruktury, zejména vůči sílící hrozbě teroristických útoků, proto byl implementován do zákona o kritické infrastruktuře, obsahuje 8 sektorů. (Ministerstvo vnútra SR, 2017)

1.5.4 Komparace vybraných států

Pro komparaci byly použity USA, kvůli jejich historicky prvnímu definování kritické infrastruktury, ty samotné tvoří větší celek než společenství států EU, jež je také blíže zmíněné. Dále byla začleněna SR z důvodu podobné velikosti jako ČR a také proto, že je součástí EU a vychází tak ze stejné evropské legislativy. V tabulce 9 se porovnávají sektory USA a EU, ty evropské jsou dále implementovány do struktur členských států, kde v tabulce 10 dochází ke komparaci sektorů kritické infrastruktury SR a ČR. Každý jednotlivý stát EU vychází ze stejného základu, ze kterého si vybere pro něj nejdůležitější prvky a začlení je do své národní legislativy.

Tabulka 9 Porovnání sektorů kritické infrastruktury USA a EU

USA	EU
chemikálie	energetika
prodejní prostory	informační a komunikační technologie
komunikace	voda
kritická výroba	potravinářství
přehrady	zdravotnictví
obranný průmysl	finanční trh
nouzové služby	veřejnost, pořádek a bezpečnost
energetika	veřejná správa
finanční služby	doprava
potravinářství a zemědělství	chemický a jaderný průmysl
státní správa	vesmír a výzkum
zdravotnictví a veřejné zdraví	
informační technologie	
jaderné reaktory, materiály a odpad	
doprava	
voda a odpadní vody	

Zdroj: vlastní výzkum

Tabulka 10 Porovnání sektorů kritické infrastruktury ČR a SR

Slovensko	ČR
doprava	energetika
elektronické komunikace	vodní hospodářství
energetika	potravinářství a zemědělství
informační a komunikační technologie	zdravotnictví
pošta	doprava
průmysl	komunikační a informační systémy
voda a atmosféra	finanční trh a měna
zdravotnictví	nouzové služby
	veřejná správa

Zdroj: vlastní výzkum

2 Cíl práce a výzkumná otázka

2.1 Cíl práce

Cílem práce je analyticky zhodnotit možné teroristické ohrožení elektrizační soustavy ČR.

2.2 Výzkumná otázka

Je česká elektrizační soustava dostatečně zabezpečena proti případnému teroristickému útoku?

3 Metodika

Rešerše vychází z odborných publikací, odborných zpráv, souvisejících zákonů a nařízení. Jejím účelem je přinést aktuální přehled o současných hrozbách, konkrétně terorismu, ohrožujících elektrizační soustavu ČR a dále tuto soustavu blíže specifikuje. Jejím účelem je poskytnout podklady pro výzkumnou část práce. Pro vyhodnocení výsledků byla vytvořená nová metoda hodnocení rizik na základě metody checklistu, dále označována pouze checklist.

Checklist se v ose x skládá ze 3 sektorů elektrizační soustavy, kdy 1. sektor obsahuje výrobny elektřiny, které jsou dále rozděleny na jadernou, uhelnou a vodní. 2. sektor tvoří přenosová soustava, která obsahuje vedení 400 kV, vedení 220 kV, stožáry, elektrické stanice a technický dispečink. 3. sektor představuje distribuční soustavu, která se dělí na vedení 110 kV, vedení menší jak 100 kV, stožáry, elektrické stanice a technický dispečink. Osa y obsahuje rizikové faktory, které mohou ohrozit uvedené sektory elektrizační soustavy, jednotlivé typy teroristických útoků jsou uvedeny a blíže specifikovány v kapitole 4.3.

Ke každému teroristickému útoku mohl daný expert přiřadit 1 ze 3 stupňů škály možného způsobeného poškození u hodnoceného prvku elektrizační soustavy:

1. stupeň označen N **-** daný útok neohrozí provoz konkrétního uzlu,

2. stupeň označen P **-** daný útok poškodí, ale nevyřadí z provozu konkrétní uzel,

3. stupeň označen V **-** daný útok konkrétní uzel vyřadí z provozu.

