TYPOLOGICKÉ ZNAKY KRITICKÉ INFRASTRUKTURY

TYPOLOGICAL FEATURES OF THE CRITICAL INFRASTRUCTURE

Josef ŘÍHA
riha.joe@volny.cz

Abstract

The objective of this paper is to identify links which are important from the Critical Infrastructure vulnerability point of view. There are briefly described and compared different procedures for the identification and designation of critical infrastructures and the assessment of the need to improve their protection. Critical Infrastructure is currently looking for its contents, structure, purpose, and political context. Suitable criteria for its identification and the assessment of potential risks are looked for and some of the first attempts of simulation and the creation of a model for a "System of Systems" are appearing. The practicism of the crisis management is being moved into the sphere of the "science of safety".

Keywords

Critical infrastructure; critical infrastructure interdependencies; criteria for criticality; key asset; points of failure; risk analysis; risk impact scale; risk mitigation; risk probability; severity of the impact; vulnerability.

Příspěvek naznačuje problém posuzování obecně uznávaných typologických znaků kritické infrastruktury. Jsou analyzovány společné a rozdílné přívlastky kritické infrastruktury na podkladě stěžejních dokumentů USA, NATO, EU a bezpečnostní strategie České republiky. Pozornost je věnována velkým komplexním systémům, problematice vnitřní vzájemné závislosti dílčích infrastruktur a zranitelnosti.

Práce byla uskutečněna za finanční pomoci Grantové agentury Akademie věd ČR – reg.č. grantu IAA711680701 „Bezpečnostní rizika v procesu posuzování vlivu na životní prostředí".

Pragmatický úvod

Představy o *kritické infrastruktuře KI* se pravděpodobně datují od roku 1983, původně pod názvem *životně důležité infrastruktury* [14]. Je to souhrnné označení pro fyzické, kybernetické a organizační (obslužné) systémy, které jsou nutné pro zajištění ochrany životů a zdraví lidí a majetku, minimálního chodu ekonomiky a správy státu. *Objekty KI* jsou vybrané stavby a zařízení veřejné infrastruktury a další prvky, které vlastní nebo provozují subjekty kritické

infrastruktury. *Subjekty KI* jsou vlastníci a provozovatelé výrobních a nevýrobních systémů vytvářející produkty nebo poskytující služby kritické infrastruktury.

Sleduje se citlivost a potencionální zranitelnost komplexních systémů. Význam přírodních pohrom z hlediska ohrožení KI v současnosti ustupuje hrozbě superterorismu na pozadí „*střetu civilizací*“ [11]. Jestliže zvládání opakujících se přírodních katastrof (povodní, tornád, hurikánů) je uspokojivě řešeno na úrovni jednotlivých států, potom tomu tak není v případě cílených teroristických akcí. I když s výhradami, tak civilizovaný svět musí akceptovat kampaň pod názvem „*War on Terror*“.

Ochrana KI eskaluje po událostech 11. září 2001, nabývá nový obsah a rozměr; v USA se bezprostředně formují první sofistikovaná opatření. Terorismus, ať již s použitím konvenčních nebo nekonvenčních zbraní, se stal aktuální ústřední výzvou pro celosvětové společenství. Ultraterorismus [26] představuje použití jaderných výbušných zbraní, radiologických zbraní, chemických zbraní a biologických zbraní, bojových chemických látek, průmyslově vyráběných toxických chemických látek, radionuklidů nebo vysoce infekčních materiálů, jakož i jakékoliv teroristické akce proti jaderným, energetickým, chemickým, petrochemickým a biologickým zařízením jednotlivci, nestátními skupinami nebo státem podporovanými aktéry proti konkrétní sociální skupině k vyvolání strachu nebo teroru. *Odhad rizika teroristického činu* na pozadí teoretických poznatků [20] tvoří součást hypotetické úvahy „*představy neuvěřitelného*“ [21].

Dynamický vývoj za časové období 1983 až 2003 dokládá vyčerpávající zpráva z vědecko výzkumného kongresového centra USA [14] pod názvem „*Kritická infrastruktura a klíčové objekty: Definice a identifikace*“. V rámci členských zemí EU byl rozvinut „*Evropský program na ochranu KI*“ EPCIP [3]. Současně lze pozorovat rozvoj příbuzných disciplín ve prospěch objektivizace a zlepšení rozhodovacích procesů na pozadí kategorie DSS; registrují se disputace na téma možností matematizace komplexní bezpečnosti, uplatnění modelové a simulační techniky, hodnocení přijatelnosti či akceptovatelnosti rizika, možností měření neměřitelných veličin aj. Systémový přístup umožňuje synergetické pojetí mimořádných událostí a aplikaci náročné teorie katastrof [28].

Ochrana KI v ČR se vyvíjí pod bezprostředním vlivem vedoucích zemí a mezinárodních organizací. Neopominutelné jsou strategické koncepty USA, NATO a EU. Aktuální definice pro federální úroveň USA vymezuje KI jako "*systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro USA a zneschopnění nebo zničení takových systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečí, nebo na jakoukoliv jejich kombinaci*"; podle „Patriot Act“, viz [7]. Pohled na národní bezpečnost je zabudován do dokumentu *Národní strategie pro domácí bezpečnost,* který je považován za koncepční dokument, který bude dále rozpracováván dalšími strategiemi zaměřenými již na konkrétní problémy (dokument není veřejně přístupný). V USA se formují první sofistikovaná opatření - 14. února 2003 byla vydána "*Národní strategie fyzické ochrany kritické*

infrastruktury a klíčových zařízení" [30] a "*Národní strategie zabezpečení kybernetického prostoru*" [31].

Američané přitom důsledně rozlišují dva pojmy, tj. kritickou infrastrukturu (*critical infrastructure*) a klíčové prvky či aktiva (*key asset*). Klíčová aktiva představují ojedinělé prvky zvláštního významu. Jsou to samostatná zařízení, jejichž vyřazení sice neohrozí národní ekonomiku, ale může být zdrcující z hlediska vzniklých škod, ztrát na životech nebo podkopání veřejného sebevědomí. Zvláštní význam je dán historickou spojitostí s nějakou událostí (památníky, sochy, pietní místa, kulturní dědictví národa apod.) nebo místa, na kterých se shromažďuje velké množství lidí a kde by měl teroristický útok za následek velké ztráty na životech (stadiony, nákupní centra – tzv. měkké cíle). Strategie ochrany KI přitom má za cíl nejenom fyzicky chránit KI, ale zároveň posilovat důvěru ve vládu, v její schopnost zabezpečit služby, které jsou prostřednictvím KI poskytovány. Tato důvěra je vnímána jako základní pilíř hospodářské stability země.

