

## **MIESTO OBRANNEJ INFRAŠTRUKTÚRY V BEZPEČNOSTNOM SYSTÉME SLOVENSKEJ REPUBLIKY**

**Peter Marchevka,<sup>1</sup> Ivan Máčovský<sup>2</sup>**

### **ABSTRAKT**

Zrútenie infraštruktúry štátu môže ohroziť samotnú výrobu potravín, vykurovanie, priemyselnú výrobu a v podstate narušiť a rozvrátiť chod celej spoločnosti. Kolaps ktoréhokoľvek štátu môže mať za následok zlyhanie infraštruktúr v regionálnom rozsahu, resp. aj v širšom geografickom priestore, ktorý je navzájom prepojený rôznymi sieťami. Narušenie kľúčových objektov infraštruktúry z dôvodu teroristického útoku, prípadne iných dôvodov, ako napr. veľkej prírodnej alebo technologickej katastrofy na území štátu by znamenalo vždy veľké straty na životoch a majetku, morálne škody alebo by viedli k dezorganizácii spoločnosti ako celku.

### **Kľúčové slova:**

Bezpečnosť, kritická infraštruktúra, terorizmus, ochrana, obrana.

### **ABSTRACT**

Collapse of the state infrastructure may endanger very production of foodstuffs, heating, industrial production, and it may substantially infract and subvert functioning of the whole society. The collapse of any country may result in infrastructures failure within a regional scale, respectively also in a broader geographical area, that is mutually interconnected by various networks.

Disruption of key infrastructure facilities due to a terrorist attack or other reasons, such as for example major natural or technological disasters in the country territory, would always involve great losses of life and property, moral damages, or it would lead to disorganization of the society as a whole.

### **Kľúčové slova:**

Bezpečnosť, kritická infraštruktúra, terorizmus, ochrana, obrana.

---

<sup>1</sup> Peter Marchevka, Ing. PhD, hlavný štátny radca, sekcia obranného plánovania MO SR Kutuzovova 8, Bratislava, e-mail: marchevkap@mod.gov.sk

<sup>2</sup> Ivan Máčovský, Ing. generálny riaditeľ, sekcia obranného plánovania MO SR Kutuzovova 8, Bratislava, e-mail: mačovskyyi@mod.gov.sk

## ÚVOD

Vývoj celosvetovej bezpečnostnej situácie, zmena charakteru hrozieb a rizík vyvolali potrebu zabezpečiť efektívnu ochranu a obranu infraštruktúry.

Po útokoch medzinárodného terorizmu v USA, v Španielsku a vo Veľkej Británii, potreba ochrany a obrany infraštruktúry na národnej a medzinárodnej úrovni výrazne narástla.

Preto jednotlivé štáty a postupne aj medzinárodné organizácie začali vytvárať inštitucionálne, legislatívne a organizačné podmienky na ochranu a obranu infraštruktúry, ktorá je strategicky dôležitá na fungovanie štátu a ktorej strata by mohla viesť k ohrozeniu života ľudí, k nezvratným, negatívnym ekonomickým a sociálnym dopadom na spoločnosť a na obyvateľov – **kritickú infraštruktúru**.

Infraštruktúra v Slovenskej republike je vysoko zraniteľná a aj veľmi prepojená, navzájom i navonok a je nevyhnutná pre chod spoločnosti aj v 21. storočí. Narušenie kľúčových objektov infraštruktúry na území štátu by znamenalo vždy veľké straty na životoch a majetku, morálne škody alebo by viedlo k dezorganizácii spoločnosti ako celku.

Oblasť ochrany a obrany kritickej infraštruktúry je pre Slovenskú republiku novou oblasťou, v ktorej sa predpokladá dynamický vývoj. Aj preto Slovenská republika sa vo svojej bezpečnostnej stratégii zaviazala vytvoriť podmienky na zaručenie bezpečnosti kritickej infraštruktúry.