Všichni experti se shodli na tom, že pro zdárně provedený teroristický útok je nezbytná znalost konkrétního provozu nebo prvku, na který útočí. Míra účinnosti konkrétního útoku je v přímé závislosti na znalosti daného provozu nebo prvku. Pokud je útok veden na nejslabší nebo nejcitlivější místo, dokáže mnohem efektivněji způsobit škody než útok mnohem silnější, který je veden neefektivně. Z tohoto hlediska vycházeli všichni experti a uváděli maximální možné škody při znalosti cíle útoku.

Sestavený checklist byl předložen expertům elektrizačních společností, konkrétně z výroben elektřiny, ti byli zastoupeni z jaderné, uhelné a vodní elektrárny, které mají v ČR dominantní postavení a největší vliv na výrobě elektřiny. Dále byl osloven expert

přenosové soustavy, expert distribuční soustavy a expert Policie ČR z oddělení krizového řízení, jež vyplnil všechny 3 sektory elektrizační soustavy z pohledu veřejné správy, díky tomu mohlo dojít ke komparaci. Tento dokument je uveden v příloze 1.

Po obdržení dat z checklistů od expertů elektrizačních společností a experta Policie ČR uvedených v tabulce 13 a 14 došlo k hodnocení výsledků. Pro lepší orientaci byly výsledky vyhodnoceny tak, že ke každé hodnotě možného poškození způsobeného teroristickým útokem byly přiřazeny 1 až 3 body podle tabulky 11. Z těch podle tabulky 12 byly vypočteny průměrné hodnoty pro prvky elektrizační soustavy i pro rizikové faktory terorismu, které jsou uvedeny v tabulce 15 a 16. Finálně byla provedena komparace výsledků analýzy expertů elektrizačních společností s výsledky analýzy experta Policie ČR. Při komparaci v tabulce 17 již došlo k detailnějšímu rozkladu všech hodnot na 5ti bodové škále podle tabulky 12. Tabulka 17 určuje průměrnou efektivnost možného teroristického ohrožení elektrizační soustavy ČR i průměrné hodnoty zranitelnosti elektrizační soustavy ČR teroristickými útoky. Z komparace vychází hodnocení teroristického ohrožení elektrizační soustavy a posouzení, zda je elektrizační soustava ČR dostatečně zabezpečena proti případnému teroristickému útoku.

Tabulka 11 Přiřazení bodů podle stupně možného poškození teroristickým útokem

legenda	***body***
1. stupeň označen N - *daný útok neohrozí provoz konkrétního uzlu*	***1***
2. stupeň označen P - *daný útok poškodí, ale nevyřadí z provozu konkrétní uzel*	***2***
3. stupeň označen V - *daný útok konkrétní uzel vyřadí z provozu*	***3***

Zdroj: vlastní výzkum

Tabulka 12 Hodnocení efektivnosti teroristického útoku

efektivnost teroristického útoku	***hodnoty***
neohrozí provoz	***1***
lehce poškodí	***1,5***
poškodí, ale nevyřadí	***2***
částečně vyřadí z provozu	***2,5***
zcela vyřadí z provozu	***3***

Zdroj: vlastní výzkum

Tato diplomová práce má sloužit pro navržení možných zlepšení v rámci elektrizační soustavy ČR a pro výuku v rámci Zdravotně sociální fakulty Jihočeské univerzity v Českých Budějovicích.

4 a 5 Vypuštěné pasáže

Následující pasáže o rozsahu 62 stran obsahují citlivé informace a jsou obsaženy pouze v archivovaném originále diplomové práce uloženém na Zdravotně sociální fakultě Jihočeské univerzity v Českých Budějovicích, v elektronické verzi byly tyto pasáže včetně příloh vypuštěny.

