KRITICKÁ INFRASTRUKTURA A RIZIKO MIMOŘÁDNÉ UDÁLOSTI

Josef Říha

Kritická infrastruktura v současné době hledá svůj věcný obsah, strukturu, bezpečnostní význam a politické souvislosti. Hledají se vhodná kritéria pro její identifikaci a posouzení potenciálního rizika; objevují se první pokusy o simulaci a vytvoření modelu pro „systém systémů". Prakticismus krizového managementu se posunuje do sféry „bezpečnostní vědy". Tomuto úsilí je věnována mimořádná pozornost a současný stav lze pokládat za nedokončenou, otevřenou strategii bezpečnostního rizika.

Úvod

Kritická infrastruktura KI *(Critical Infrastructure)* jsou fyzické, kybernetické a organizační (obslužné) systémy, které jsou nutné pro zajištění ochrany životů a zdraví lidí a majetku, minimálního chodu ekonomiky a správy státu. Sleduje se citlivost a potenciální zranitelnost komplexních systémů.

Otázky ochrany kritické (původně životní) infrastruktury eskalují po událostech 11. září 2001, nabývají nový obsah a rozměr; v USA se formují první sofistikovaná opatření. Motivací je vznik *superterorismu* jako nového rozměru terorismu na pozadí „střetu civilizací" [11]. Terorismus, ať již s použitím konvenčních[1)] nebo nekonvenčních zbraní, se stal aktuální ústřední výzvou pro celosvětové společenství. Ultraterorismus [27] lze chápat jako 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 vedené jednotlivci, nestátními skupinami nebo státem podporovanými aktéry proti konkrétní sociální skupině k vyvolání strachu nebo teroru.

Dynamický vývoj za časové období 1983 až 2003 dokládá vyčerpávající zpráva z vědecko-výzkumného kongresového centra USA pod názvem „*Kritická infrastruktura a klíčové objekty: Definice a identifikace*" [17]. V rámci členských zemí EU byl rozvinut „*Evropský program na ochranu KI*" EPCIP [6]. Současně lze pozorovat rozvoj příbuzných disciplín ve prospěch objektivizace a zlepšení rozhodovacích procesů na pozadí kategorie DSS[2)]; 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 kumulativní a synergické pojetí mimořádných událostí a aplikaci náročné teorie katastrof [31]. Vytváří se základy trans-, pluri-, inter-, multi-disciplinární „bezpečnostní vědy" [24], toho času těžko uchopitelné.

Relevantní je změna myšlení a postojů – lidstvo se v posledních letech transformovalo na *společnost rizika* a jeho mentalita se podstatně změnila. Negativní zkušenosti s haváriemi jaderných reaktorů, chemických provozů a četné přírodní pohromy nadále zvyšují nedůvěru ve vědecké poznatky a dobrozdání expertů. Omylnost vědy potvrzují kontroverzní názory vědců na rizikové otázky, kde je snaha uplatňovat (nevědecký) princip PP. Navíc přestává platit dříve uznávaný postulát, že věda je neutrální a technologie je schopna vyřešit jakýkoliv problém. Vytváří se situace, kdy lidstvo má strach z důsledků změn, které nekontroluje a kde v rozhodovacím procesu převládá faktor rizika. Jde o situaci, v níž „lidé přestávají věřit v božstva technicko-ekonomických zázraků", cit. O. Suša [28]. *Společnost rizika* je charakterizována řadou klíčových faktorů v přímé souvislosti s hlavními *rysy postmoderní společnosti*. Glosovaně to je:

- rostoucí individualismus;
- jazyk vědy a techniky vylučuje účast veřejnosti a další podporu možného rozhodování;
- roste závislost na vědě a technice, což prezentují rizika životního prostředí, které jednotlivec nemůže řídit;
- globální rizika životního prostředí nerespektují individuální majetek;
- vědecké poznatky rizika životního prostředí se mění s „bezpečnou" úrovní expozice množství chemických látek a emisí;
- stát není schopen garantovat bezpečnost;
- vědecká predikce a názory expertů jsou chybné.