## 1 KRITICKÁ INFRAŠTRUKTÚRA V SLOVENSKEJ REPUBLIKE

*Z analýzy a odporúčaní skupiny expertov k novej strategickému koncepcii NATO v časti **Ochrana pred nekonvenčnými hrozbami** konštatuje, že „aj za predpokladu, že NATO si naďalej udrží ostražitosť, je šanca priameho vojenského útoku na hranice Aliancie malá, aspoň v predvídateľnej budúcnosti. Zistili sme však, že v súčasnej dobe by sa mohli skôr objaviť menej konvenčné hrozby voči Aliancii z väčšej vzdialenosti, ktoré by mohli predstavovať hrozbu pre bezpečnosť doma. Medzi tieto hrozby patria útoky zbraňami hromadného ničenia, teroristické útoky a aktivity zamerané na poškodenie spoločnosti prostredníctvom kybernetických útokov alebo nezákonného narušenia kritickej dôležitých prepravných trás. Na ochranu pred týmito hrozbami, ktoré možno nedosiahnu úroveň útokov spadajúcich pod článok 5, musí NATO upraviť svoj prístup k obrane územia Aliancie a zároveň rozšíriť svoje schopnosti zvíťaziť vo vojenských operáciách a všeobecnejších bezpečnostných misiách mimo svojich hraníc.“*

V reakcii na netradičné hrozby sú diskutované predovšetkým reakcie na terorizmus, kybernetickú zraniteľnosť, energetickú bezpečnosť a klimatické zmeny.[3]

NATO pripúšťa, že kybernetické útoky sú rastúcou hrozbou bezpečnosti pre Alianciu a jej členov. Preto okrem iného veľké úsilie sa musí venovať rozširovaniu monitoringu kritickej infraštruktúry a zhodnoteniu a náprave akýchkoľvek nedostatkov, ktoré budú odhalené aj v Slovenskej republike.

**Bezpečnostná stratégia Slovenskej republiky** okrem iného uvádza, že Slovenská republika prijme opatrenia na obmedzenie zraniteľnosti prvkov kritickej infraštruktúry,

s dôrazom na informačné a komunikačné systémy a na minimalizáciu negatívnych následkov útokov na ne. Bude pokračovať v aktivitách zameraných na bezpečnosť a integritu informačných a komunikačných systémov, zvlášť systémov nevyhnutných pre bezpečný výkon základných funkcií štátu. Bude pokračovať v spolupráci so zahraničnými partnermi na aktivitách zvyšujúcich bezpečnosť systémov vzájomnej komunikácie a výmeny informácií, zvlášť v oblasti prenosu a ochrany utajovaných informácií.[1]

Kritická infraštruktúra sa v doterajšom ponímaní stotožňovala iba s obrannou infraštruktúrou[2], ktorá je časťou kritickej infraštruktúry, ale nepredstavuje celú kritickú infraštruktúru.

## 2. OBRANNÁ INFRAŠTRUKTÚRA SLOVENSKEJ REPUBLIKY

*Bezpečnostná stratégia Slovenskej republiky* v kapitole 8., Obrana štátu, vláda Slovenskej republiky deklaruje, že bude budovať a udržiavať primeranú obrannú infraštruktúru a vytvárať podmienky na jej ochranu a obranu a fungovanie v krízových stavoch.

Súčasťou kritickej infraštruktúry podľa zákona o kritickej infraštruktúre je obranná infraštruktúra podľa osobitného predpisu, konkrétne podľa § 26 a 27 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov.[6]

*Zákon číslo 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy Slovenskej republiky v znení neskorších predpisov* vo všeobecnosti ustanovuje, že ministerstvá a ostatné ústredné orgány štátnej správy v rozsahu vymedzenej pôsobnosti zodpovedajú za úlohy obrany a vytváranie podmienok na realizáciu požiadaviek zabezpečovania príprav na obranu a ochranu.

### 2.1 OBJEKTY OSOBITNEJ DÔLEŽITOSTI A ĎALŠIE DÔLEŽITÉ OBJEKTY

*Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov* ustanovuje úlohy ministerstvám, ostatným ústredným orgánom štátnej správy a ďalším orgánom štátnej správy s celoštátnou pôsobnosťou, krajským úradom, obvodným úradom, obciam a vyšším územným celkom na úseku obrany štátu.