Závěr

Sociogenní hrozby, jejichž součástí je i terorismus, sice představují podle Analýzy hrozeb pro ČR z roku 2015 jen 10 % celkového ohrožení ČR, avšak útočníkem je člověk, jež je tvor velmi zvídavý a nevyzpytatelný. Na rozdíl od jiných ohrožení dokážou teroristické útoky cílit na nejzranitelnější a nejcitlivější místa a útočit koordinovaně. Nelze jen spoléhat na to, že k teroristickým útokům v této zemi nedošlo a proto se na ně není třeba připravovat. Je nezbytné vyhodnocovat rizika, uvědomovat si možné škody a následky způsobené těmito útoky a podle toho relevantně investovat do protiopatření. Bezpečnostní opatření nejen snižují způsobené následky provedenými útoky, ale také působí preventivně, kdy jednotlivé útočníky od útoků odrazují. To ospravedlňuje investice do zabezpečení, kdy dochází k předcházení škodám na majetku. Co je ale hlavní, chrání společnost, její životy a zdraví.

Po provedení analytického zhodnocení možného teroristického ohrožení elektrizační soustavy ČR vyvstaly otázky:

Je dostatečné zajištění bezpečnosti základními útvary policie?

Jsou dostatečné dojezdové časy specializovaných útvarů policie?

Je dostatečné zabezpečení technickými prostředky jednotlivých subjektů?

Je dostatečné zabezpečení ostrahou jednotlivých subjektů?

Je bezpečné zveřejňovat provozy subjektů na leteckých nebo satelitních snímcích?

Je zřejmé, že ideálně jsou zabezpečeny jaderné elektrárny ČR, které jsou odolné vůči napadení teroristickými útoky. Nyní však vyvstává otázka, zda se dají způsobit podobné škody napadením jiných prvků elektrizační soustavy ČR. Zda je nutné útočit na jaderné elektrárny, když elektrické stanice přenosové soustavy jsou zabezpečeny mnohem méně, přitom jejich vyřazení může způsobit odstávku výroben elektřiny. Na celkovou funkčnost elektrizační soustavy ČR nebude mít pravděpodobně vliv vyřazení jedné nebo několika výroben elektřiny (netýká se jaderných elektráren), to samé zřejmě platí pro elektrické stanice přenosové soustavy. Co by však mohl být pravděpodobně největší problém, kdyby došlo k napadení a dlouhodobému vyřazení technického dispečinku, nejhůře i záložního technického dispečinku, jež nejsou tak dobře zabezpečeny.

Seznam použitých zdrojů

1 *Analýza hrozeb pro Českou republiku*, 2015. [online]. Hasičský záchranný sbor ČR. [cit. 2016-25-11]. Dostupné z: http://www.hzscr.cz/soubor/analyza-hrozeb-zprava-pdf.aspx

2 *APS power grid has endured 9 minor acts of sabotage in recent years*, 2015. Azcentral [online]. 200 East Van Buren Phoenix, AZ 85004 [cit. 2017-04-02]. Dostupné z: http://www.azcentral.com/story/money/2015/03/25/aps-power-grid-endured-minor-acts-sabotage-recent-years/70409172/

3 *Arkansas Man Sentenced to 15 Years for Attacks on Central Arkansas Power Grid*, 2015. U.S. Department of Justice [online]. 950 Pennsylvania Avenue, NW Washington, DC 20530-0001 [cit. 2017-04-02]. Dostupné z: https://www.justice.gov/opa/pr/arkansas-man-sentenced-15-years-attacks-central-arkansas-power-grid-0

4 *Audit národní bezpečnosti*, 2016. [online]. Ministerstvo vnitra ČR. [cit. 2016-01-12]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

5 BAEV, P., 2011. *The North Caucasus: a Hotbed of Terrorism in Metamorphosis*. 27 RUE DE LA PROCESSION, 75740 PAPRIS CEDEX 15 - FRANCE: Ifri. ISBN 978-2-86592-862-0.

6 BENEŠ, I., 2007. *Energetická bezpečnost: informační příručka*. Praha: Cityplan. ISBN 978-80-254-1244-2.

7 *Bezpečnostní strategie České republiky*, 2015. [online]. Ministerstvo zahraničních věcí ČR. [cit. 2016-05-11]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

8 BRZYBOHATÝ, M., 1999. *Terorismus*. Praha: Police History. ISBN 80-902-6701-7.

9 CARUSO, R., LOCATELLI, A., 2014. *Understanding terrorism: a socio-economic perspective*. Bingley, England: Emerald Group Publishing Limited. Contributions to conflict management, peace economics and development, v. 22. ISBN 978-1-78350-828-0.