Za zcela nový fenomén lze pokládat posuzování odolnosti komplexních systémů, které jsou daleko od stability (*Systems Far From Equilibrium*). Jestliže pro systém v dynamické rovnováze je cílem výchylku vrátit do původního rovnovážného stavu (viz představa homeostáze), pak tento požadavek pro případ soustavy v silně nerovnovážném stavu je nelogický. Řešení spočívá v zajištění pružnosti

1) Je třeba vzít v úvahu údery konvenční výzbrojí na infrastruktury civilizované společnosti, tj. na energetická, chemická, jaderná a jiná zařízení. Tyto jevy se sice značně podobají mírovým haváriím, ale vzhledem ke spouštěcímu mechanismu se od nich liší rozsahem a rychlostí nástupu ničivých faktorů. Do této skupiny lze fakticky zařadit i hrůzný scénář z 11. září 2001. Záměrná havárie dvou Boeingů 767 a jednoho Boeingu 757 se sebevražedným navedením na dvojici věží Světového obchodního centra v New Yorku a budovu Pentagonu ve Washingtonu měla charakter koncového navedení řízených střel s obrovskou destrukční silou vzhledem ke kombinaci kinetické energie letících těles a tepelné energie hořícího leteckého paliva.

2) DSS – Decision Support Systems (formalizované podpůrné systémy pro rozhodovací proces).

Kategorie indikátorů	Příklad indikátoru
Vzájemných vztahů	Systemická schopnost aktivovat latentní fórum pro proces rozhodování, výměnu znalostí apod.
Procesní	Synergický efekt, který se objevuje v důsledku interakcí nebo na styčných plochách mnoha hledisek. Stupeň otevřenosti institucionálních struktur.
Relativní	Měření míry pružnosti (plasticity) namísto tradiční stability.
Trendové	Stabilita v oblasti periodicity. Směr vývoje.

Tab. 1: Indikátory odolnosti pro systémy v silně nerovnovážném stavu; podle [19]

z hlediska funkce systému, struktury, procesů. Důraz je kladen na možnost volby, generování scénářů, omezení míry nejistoty. Uvádí se význam indikátorů odolnosti. V tabulce 1 jsou uvedeny příklady indikátorů odolnosti pro systémy v silně nerovnovážném stavu. V té souvislosti N. Powell [19] zdůrazňuje, že nastala doba pro „zásadní konceptuální přehodnocení odolnosti", které je prováděno ve smyslu posuzování impaktu IA (*Impact Assessment*). V teoretické oblasti [9], [12], [14], [15], [21], [22], [25] půjde o řešení vnitřních vzájemných závislostí (*Input-Output Model for Interdependent Infrastructure*) a o zvýšenou bezpečnost KI v podobě konceptu SoS (*System of Systems*); nicméně v řadách expertů existují pochybnosti [21] o budoucích možnostech modelovat kategorii KI.

Kritická infrastruktura – kritéria

Všeobecný konsenzus o strategickém významu KI diktuje potřebu jednoznačně definovat tuto kategorii v mezinárodním měřítku. Hlubší analýza dostupných dokumentů umožňuje diferencovat aktuální koncept vnímání KI na národní úrovni, na úrovni EU a NATO a na federální úrovni USA. Z hlediska systémového přístupu je kategorie KI vnímána jako „systém systémů". Definice KI v pojetí domácích aktérů tvoří obsah Bezpečnostní strategie ČR, která byla schválena vládou dne 10. prosince 2003: Kritickou infrastrukturou se rozumí *„výrobní i nevýrobní systémy, jejichž nefunkčnost by měla vážné dopady na bezpečnost, ekonomiku a zachování nezbytného rozsahu dalších základních funkcí státu při krizových situacích"* [13]. Definice 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*" [4]. 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 jako členský stát EU má dále koncept *Evropské kritické infrastruktury* ECI (*European Critical Infrastructure*), 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*" [4].

Další úhel pohledu na řešení této problematiky, který má přímý vliv na ČR jako členský stát 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 nejkritičtější z uvedených schopností patří hromadná evakuace a informování, varování a vyrozumění veřejnosti.

V pojetí dokumentů USA představují KI *„systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro USA a zneschopnění nebo zničení takových systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečí, nebo na jakoukoliv jejich kombinaci*"; podle „Patriot Act"[3] viz [8], [30], [32], [33]. Američané přitom důsledně rozlišují dva pojmy „critical infrastructure" (kritická infrastruktura) a „key asset" (klíčová aktiva). Klíčovými aktivy se zde rozumí samostatná zařízení, jejichž vyřazení sice neohrozí národní ekonomiku, ale může být náročné z hlediska škod, ztrát na životech nebo podkopání sebevědomí. Do této kategorie se řadí jaderné elektrárny, stadiony, národní památky, pomníky apod.

