

## OCHRANA A OBRANA KRITICKÉ INFRASTRUKTURY ÚSKALÍ A MOŽNOSTI ROZVOJE V ČESKÉ REPUBLICE

### CRITICAL INFRASTRUCTURE PROTECTION AND DEFENSE DIFFICULTIES AND POSSIBILITIES OF DEVELOPMENT IN THE CZECH REPUBLIC

Petra SKALICKÁ  
SkalickaPetra@post.cz

#### Abstract

*This article summarizes one of the outputs of the author's research activities, which focuses on the critical infrastructure protection and the possibilities of its development. The text describes the current situation and circumstances (context) the critical infrastructure protection in the Czech Republic using SWOT analysis and also proposes specific steps to streamline one of the problems identified, which is the disunity of the concept of defensive infrastructure and critical infrastructure.*

#### Key Words

*Critical infrastructure; defensive infrastructure; SWOT analysis; systems approach.*

#### ÚVOD

Kritická infrastruktura je jedním ze základních zájmů chráněných státem, proto též ochrana kritické infrastruktury je nedílnou součástí řízení bezpečnosti území. Od poslední novely krizového zákona z roku 2011 [7], která zakotvila základní terminologii a principy ochrany kritické infrastruktury v České republice, však její rozvoj stagnuje vyjma několika sektorových iniciativ, jako jsou oblast kybernetické, energetické a dopravní bezpečnosti. S odstupem času je přitom zjevné, že některé aspekty nebyly zmiňovanou zákonnou novelou vhodně postíženy a mohou vytvářet či již vytváří bariéry takového rozvoje.

Výzkumná činnost autorky se zaměřila na některé nedostatečně řešené oblasti ochrany kritické infrastruktury v České republice, a to jednak metodou komparativní analýzy s vybranými zahraničními státy a jednak hloubkovými rozhovory s odborníky z praxe. Tyto nástroje poskytly důvodné argumenty, proč je namístě tuto problematiku řešit a rozvíjet. Článek staví na výstupech z provedeného průzkumu, které dále analyzuje za účelem celistvého pochopení vlastní situace, resp. současného stavu ochrany kritické infrastruktury a vytvoření komplexního obrazu o tom, kde Česká republika stojí a kam směřuje (by mohla směřovat). K tomuto využívá manažerskou techniku, konkrétně analýzu SWOT<sup>1</sup>. Byť jde o jednu z metod strategické analýzy určené k odhalení pozice konkrétní firmy v konkurenčním prostředí, lze ji aplikovat k finalizaci pohledu na aktuální úroveň ochrany kritické infrastruktury v České republice, resp. zjištění hrozeb a příležitostí, na které je třeba reagovat.

Na jeden z výstupů analýzy, konkrétně identifikovaný problém nejednotného pojetí obranné a kritické infrastruktury státu, je zaměřena pozornost detailněji. Cílem je na tomto případě poukázat na možnosti jeho řešení, čímž by zároveň byl v této dílčí oblasti dosažen kýžený rozvoj ochrany kritické infrastruktury státu.

## ANALÝZA STÁVAJÍCÍHO STAVU

Identifikace a porozumění silným a slabým stránkám, odhalení příležitostí a hrozeb ochrany kritické infrastruktury je nezbytným předpokladem k stanovení strategie jejího rozvoje a efektivnějšího zajišťování. Inspirací pro zvolení SWOT analýzy se stala Koncepce ochrany obyvatelstva [5], která také s tímto nástrojem pracuje. Již identifikované výstupy jsou však mnohem podrobněji rozpracovány, díky čemuž je dán komplexní základ pro strategické řízení bezpečnosti a odolnosti kritické infrastruktury v České republice.