Další úhel pohledu na řešení této problematiky, který má přímý vliv na ČR jako členského státu NATO, vnáší Výbor pro civilní ochranu Severoatlantické aliance. Informační zpráva z února 2003 je zaměřena na definování vzájemných závislostí jednotlivých prvků KI a ohodnocení těchto závislostí z pohledu zabezpečení rozhodujících činností v případě vzniku závažných mimořádných událostí. Jde o vliv na tzv. schopnosti státu reagovat na mimořádnou událost, resp. krizovou situaci. Zpráva pojednává o deseti následujících schopnostech, které by mohly prvky kritické infrastruktury ovlivňovat: *centrální schopnost reakce, zásobování (doplňování) základních služeb, místní schopnost reakce, dekontaminace, místní očista, vakcinace a ošetřování, péče o hromadně zraněné, hromadná evakuace, zjišťování ohrožení a jejich pojmenování, informování, varování a vyrozumění veřejnosti***.** Jednání výboru došlo k závěru, že mezi dvě nejkritičtější z uvedených schopností patří hromadná evakuace a informování, varování a vyrozumění veřejnosti.

Rada EU ve svých závěrech nazvaných *Předcházení, připravenost a reakce na teroristické útoky* a *Program solidarity EU o následcích teroristických hrozeb a útoků* přijatých na zasedání Rady v prosinci 2004 podpořila záměr Komise navrhnout *Evropský program na ochranu kritické infrastruktury* EPCIP a souhlasila, aby Komise zřídila *Výstražnou informační síť kritické infrastruktury* CIWIN. Definice KI v pojetí EU zahrnuje *„fyzické prostředky, obslužná a informační technologická zařízení, sítě a objekty (prvky) infrastruktury, jejichž poškození nebo zničení by mohlo mít vážný impakt na zdraví, bezpečnost nebo hospodářskou prosperitu obyvatelstva nebo efektivní funkci vlády*“; cit. [2]. V podrobnějším členění se uznávají tři základní skupiny objektů (prvků):

- Veřejné, soukromé a vládní objekty infrastruktury a vzájemně vnitřně propojené kybernetické a fyzikální sítě;
- Procedury a relevantní jednotlivosti mající kontrolu nad funkcemi kritické infrastruktury;
- Objekty s kulturním nebo politickým významem a dále tzv. „měkké cíle“ v podobě masových akcí (sportovních, kulturních apod.).

Přímý vliv na ČR z pozice členství v EU má dále koncept *Evropské kritické infrastruktury* ECI, zohledňující přeshraniční efekty. Zahrnuje „*fyzické prostředky, obslužná a informační technologická zařízení, sítě a objekty (prvky) infrastruktury, jejichž poškození nebo zničení by mohlo mít vážný impakt na zdraví, bezpečnost nebo hospodářskou prosperitu obyvatelstva nebo efektivní funkci vlády dvou nebo více členských zemí*“; cit. [2].

Vláda ČR na svém zasedání dne 25. února 2008 schválila novou *Koncepci ochrany obyvatelstva do roku 2013 s výhledem do roku 2020*, viz [32]. Nová koncepce klade zvýšený důraz na problematiku ochrany kritické infrastruktury – neboli životně důležité infrastruktury nezbytné pro řádné fungování veřejné správy a společnosti jako takové (např. dodávky elektřiny, tepla, potravin, pitné vody, pohonných hmot apod.). V rámci koncepce by měl být vytvořen *Národní program* ochrany kritické infrastruktury založený na zpracování dílčích strategií, koncepcí a analýz určených pro jednotlivé oblasti (sektory, odvětví) kritické infrastruktury a z nich vycházejících stanovení konkrétních úkolů, jejich nositelů a termínů plnění. Návrh definice KI v ČR, která je výsledkem práce odborné pracovní skupiny KI BRS zní: „*Kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva*“, cit. [33].

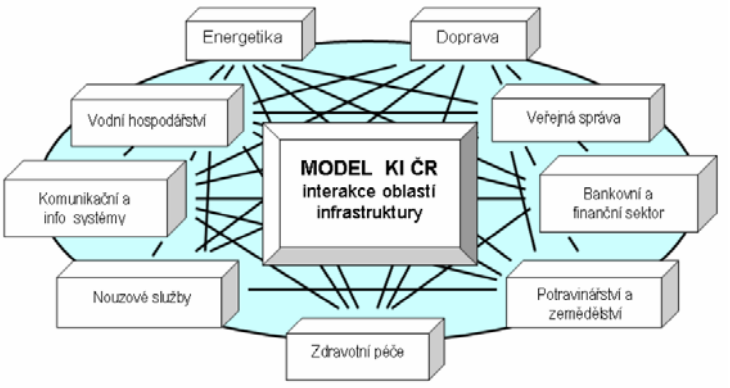
Kritická informační infrastruktura státu – slouží k informačnímu zajištění řádné funkceschopnosti kritické infrastruktury státu a označuje komplex informačních a komunikačních systémů a jejich služeb. Obsahuje součásti jako jsou telekomunikace, počítačové systémy a jejich programové vybavení, internet, přenosové sítě, poskytované služby atd.

Indikace objektů kritické infrastruktury

Znaky KI se odvíjejí z přijaté definice, získaných zkušeností a z teoretických poznatků aktuálně se rozvíjející bezpečnostní vědy [19], [23]. Pro indikaci existují různá teoretická východiska. Administrativně byrokratický systém přistoupil v první etapě řízené ochrany k tvorbě *prostých seznamů* KI. Podle praxe v různých zemích lze rozlišit:

(1) Seznam sektorů, objektů a služeb s kvalitativní (mlhavou) charakteristikou – např. „JE, vodárenská nádrž, energovod, dopravní koridor“;
(2) Seznam sektorů, objektů a služeb s kvantitativní (numerickou) charakteristikou – např. „teplárna s instalovaným tepelným výkonem vyšším než 30 MW“, viz model pro přežití obyvatelstva v určité oblasti jako OMN podle [13];
(3) Seznam kritických (životně důležitých) společenských funkcí, jako indikačních kritérií pro výběr a označení KI – např. „vyřazený objekt vyvolá dopad mimořádné události s postihem více než 1000 osob, na celou obec nebo plochu nad 1 km^2 “ (tj. vznik nouzové situace kategorie 5) podle [4].