V tabulce 2 jsou vysvětleny důvody, které v průběhu času obecně generují kritickou infrastrukturu z hlediska

3) Patriot Act – tzv. protiteroristický zákon v USA.

životně důležitých funkcí pro společnost [16].

K upřesnění obsahu má přispět spolupráce expertních týmů členských států EU; aktuální je dokument „*Green Paper*“ (Zelená kniha), prezentovaný Evropskou komisí 17. 11. 2005 jako výzva členským státům podílet se na vytvoření účinné evropské ochrany KI [4] a „*Evropský program na ochranu KI*“ EPCIP (*The European Programme for Critical Infrastructure Protection*) [6]. Výsledná zpráva z roku 2007 obsahující katalog kritérií však zůstane pro veřejnost nepřístupná [7].

V ČR je akceptováno (rozhodnutí VCNP 24.09.2002) pojímat zaměření *národní kritické infrastruktury* na následujících devět oblastí:

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

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, jakými jsou telekomunikace, počítačové systémy a jejich programové vybavení, internet, přenosové sítě, poskytované služby atd.

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 či nouzové situace (tzn. kdy „téměř nic nefunguje“).

Předmětem odborného zájmu je *stanovení kritérií*, na základě kterých lze rozhodovat, které prvky nebo subjekty lze zařadit do KI (porovnej s tab. 2). *Kritéria výběru* by měla být založena na odborných poznatcích s přihlédnutím k rozsahu, závažnosti a časovému faktoru.

Pro určení subjektů kritické infrastruktury 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 hod., 48 hod., za týden, později).

Na základě uvedených kritérií je možné v každé oblasti a na úrovni státu stanovit, které subjekty budou patřit mezi kritickou infrastrukturu.

Názorný demo-příklad nabízí koncept posuzování KI ve SR z roku 2006, viz [1]. Prvek národní infrastruktury může být zařazen jako prvek KI tehdy, když je důležitý pro některou oblast

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				✦

Tab. 2: Důvody, které v průběhu času obecně generují kritickou infrastrukturu z hlediska životně důležitých funkcí pro společnost; podle [16]

bezpečnosti státu a zároveň splňuje 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 to 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.

Další etapou zvýšení bezpečnosti je *řízení rizika* (management rizika). Uplatněním postupů řízení rizika lze zaměřit pozornost na oblasti odhadnutého největšího rizika, ale je nutné vzít v úvahu i konkrétní hrozbu, stávající úroveň bezpečnostní ochrany a účinnost přijímaných opatření pro zajištění kontinuity fungování celého systému.

„Systém systémů“ a mimořádná událost

Ochrana KI musí být zajištěna pomocí opatření *preventivních, zmírňujících, připravenosti složek, zdrojů, zařízení a pomůcek na zvládnutí dopadů pohrom a hlavně cílených útoků na kritickou infrastrukturu, schopností zvládnout kritické situace a zajistit rychlou obnovu.*

Na každý systém a jeho evoluční vývoj působí okolí systému. Tento systém vnější podněty buď absorbuje nebo neabsorbuje, buď vznikne nová struktura nebo původní systém zaniká [31]. Ve druhém případě jde o zápornou mimořádnou událost, která neočekávaně naruší svojí intenzitou objekt svého působení do té míry, že ho destruuje do nefunkceschopné podoby nebo ho úplně rozloží. Dochází ke zkáze energetických, materiálových a informačních toků a sítí, k ničení společenské a technické infrastruktury, technologických celků, dopravních prostředků a komunikací, k poškození až kritickému zhoršení životních podmínek pro stávající formy botanického a zoologického původu.

Koncepce zabezpečení ochrany KI vychází z faktu, že každý systém se skládá z prvků, vazeb a toků, z nichž některé tvoří kritická místa, která způsobují, že systém neplní funkci, ke které je určen a nebo k tomu významně přispívají. Subjekty KI jsou navzájem propojené a jsou na sobě závislé. V důsledku tohoto uspořádání navzájem závislých infrastruktur může docházet k řetězovému hromadění problémů, které mohou způsobovat neočekávané a stále vážnější selhávání nezbytných služeb v případě velkých nehod způsobených teroristickým útokem. Jinými slovy následkem uvedené vzájemné závislosti CII jsou tyto infrastruktury výrazně zranitelné a citlivé k narušení nebo zničení. Uvedená vlastnost vede experty k označení kategorie KI jako „systém systémů“ [21], [25].