### Silné stránky

Mezi silné stránky stávajícího zajištění ochrany kritické infrastruktury v České republice lze zařadit:

- Funkčnost kritické infrastruktury (žádné významné případy selhání či omezení kritické infrastruktury v historii České republiky).
- Historické základy ochrany kritické infrastruktury (postupné budování zkušeností).
- Existence právní úpravy (obecné zakotvení).
- Bezpečnostní priorita (dle Bezpečnostní strategie České republiky [1]).
- Zakotvení veřejné správy mezi odvětví kritické infrastruktury.
- Rozvinutá sektorová ochrana kritické infrastruktury (zejména kybernetická, energetická a ochrana měkkých cílů).
- Uplatnění systémového přístupu v blízkých oblastech (ochrana obyvatelstva, audit národní bezpečnosti).
- Provedená analýza hrozeb jako možný výchozí podklad pro hrozby ochrany kritické infrastruktury.
- Aktivita v rámci Evropské unie – nastavené komunikační kanály, účast při jednáních, určení prvků evropské kritické infrastruktury.
- Připravenost a odbornost subjektů kritické infrastruktury v soukromém sektoru (zejména energetika).
- Zavedený bezpečnostní výzkum a zájem o něj ze strany řešitelů projektů.

### Slabé stránky

Naopak jako slabé stránky stávajícího zajištění ochrany kritické infrastruktury v České republice se jeví:

- Nesystémový přístup, podceňování problematiky.
- Neexistence platného strategického dokumentu.
- Neurčitá terminologie a kritéria pro určování prvků kritické infrastruktury.
- Nesoulad pojetí kritické a obranné infrastruktury.
- Absence zapojení územní úrovně, nerozlišování územní kritické infrastruktury, včetně klíčových prvků (tzv. *key assets*), popř. měkkých cílů.
- Nedostatečné zapojení všech subjektů kritické infrastruktury, nedostatečná zpětná vazba a metodická podpora.
- Nedostatečná metodická podpora gestorů jednotlivých odvětví kritické infrastruktury, nekoordinovanost a nejednotnost stanovených odvětvových kritérií.
- Nezohlednění všech chráněných zájmů.
- Pojetí ochrany kritické infrastruktury jako součást ochrany obyvatelstva (nekonceptní přístup).
- Převažující absence systému řízení rizik ochrany kritické infrastruktury na národní a lokální úrovni a podpory jeho zavádění u subjektů kritické infrastruktury.

- Převažující absence systému řízení kontinuity, resp. podpory jeho zavádění u subjektů kritické infrastruktury.
- Finanční nákladnost modernizace infrastruktury, pokud má obstát z hlediska technického pokroku.
- Neexistence kontingenčního plánování.
- Absence systémového řízení bezpečnosti území, na kterém je vystavěn udržitelný rozvoj území.
- Nedostatečná motivace subjektů kritické infrastruktury z veřejného sektoru při řízení ochrany kritické infrastruktury, nedostatečná personální kapacita, nedostatky v zajištění koncepční ochrany kritické infrastruktury.
- Absence scénářů krizových situací (v důsledku absence registru rizik).
- Absence analýzy vzájemných závislostí.

### **Příležitosti**

Potenciálními příležitostmi stávajícího zajištění ochrany kritické infrastruktury v České republice jsou:

- Stanovení nových odvětví kritické infrastruktury a kritérií (měkké cíle, soudy, obrana apod.).
- Rozšíření pojetí kritické infrastruktury na územní úroveň.
- Realizace PPP projektů<sup>2</sup> v oblasti ochrany kritické infrastruktury, jejich politická podpora.
- Rozšíření analýzy hrozeb – zapojení subjektů kritické infrastruktury a územní úrovně (včetně tvorby typových plánů), vytvoření národního registru rizik, aktualizace katalogu krizových opatření se zaměřením na funkčnost kritické infrastruktury.
- Vytvoření plánu kontinuity kritické infrastruktury veřejného sektoru na národní a lokální úrovni.
- Setkávání v rámci Výboru pro civilní nouzové plánování za účelem řešení ochrany kritické infrastruktury (základní platforma) se zapojením soukromého sektoru či subjektů kritické infrastruktury.
- Rozvoj územního plánování jako předpoklad řízení bezpečnosti území.
- Zkušenosti subjektů kritické infrastruktury soukromého sektoru a jejich zájem účastnit se společných projektů a aktivně se zapojit.
- Nové technologické možnosti pro sdílení zkušeností a informací.
- Bezpečnostní výzkum a technologický pokrok včas promítnuté do praxe.
- Zapojení vysokých škol do vzdělávání a metodické podpory.
- Alternativní, vícezdrojové financování.
- Aplikace inspirativních zahraničních přístupů (projektů, osvědčených postupů), poučení se z jejich chyb.
- Spolupráce v rámci skupiny V4<sup>3</sup> (vhodná platforma pro rozvoj ochrany kritické infrastruktury na mezinárodní úrovni).