Definuje pojem **obranná infraštruktúra** ako súhrn pozemkov, stavieb, budov a zariadení, telekomunikačných, komunikačných a dopravných systémov, ktoré slúžia v čase vojny alebo vojnového stavu na **zabezpečenie obrany štátu**.

V rámci prípravy na obranu štátu je ustanovená povinnosť vykonávať výber a zaradenie prvkov obrannej infraštruktúry do kategórie **objektov osobitnej dôležitosti** alebo do kategórie **ďalších dôležitých objektov** pre obranu štátu a určiť spôsob ich ochrany a obrany.

Aktualizácia zaradenia prvkov obrannej infraštruktúry do jednotlivých kategórií a spôsob ich ochrany a obrany je vykonávaná každoročne k 30. júlu.

V zozname zaradenia je uvedený spôsob ochrany a obrany prvku obrannej infraštruktúry v čase bezpečnosti, výnimočnom stave, vojnovom stave, v čase vojny a v boji proti terorizmu.

Prílohou zoznamu je **Metodické usmernenie na ochranu a obranu strategických objektov**. Poskytuje vlastníkom a správcom strategických objektov metodickú pomoc pri zabezpečovaní ochrany kategorizovaných objektov a spresňuje hlavné zásady a súčinnostné otázky pri obrane strategických objektov. Ide o opatrenia, ktoré sú vykonávané v stave bezpečnosti a za krízovej situácie na zabezpečenie funkčnosti strategických objektov, ktoré sú nevyhnutné na obranu štátu.

Cieľom je zaistiť, aby sa ochrana týchto objektov zabezpečovala s využitím moderných technológií, ale najmä aby boli elektronické zabezpečovacie systémy ochrany objektov osobitnej dôležitosti prepojené na pult centralizovanej ochrany Policajného zboru za účelom vykonania efektívneho zákroku predurčených síl a prostriedkov v prípade narušenia objektu.

Ustanovuje, že fyzickú ochranu objektu môžu vykonávať civilné bezpečnostné služby, vlastní zamestnanci správcu alebo vlastníka objektu a vyčlenení príslušníci Policajného zboru Slovenskej republiky.

Spresňuje požiadavky na mechanické zábranné prostriedky, ktoré majú byť vybudované tak, aby ich nebolo možné neoprávnene prekonať v čase kratšom, ako je čas potrebný na spoľahlivú detekciu a spozorovanie narušiteľa priemyselnou televíziou alebo členmi fyzickej ochrany. Na koordináciu systému ochrany objektu sú ustanovené požiadavky na riadiace centrum.

V druhej časti sú ustanovené podmienky, za akých sa vykonáva obrana objektu vrátane vymedzenia súčinnostných otázok medzi vojenským veliteľom objektu a zamestnancami, ktorí sú prítomní v objekte.

V záverečnej časti je ustanovený rozsah dokumentácie, ktorá sa vedie na zabezpečenie ochrany a obrany objektov vrátane stupňa jej utajenia.

Finančné prostriedky na ochranu objektov obrannej infraštruktúry zaradených do kategórie objektov osobitnej dôležitosti a do kategórie ďalších dôležitých objektov sú zabezpečované z prostriedkov štátneho rozpočtu v rámci výdavkov na úlohy hospodárskej mobilizácie.

Finančné prostriedky na obranu objektov obrannej infraštruktúry zaradených do kategórie objektov osobitnej dôležitosti a do kategórie ďalších dôležitých objektov sú zabezpečované z prostriedkov štátneho rozpočtu v rámci kapitoly Ministerstva obrany Slovenskej republiky.