Podle obecné uzance je *mimořádnou událostí* MU (*Extraordinary*

Impaktový faktor	VÁŽNÝ–KRITICKÝ	VYSOKÝ	PRŮMĚRNÝ	SLABÝ
Skóre	**= 15**	**= 5**	**= 3**	**= 1**
Hustota obyvatelstva; potenciální dopad	Nad 10 tis. obyvatel	1 až 10 tis. obyvatel	100 až 1000 obyvatel	Méně než 100 obyvatel
Ekonomický impakt; přímé náklady na obnovu	$> 1.10^9$ $	100.10^6 až 1.10^9 $	10.10^6 až 100.10^6 $	$< 10.10^6$ $
Dopad na sektor KI s možností zhroucení	v rozsahu mezinárodním	v rozsahu národním	v rozsahu regionálním	na místní úrovni
Dopad na vnitřní závislost dílčích systémů KI	oslabení jiných sektorů	významný impakt nebo narušení jiných sektorů	úprava impaktu na důležité poslání jiných sektorů	slabý impakt na důležité poslání jiných sektorů
Impakt na služby; očekávaný bezprostřední dopad	vysoké náklady napříč resorty, dlouhý čas obnovy nad 1 rok	vysoké náklady, čas obnovy několik měsíců až rok	průměrné náklady, čas obnovy několik dnů až týdnů	nízké náklady, čas obnovy několik hodin až dnů
Ovlivnění důvěry veřejnosti	vysoké riziko na národní úrovni a pochybnosti o možnostech kontroly	veřejnost vnímá vysoké národní riziko a nízkou schopnost kontroly	veřejnost vnímá průměrné riziko a průměrnou schopnost kontroly	veřejnost vnímá slabé riziko a vysokou schopnost kontroly

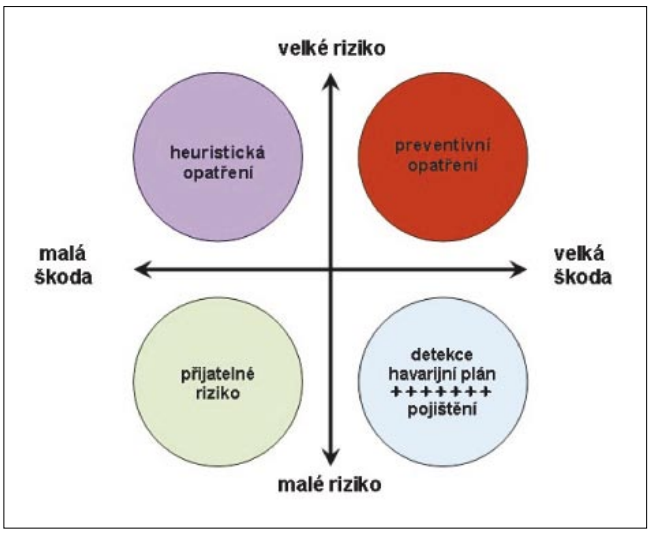
Tab. 3: Screeningový model pro posouzení priority dopadů na KI; podle [20]

Event) každá událost, která překonává určitou limitu (mez) normálního průběhu dějů a procesu (obecně je přijímána limita 3–5 % u technologických a ekonomických systémů z plánované kodifikované či schválené sledované hodnoty systému ve směru kladném i záporném), cit. I. Veverka [34]. V kontextu KI (a podle domácí legislativy) je MU „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". Věcný obsah tohoto výkladu fatálně zaostává za potřebami praxe. Podle [18] např. nezahrnuje dlouhodobý výpadek elektrického proudu, selhání dodávek pitné vody, nedostatek nezbytných surovin (ropa), dlouhodobé selhání komunikačního spojení, které mohou představovat významné pohromy pro lidskou společnost. Proto v souladu s EU a s dalšími vyspělými zeměmi je vhodné používat v odborných analýzách pojem „nouzová situace" (*Emergency Situation*) a pro potřeby analýz je dělit do podrobnějších kategorií.

V tabulce 3 je uveden screeningový model KI pro posouzení priority dopadů pro relevantní impaktové faktory a čtyřstupňovou verbálně numerickou stupnici (skóre 15; 5; 3; 1) podle úředních dokumentů používaných v Kanadě [20]. Zjišťuje se hodnota celkového skóre pro každý scénář a jejich hierarchizace podle zásady „*čím menší →→ tím lepší*". K dobrému pochopení obsahu tabulky je třeba studovat doplňující komentář.