### **Hrozby**

Identifikovat lze následující hrozby stávajícího zajištění ochrany kritické infrastruktury v České republice:

- Nekomplexní či nadhodnocené prvky kritické infrastruktury (evropské kritické infrastruktury).
- Neschopnost predikce domino dopadů (neznalost vzájemných závislostí).
- Neznalost potřeb subjektů kritické infrastruktury, neadekvátní odhad potřebných zdrojů ke zvládnutí krizové situace.

- Absence systémového konceptu financování ochrany kritické infrastruktury, výdajového titulu, tj. možný krach prvků (odvětví) kritické infrastruktury.
- Zhoršení dopadů krizových situací v důsledku nefunkční spolupráce a komunikace se subjekty kritické infrastruktury (výměny informací).
- Zkreslení scénářů rozvoje dopadů krizové situace v důsledku neexistující výměny informací o (skoro)nehodách kritické infrastruktury.
- Nedostatečné povědomí o ochraně kritické infrastruktury, zejména u bezpečnostních ředitelů veřejnoprávních subjektů kritické infrastruktury, tj. panika a neschopnost zvládnání konkrétní krizové situace, nefunkční odezva, nezkušenost v rozhodování, zhoršení dopadů (újmny).
- Kolaps zastaralé infrastruktury.
- Stárnutí populace, nerealizovaná reforma důchodového systému.
- Zaostávání územní kritické infrastruktury v důsledku nezohlednění jejich potřeb.
- Tendence prioritizovat některé hrozby (teroristické, kybernetické, hybridní) vedoucí k opomínání jiných (včetně zanedbání prevence a přípravy).
- Neočekávané domino či kaskádové dopady i na straně občanů (veřejnosti).
- Privatizace, komercializace bezpečnosti.
- Neodhalení (opožděné odhalení) všech rizik v důsledku jejich nepravidelného a nekoncepčního řízení.
- Selhání kontroly, formalizovaných postupů, externích služeb, nekvalifikovaných či nepřipravených odpovědných pracovníků (zejména bezpečnostních manažerů veřejné i soukromé sféry), neschopnost systému řešit případy nefunkčnosti kritické infrastruktury.

## STRATEGIE ŘEŠENÍ STÁVAJÍCÍHO STAVU

Z výše uvedeného vyplývá, že slabé stránky převyšují silné a hrozby příležitosti. Přesto je jejich množství nemalé, proto lze vytvořit i funkční strategie zlepšení stávající situace. Na základě získaných poznatků o vnitřním a vnějším prostředí lze vytvořit matici SWOT, která kombinuje získaná data a formuluje souhrnné strategie.

	Slabé stránky (W)	Silné stránky (S)
Příležitosti (O)	<b>WO strategie (hledání)</b> Překonání slabých stránek využitím příležitostí	<b>SO strategie (využití)</b> Využití silných stránek ve prospěch příležitostí
Hrozby (T)	<b>WT strategie (vyhýbání)</b> Minimalizace slabé stránky a vyhnutí se ohrožení	<b>ST strategie (konfrontace)</b> Využití silných stránek k odvrácení ohrožení

Zdroj: Grasseová, Dubec, Řehák [3]

Obr. 1  
Matice SWOT

### SO strategie

Nabízí se následující možnosti, jak využít silné stránky k včasné a adekvátní reakci na příležitosti:

- Využít vybudované základy ochrany kritické infrastruktury v České republice pro vytvoření systémového konceptu.