10 *CBRN terorismus – vážná hrozba 21. století*, 2005. www.natoaktual.cz [online]. Výstavní 8, Ostrava 9, 709 00: Jagello 2000 [cit. 2017-04-17]. Dostupné z: http://www.natoaktual.cz/cbrn-terorismus-vazna-hrozba-21-stoleti-d9o-/na_analyzy.aspx?c=A050510_094008_na_analyzy_m02

11 *ČEPS, a.s.: Činnosti*, 2017. [online]. © ČEPS, a.s., 2017 [cit. 2017-02-23]. Dostupné z: http://www.ceps.cz/CZE/Cinnosti/Stranky/Default.aspx

12 EDWARDS, M., 2014. *Critical infrastructure protection*. CENTRE OF EXCELLENCE--DEFENCE AGAINST TERRORISM, ANKARA a TURKEY. The authors and IOS Press. Nieuwe Hemweg 6B, 1013 BG Amsterdam, Netherlands: IOS Press BV. ISBN 978-161-4993-575.

13 *Energetický regulační věstník*, 2014. [online]. Energetický regulační úřad. [cit. 2017-14-03]. Dostupné z: https://www.eru.cz/documents/10540/613886/ERV_3_2014/82ed8b31-5e48-45d3-b6b0-c44911b73fe4

14 *Energetický regulační věstník*, 2015. [online]. Energetický regulační úřad. [cit. 2017-14-03]. Dostupné z: https://www.eru.cz/documents/10540/1174016/ERV_2_2015/5c5852a5-312d-4704-887e-2c1b6db648e4

15 *Energetický regulační věstník*, 2016. [online]. Energetický regulační úřad. [cit. 2017-14-03]. Dostupné z: https://www.eru.cz/documents/10540/2041142/ERV_4_2016.pdf/819c9b7a-346d-4c6b-bfa4-5dcd59db7f78

16 GORTNEY, W. E., 2012. *Counter-Improvised Explosive Device Operations: Joint Publication 3-15.1* [online]. 09 January 2012. VADM, USN: JOINT CHIEFS OF STAFF [cit. 2017-04-17]. Dostupné z: http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf

17 HROMADA, M., 2014. *Ochrana kritické infrastruktury ČR v odvětví energetiky*. V Ostravě: Sdružení požárního a bezpečnostního inženýrství. ISBN 978-80-7385-144-6.

18 *Kodex přenosové soustavy, část I.*, 2014. [online]. Česká energetická přenosová soustava, a.s. [cit. 2017-16-03]. Dostupné z: https://www.eru.cz/documents/10540/479698/CI_k_prip.pdf/30617b53-ff12-49cf-9445-6bb918cddc06

19 *Kodex přenosové soustavy, část II.*, 2014. [online]. Česká energetická přenosová soustava, a.s. [cit. 2017-16-03]. Dostupné z: https://www.eru.cz/documents/10540/479698/CII_k_prip.pdf/098792a3-e424-4a52-a1a3-a51a983bf8bc

20 *Kodex přenosové soustavy, část V.*, 2014. [online]. Česká energetická přenosová soustava, a.s. [cit. 2017-16-03]. Dostupné z: https://www.eru.cz/documents/10540/479698/CV_k_prip.pdf/2f28f90c-30aa-4040-85a6-053fd4fe3048

21 *Komplexní strategie České republiky k řešení problematiky kritické infrastruktury*, 2010. [online]. Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR. [cit. 2016-25-11]. Dostupné z: http://www.hzscr.cz/soubor/komplexni-strategie-ki-doc.aspx

22 *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030*, 2013. [online]. Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR. [cit. 2016-25-11]. Dostupné z: https://www.google.com/url?q=http://www.hzscr.cz/soubor/koncepce-oo-2020-2030-pdf.aspx&sa=U&ved=0ahUKEwj_quXX5dvTAhVCXRQKHbK1CjkQFggGMAE&client=internal-uds-cse&usg=AFQjCNEJFhS8nZUBd7UKXJTpPzIc-3EmoA

23 LEWIS, T. G., 2015. *Critical infrastructure protection in homeland security: defending a networked nation*. Second edition. Hoboken, New Jersey, United States of America: John Wiley. ISBN 978-111-8817-636.