Zájemce o hlubší poznání se odkazuje na obsáhlou tabulku v dokumentu [5], kde jsou rizikové faktory pro každý systém (projekt, záměr) identifikovány z hlediska jejich potenciálně negativního impaktu s vyjádřením míry integrované bezpečnosti a přijímaného rizika, tj. podle členění na riziko velké, průměrné a malé; nepatřičné faktory jsou opomenuty (tzn. pro určitý případ nevhodné faktory nejsou aplikovány).

Bezpečnost je bytostně spojena s hrozbami a jejich riziky. Bezpečnost (ve smyslu *safety* a s přihlédnutím k OECD) podle [26] je praktická (skutečná) jistota, že nenastanou nežádoucí účinky (jevy) následkem působení nějakého činitele (např. nebezpečná chemická látka nebo přípravek, fyzikální externí jevy aj.) za určitých okolností. Bezpečnost podle [10] (ve smyslu *security*) v jakémkoliv budoucím období můžeme hodnotit jako postačující nebo zachovanou, nepřesáhnou-li v novém časovém horizontu hrozby a jejich rizika únosnou míru. Tato míra je zpravidla vyjádřena formulováním *chráněných hodnot*, jejichž ztráta nebo narušení je považována za nepřípustnou. I tato míra se může s časem měnit. *Hrozby* (*threat*) mají v sobě náboj potenciální možnosti vzniku. Tedy mohou, ale nemusejí se projevit. *Riziko* (*risk*) představuje kvantifikaci pravděpodobnosti výskytu hrozby. *Ohrožení* (*hazard*) představuje naplnění charakteristik hrozby do krizového stavu, kdy skupina států, stát nebo obec přijímají ochranná opatření proti uskutečnění nebo pro zmírnění hrozby (např. vyhlášení prvého stupně povodňového ohrožení).



Obr. 1: Rozhodovací prostor pro volbu typu opatření na základě vyhodnocení velikosti rizika a očekávaného důsledku

Na obrázku 1 je uvedeno elementární schéma pro volbu typu opatření na základě vyhodnocení dvou parametrů, tj. velikosti rizika a očekávaného důsledku.

Výraz *riziko* je konvolucí, tj. spřažením *nebezpečí*, *zranitelnosti* a *expozice*, tj. doby, po kterou nebezpečí působilo. U přírodních nebezpečí lze riziko snížit, nelze však snížit nebezpečí. Lze rozlišovat významové odstíny pojmu riziko (s přihlédnutím ke stávající praxi) jako *globální riziko* možné negace antropocentrického zájmu, jako *riziko-in* (skutečné riziko), tzn. stav či proces časoprostorového úseku vývoje systému včetně dalších souvislostí šíření destruktivních projevů v pojetí kumulativního a synergického efektu[4] a konečně jako *konkrétní riziko* v běžném jazyce pro konkrétní čas a prostor za zcela zřejmých předmětných souvislostí, při nichž může v nedaleké budoucnosti dojít ke škodě, ztrátě, postižení, zranění či úmrtí.

Nicméně v běžné praxi je riziko obecně definováno jako součin pravděpodobnosti a důsledku nežádoucí události, např. úrazu, poškození životního prostředí nebo ekonomické ztráty [23]. Obvykle je popsáno spojitou nebo přetržitou veličinou, která může nabývat různých hodnot. Cílem rizikového inženýrství je jeho *odhad*, jehož předpokladem je *identifikace nebezpečí*, formulace *scénáře nebezpečí* a *kvantifikace rizika*. Jde o tři operace, které poskytnou odpověď na tři otázky:

- identifikace nebezpečí → *jaké nepříznivé události mohou nastat?*
- scénář nebezpečí → *jaká je pravděpodobnost výskytu takových událostí?*
- kvantifikace rizika → *pokud některá nepříznivá událost nastane, jaké to bude mít následky?*

4) Pojmy „*kumulativní a synergické účinky*" jsou běžné v oblasti EIA/SEA; podle dokumentu SEVESO II byly pro oblast bezpečnostního rizika nahrazeny výrazem „*domino-efekt*" (*Domino Effect*).