- Využít obecnou právní úpravu k stanovení nových odvětví kritické infrastruktury, k realizaci projektů PPP v oblasti ochrany kritické infrastruktury.
- Inspirovat se systémovým přístupem uplatněným v kybernetické bezpečnosti, ochraně obyvatelstva k nastavení systémového konceptu ochrany kritické infrastruktury.
- Využít analýzu hrozeb pro zdokonalení bezpečnostní dokumentace a plánování kontinuity na územní a odvětvové úrovni, včetně veřejného sektoru.
- Využít připravenost a odbornost subjektů kritické infrastruktury především ze soukromého sektoru pro sdílení zkušeností, postupů a informací a podání zpětné vazby například při jejich účasti ve VCNP, popř. v rámci jiné platformy, kde by se setkávali zástupci veřejného a soukromého sektoru.
- Využít funkčnost kritické infrastruktury k prevenci, poučení se ze zkušeností a využívání těchto poznatků při vytváření systémového konceptu ochrany kritické infrastruktury (jako zpětná vazba pro gesční i koordinační orgány ochrany kritické infrastruktury).
- Zefektivnit odvětví Veřejná správa vhodnější definicí kritérií.
- Využít zavedený bezpečnostní výzkum k rozvoji územního plánování, k předávání zkušeností, nových poznatků a know-how subjektům kritické infrastruktury.

### ST strategie

Konfrontační strategie využívá silných stránek k odvrácení ohrožení. V případě ochrany kritické infrastruktury se nabízí následující možnosti:

- Využít vybudované základy ochrany kritické infrastruktury v České republice pro vytvoření systémového konceptu s mapováním vzájemných závislostí, funkčním řízením rizik a funkčními součinnostními vazbami mezi soukromým a veřejným sektorem.
- Využít obecnou právní úpravu ke konkrétní specifikaci kritérií na principu nenahraditelnosti, konkretizace prvků na národní a lokální úrovni.
- Inspirovat se systémovým přístupem uplatněným v kybernetické bezpečnosti, ochraně obyvatelstva ke specifikaci požadavků na subjekty kritické infrastruktury, minimálních požadavků na úroveň (standard) bezpečnosti, k zajištění přiměřeného pokroku (postupným odstraněním zastaralosti infrastruktury) a také k poučení se z chyb, které byly zaznamenány s cílem potlačit na minimum snahy o komercializaci tématu.
- Využít analýzu hrozeb k vytvoření scénářů dopadů krizových situací založených na vzájemných závislostech, k vystavění nového konceptu řízení rizik na národní a územní úrovni, který by byl pravidelně aktualizován za účelem odhalení a předcházení i neočekávaných situací (budovat kontingenční plánování a resilienci).
- Zefektivnit odvětví Veřejná správa úpravou postupů a zlepšením metodického vedení s cílem čtenější kontroly, zavedení funkčních postupů, vyššího povědomí a kvalifikovanosti.
- Využít funkčnost kritické infrastruktury k prevenci, poučení se z příkladů ke zvyšování povědomí, včetně osvěty veřejnosti.

### WO strategie

Potenciální způsoby, jak pomocí příležitostí překonat slabé stránky, jsou následující:

- Stanovením nových odvětví kritické infrastruktury a kritérií a zpřesněním právní úpravy lze dosáhnout terminologického sjednocení, předejít neurčitosti právní úpravy, stírat rozdíly mezi obrannou a kritickou infrastrukturou, zohlednit veškeré chráněné zájmy při zajišťování ochrany kritické infrastruktury.

- Rozšířením pojetí kritické infrastruktury na územní úroveň lze zapojit i územní úroveň do řízení ochrany kritické infrastruktury a zohlednit více i měkké cíle, resp. klíčové prvky.
- Realizací PPP projektů lze motivovat subjekty kritické infrastruktury, zvyšovat povědomí a do určité míry podporovat zájem na modernizaci infrastruktury.
- Rozšířením analýzy hrozeb nalézt řešení i pro neočekávané události, podpořit zavedení kontingenčního plánování.
- Rozvojem územního plánování budovat systémové řízení bezpečnosti, čímž potlačit nesytemové prvky aktuálního konceptu ochrany kritické infrastruktury.
- Alternativním, vícezdrojovým financováním usnadnit financování modernizace infrastruktury a bezpečnostních opatření subjektů kritické infrastruktury.

## **WT strategie**

Strategie, které mohou pomoci překonat slabé stránky a zároveň se vyhnout hrozbám ochrany kritické infrastruktury, se nabízí následující.