24 LODGE, T., 2004. The ANC and the development of party politics in modern South Africa. *The Journal of Modern African Studies*, 42.02: 189-219.

25 MAULE, P., 2015. *Energetická bezpečnost v aktualizované Státní energetické koncepci České republiky: úloha rozvoje decentralizovaných energetických zdrojů*. Plzeň: Česká fotovoltaická asociace. ISBN 978-80-906281-0-6.

26 MIKA, O. J., 2003. *Současný terorismus: řešení krizových situací*. Praha: Triton. ISBN 80-725-4409-8.

27 *Military-Style Raid on California Power Station Spooks U.S.*, 2013. FOREIGN POLICY [online]. 11 Dupont Circle NW, Suite 600 Washington, DC 20036 [cit. 2017-04-02]. Dostupné z: http://foreignpolicy.com/2013/12/27/military-style-raid-on-california-power-station-spooks-u-s/

28 *MV SR: Krízové* riadenie, 2017. [online]. © 2017 Ministerstvo vnútra SR [cit. 2017-02-24]. Dostupné z: http://www.minv.sk/?Ochrana_kritickej_infrastruktury

29 *Národní program ochrany kritické infrastruktury*, 2010. [online]. Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR. [cit. 2016-25-11]. Dostupné z: http://www.hzscr.cz/soubor/narodni-program-ochrany-ki-doc.aspx

30 Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, 2010. [online]. [cit. 2017-14-02]. In: *Sbírka zákonů České republiky*, částka 149, . 5623-30. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/

31 *Policie prověřuje výbuchy, které poškodily vedení u solární elektrárny*, 2016. iDNES.cz [online]. Karla Engliše 519/11, 150 00 Praha 5. [cit. 2017-05-02]. Dostupné z: http://usti.idnes.cz/vybuch-poskodil-elektricke-vedeni-na-teplicku-f4b-/usti-zpravy.aspx?c=A160505_191123_usti-zpravy_cen

32 *Situační zpráva o vybraných oblastech bezpečnosti za období 1.1. do 30.6.2014*, 2014. [online]. Odbor bezpečnostní politiky Ministerstva vnitra ČR. [cit. 2017-12-02]. Dostupné z: https://www.google.com/url?q=http://www.mvcr.cz/soubor/situacni-zprava-2014-1-final-pdf.aspx&sa=U&ved=0ahUKEwiq1aC36dPTAhWJDxoKHVMDAJ0QFggKMAI&client=internal-uds-cse&usg=AFQjCNE9bV7xrmzX85G2x2TQJkwneOw9ow

33 *Situační zpráva o vybraných oblastech bezpečnosti za období 1.7. do 31.12.2014*, 2015. [online]. Odbor bezpečnostní politiky Ministerstva vnitra ČR. [cit. 2017-12-02]. Dostupné z: http://www.mvcr.cz/clanek/situacni-zprava-o-vybranych-oblastech-bezpecnosti-ve-ii-pololeti-2014.aspx

34 Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu, 2008. [online]. [cit. 2016-19-11]. In: *Úřední věstník Evropské unie*, částka 345, s. 75-82. Dostupné z: http://eur-lex.europa.eu/legal-

content/CS/TXT/HTML/?uri=CELEX:32008L0114&qid=1493808962162&from=CS

35 STEININGER, R., 2003. *South Tyrol: a minority conflict of the twentieth century*. New Brunswick, NJ: Transaction Publishers. ISBN 978-0-7658-0800-4.