Závěry

Hrozba superterorismu a možnost střetu civilizací akceleruje rozvoj bezpečnostní vědy. Priorita pozornosti je přisouzena kritické infrastruktuře. Možnosti racionálního řešení komplikují postoje postmoderní společnosti[5].

Bezpečnostní riziko lze chápat jako pravděpodobnou, více či méně reálnou hrozbu, že bude ohrožena integrita určitého subjektu (jedince nebo společenského útvaru jako celku) kriminálním činem nebo jemu se blížícími důsledky činnosti jiných lidí. Nezahrnuje jenom objektivní možnost výskytu určité události (ohrožující osobu, zdraví, majetek, atd.), nýbrž také subjektivně vnímanou pravděpodobnost, která spoluurčuje definici situace a chování aktéra v ní. V tomto směru dochází ke spojení racionálního kalkulu s vyhodnocením významu možných důsledků ve vazbě na aktivní chování. Riziko jako komplexně (kognitivně, emočně i volně) pojímaná struktura aktivuje seberegulační mechanismy, směřující k obnovení rovnováhy, a to formou jak preventivních, tak reparačních kroků. Bezpečnostní rizika působí z dlouhodobého hlediska spíše erozivně, často neaditivně kumulují jednotlivé efekty, zároveň se prosazují selektivně, ve vazbě na sociální diferenciaci společnosti. Vedle ztrát na životech jsou ve hře i matoucí konotace politické (nedůvěra vládě), hospodářské (ochromení ekonomiky) a psychologické (šok, panika).

Pro českou veřejnou správu představuje největší přínos aplikace takových formalizovaných metod, které umožňují volbu, generování a vyhodnocování scénářů pomocí multikriteriální rizikové analýzy a současně omezují míru nejistoty. Tento koncept by měl tvořit zásadní požadavek z důvodu bezpečnostního rizika [21], [35]. Bez skrupulí musí být ke spolupráci přizván soukromý sektor (v duchu *Regional Public-Private Partneships*).

Nicméně budoucnost významně zarámují uznávané priority hédonisticky orientované liberální společnosti.

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

Použité zkratky:

CII – Critical Infrastructure Interdependencies – vnitřní vzájemná závislost kritické infrastruktury

CIS – Computing & Information Services – výpočetní a informační služba

EC – European Community – Evropské společenství

ECI – European Critical Infrastructure – evropská kritická infrastruktura

EEA – European Environmental Agency – Evropská agentura pro životní prostředí

EIA – Environmental Impact Analysis/Assessment – posuzování vlivů na životní prostředí

EPCIP – The European Programme for Critical Infrastructure Protection – Evropský program na ochranu kritické infrastruktury

EU – Evropská unie

IA – Impact Assessment – posuzování vlivu

KI – kritická infrastruktura

MU – mimořádná událost

MUT – Multiatribute Utility Theory – axiomatická teorie kardinálního užitku

NATO – North Atlantic Treaty Organisation – Severoatlantický pakt

OECD – Organization for Economic Cooperation and Development – Organizace pro hospodářskou spolupráci a rozvoj

PHA – Preliminary Hazard Analysis; Process Hazard Analysis – předběžné posouzení nebezpečí

PP – Precaution Principle – princip předběžné opatrnosti

ROP – regionální operační program

SEA – Strategic Environmental Assessment – strategické posuzování vlivu na životní prostředí

SoS – System of Systems – systém systémů

VCNP – Výbor pro civilní nouzové plánování

VVN – velmi vysoké napětí

ŽP– životní prostředí

Použité zdroje:

[1] *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany.* Usn. vlády SR, 2006. Web: <http://www.economy.gov.sk/pk/2130-2006-1000/ma.htm>.

[2] BABINEC, F. *Management rizika.* Slezská Univerzita v Opavě. 95 stran. Web: <www.math.slu.cz/studmat/AnalyzaRizik/AnalyzaRizik-1.pdf>.

[3] BIRKMANN, J. – WISNER, B. *Measuring the Un-Measurable. The Challenge of Vulnerability.* Studies Of the University: Research, Counsel, Education. Publ. Ser. of UNU-EHS, No.5/2006. Web: <http://www.ehs.unu.edu/file.php?id=212>.

[4] *Green Paper on a European Programme for Critical Infrastructure Protection.* COMMISSION OF THE EUROPEAN COMMUNITIES. Brussels, 17.11.2005. COM(2005) 576 final. Web: <http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf>. V českém znění bez příloh je dostupné na: Web: <http://europa.eu.int/eur-lex/lex/staging/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:CS:DOC>.