V souladu s konceptem ad (1) je pro ČR definováno 9 oblastí KI nerovnoměrně zahrnujících 37 produktů nebo služeb [33]; schéma viz obr. 1. V té souvislosti je pozoruhodný legislativní a metodický předstih v domácím resortu obrany při vyhodnocování a výběru *objektů možného napadení* OMN. Ve vládou schválené *Směrnici k výběru objektů obranné infrastruktury a zpracování dokumentace* z roku 2007 je zřetelný překryv a duplicita výběru nevojenských rizikových objektů a služeb s tím, že doporučená kritéria jsou plně využitelná pro KI na úrovni krajů [13].



Obr. 1
Schéma interakcí oblastí kritické infrastruktury v ČR definovaných podle stavu v roce 2007

Prosté seznamy KI v současné době dominují ve většině národních strategií bezpečnostního rizika a vzájemně nepředstavují podstatné rozdíly. Aktéři v této oblasti se snaží výběr objektů KI opřít o *soubor kritérií* a tím zdůvodnit potřebnou ochranu ekonomicky, společensky a politicky. Jde o nesnadný úkol, jehož význam nemusí být prvořadý. Naznačuje to aktuální posun myšlení do oblasti celostního, holistického konceptu KI.

Podle dosavadních zkušeností kritéria KI vytváří dvě skupiny souborů, jednak *kritéria průřezová* (cross-cutting criteria), jednak *kritéria sektorová* (sectoral criteria). Společně představují *referenční soubor kritérií*. Průřezová kritéria jsou generována na základě posouzení závažnosti a míry narušení nebo potenciální destrukce KI. Závažnost se zpravidla hodnotí pomocí verbálně-numerické stupnice pro posouzení *závažnosti* ohrožení KI. Obecně a podle možností pro každou situaci průřezová kritéria hodnotí účinky na veřejnost (počet ovlivněných osob); ekonomiku (význam ekonomických ztrát nebo pokles výroby a služeb); životní prostředí; politickou situaci; psychologickou oblast; časový faktor a efekt; dostupné varianty a scénáře.

Sektorová kritéria se týkají prioritních odvětví (hospodářských oblastí) KI. Je třeba uplatňovat vhodnou metodu pro určování pořadí (priority) infrastruktury napříč spektrem sektorů, zachovat jednoduchost, umožnit opakovatelnost. Je nutná spolupráce s relevantními subjekty KI (stakeholders) a kompetentními představiteli resortů (odvětví).

V širších souvislostech nelze přehlédnout institut *chráněných zájmů společnosti*. Chráněné zájmy lidské společnosti v širším slova smyslu představuje soubor: život člověka (cena života člověka); zdraví člověka (prevence a ochrana zdraví; hygiena člověka); majetek (kritický majetek); kritická infrastruktura (viz model KI ČR), životní prostředí (stabilita systému ŽPČ – biodiverzita); rozvoj lidského společenství (udržitelný rozvoj, nejlepší dostupná technologie); systém výchovy, výuky, osvěty ve vztahu k bezpečnosti člověka a společnosti (globální výchova se zřetelem na bezpečnost), globální (vojenská) bezpečnost.

Fabulace udržitelného rozvoje [21] usiluje o virtuální kategorie udržitelné kritické infrastruktury v odvětví energetiky, dopravy, apod., viz *Zelená kniha* [2]; děje se tak především na podkladě dokumentu „*Řídicí principy trvale udržitelného rozvoje evropského kontinentu*“, který byl přijat v roce 2000 zasedáním Konference ministrů zodpovědných za územní plánování (CEMAT) a je od svého schválení používán 41 členskými zeměmi CEMAT pro posuzování udržitelnosti rozvoje. Součástí Řídicích principů jsou *Zásady politiky udržitelného územního plánování v Evropě*, které stanoví zásadních deset principů.

Počáteční přístupy k modelům KI se snaží pro jejich bezpečnostní analýzu aplikovat různé metody operačního výzkumu a systémové metody rozhodování. Významné je uplatnění axiomatické teorie kardinálního užitku MUT a formalizované metody multikriteriální analýzy např. TUKP. Jejich součástí je rozsáhlá typologie[1)] vícerozměrných modelů diskrétního a spojitého typu (vč. diferencovaných vlastností typu *Soft* nebo *Hard*), uváděné pod různými názvy např. „*interactive/discrete, multicriterion/integrated, development/security, vulnerability/risk, impact/spatial, choice/environmental, impact/concordance – analysis*“ apod., jak autor uvedl v [22].

Typologické znaky KI jsou v oficiálních dokumentech zpravidla identické, odlišnosti se vyskytují pouze výjimečně. Nicméně *stanovení kritérií výběru* je v současné době označováno za prvořadý odborný úkol v oblasti řízené ochrany KI; v domácích podmínkách běží několik výzkumných úkolů, v rámci EU má k upřesnění přispět spolupráce expertních týmů; aktuálním byl dokument „*GREEN PAPER*“, prezentovaný CEC 17. 11. 2005 jako výzva členským státům podílet se na vytvoření účinné evropské ochrany KI, viz [2] a „*Evropský program na ochranu KI*“ EPCIP [3]. Výsledná zpráva z roku 2007 obsahující katalog kritérií má zůstat pro veřejnost nepřístupná.

V další části textu jsou uvedeny poznatky, které lze pokládat za relevantní pro možnost označení objektu KI. Pro určení příslušnosti do KI je třeba posoudit zejména:

- *rozsah* – ztráta prvku kritické infrastruktury se hodnotí podle velikosti zeměpisné oblasti, která by mohla být jeho ztrátou nebo nedostupností postižena – vnitrostátní, mezinárodní, regionální nebo místní;

- *závažnost* – stupeň dopadu nebo ztráty funkce může být hodnocen jako žádný, minimální, mírný nebo velký. Mezi kritéria, která lze pro hodnocení velikosti použít, patří zejména:
  - dopad na obyvatele (počet zasažených obyvatel, ztráty na životech, onemocnění, vážné zranění, nutnost evakuace),
  - hospodářský dopad (vliv na HDP, závažnost hospodářských ztrát nebo zhoršení kvality výrobků nebo služeb),
  - životní prostředí (rozsah poškození, ovlivněné složky životního prostředí),
  - synergické jevy (mezi jinými prvky kritické infrastruktury),
  - politické dopady;
- *časové faktory* – závažnost dopadů na jednotlivé subjekty v závislosti na čase (tj. okamžitě, za 24, 48 hod, za týden, později).