- Podporovat spolupráci soukromého a veřejného sektoru při specifikaci vzájemných závislostí za účelem odstranění přehlížených mezer v důsledku preference určitého sektoru nebo určité hrozby na úkor ostatních a systémového pojetí bezpečnosti kritické infrastruktury. Budování znalostí o propojených vazbách mezi systémy kritické infrastruktury a systému výměny zkušeností a informací napříč odvětvími kritické infrastruktury.
- Plánováním kontinuity definovat klíčové činnosti a odhalit vzájemné závislosti za účelem předcházení krizovým situacím, resp. řešení a minimalizace možných dopadů.
- Systémovým vzděláváním, bezpečnostním výzkumem a technologickým pokrokem motivovat ke zvyšování povědomí subjektů kritické infrastruktury o moderních trendech a přístupech ke zvýšení bezpečnosti kritické infrastruktury, osvětě subjektů kritické infrastruktury i veřejnosti o vzájemných závislostech kritické infrastruktury a možnostech jejich řešení a o aktuálních bezpečnostních hrozbách a rizicích, která je třeba systémově řídit k zajištění přiměřené úrovně ochrany kritické infrastruktury.
- Aplikací inspirativních zahraničních přístupů do podmínek České republiky usilovat o zvýšení úrovně ochrany kritické infrastruktury v České republice, posílení vzájemné spolupráce veřejného a soukromého sektoru, potlačení slabých stránek a předcházení hrozbám.

## **SHRNUTÍ ANALÝZY A DISKUSE**

Z provedené analýzy SWOT vyplynulo, že oblast ochrany kritické infrastruktury se potýká se značným množstvím hrozeb a slabých stránek. Maticová struktura a formulované strategie však nabízí řešení, jak s využitím stávajících možností a vybudovaných základů dosáhnout zlepšení a rozvoje. Klíčovým aspektem, který se jako červená niť prolíná všemi strategiemi, je uplatnění systémového přístupu a posílení spolupráce soukromého a veřejného sektoru. Tyto faktory lze označit za průřezové nástroje rozvoje ochrany kritické infrastruktury.

Pokud bude však česká republika nadále preferovat sektorový přístup (kybernetickou bezpečnost) či dílčí zájmy (ochranu obyvatelstva) a uzavírat se spolupráci napříč sektory i úrovněmi řízení, lze předjímat, jak prokazuje analýza SWOT, trvalou stagnaci, zhoršování postavení a de facto i zvětšování propasti mezi ní a zahraničními státy, které jsou na poli ochrany kritické infrastruktury aktivnější, což může podkopat i základy mezinárodní spolupráce.

Vzhledem ke skutečnosti, že výchozím podkladem pro analýzu SWOT byla autorkou vybraná data získána zejména obsahovou a komparativní analýzou a expertními rozhovory, lze zpochybnit subjektivnost tohoto výběru nebo nedostatečnost všech relevantních informací, resp. jejich neuvedení. Stejně tak formulování strategií může být v důsledku tohoto neúplné a subjektivně zkršené. Cílem analýzy však bylo odhalit skryté možnosti, jakým směrem by bylo vhodné a možné s využitím stávajících nástrojů posunout či alespoň směřovat výkon ochrany kritické infrastruktury, popř. co hrozí v případě, že tento směr nebude následován. Analýza tedy neaspíruje na zevrubné a úplně odhalení všech souvislostí, spíše nalezení možností, strategických směrů, popř. trendů. Z tohoto hlediska ji lze hodnotit jako inspirativní podklad pro pokračování výzkumné činnosti, například pro formulaci návrhů pro rozvoj ochrany kritické infrastruktury. Potenciál však má případně i pro zvláštní výzkumné aktivity obdobného zaměření.

## NÁVRH ŘEŠENÍ IDENTIFIKOVANÉHO PROBLÉMU

Obranná infrastruktura a její koncept má své dlouholeté místo v rámci řízení bezpečnosti státu, proto mohla (měla) být inspirací při vzniku konceptu ochrany kritické infrastruktury.

### Popis problému

Jednou z výše identifikovaných slabých stránek je též nesoulad pojetí kritické a obranné infrastruktury. Jde o problém, který lze identifikovat od počátku snah o zakomponování ochrany kritické infrastruktury do podmínek České republiky a souvisí s jejím pojetím jakožto předmětu národního (státu) nikoli lokálního (kraje, obce) zájmu.

