KRITICKÁ INFAŠTRUKTÚRA V EURÓPSKEJ ÚNII A V SEVEROATLANTICKEJ ALIANCII

Peter Marchevka[1]

SUMMARY:

"Infrastructure" in last time definite mainly with reference to adequacy to defence of the state. Growing follicle threat international terrorism but leads to reinterpretation designation „infrastructure" in context national security. There is a change of to reappraisal to requisites individual element infrastructure of the state, that are or they will be consider inevitable at him existence as such and survival his inhabitant. These element infrastructure they will be consider "critical infrastructure". The article trial about juridical secure protect and defiance critical infrastructure in the European Union and Organization North Agreements

Key word: *Security, Infrastructure, Critical Infrastructure, Terrorism, Protection, Defensive.*

ÚVOD

Jedným z rozhodujúcich problémov v dynamicky sa meniacom vývoji európskej integrácie v poslednom období je skutočnosť, že **Európska únia** definitívne prekročila rámec obyčajného ekonomického nadnárodného zoskupenia a jasne deklarovala svoju ambíciu zastávať pozíciu významného politického a bezpečnostného aktéra na globálnej úrovni.
Okrem tradičných hrozieb, akými boli a sú prírodné katastrofy, nedbalosť, technologické havárie, neoprávnené vniknutie do počítačových systémov alebo trestná činnosť, sa na bezpečnostnej scéne objavila nová hrozba - medzinárodný terorizmus. [1]
Tento fenomén sústreďuje svoje úsilie okrem tradičných cieľov osobitne na infraštruktúru štátov s cieľom spôsobiť masové obete, škody, vyvolať strach a pocit ohrozenia.

V euro-atlantickej oblasti je približne 15 000 000 kilometrov vozoviek, 675 900 km železničných tratí, asi 23 000 letísk alebo letiskových zariadení a okolo 230 nákladných prístavov. V tomto teritóriu je približne 1,4 miliardy telefónnych liniek tak pevných, ako aj mobilných a stále sa rozrastajúci počet užívateľov internetu. [10]
Vývoj celosvetovej bezpečnostnej situácie, zmena charakteru hrozieb a rizík vyvolali potrebu zabezpečiť efektívnu ochranu a obranu tejto 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.*** Riešenie jej ochrany a obrany nie je mysliteľné bez spolupráce so **Severoatlantickou alianciou -** NATO.

V prvej časti príspevku popíšem kreovanie, právny rámec a postavenie kritickej infraštruktúry v Európskej únii a NATO. V ďalšej časti príspevku, ktorý bude publikovaný v nasledujúcom čísle prezentujem postavenie kritickej infraštruktúry v Slovenskej republike.

[1] Ing. PhD., Ministerstvo obrany Slovenskej republiky, Sekcia obranného plánovania, Kutuzovova 8 Bratislava, e-mail: peter.marchevka@mod.gov.sk

1. PRÁVNA ÚPRAVA NA ÚROVNI EURÓPSKEJ ÚNII

Spoločná zahraničná a bezpečnostná politika Európskej únie zahŕňa otázky týkajúce sa bezpečnosti, vrátane postupného vymedzovania spoločnej obrannej politiky, ktorá vedie k spoločnej obrane. Politika únie nemá vplyv na osobitý charakter bezpečnostnej a obrannej politiky členských štátov a rešpektuje záväzky, ktoré vidia v uskutočňovaní svojej obrany v NATO podľa Severoatlantickej zmluvy. Sú to otázky, ktoré zahŕňajú humanitárne a záchranné úlohy, misie na udržanie mieru a úlohy bojových síl pri riešení krízových situácií vrátane nastoľovania mieru.