V tab. 1 jsou formou incidenční matice [14] vysvětleny důvody, které v průběhu času obecně generují kritickou infrastrukturu z hlediska životně důležitých funkcí pro národní obranu, bezpečnost ekonomiky, bezpečnost a zdraví člověka a národní morálku. Podle slovenské praxe [34] musí být splněno alespoň jedno z následujících kritérií:

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

Tabulka 1
Důvody, které v průběhu času obecně generují kritickou infrastrukturu z hlediska životně důležitých funkcí pro společnost; podle [14]

Infrastruktura	Kritéria, která lze pokládat za životně důležitá pro:			
	☛ národní obranu	☛ bezpečnost ekonomiky	☛ bezpečnost a zdraví člověka	☛ národní morálku
telekomunikace	✦	✦		
energetika	✦	✦		
finance		✦		
doprava	✦	✦		
voda			✦	
pohotovost			✦	
vláda			✦	
zdravotní služby			✦	
národní obrana	✦			
zahraniční služby	✦			
účinnost práva			✦	
zahraniční záležitosti	✦			
nukleární zařízení, elektrárny			✦	
zvláštní události				✦
potraviny/zemědělství			✦	
drobná výroba		✦		
chemie			✦	
obranný průmysl	✦			
poštovní služby			✦	
národní památníky, symboly				✦

Dokument [9] ze dne 5. června 2008 potvrdil předcházející koncept [8], který precizoval způsob identifikace ECI (Article 3 – *Identification of European Critical Infrastructure*). Formálně byla oznámena dohoda a politický souhlas se způsobem identifikace a označování ECI. Byla deklarována tři stěžejní průřezová (robustní) kritéria, která představují nezbytnou podmínku pro název „kritická infrastruktura“, tj.

(a) *kritérium osobní újmy* (casualties criterion) *tzn. bezpečnost*, vyjádřené počtem zemřelých, zraněných;
(b) *kritérium ekonomické* (economic effects criterion), vyjádřené významem ekonomické ztráty, popř. poklesem výroby nebo služeb, včetně potenciálních environmentálních efektů;

(c) *kritérium společenské* (public effects criterion), vyjádřené impaktem na důvěru vládě, dopadem na tělesné a duševní zdraví a rozvratem běžného denního způsobu života, včetně rozpadu veřejných služeb (např. ambulantní a terénní služby sociální péče).

V závěru roku 2008 byla uveřejněna *Směrnice Rady*[2)] *o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu*; obsah hluboce zaostal proti prvopočáteční představě následkem zdrcující kritiky některých členských zemí EU. Kategorie ECI[2)] [9] je omezena pouze na oblast energetiky a dopravy, popř. na sektor informatiky. Fatální torzo písemnictví dokládá nedostatek invence bruselských úředníků ve prospěch vytvořených institucí pro ochranu KI. Schází širší „vize" nebo filosofie CIP.

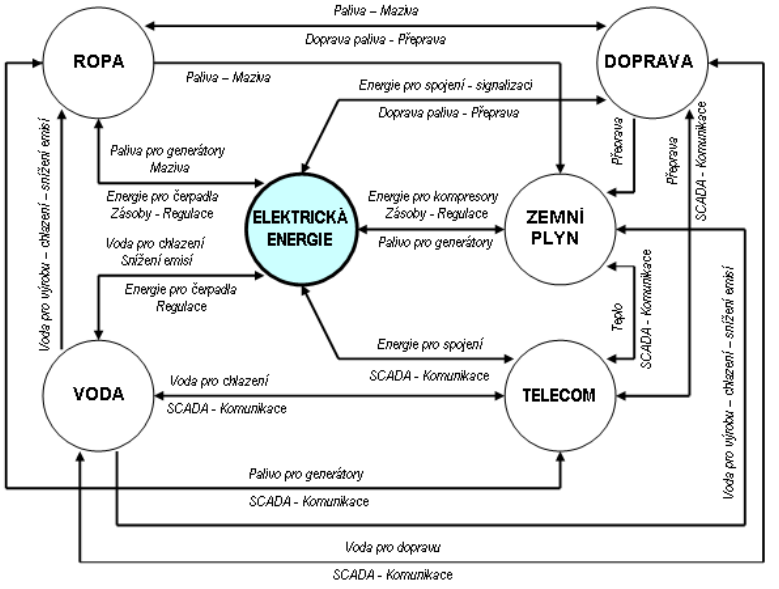
Pro indikaci objektů KI jsou vyvíjeny pomocné rozhodovací nástroje typu DSS využívající strojovou výpočetní techniku. Např. kanadská konzultační firma *The Zeta Group, Inc*. v Ottawě [35] nabízí software pod označením „CritiCalc®", který formalizovaným způsobem identifikuje kritickou infrastrukturu a stupeň kritičnosti. Ve spojení s GIS má uživatel okamžitou vizualizaci a mapový průmět objektů KI do území. V USA byl již v roce 2003 generován analytický hierarchický proces AHP, formalizovaná metoda posuzování zranitelnosti VAM, expertním způsobem stanoveno deset stěžejních kritérií vč. jejich váhy metodou párového porovnání a software „IARDstick". Červenou niť pomocného nástroje představuje „anatomie rizika[3)]".

Specifické zvláštnosti

Specifické zvláštnosti se odvíjejí z hlediska systémového přístupu, kde je kategorie KI vnímána jako *„systém systémů"* SoS. Zároveň představují oblast pro přednostní teoretický výzkum [17], [24]. Půjde o řešení *vnitřní vzájemné závislosti dílčích infrastruktur* (*Input-Output Model for Interdependent Infrastructure*) a *zranitelnost* (*napadnutelnost*) [22]. Mimořádný význam musí být věnován simulaci a modelování *velkých komplexních systémů kritické infrastruktury* LCCI [25]. Znalost jednotlivých dílčích subsystémů pro analýzu nepostačuje, je třeba analyzovat vzájemné propojení a interakce (viz význam průřezových kritérií). Současné nedostatky spočívají v nesprávné definici objektů, v nevhodném modelování a v nevhodné strategii řešení. Pod tlakem jednotlivých subjektů je hlavní pozornost často věnována funkci a bezpečnosti pouze některým dílčím subsystémům, nikoliv komplexnímu systému jako celku. Existuje rozsáhlý soubor příčin a zdrojů chyb v analýze bezpečnostního rizika, které lze minimalizovat pouze důslednou aplikací systémového přístupu a osobní zkušeností analytika (operátora) v oblasti CIP. Posuzování kritičnosti složek KI není triviální záležitostí – v různých situacích mají různou roli aktivní, reaktivní, kritickou nebo tlumící (nikoliv aditivní). Např. existence více reálných variant pro dopravu lidí nebo zboží z místa A do místa B obecně snižuje míru kritičnosti dopravní infrastruktury. Soubor relevantních vlastností složek tvoří problém zranitelnosti KI. Na základě poznatků z práce [25] vznikají pochybnosti o smysluplnosti tvorby identifikačních

kritérií pro KI. Pro národní a nadnárodní strategii je zřejmě nutný *holistický koncept* CIP, jak potvrzuje zjištění skutečného trendu v mezinárodním měřítku podle [16].