Z historického hlediska byl v České republice uplatňován lokální přístup k ochraně infrastruktury. Gesčně spadala pod Ministerstvo obrany v návaznosti na požadavky Organizace Severoatlantické smlouvy (NATO) a jejího strategického konceptu civilního nouzového plánování. Tzv. *obránná infrastruktura* rozlišuje infrastrukturu vojenskou i nevojenskou, která se do značné míry překrývá s kritickou infrastrukturou. Platí přitom zákonitost, že *„obránná infrastruktura stejně jako kritická infrastruktura vychází z infrastruktury státu, která je jedinečná. Pouze přívlastky se jí snažíme podle různých účelů a důvodů kategorizovat, ... jde o tu samou infrastrukturu.“* [6]

Přínosné a inspirativní je rozlišování obrané infrastruktury podle důležitosti na objekty důležité pro obranu státu (ODOS, infrastruktura vojenská i nevojenská) a objekty možného napadení (OMN, nevojenská infrastruktura). Pokud by byla vytvořena v rámci konceptu ochrany kritické infrastruktury úroveň *„nižší důležitosti“* pro stát, která by byla delegována na krajskou úroveň, mohly by se tímto oba koncepty propojit. Zároveň by kritická infrastruktura přestala být výsostnou záležitostí státu, čímž by se přiblížila regionům a občanům. Z obdobného důvodu je systém krizového řízení vystaven na odstupňování krizových stavů dle závažnosti krizové situace, kdy v nekrizových stavech je nahrazen systémem integrovaného záchranného systému. Lokální pojetí by odpovídalo i původnímu záměru novely krizového zákona, kterým byla vedle transpozice evropské směrnice (řešení problematiky na národní úrovni) též úprava *„nejasných vztahů a kompetencí v oblasti krizového řízení na krajské a obecní úrovni.“* [2]

### Návrhy řešení

Ve výše uvedených návrzích strategií pro zefektivnění stávajícího systému ochrany kritické infrastruktury byla navrhována pro popsany problém především strategie potlačení této

slabé stránky za využití příležitostí. Níže jsou zmíněny konkrétní možnosti, jak dojít k vyřešení problému a zároveň dosáhnout rozvoje v dané oblasti řízení bezpečnosti.

Pro výstavbu funkčního a dlouhodobě-udržitelného systému ochrany kritické infrastruktury je jedním z hlavních předpokladů terminologická přesnost a účelová kategorizace sektorů kritické infrastruktury. Absence těchto předpokladů činí stávající systém určování kritické infrastruktury v České republice zmatečným, a proto jsou jeho výstupy a definované prvky kritické infrastruktury zpochybnitelné. Řešením by mohlo být přijetí systémových opatření, přehodnocení současné právní úpravy a přenastavení současných postupů určování prvků kritické infrastruktury.

Základem přesného určování prvků kritické infrastruktury je *definice základních pojmů*. Jako řešení se nabízí novela krizového zákona. Provázáním ochrany s obranou kritické infrastruktury by mohla být usnadněna stávající nevyhovující výkladová praxe. Právní úprava vzájemného vztahu kritické a obranné infrastruktury prozatím neexistuje. Nabízí se vytvořit kategorii například „*bezpečnostní infrastruktury státu*“, která by se členila na podkategorie (obranou infrastrukturu a kritickou), přičemž určující pro uplatnění přístupů ochrany či obrany infrastruktury by byl vyhlášený krizový stav [6]. Taková úprava by si však kromě legislativních vyžádala též změny v samotném pojetí kritické infrastruktury. V současné době se oba instituty právě v tomto míjejí – kritická infrastruktura je upravena na úrovni národní a nadnárodní, obranná infrastruktura se zaměřuje mimo jiné na regionální infrastrukturu a zapojuje krajskou úroveň veřejné správy. Již samotná definice obranné infrastruktury<sup>4</sup> zahrnuje více možných prvků (objektů) než definice kritické infrastruktury, protože mimo stavby, pozemky a zařízení považuje za součást obranné infrastruktury též související nezbytné služby a výrobní a nevýrobní systémy potřebné k zajištění provozu. Sjednocení pojetí by napomohlo i k užší provázanosti bezpečnostní plánovací dokumentace.