[5] *Risk Analysis Matrix.* Computing & Information Services, 3.4.2003. Web: <http://cis.tamu.edu/ca/custapps/RiskMatrix.php>.

[6] *The European Programme for Critical Infrastructure Protection (EPCIP).* MEMO/06/477. European Commission, Brussels, 12 December 2006. Web: <www.europa.eu/.../06/477&format=HTML&aged=0&language=EN&guiLanguage=en>.

[7] *Commission takes first step towards improving Critical Infrastructure Protection.* IP/07/133. European Commission, Brussels, 2nd February 2007. Web: <http://ec.europa.eu/dgs/energy_transport/security/infrastructure/index_en.htm>.

5) Neschopnost byrokracie a absenci myšlení v souvislostech si autor ověřil v rámci kauzy SEA ROP v průběhu roku 2006. Např. nadšeně propagované cyklostezky financované ze strukturálních fondů EU umožňují razantní přístup (a únik) teroristům ke klíčovému křížení s energetickými liniemi VVN. Koordinovaný útok pouze na několika málo místech může způsobit „black-out“ v celostátním měřítku s kaskádovitým a zdrcujícím efektem druhotných a časově odložených impaktů.

[8] *The USA Patriot Act.* (Public Law 107-56, October 26, 2001). Electronic Privacy Information Centre. Web: <http://www.epic.org/privacy/terrorism/usapatriot/>.

[9] HAIMES, Y. Y. *Risk-Based Framework for Modeling Infrastructure Interdependencies.* Center for Risk Management of Engineering Systems University of Virginia, Charlottesville. Proc. of the „USC Terrorism Risk Analysis Symposium", Los Angeles, California, January 14, 2005. Web: <www.usc.edu/dept/create/assets/002/51839.pdf>.

[10] JANOŠEC, J. *Strategicky významné změny pro přípravu variant budoucí bezpečnosti.* Web: <www.army.cz/mo/obrana_a_strategie/1-2004cz/janosec.pdf>.

[11] KRULÍK, O. *Zpráva Komise Kongresu o teroristických útocích z 11. září 2001.* Překlad "9/11 Report", 2002. Web: <http://news.findlaw.com/wp/docs/911rpt/index.html. MV ČR. E-Mail: Obpsekr@mvcr.cz>.

[12] LEE, E. E. et al. *Extreme Events and the Sustainability of Civil Infrastructure Systems.* Department of Decision Sciences and Engineering Systems, Rensselaer Polytechnic Institute, Troy, New York, 2004. Web: <www.rpi.edu/~mitchj/papers/sustainability.pdf>.

[13] LINHART, P. – RICHTER, R. *(2003):* Ochrana kritické infrastruktury. *In: Krizové řízení, č. 3, 2003, s. 112.* Web: <http://www.mvcr.cz/casopisy/112/3_2003/linhart.html>.

[14] LINNEROOTH-BAYER, J. *Risk and Vulnerability Program. IIASA, 2006.* Web: <www.iiasa.ac.at/Research/*RAV*/RAVPlan.pdf>.

[15] LÖVKVIST-ANDERSEN, A. L. et al Modelling Society's Capacity to Manage Extraordinary Events Developing a Generic Design Basis (GDB) Model for Extraordinary Societal Events using Computer-Aided Morphological Analysis. In: *Proc. of the SRA (Society for Risk Analysis) Conference in Paris 15–17 November, 2004.* Web: <www.swemorph.com>.

[16] MOTEFF, J. – COPELAND, C. – FISCHER, J. *Critical Infrastructures: What Makes an Infrastructure Critical? Resources, Science, and Industry Division. Congressional Research Service.* The Library of Congress. Washington D.C.,August 30, 2002. Web: <http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf>.

[17] MOTEFF, J. – 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. Web: <http://www.fas.org/sgp/crs/RL32631.pdf>.

[18] *Základní scénář vývoje nakládání s vodami, užívání vod a vlivů na vody do roku 2015.* Ministerstvo zemědělství ČR, květen 2004, cel. 264 stran.

[19] POWELL, N. Re-conceptualising Resilience for Impact Assessment in Conditions of Systemic Uncertainty. In: *Proceedings from the 3rd Nordic EIA/SEA Conference, 22–23. November 1999, pp. 163-174.* Web: <www.nordregio.se/Files/r003powell.PDF>.