V júni 2004 požiadala Európska rada o prípravu celkovej stratégie na ochranu kritických infraštruktúr. Komisia v nadväznosti na to prijala 20. októbra 2004 **oznámenie o ochrane najdôležitejšej infraštruktúry v boji proti terorizmu**, v ktorom predložila návrhy, ako na európskej úrovni zlepšiť predchádzanie teroristickým útokom na kritickú infraštruktúru, pripravenosť a reakciu na ne.[9] Komisia dospela k zisteniu, že problematiku musí riešiť v rámci integrovanej európskej stratégie vzhľadom na potrebu ochrany občanov Európskej únie pred rizikami v súvislosti s teroristickými útokmi, ale aj s prírodnými katastrofami, technologickými haváriami a krízami spojenými s chorobami, pandémiami a inými, bližšie nešpecifikovateľnými krízami s často značnými cezhraničnými následkami. [4]

Dňa 5. novembra 2004 bol schválený **Haagsky program**, podľa ktorého efektívne riadenie cezhraničných kríz v rámci Európskej únie si vyžaduje nielen posilnenie súčasných činností civilnej ochrany a hlavnej infraštruktúry, ale aj účinné zameranie sa na aspekty verejného poriadku a bezpečnosti v takýchto krízach. Z tohto dôvodu Európska rada vyzývala Komisiu, aby vytvorila integrované opatrenia EÚ pre krízové riadenie, ktoré by bolo implementované najneskôr do 1. júla 2006. Opatrenia mali riešiť ďalšie hodnotenie kapacít, rezerv, vzdelávania, spoločných cvičení a operačných plánov pre riadenie občianskych kríz členských štátov.

Následne, Komisia prijala 17. novembra 2005 **Zelenú knihu o európskom programe na ochranu najdôležitejšej infraštruktúry**, v ktorej predstavila rôzne možnosti na vytvorenie programu a zriadenie Varovnej informačnej siete kritickej infraštruktúry. Hlavným cieľom Zelenej knihy je získať spätnú väzbu v otázke politických alternatív **Európskeho programu na ochranu kritickej infraštruktúry** (Europe Program Critical Infrastructure Protection - ďalej len „EPCIP“) zapojením širokého počtu zainteresovaných subjektov. Účinná ochrana najdôležitejšej infraštruktúry si vyžaduje komunikáciu, koordináciu a spoluprácu na vnútroštátnej úrovni a na úrovni EÚ medzi všetkými zainteresovanými subjektmi: majiteľmi a prevádzkovateľmi infraštruktúry, regulátormi, profesnými orgánmi a priemyselnými združeniami v spolupráci so všetkými úrovňami vlády a s verejnosťou. Obsahom Zelenej knihy sú alternatívne spôsoby, ktorými by Komisia mohla reagovať na požiadavku Rady na zavedenie EPCIP a Varovnej informačnej siete kritickej infraštruktúry (Critical Infrastructure Warning Information Network - ďalej len „CIWIN“) a predstavuje druhú fázu konzultačného procesu o zavedení Európskeho programu na ochranu najdôležitejšej infraštruktúry.

Opatrenia uvedené v Zelenej knihe, týkajúce sa riadenia následkov, sú pre väčšinu narušení zhodné, resp. podobné, ochranné opatrenia sa líšia v závislosti od povahy hrozby. Medzi hrozby, ktoré by podstatne znížili schopnosť zabezpečovať základné potreby a bezpečnosť obyvateľstva, udržať poriadok a poskytovať minimálne základné verejné služby alebo riadne fungovanie ekonomiky, patria úmyselné útoky a prírodné katastrofy.

V reakciách na Zelenú knihu sa zdôraznila pridaná hodnota, ktorú predstavuje rámec Spoločenstva pre ochranu kritickej infraštruktúry. Uznala sa potreba zvýšiť schopnosť ochrany kritickej infraštruktúry v Európe a pomôcť znížiť zraniteľné miesta tejto infraštruktúry. Súčasne sa zdôraznil aj význam kľúčových zásad subsidiarity, proporcionality a komplementarity, ako aj dialógu so zainteresovanými stranami. Európsky parlament zdôraznil, že hlavnú zodpovednosť za ochranu infraštruktúry majú členské štáty, najmä národní majitelia alebo operátori infraštruktúry.