Problém je vizualizován na obr. 2[4)], kde klíčovou pozici v rámci KI zřetelně zaujímá dílčí struktura elektrické energie.



Obr. 2
Schéma pro posouzení vnitřní vzájemné závislosti dílčích struktur kritické infrastruktury; podle [10], [18], [25]

Poznámka k obr. 2:
Systém SCADA *(Supervisory Control And Data Acquisition)* vyjadřuje řízení a sběr dat, nejčastěji průmyslový řídící systém, počítačový systém sledování a kontrolu procesu.

Zdůrazňuje se [16], že identifikace vnitřní vzájemné závislosti dílčích infrastruktur u komplexních systémů je obtížná až nemožná. V odborné literatuře se uvádí klasický globální impakt z roku 1993, kdy požár chemické továrny Sumitomo Chemical Co. v Japonsku způsobil dlouhodobý celosvětový nedostatek počítačových čipů. Přitom produktem této výroby nebyly počítače nebo počítačové čipy, ale vysoce tvrzená epoxidová pryskyřice v objemu cca 60 % celosvětové produkce, používaná v počítačovém průmyslu. Obdobně [17] nacházíme pochybnosti o budoucích možnostech modelovat kategorii KI.

Potenciální impakt selhání *vnitřní vzájemné závislosti dílčích infrastruktur* je přirovnáván k triviální aplikaci efektu sněhové koule, tj. nabalování problémů, kdy se situace prudce zhoršuje (např. interakce energetické sítě se sítí telekomunikací, kdy výpadek dodávky elektrické energie následně po opravě neumožní oživit nefunkční síť telekomunikací). Pro hlubší analýzu se rozlišují čtyři kategorie různého typu *vnitřní vzájemné závislosti dílčích infrastruktur* [18], tj.

- fyzikální – vzájemná závislost na produktech a službách;
- kybernetická – viz systémy SCADA, PCS;
- geografická – společný průmět do území a tím zvýšené riziko selhání v důsledku jedné MU (např. společný koridor železnice, energovodu, vodovodního řadu apod.);
- logická – závislost stavu jedné infrastruktury na stavu druhé (např. závislost budoucnosti ropy na ceně zemního plynu a následně na změnách nově budované infrastruktury).

Uvedená základní bibliografická taxonomie je rozšířena [15] o další typy vztahů *vnitřní vzájemné závislosti dílčích infrastruktur*, tj. o interakci informativní, geoprostorovou, politicko-procedurální a společenskou. V práci je formalizován proces modelování *vnitřní vzájemné závislosti dílčích infrastruktur* a aplikována incidenční matice interakcí vč. tříbodové verbálně numerické stupnice. Akcent je kladen na dimenzi časoprostoru. Podrobně jsou diskutovány silné a slabé stránky metody HLA a DIS používané ministerstvem obrany USA pro modelování a simulaci bezpečnostních situací.

V dokumentu australské vlády [1] se zdůrazňuje charakteristika kritičnosti jako primárního kritéria bezvýhradně s nejvyšší prioritou posouzení. Program CIPMA představuje pomocný nástroj typu DSS s cílem poskytnout objektivní analýzu a model KI. Standardně jsou identifikovány vazby uvnitř sektoru a napříč sektory, chování komplexního systému (sítě), slabá místa a body možného selhání, pro zvládání MU jsou nutné scénáře a varianty. Základ tvoří dotazníkový protokol, obsahující sedm postupných kroků analýzy, hodnocení a závěrečné klasifikace kritičnosti.

Fenomén *vnitřní vzájemné závislosti dílčích infrastruktur* zvyšuje *riziko selhání*. V tomto směru se rozlišují tři hlavní kategorie selhání ve smyslu efektu *kaskády*, *eskalace* a *společné příčiny* na stejném místě a čase. Pojmy „*kumulativní a synergické účinky*“ jsou běžné v oblasti EIA/SEA; podle dokumentu SEVESO II[5)] byly pro oblast bezpečnostního rizika nahrazeny výrazem „*domino-efekt*“. Rozumí se tím situace, kdy událost u jednoho objektu/zařízení může být příčinou události u jiného objektu/zařízení, a tím může dojít ke zvýšení pravděpodobnosti vzniku závažné havárie a ke zvýšení jejích následků v důsledku umístění podniků nebo skupiny podniků a nebezpečných látek. Zpravidla je třeba zabránit vzniku domino efektu, k rozšíření havárie a dalšímu šíření destrukce (např. bezodkladná demolice narušených staveb, odstřel překážek při záplavách, odstraňování bahenních nánosů). „*Kaskádovitý efekt*“ selhání je situace, kdy porucha v jedné infrastruktuře způsobí poruchu ve druhé infrastruktuře. „*Eskalující efekt*“ selhání je situace, kdy porucha v jedné infrastruktuře nezávisle zhoršuje poruchu ve druhé infrastruktuře (tzn. čas na obnovu funkce a renovaci narůstá).

Rámec taxonomie vnitřních vzájemných závislostí komplexního systému infrastruktury zahrnuje šest hlavních „dimenzí“, cit. [17], [18]. Pro počáteční krok výzkumu se uvažují faktory ovlivňující proces analýzy vnitřní vzájemné závislosti KI a rámec následujících hledisek: typy vnitřních vzájemných závislostí; infrastrukturu prostředí; spojení a odezvu chování; charakteristiky infrastruktury; typy selhání; stav řízení. Faktory ovlivňující proces analýzy vnitřní vzájemné závislosti KI jsou uvedeny v tab. 2.