[20] *PSEPC Assets criteria. Public Safety and Emergency Preparedness Canada, Ottawa, Canada. 20 January 2004.* Web: <www.psepc.gc.ca/prg/em/nciap/assets_criteria-en.asp>.

[21] RINALDI, S. M. Modeling and Simulating Critical Infrastructures and Their Interdependencies. In: *Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.* Sandia National Laboratories. Sandia. Web: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1265180>.

[22] RINALDI, S. M. – PEERENBOOM, J. P. – KELLY, T. K. Critical infrastructure interdependencies. (Identifying, Understanding, and Analyzing). In: *IEEE Control Systems Magazine, Vol. 21, December 2001, pp.12-25.* Web: <www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf>.

[23] ŘÍHA, J. Koncept a teorie bezpečnostního rizika. In: *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva, roč. IV, č. 11, 2005, s. 22–25.* ISSN 1213-7057. Web: <http://www.mvcr.cz/casopisy/112/2005/listopad/index.html>.

[24] SAK, P. Bezpečnostní věda – důsledek vývoje civilizace. In: *Britské listy, 12. 11. 2004.* ISSN 1213-1792. Web: <www.blisty.cz/art/20569.html.

[25] *SANTOS, J. R. – HAIMES, Y. Y. Impact Assessment of Major Economic Disruptions using the Inoperability Input-Output Model (IIM).* Center for Risk Management of Engineering Systems University of Virginia, Charlottesville, 2005. Web: <http://www.sanken.keio.ac.jp/papaios/iioa/conf/2005/paper/jsantos.pdf>.

[26] SLUKA, V. ed. *Výkladový terminologický slovník některých pojmů používaných v analýze a hodnocení rizik pro účely zákona o prevenci závažných havárií.* VÚBP – Odborné pracoviště pro prevenci závažných havárií, 2005. Web: <www.vubp.cz/html_oppzh/metodiky/vykladovy_slovnik_brezen05.pdf>.

[27] STŘEDA, L. – MATOUŠEK, J. Globální úsilí v boji proti terorismu – aktuální výzva současnosti. In: *Sborník Mezinárodní konference medicíny katastrof. Zlín 24.–26.06.2002.* Web: <http://www.egozlin.cz/upload.cs/c/cde82244_0_streda_matousek_sujb_2002.pdf>.

[28] SUŠA, O. *Byrokracie, riziko a diskuze o krizi životního prostředí.* Filozofický ústav AV ČR. 01.10.2006. Web: <http://www.risk-management.cz/tisk.php?clanek=150>.

[29] ŠEBEK, J. *Ochrana infrastruktury před teroristickými útoky.* 20.09.2005. Web: <http://www.techportal.cz/>.

[30] ŠENOVSKÝ, P. *Stav řešení ochrany kritické infrastruktury na území USA.* FBI VŠB-TU Ostrava 2005. Web: <www.homel.vsb.cz/~sen76/inform/ki.pdf>.

[31] TUZAR, A. *Teoretické aspekty zkoumání mimořádných událostí.* Dopravní fakulta Jana Pernera, Univerzita Pardubice. 16.02.2000. Web: <http://cep.mdcr.cz/odd540/doc/seminar/aspekty.doc>.

[32] *US DHS National Strategy to Secure Cyberspace. U. S. Department of Homeland Security. The White House. Washington D. C., February 2003.* 76 pp. Web: <www.us-cert.gov/reading_room/cyberspace_strategy.pdf>.

[33] *US DHS The National Strategy for Physical Protection of Critical Infrastructures and Key Assets. U. S. Department of Homeland Security.* The White House. Washington D. C., February 2003. 96 pp. Web: <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

[34] VEVERKA, I. Mimořádné události a krizové řízení. In: *Sborník přednášek Požární ochrana 2001, s. 500–503,* SPBI, Ostrava 2001, ISBN: 80-86111-87-3.

[35] VOELLER, J. G. CIPP – Critical Infra-Structure Protection Priorities. In: *The Construction Sciences Research Foundation, Inc. Baltimore, USA.* Updated March 5, 2005. Web: <http://www.csrf.org/pubs/cipp.html>.

prof. Ing. Josef Říha, DrSc.
emeritní profesor ČVUT v Praze

ENGLISH ABSTRACT

Critical Infrastructure and the Incident Risk, by Josef Říha

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". These efforts are closely observed, with the actual situation considered as an unfinished and open strategy of safety risk.