V decembri 2005 Rada pre spravodlivosť a vnútorné veci požiadala Komisiu, aby predložila návrh EPCIP a rozhodla, že by mal byť založený na prístupe, ktorý zohľadní všetky riziká a ktorý by prednostne čelil hrozbám vyplývajúcim z terorizmu. Tento prístup v procese ochrany kritickej infraštruktúry by zohľadňoval hrozby spôsobené človekom, technologické hrozby a prírodné katastrofy, ale

prioritou by bola hrozba vyplývajúca z terorizmu.
V texte oznámenia sa okrem iného konštatovalo, že sa zvyšujú možnosti pre katastrofické útoky teroristov, ktoré postihujú najdôležitejšiu infraštruktúru. Dôsledky možných útokov na priemyselné kontrolné systémy najdôležitejšej infraštruktúry môžu kolísať v širokom rozsahu. Všeobecne sa predpokladá, že úspešný elektronický útok by si vyžiadal málo zranení alebo obetí na životoch, ak vôbec nejaké, mohol by však spôsobiť škody na životne dôležitých infraštruktúrnych službách, napr. na verejnej sieti telefonického spojenia, naopak útok na kontrolné systémy chemických zariadení alebo zariadení kvapalného zemného plynu by mohol spôsobiť oveľa rozsiahlejšie straty na životoch, alebo aj značné materiálne škody, ktoré by mohli mať dlhodobé trvanie.

Medzi najdôležitejšie druhy infraštruktúry patria:

- energetické zariadenia a siete, výroba elektrickej energie,
- rafinérie, výroba pohonných hmôt a plynu, skladovacie zariadenia, prenosové a distribučné systémy,
- komunikačné a informačné technológie, telekomunikácie, televízne a rozhlasové vysielacie systémy, programové a technické prostriedky a internet,
- financie, bankovníctvo,
- zdravotníctvo,
- potravinový priemysel, výrobné prostriedky a distribúcia,
- voda, vodovodné potrubia a siete, stoková sieť, čistiarne, priehrady a vodné nádrže,
- doprava,
- výroba, skladovanie a preprava nebezpečného tovaru,
- štátna správa, kľúčové štátne pracoviská, krízové pracoviská a zariadenia, informačné siete, majetkové hodnoty a pamiatky.[9]

Cieľom Európskeho programu na ochranu najdôležitejšej infraštruktúry a úlohou Komisie je zabezpečiť existenciu adekvátnych a rovnakých úrovní ochrannej bezpečnosti pre najdôležitejšiu infraštruktúru, minimálnych jednotlivých prípadov zlyhania a rýchlych, testovaných mechanizmov obnovy v celej Európskej únii. Európsky program na ochranu najdôležitejšej infraštruktúry bude nepretržitý proces a bude potrebná jeho pravidelná kontrola, aby sa držal krok s problémami a požiadavkami Spoločenstva.

Zámerom programu je poskytnúť pomoc priemyslu a vládam členských štátov Európskej únii pri rešpektovaní jednotlivých mandátov a zodpovednosti prostredníctvom CIWIN. Vytvorenie tejto siete má pomôcť hlavne pri stimulovaní výmeny informácií o spoločných hrozbách a zraniteľnostiach a adekvátnych opatreniach a stratégiách na zmiernenie rizík, ktoré majú prispieť k ochrane najdôležitejšej infraštruktúry. Preto by členské štáty zo svojej strany mali zabezpečiť, aby boli príslušné informácie postúpené všetkým relevantným vládnym rezortom a úradom, vrátane organizácií pohotovostných služieb, informujúc príslušné subjekty priemyselného sektora tak, aby tieto zase informovali postihnutých vlastníkov a prevádzkovateľov najdôležitejšej infraštruktúry cez sieť kontaktov vybudovanú v členských štátoch.

Ako sa už na viacerých miestach zdôraznilo, v prípade absencie sektorových noriem, alebo medzinárodných predpisov, Európsky výbor pre normalizáciu (ďalej len „CEN“) a ďalšie relevantné normalizačné organizácie by mohli navrhnúť jednotné bezpečnostné sektorové a upravené normy pre najrozličnejšie zainteresované odvetvia. Takéto normy by mali byť navrhnuté aj na medzinárodnej úrovni cestou Medzinárodnej organizácie pre normalizáciu (ISO), aby sa v tomto ohľade vytvorili primerané rovnaké podmienky.