Tabulka 2
Faktory ovlivňující proces analýzy vnitřní vzájemné závislosti KI; podle [17]

Faktor	**Působící vlivy na proces analýzy**
Měřítko času	Dynamika vývoje infrastruktury se mění v obrovském rozpětí např. od milisekund až po desítky let (výstavba nových hlavních zařízení). Různé infrastruktury budou mít různá časová měřítka důležitosti.
Geografické měřítko	Specifické scénáře se mění v měřítku pro velikost obcí a měst, až po měřítko celostátní a mezinárodní. Měřítko ovlivňuje výsledek a množství požadovaných dat vzájemné závislosti infrastruktury pro modely.
Kaskádovitý efekt a efekty vyššího řádu	Porucha v jedné infrastruktuře způsobí poruchy v dalších infrastrukturách a vytvoří poruchy druhého a vyššího řádu.
Sociálně psychologické prvky	Infrastruktury představují sociálně-technické systémy. Sociální sítě a způsob odezvy může ovlivnit provoz infrastruktury, např. šíření infekce a odezvu v infrastruktuře veřejného zdravotnictví.
Provozní postupy	Specifické postupy společností ovlivňují stav infrastruktury např. odezvou a kolísáním tržního hospodářství.
Obchodní politika	Společné obchodní politiky ovlivňují provoz infrastruktur.
Procesy obnovy a rekonstrukce	Specifické postupy společností ovlivňují stav infrastruktury v průběhu krize a záchrany; mohou ovlivnit spolupráci mezi různými vlastníky infrastruktury. Procesy pro obnovu napříč infrastrukturou nemusí existovat.
Politický režim, legislativa, předpisy	Činnost vlády ovlivní provoz a chování jako odezvu na odvrácení následků mimořádné události a obnovu.
Zájmy zúčastněných subjektů	Motivace zúčastněných subjektů je diferencovaná, což ovlivňuje požadavky na analýzu vnitřní vzájemné závislosti infrastruktury.

Zranitelnost (*napadnutelnost*) KI představuje silně sofistikovaný problém s dosud otevřenou strategií, aplikaci teorie podmíněné pravděpodobnosti a konvoluce, podrobněji [22]. Hrozbu zranitelnosti KI členských zemí EU lze

dokumentovat na přírodní pohromě z roku 2002 (cyklón Ilse) a technické MU z roku 2006 (blackout).

- 12. srpna 2002 – cyklón způsobil záplavy v povodí Labe a Dunaje. V Německu, Rakousku a ČR povodně způsobily destrukci KI včetně dopravních sítí, vodních zdrojů, čistíren odpadních vod, energetických systémů apod. Např. v Rakousku bylo zničeno 250 silničních a železničních mostů.
- 4. listopad 2006 – náhlé přerušení VVN 380 kV v Německu způsobilo výpadek dodávky elektřiny na území Německa, Francie, Belgie, Holandska, Itálie, Rakouska, Švýcarska, Řecka, Maroka, Portugalska, Španělska a ČR po dobu 120 minut; postiženo bylo cca 15 mil. obyvatel.

Bezpečnostní riziko a očekávaný vývoj

Výsledky komparativních studií potvrzují existenci rozdílů mezi státy v definiční oblasti, interpretaci, ve způsobu měření kritičnosti [16]. Poznatky z práce [25] a diferencovaný přístup skandinávských zemí (Norsko, Švédsko, Finsko), které uplatňují širší pohled na kritičnost situace zároveň zpochybňují utilitární koncept EU k ECI. Namísto prostého výčtu KI a v porovnání s EPCIP se klade větší důraz na kritičnost důsledků selhání infrastruktury; řeší se „kritičnost společenských funkcí“ [16]. Pro občana je významná bezpečnost pro prosté přežití v místě své existence (bydliště, obec, region) se zvláštním zřetelem na vznik situace nejvyšší nouze a ostrovní způsob řízení krizové situace; podle švédského modelu má bezpečnostní problém obce prioritu před celostátním bezpečnostním problémem vlády [16]. V labyrintu rodící se terminologie bude účelné vzájemně diferencovat kritickou a krizovou infrastrukturu. *Krizová infrastruktura* zajišťuje základní, existenčně nezbytné důležité funkce systému v podmínkách krizové situace (tzn. kdy „téměř nic nefunguje“).

Lze očekávat, že stejným směrem se bude vyvíjet proces EIA/SEA. Rozvojové aktivity nových záměrů a aktivit musí být z hlediska bezpečnosti navrhovány v potřebném počtu reálných scénářů, posuzovány na podkladě axiomatické teorie kardinálního užitku MUT a hodnoceny metodou multikriteriální analýzy; pozice kritéria kritičnosti (bezpečnosti) musí mít v katalogu kritérií absolutní preferenci.

Závěry

Pro identifikaci a hodnocení objektů/subjektů KI je třeba ztrátu funkce, produktů, poskytovaných služeb atd., posuzovat zejména z hlediska *rozsahu, závažnosti* a *časové dimenze*. Uplatnění pomocných nástrojů umožňuje každé oblasti (regionu, kraje) a na úrovni státu rozhodnout, které objekty/subjekty musí bez výhrad patřit do kritické infrastruktury. Zvyšování bezpečnosti má vlastní ekonomický rozměr – jde o hledání virtuální rovnováhy mezi vynaloženými

prostředky na straně jedné a hodnotou chráněných zájmů společnosti na straně druhé. Kauza EPCIP je zpochybňována[6)] z mnoha důvodů s ohledem na rozdíly v národních modelech CIP z hlediska definice, interpretace, typologie, zásadní účinnosti a způsobu měření kritičnosti, s ohledem na nepřekonatelné heterogenní podmínky členských států, absenci národní strategie ochrany KI a nedostatky domácí kontroly, deformaci kompetencí a nepřijatelnou byrokracii EU, neujasněnou funkci mezinárodních organizací, nepřijatelné zvyšování preventivních aktivit na úkor smysluplné odolnosti systémů; EPCIP naráží na národní odpor, nesouhlas expertů s technickými návrhy řešení a především na hlavní čtyři argumenty, tj.: (1) ignorance dobrých národních zkušeností s odolností infrastruktury a tím málo zdůvodněný koncept prevence ve smyslu „worst-case scenario“, (2) větší část prvků KI (podle odhadu cca 85 %) je ve správě soukromého sektoru, (3) absurdita neobjasněné dělby kompetencí mezi členskými státy a EU, (4) nesprávný předpoklad, že mohutná KI je zároveň odolná a že nemůže být porušena. Za frustrující je pokládána skutečnost, že fenomén *vnitřní vzájemné závislosti dílčích infrastruktur* v evropském programu EPCIP není uvažován.

Zajištění bezpečnosti pro „*kritické (životně důležité) společenské funkce*“ infrastruktury představuje širší koncept ochrany KI a posun k holistickému vnímání. Pro další vývoj je třeba na národní úrovni uplatňovat principy subsidiarity, předběžné opatrnosti (tab. 3) a budování odolných systémů KI.