36 *Strategie České republiky pro boj proti terorismu*, 2013. [online]. Odbor bezpečnostní politiky Ministerstva vnitra ČR. [cit. 2016-05-11]. Dostupné z: http://www.mvcr.cz/soubor/strategie-ceske-republiky-pro-boj-proti-terorismu-pdf.aspx

37 *Systém vyhlašování stupňů ohrožení terorismem*, 2016. [online]. Ministerstvo vnitra ČR. [cit. 2016-01-12]. Dostupné z: http://www.mvcr.cz/soubor/system-vyhlasovani-stupnu-ohrozeni-terorismem.aspx

38 ŠENOVSKÝ, M., ADAMEC, V., ŠENOVSKÝ, P., 2007. *Ochrana kritické infrastruktury*. V Ostravě: Sdružení požárního a bezpečnostního inženýrství. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-025-8.

39 *Terrorist Attack Left All of Yemen In Darkness Last Week: Another Wake-Up Call*, 2014. Forbes: Energy [online]. © 2017 Forbes Media LLC. [cit. 2017-04-02]. Dostupné z: https://www.forbes.com/sites/peterdetwiler/2014/06/19/terrorist-attack-left-all-of-yemen-in-darkness-last-week-another-wake-up-call/#2e79ce557e36

40 VANTUCH, P., 2011. *Trestní zákoník s komentářem: komentář k zákonu č. 40/2009 Sb., ve znění pozdějších předpisů*. Olomouc: ANAG. Právo (ANAG). ISBN 978-80-7263-677-8.

41 *Výroba elektřiny: Energie z obnovitelných zdrojů*, 2017. https://www.cez.cz [online]. Duhová 2/1444, Praha 4: Copyright 2017 ČEZ [cit. 2017-03-23]. Dostupné z: https://www.cez.cz/cs/vyroba-elektriny/obnovitelne-zdroje.html

42 *Výroba elektřiny: Jaderná energetika*, 2017. https://www.cez.cz [online]. Duhová 2/1444, Praha 4: Copyright 2017 ČEZ [cit. 2017-03-23]. Dostupné z: https://www.cez.cz/cs/vyroba-elektriny/jaderna-energetika.html

43 *Výroba elektřiny: Mapa výrobních zdrojů*, 2017. https://www.cez.cz [online]. Duhová 2/1444, Praha 4: Copyright 2017 ČEZ [cit. 2017-03-23]. Dostupné z: https://www.cez.cz/cs/vyroba-elektriny/mapa-vyrobnich-zdroju.html#!

44 *Výroba elektřiny: Paroplynové elektrárny*, 2017. https://www.cez.cz [online]. Duhová 2/1444, Praha 4: Copyright 2017 ČEZ [cit. 2017-03-23]. Dostupné z: https://www.cez.cz/cs/vyroba-elektriny/paroplynove-elektrarny.html

45 *Výroba elektřiny: Uhelné elektrárny*, 2017. https://www.cez.cz [online]. Duhová 2/1444, Praha 4: Copyright 2017 ČEZ [cit. 2017-03-23]. Dostupné z: https://www.cez.cz/cs/vyroba-elektriny/uhelne-elektrarny.html

46 *Výroba elektřiny: Voda*, 2017. https://www.cez.cz [online]. Duhová 2/1444, Praha 4: Copyright 2017 ČEZ [cit. 2017-03-23]. Dostupné z: https://www.cez.cz/cs/vyroba-elektriny/obnovitelne-zdroje/voda.html

47 Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), 2000. [online]. [cit. 2017-14-02]. In: *Sbírka zákonů České republiky*, částka 73, s. 3475-87. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/

48 Zákon č. 361/2000 Sb., Zákon o provozu na pozemních komunikacích a o změnách některých zákonů, 2000. [online]. [cit. 2017-14-02]. In: *Sbírka zákonů České republiky*, částka 98, s. 4570-616. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/

49 Zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), 2000. [online]. [cit. 2017-14-02]. In: *Sbírka zákonů České republiky*, částka 131, s. 7142-89. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/

50 Zákon č. 40/2009 Sb., Zákon trestní zákoník, 2009. [online]. [cit. 2017-14-02]. In: *Sbírka zákonů České republiky*, částka 11, s. 354-464. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/

51 Zákon č. 45/2011 Sb., o kritickej infraštruktúre, 2011. [online]. [cit. 2017-14-02]. In: *Nové ASPI*, částka 19, s. 434-42. Dostupné z: http://www.noveaspi.sk/products/lawText/1/73766/1/2