V rámci procesu určování prvků kritické infrastruktury nelze opominout ani důslednou *kategorizaci sektorů kritické infrastruktury*, která vychází z odvětvových kritérií a měla by odrážet bezpečnostní rizika státu a vzájemné závislosti kritické infrastruktury. Česká republika zařadila jako kritické většinu podstatných sektorů infrastruktury. Opomíjena je tzv. sociální infrastruktura (školaství, výzkum, bydlení, soudnictví apod.) a právě obrana státu, která není ani součástí (pododvětvím) sektoru nouzových služeb. Nabízí se proto prostřednictvím novely krizového zákona doplnit do výčtu odvětví či pododvětví kritické infrastruktury či alespoň odvětvových kritérií nové činnosti, resp. oblasti, které svým významem naplňují definiční znaky kritické infrastruktury. V úvahu pro další členění připadají odvětví Nouzových služeb nebo Veřejné správy, konkrétně pododvětví Ostatní veřejná správa. Inspirovat se lze zahraničními státy, jako jsou Spojené království, Spojené státy americké či Nový Zéland, které obranu či obranný průmysl považují za jedno z odvětví kritické infrastruktury.

Při posuzování soudobých zahraničních přístupů k zajišťování ochrany kritické infrastruktury lze souhrnně konstatovat, že úsilí je směřováno k naplnění pěti cílů, které jsou zároveň *základními opatřeními systémového přístupu*:

- Podporování all-hazard přístupu<sup>5</sup>.
- Zaměření pozornosti na kaskádové dopady, obzvláště vznikající v důsledku vzájemných závislostí.
- Zdůraznění sdílené odpovědnosti všech úrovní veřejné správy, soukromého sektoru i občanů za zajištění ochrany a odolnosti kritické infrastruktury.
- Posilování spolupráce veřejného a soukromého sektoru.
- Zavedení sdílení informačních a komunikačních kanálů za účelem výměny informací a postupů nejlepší praxe a stanovení povinnosti zainteresovaných subjektů informovat o plánovaných a provedených zásadních rozhodnutích souvisejících s kritickou infrastrukturou.



Tyto zásady zároveň odráží ústřední cíl všech přístupů, kterým je zajištění takové ochrany, která vede k resilienci (odolnosti) kritické infrastruktury, což v určitém výkladu lze považovat za pojem propojující bezpečnost a udržitelný rozvoj [4]. Systémový přístup konkrétně pro specifika České republiky je obtížné vymezit. Je kombinací takových kroků, které zajistí nadhled, koordinaci, souvislost a synergii všech činností. Přispěním v podmínkách České republiky by bylo jasné vymezení vztahů mezi systémy ochrany obyvatelstva a kritické infrastruktury, mezi ochranou a obranou kritické infrastruktury (kritická vs. obranná), nastavení komunikačních vazeb na všech úrovních řízení i navenek, především k soukromému sektoru.

## ZÁVĚR

Svým charakterem, nevyzpytatelností, různorodostí je ochrana kritické infrastruktury jednou z nejobtížněji říditelných oblastí bezpečnosti a zároveň klíčovým tématem bezpečnostní politiky státu. Vazby spojující prvky kritické infrastruktury jsou velmi křehké, narušení jediné může způsobit kolaps celého systému, přičemž s propojeností a sofistikovaností systému roste též jeho zranitelnost.

Článek identifikuje některé problematické oblasti a výzvy ochrany kritické infrastruktury za pomoci SWOT analýzy. Přičemž prokazuje, že tato metoda je univerzálním nástrojem pro podporu rozhodování i v této specifické oblasti řízení. Její výsledky poskytují návrhy na řešení slabých stránek a hrozeb. Lze je dále využít k formulaci návrhů na řešení stávajícího stavu s cílem dosažení rozvoje ochrany kritické infrastruktury.

Pokud nedojde ke zlepšení situace a zajištění ochrany kritické infrastruktury bude nedostatečné, resp. úroveň stagnovat, lze předjímat naplnění hrozeb, přibývání slabých stránek na úkor silných a zmeškání příležitostí, které stanovila analýza SWOT. V důsledku tato situace povede k pravděpodobně vyšším dopadům a újmám vznikajícím v důsledku nefunkčnosti kritické infrastruktury. Navrhované možnosti řešení jsou jedny z mnoha způsobů, díky kterým by bylo možné těmto trendům čelit.