Tabulka 3
Objasnění pojmů pro oblast předběžné opatrnosti a včasného varování; podle [4]

Podmínky rozhodování za situace	**Charakteristika a dobový údaj o získání znalostí (úroveň poznání pro zvolený příklad)**	**Příklady vhodného opatření pro kauzu včasného varování**
A	**B**	**C**
→ rizika (*Risk*)	„známé“ impakty, „známá“ pravděpodobnost např. vliv asbestu na dýchací potíže; rakovina plic; od roku 1965	▶▶ **Předcházení události** (*Prevention*): omezit známé riziko, např. vyloučit expozici asbestovému prachu
→ nejistoty (*Uncertainty*)	„známé“ impakty, „neznámá“ pravděpodobnost např. antibiotika v potravě zvířat a spojená resistence člověka na tato antibiotika; od roku 1969	▶ **Bezpečnostní opatření** (*Precautionary prevention*): omezit potenciální nebezpečí, např. snížit či vyloučit expozici člověka antibiotikům v potravě zvířat

Tabulka 3 - pokračování

Podmínky rozhodování za situace	Charakteristika a dobový údaj o získání znalostí (úroveň poznání pro zvolený příklad)	Příklady vhodného opatření pro kauzu včasného varování
A	**B**	**C**
→ nevědomosti - neznalosti (*Ignorance*)	„neznámé“ impakty, „neznámá“ pravděpodobnost např. neočekávané/překvapující“ poškození ozonové vrstvy vlivem chlorofluorouhlovodíku - freonu (CFC); před rokem 1974	▷ **Opatrnost** (*Precaution*): očekávat, identifikovat a redukovat impakt z „překvapení“, např. uplatnit některé vlastnosti chemických látek (odolnost, bioakumulace) jako indície potenciální škody; využít co nejširší informace, monitoring, podpořit solidní, odlišné a adaptabilní technologie, aj.

POZNÁMKY:

[1)] ŘÍHA, J. (2001): *Posuzování vlivů na životní prostředí. Metody pro předběžnou rozhodovací analýzu EIA*. Vydavatelství ČVUT Praha, 477 stran. ISBN 80-01-02353-2.

[2)] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 *on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (Text with EEA relevance). In: Official Journal of the European Union L 345/75, 23.12.2008.

[3)] ROWE W. D. (1977): *An Anatomy of Risk.* John Wiley & Sons, N. York - London, ISBN 0471-01994-1.

[4)] Systém SCADA *(Supervisory Control And Data Acquisition)* vyjadřuje řízení a sběr dat, nejčastěji průmyslový řídící systém, počítačový systém sledování a kontrolu procesu.

[5)] SEVESO II představuje standardizované průmyslové bezpečnostní předpisy EU, tj. Směrnici Rady 96/82/EC s úpravami podle Směrnice Rady 2003/105/EC.

[6)] FRITZON, Å. et. al. (2007): *Protecting Europe's Critical Infrastructure: Problems and Prospects.* In: Contingency Today, 04 June 2007. Web:http://www.contingencytoday.com/online_article/Protecting%20Europe's%20Critical%20Infrastructure:%20Problems%20and%20Prospects/357.

Zkratky

BRS	BEZPEČNOSTNÍ RADA STÁTU
CEC	COMMISSION OF THE EUROPEAN COMMUNITIES
CEMAT	LA CONFÉRENCE EUROPÉENNE DES MINISTRES RESPONSABLES DE L'AMÉNAGEMENT DU TERRITOIRE
CI	CRITICAL INFRASTRUCTURE

CII	CRITICAL INFRASTRUCTURE INTERDEPENDENCIES
CIP	CRITICAL INFRASTRUCTURE PROTECTION
CIPMA	CRITICAL INFRASTRUCTURE PROTECTION MODELLING AND ANALYSIS PROGRAM
CIWIN	CRITICAL INFRASTRUCTURE WARNING INFORMATION NETWORK
DIS	DISTRIBUTED INTERACTIVE SIMULATION
DSS	DECISION SUPPORT SYSTEMS
ECI	EUROPEAN CRITICAL INFRASTRUCTURE
EIA	ENVIRONMENTAL IMPACT ANALYSIS/ASSESSMENT
EPCIP	THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION
GIS	GROGRAPHIC INFORMATION SYSTEMS
HLA	HIGH LEVEL ARCHITECTURE
IARDSTICK	INFRASTRUCTURE ASSURANCE READINESS DECISION STICK
KI	KRITICKÁ INFRASTRUKTURA
LCCI.	LARGE COMPLEX CRITICAL INFRASTRUCTURES
MU	MIMOŘÁDNÁ UDÁLOST
MUT	MULTIATRIBUTE UTILITY THEORY
NATO	NORTH ATLANTIC TREATY ORGANISATION
OMN	OBJEKT MOŽNÉHO NAPADENÍ
PCS	PROCESS CONTROL SYSTÉM
SCADA	SUPERVISORY CONTROL AND DATA ACQUISITION
SEA	STRATEGIC ENVIRONMENTAL ASSESSMENT
SOS	SYSTEM OF SYSTEMS
TRS	TOTAL RISK SCORE
TUKP	TOTÁLNÍ UKAZATEL KVALITY PROSTŘEDÍ
UFC	UNIFIED FACILITIES CRITERIA
VVN	VELMI VYSOKÉ NAPĚTÍ
ŽPČ	ŽIVOTNÍ PROSTŘEDÍ ČLOVĚKA

Résumé

The objective of this paper is to identify links which are important from the Critical Infrastructure vulnerability point of view. There are briefly described and compared different procedures for the identification and designation of Critical Infrastructures and the assessment of the need to improve their protection.

„Critical Infrastructure[1)] means an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions".

Critical infrastructure is currently looking for its contents, structure, purpose, and political context. Suitable criteria for its identification and the assessment of potential risks are looked for and some of the first attempts of simulation and the creation of a model for a "System of Systems" are appearing.

Developing an awareness of the challenges entailed in the protection of Critical Infrastructures is an important first step. Before one can take effective measures to improve the protection of Critical Infrastructures, it is necessary to understand how these function and to identify and analyse the critical processes within the Critical Infrastructures. Analyses aimed at identifying the probabilities of failure and their possible consequences and damaging effects typically fall into the specialist area of risk analysis and risk management. There are many different methods of conducting a risk analysis. Frequently these entail a very similar structure under which objects, threats, vulnerabilities and probabilities are catalogued and links between them are defined. The outcomes of such methodologies are quantifications of the losses that may be expected or categories of risks. However, these methods are not sufficiently focused to be helpful with regard to the analysis of Critical Infrastructures.

In order to facilitate improvements in the protection of Critical Infrastructures, common methodologies may be developed for the identification and classification of risks, threats and vulnerabilities to infrastructure assets. The practicism of the crisis management is being moved into the sphere of the "science of safety". These efforts are closely observed, with the actual situation considered as an unfinished and open strategy of safety risk.

Literatura

[1] AGD. *Critical Infrastructure Protection Modelling and Analysis Program, Tasking and Dissemination Protocols.* Australian Government, Attorney-General's Department, October 2007. Dostupný z WWW: <www.ag.gov.au>.