52 Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014. [online]. [cit. 2016-19-11]. In: *Sbírka zákonů České republiky*, částka 75, s. 1926-36. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/

Seznam obrázků

Obrázek 1 Zjednodušené zobrazení elektrizační soustavy 20

Obrázek 2 Množství přenesené elektřiny v přenosové soustavě 24

Obrázek 3 Působnost provozovatelů distribuční soustavy na území ČR 27

Obrázek 4 Typy nebezpečí 31

Obrázek 5 Stupně ohrožení terorismem 45

Obrázek 6 Mapa tepláren a uhelných elektráren 61

Obrázek 7 Mapa jaderných elektráren 62

Obrázek 8 Mapa paroplynových a plynových elektráren 64

Obrázek 9 Mapa vodních a přečerpávacích elektráren 65

Obrázek 10 Mapa fotovoltaických a větrných elektráren 66

Obrázek 11 Schéma sítí 400 a 220 kV 67

Obrázek 12 Efektivnost možného teroristického ohrožení elektrizační soustavy ČR 99

Obrázek 13 Zranitelnost elektrizační soustavy ČR teroristickými útoky 107

Seznam tabulek

Tabulka 1 Odvětvová kritéria 14

Tabulka 2 Podoblast Elektřina 15

Tabulka 3 Roční výroba elektřiny 2010 21

Tabulka 4 Roční výroba elektřiny 2016 22

Tabulka 5 Struktura zdrojů elektrizační soustavy v ČR 23

Tabulka 6 Délka vedení ČEPS, a.s. v provozu 24

Tabulka 7 Zařízení ČEPS, a.s. 25

Tabulka 8 Základní technické informace provozovatelů distribuční soustavy ČR 27

Tabulka 9 Porovnání sektorů kritické infrastruktury USA a EU 49

Tabulka 10 Porovnání sektorů kritické infrastruktury ČR a SR 49

Tabulka 11 Přiřazení bodů podle stupně možného poškození teroristickým útokem 52

Tabulka 12 Hodnocení efektivnosti teroristického útoku 52

Tabulka 13 Checklist expertů elektrizačních společností 73

Tabulka 14 Checklist experta Policie ČR oddělení krizového řízení 74

Tabulka 15 Hodnocení elektrizační soustavy ČR experty elektrizačních společností 75

Tabulka 16 Hodnocení elektrizační soustavy ČR expertem Policie ČR 76

Tabulka 17 Komparace hodnocení elektrizační soustavy ČR 77

Tabulka 18 Výrobny elektřiny z pohledu expertů elektrizačních společností 79

Tabulka 19 Přenosová soustava z pohledu expertů elektrizačních společností 80

Tabulka 20 Distribuční soustava z pohledu expertů elektrizačních společností 82

Tabulka 21 Výrobny elektřiny z pohledu experta Policie ČR 87

Tabulka 22 Přenosová soustava z pohledu experta Policie ČR 88

Tabulka 23 Distribuční soustava z pohledu experta Policie ČR 90

Tabulka 24 Komparace výsledků výroben elektřiny 94

Tabulka 25 Komparace výsledků přenosové soustavy 95

Tabulka 26 Komparace výsledků distribuční soustavy 97

Seznam příloh

Příloha 1 Checklist zranitelnosti elektrizační soustavy České republiky teroristickými útoky 128

Seznam zkratek

BAS - Výbor pro osvobození jižního Tyrolska

CBRNE - chemické, biologické, radioaktivní látky, jaderné materiály a výbušniny

CIWIN - Výstražné informační sítě kritické infrastruktury

ČEPS - Česká energetická přenosová soustava

ČEZ - České energetické závody

ČR - Česká republika

EPCIP - Evropský program na ochranu kritické infrastruktury

EU - Evropská unie

IT - informační technologie

IZS - integrovaný záchranný systém

NATO - Severoatlantická aliance

NBÚ - Národní bezpečnostní úřad

Směrnice o EKI - Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

SR - Slovenská republika

USA - Spojené státy americké