## **2.2 Podpora hostiteľskej krajiny**

*Podpora zo strany hostiteľskej krajiny – Host Nation Support* je definovaná ako civilná a vojenská pomoc poskytovaná v mieri, kríze, alebo vo vojne hostiteľskou krajinou spojeneckým silám a organizáciám NATO, ktoré prechádzajú územím hostiteľskej krajiny alebo sú na ňom rozmiestnené. Slovenská republika ako hostiteľská krajina poskytuje podporu v čo najširšom možnom rozsahu v súlade s národnou legislatívou, národnými prioritami a aktuálnymi kapacitami, ktoré má k dispozícii.

Za týmto účelom je vypracovaný *Katalóg národných spôsobilostí pre podporu hostiteľskej krajiny*, ktorý je každoročne aktualizovaný a zasielaný na veliteľstvo síl NATO v Európe - *Supreme Headquarters Allied Powers Europe (SHAPE)*.

Podpora hostiteľskej krajiny je plánovaná:

- a. V čase **mieru**, kedy sa bude zabezpečovať najmä pobyt síl NATO na území Slovenskej republiky pri cvičeniach alebo výpomoci vo výnimočnom alebo núdzovom stave.
- b. Pri **tranzite** krajinou pred vykonaním operácie mimo územie Slovenskej republiky.
- c. V prípade **vojenskej operácie** NATO na území Slovenskej republiky.

V prípade vojenskej operácie si zo strany Slovenskej republiky bude vyžadovať najvyššiu úroveň podpory ako hostiteľskej krajiny v situácii pravdepodobného prechodu hospodárstva Slovenskej republiky na vojnový stav so zvýšenými požiadavkami na podporu rozvinutých Ozbrojených síl Slovenskej republiky a súbežným narušovaním hospodárstva nepriateľskými akciami a jeho bojovou činnosťou.

## ZÁVER

Infraštruktúra Slovenskej republiky je podobná ako infraštruktúra iných štátov - doprava, energetika, chemický priemysel, obranný priemysel, výroba a transport nebezpečných látok, informačné technológie a telekomunikácie, finančné inštitúcie a poisťovne, zásobovanie pitnou vodou, potravinami, zdravotné a záchranné služby, odstraňovanie odpadu, štátna administratíva, verejná správa, súdy, polícia, ozbrojené sily, colná správa, médiá, výskumné a vzdelávacie inštitúcie, národné kultúrne pamiatky. Každá zo súčastí infraštruktúry spadá do pôsobnosti niektorého z ústredných štátnych orgánov, resp. orgánov miestnej samosprávy.

Identifikácia a ochrana kritickej infraštruktúry je náročný a dlhotrvajúci proces. Z hľadiska zabezpečenia bezpečnosti štátu je to však úloha, u ktorej sa dá predpokladať vzhľadom na vývoj technológií, stále väčší význam a prioritné postavenie. Zároveň vytvára podmienky na zvládnutie mimoriadnych udalostí a krízových situácií. Pripravené plány a postupy musia obsahovať identifikáciu vzájomných závislostí jednotlivých prvkov kritickej infraštruktúry a posúdenie týchto závislostí z pohľadu zabezpečenia rozhodujúcich činností v prípade vzniku závažných mimoriadnych udalostí.

## LITERATÚRA

- [1] Bezpečnostná stratégia Slovenskej republiky, Národná rada Slovenskej republiky, Bratislava 2005
- [2] Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany, vláda Slovenskej republiky, uznesenie č. 120/2007, Bratislava 2007
- [3] MARCHEVKA P.: Súčasnosc' a budúcnosc' kritickej infraštruktúry v Slovenskej republike - In.: Zborník z vedeckej konferencie s medzinárodnou účasťou –

Riešenie regionálnych disparít a nerovnovážnych stavov v prírodnom a hospodárskom prostredí, Slovenská akadémia pôdohospodárskych vied, Zborník v tlači, Veľká Lomnica 2009

- [4] Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, vláda Slovenskej republiky, uznesenie č. 185/2008, Bratislava 2008
- [5] Smernice Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritickej infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ, L 345/75, 23.12.2008), Brusel 2008

Článok recenzoval:  
doc. Ing. Miroslav Tomek, PhD.