## Résumé

*Critical infrastructure is one of the fundamental interests protected by the State, therefore, also the protection of critical infrastructure is an integral part of the safety management of the territory. In the Czech Republic, however, its development is stagnant with the exception of several sectoral initiatives, such as cyber, energy and transport security. The article identifies some critical areas and challenges for the protection of critical infrastructure by using SWOT analysis. This demonstrates that this method is a versatile tool for decision support in this specific field of management. Its results provide proposals to deal with weaknesses and threats. They can also be used to formulate proposals to solve the current state with the aim of achieving the development of critical infrastructure protection.*

*On one of the outputs specifically identified by the SWOT analysis, the problem of inconsistent the concept of defence and critical infrastructure of the State, is designed to focus attention in more detail. The aim in this case is to point out the possibility of a solution, thus achieving the desired development of critical infrastructure protection in this sub-region.*

*The key finding presented in the article is the fact that the terminological precision and purposeful categorization of critical infrastructure sectors is one of the key prerequisites for the construction of a functional and long-lasting critical infrastructure protection system. This also applies for the case of the inconsistency of the concept of protection and defence critical infrastructure. Contributing to the unification of these concepts in the Czech Republic would be the introduction of a systems approach, in particular, a clear definition of the relationship*

*between systems of the population protection and the critical infrastructure protection and between the protection or defence critical infrastructure (critical vs. defensive infrastructure), the setting up of communication links at all levels of management as well as externally, primarily to the private sector.*

*If there is no improvement of the situation and ensuring the critical infrastructure protection is insufficient, or stagnate, it can be anticipate the fulfilling the threats, expansion of weaknesses and missing opportunities that the SWOT analysis has demonstrated. As a result, this situation will lead to likely higher impacts and losses resulting from the malfunctioning of critical infrastructure. The proposed solutions are one of the many ways in which these trends can be countered.*

## POZNÁMKY:

---

- <sup>1</sup> Zkratka je vytvořena z anglického názvu: S – Strengths (silné stránky), W – Weaknesses (slabé stránky), O – Opportunities (příležitosti), T – Threats (hrozby).
- <sup>2</sup> Tzv. Public Private Partnership (PPP) projekty jsou takovou formou spolupráce, jejímž předmětem je smluvní ujednání veřejného a soukromého sektoru o zajištění veřejných služeb či veřejné infrastruktury (nejčastěji výstavba, renovace, údržba, správa) a sdílení rizika.
- <sup>3</sup> Visegrádská skupina; Visegrádská čtyřka (aliance čtyř států střední Evropy: České republiky, Maďarska, Polska, Slovenska).
- <sup>4</sup> Definice je citována z vládou schváleného Plánu operační přípravy státního území České republiky, který je veřejně utajovaným dokumentem.
- <sup>5</sup> Přístup zohledňující všechny typy hrozeb.

## Literatura

- [1] *Bezpečnostní strategie České republiky* [online]. Praha: Ministerstvo zahraničních věcí, 2015 [cit. 2017-03-01]. ISBN 978-80-7441-005-5. Dostupné z: <https://goo.gl/b6y43S>
- [2] Důvodová zpráva k zákonu č. 430/2010 Sb., kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) v posledním znění.
- [3] GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. 2. vyd. Brno: BizBooks, 2012. ISBN 978-80-265-0032-2.
- [4] HROMADA, Martin. *Systém a způsob hodnocení odolnosti kritické infrastruktury*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. ISBN 978-80-7385-140-8, s. 45 an.
- [5] *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030* [online]. Praha: Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru ČR, 2013 [cit. 2017-03-01]. Dostupné z: <https://goo.gl/tPgWdc>
- [6] ŤULÁK, Pavel a Jaroslav SKALNÍK. Obranné plánování a zabezpečení ochrany kritické infrastruktury Armády ČR. In: Kolektiv autorů. *Ochrana kritické infrastruktury*. 1. vyd. Praha: Česká asociace bezpečnostních manažerů, 2011, s. 83. ISBN 978-80-260-1215-3.
- [7] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů v posledním znění.