[2] CEC. *Green Paper on a European Programme for Critical Infrastructure Protection.* Brussels: Commission of the European Communities, 17.11.2005. COM(2005) 576 final.

[3] EC. *The European Programme for Critical Infrastructure Protection (EPCIP)*. MEMO/06/477. Brussels: European Commission, 12 December 2006.

[4] EEA. *Late lessons from early warnings: the Precautionary Principle 1896-2000*. [Environmental issue report No 22]. Copenhagen: European Environmental Agency, 2001.

[5] EGAN, M. J. Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Contingencies and Crisis Management*, Volume 15, Number 1, March 2007, p. 4-17.

[6] EK. *Návrh Směrnice Rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu*. Brusel: KOMISE EVROPSKÝCH SPOLEČENSTVÍ, 12.12.2006.

[7] EPIC. *The USA Patriot Act.* [Public Law 107-56, October 26, 2001]. Electronic Privacy Information Centre, 2005. Dostupný z WWW: <http://www.epic.org/privacy/ terrorism/usapatriot/>.
[8] EU Council. *Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*. 5051/2/08 REV 2. Brussels, 19 February 2008.
[9] EU Council - Justice and Home Affairs Council. *European Critical Infrastructure*. Factsheet. Luxembourg, 5 June 2008.
[10] HARDENBROOK, B. *Critical Infrastructure Interdependencies and Regional Public–Private Partnerships*. Pacific NorthWest Economic Region (PNWER), 2006. Dostupný z WWW: <www.pnwer.org>.
[11] KRULÍK, O. *Zpráva Komise Kongresu o teroristických útocích z 11. září 2001*. [Překlad "9/11 Report"]. MV ČR, 2002. Dostupný z WWW: <http://news.findlaw.com/ wp/docs/911rpt/index.html>.
[12] MARTÍNEK, B. Východiska a principy zajištění ochrany KI v ČR. In *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva*, roč. VII, č. 4, s. 22-24. ISSN 1213-7057. 2008.
[13] MO ČR. *Směrnice k výběru objektů obranné infrastruktury a zpracování dokumentace.* 1. aktualizované vydání, schválené usnesením vlády č. 1436 ze dne 19. prosince 2007.
[14] MOTEFF, J. a PARFOMAK, P. *Critical Infrastructure and Key Assets: Definition and Identification.* [CRS Report for Congress. Congressional Research Service, Resources, Science, and Industry Division]. October 1, 2004.
[15] PEDERSON, P. et al. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research.* Idaho: Idaho National Laboratory, Critical Infrastructure Protection Division, Idaho Falls, August 2006.
[16] PURSIAINEN, Ch., ed. *Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection.* [Nordregio Report 2007:5]. Stockholm, 2007.
[17] RINALDI, S.M. Modeling and Simulating Critical Infrastructures and Their Interdependencies. In *Proceedings of the 37th Hawaii International Conference on System Sciences*. Sandia: Sandia National Laboratories, 2004.
[18] RINALDI, S.M., PEERENBOOM, J.P. a KELLY, T.K. Critical infrastructure interdependencies. (Identifying, Understanding, and Analyzing). *IEEE Control Systems Magazine*, vol. 21, December 2001, p.12-25.
[19] ŘÍHA, J. Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj*, roč. X, č. 4, s. 44–51. ISSN 1212-0855. 2007.
[20] ŘÍHA, J. Odhad rizika teroristického činu. *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva*, roč. VII, č. 3, s. 22-26. ISSN 1213-7057.
[21] ŘÍHA, J. Osudová vize 2050 - představa neuvěřitelného. *Vojenské rozhledy*, roč. 17 (49), č. 3, s. 3-10. ISSN 1210-3292.
[22] ŘÍHA, J. Zranitelnost infrastruktury a systémů životního prostředí. *SPEKTRUM 2008*, roč. 8, č. 1. ISSN 1211-6920.

[23] SAK, P. Bezpečnostní věda - důsledek vývoje civilizace. *Britské listy*, 12.11.2004. ISSN 1213-1792.
[24] SANTOS, J.R. a HAIMES, Y.Y. *Impact Assessment of Major Economic Disruptions using the Inoperability Input-Output Model (IIM).* Charlottesville: Center for Risk Management of Engineering Systems University of Virginia, 2005.
[25] SCHMITZ, W. Modelling and Simulation for Analysis of Critical Infrastructures. In STEIN, W. et al. *Critical Infrastructure Protection (CIP) - Status and Perspectives*. Preprints of the First GI Workshop on CIP. Frankfurt a. M.: Johann Wolfgang Goethe-Universität, 2003, p. 73-84.
[26] STŘEDA, L. a MATOUŠEK, J. Globální úsilí v boji proti terorismu – aktuální výzva současnosti. In *Sborník Mezinárodní konference medicíny katastrof*. Zlín 24.-26.06.2002.
[27] SVENDSEN, N.K. and WOLTHUSEN, S.D. *Connectivity models of interdependency in mixed-type critical infrastructure network.* [Information Security Technical Report 12 (2007) 44 – 55]. Elsevier, 12 March 2007.
[28] TUZAR, A. *Teoretické aspekty zkoumání mimořádných událostí*. Pardubice: Dopravní fakulta Jana Pernera, Univerzita Pardubice, 16.02.2000.
[29] US DHS. *National Strategy to Secure Cyberspace*. Washington D.C.: U.S. Department of Homeland Security, The White House, February 2003. 76 p.
[30] US DHS. *The National Strategy for Physical Protection of Critical Infrastructures and Key Assets.* Washington D.C.: U.S. Department of Homeland Security, The White House, February 2003. 96 p.
[31] US DHS. *Vulnerability Assessment Methodologies Report.* Washington D.C.: US Department of Homeland Security, The White House, July 2003.
[32] Vláda ČR. *Národní program ochrany kritické infrastruktury.* Usn. vlády ČR č. 170 ze dne 25. února 2008.
[33] Vláda ČR. *Oblasti kritické infrastruktury v ČR*. Usn. vlády ČR č. 1436 ze dne 19. prosince 2007 (usnesení BRS ze dne 3. července 2007 č. 30).
[34] Vláda SR. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany*. Usn. vlády SR, 2006. Dostupný z WWW: <http://www.economy.gov.sk/pk/2130-2006-1000/ma.htm>.
[35] ZETA Group. *CritiCalc*. Ottawa: The ZETA Group Inc., ON, Canada, 2008. Dostupný z WWW: <http://www.zetagroup.ca/PDF/criticalc-brochure.pdf>.