Dňa 8. decembra 2008 prijala Rada Európy **smernicu 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu**. Predstavuje prvú fázu etapovitého prístupu k identifikácii a označeniu európskej kritickej infraštruktúry a zhodnoteniu potreby zlepšiť jej ochranu. Smernica sa zameriava najmä na sektor energetiky a dopravy, následne ich preskúma s cieľom vyhodnotiť a posúdiť, či je potrebné, aby sa do rozsahu pôsobnosti zahrnuli aj niektoré ďalšie sektory, ako napríklad sektor informačných a komunikačných technológií a iné. Čo je však potrebné zdôrazniť, primárnu a konečnú zodpovednosť za ochranu Európskej kritickej infraštruktúry nesú členské štáty a vlastníci alebo prevádzkovatelia kritickej infraštruktúry. [7]

Smernica ustanovuje postup identifikácie európskej kritickej infraštruktúry. Tento postup je opísaný v článku 3 a prílohe III Smernice. Smernica zároveň stanovuje aj postup označenia európskej kritickej infraštruktúry a tento postup je opísaný v článku 4 Smernice.

Každý členský štát identifikuje len tie potencionálne európske kritické infraštruktúry podľa postupu uvedeného v prílohe III Smernice, ktoré spĺňajú prierezové a sektorové kritériá a tiež zodpovedajú definícii „kritickej infraštruktúry“ a definícii „európskej kritickej infraštruktúry“.

Potencionálna európska kritická infraštruktúra, ktorá nespĺňa požiadavky niektorého z uvedených nadväzujúcich krokov, sa nepovažuje za európsku kritickú infraštruktúru a vylúči sa z postupu. Potencionálna európska kritická infraštruktúra, ktorá zodpovedá definíciám „kritickej infraštruktúry“ a „európskej kritickej infraštruktúry“, musí byť podrobená ďalším krokom podľa tohto postupu.

Každý členský štát má povinnosť identifikovať kritické infraštruktúry, ktoré sa môžu označiť ako európska kritická infraštruktúra.

Potenciálna európska kritická infraštruktúra, ktorá nespĺňa požiadavky jedného z týchto nadväzujúcich krokov, nie je považovaná za európsku kritickú infraštruktúru a je vylúčená z postupu.[7] Postup označenia a zároveň práva a povinností členských štátov uvádza článok 4 Smernice.

2. RIEŠENIE KRITICKEJ INFRAŠTRUKTÚRY V RÁMCI SEVEROATLANTICKEJ ALIANCIÍ

Na istambulskom samite v roku 2004 bol schválený národnými riaditeľmi pre vyzbrojovanie program obrany proti terorizmu (Defence Against Terrorism - DAT).

Projekt je zameraný na desať oblastí a na rozvoj moderných technológií, ktoré spĺňajú najpotrebnejšie bezpečnostné potreby obrany proti terorizmu. Jednou z oblasti je aj ochrana kritickej infraštruktúry, ktorá zastrešuje programy zamerané na obranu infraštruktúry NATO. Je úzko prepojený s inými iniciatívami, ako je ochrana prístavov, spravodajstvo, prieskum, pozorovanie a zisťovanie cieľov obrany proti terorizmu.

Na summite v Štrasburgu/Kehli v apríli 2009 lídri Aliancie poverili Generálneho tajomníka Andersa Fogh Rasmussena zriadením skupiny odborníkov z rôznych oblastí, aby pripravili pôdu pre novú Strategickú koncepciu NATO.

Z analýzy a odporúčaní skupiny expertov k novej strategickej koncepcií 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 kriticky 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 NATO 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 venované rozširovaniu monitoringu kritickej infraštruktúry NATO a zhodnoteniu a náprave akýchkoľvek nedostatkov, ktoré budú odhalené.

Ochrana kritickej infraštruktúry bola a je kľúčovým zameraním pre plánovanie v NATO, činnosť na ktorej sa podieľajú všetky krajiny Euroatlantickej partnerskej rady (Euro-Atlantic Partnership Council – EAPC). Medzinárodná spolupráca uľahčuje zdieľanie relevantných informácií o potenciálnych zdrojoch hrozieb a ich možných dosahoch, hodnotení a výmene skúseností, osvedčených postupoch a nevyhnutných podkladoch pre prácu na ochrane kritickej infraštruktúry. Neoddeliteľnou súčasťou ochrany kritickej infraštruktúry je oblasť školení, tréningu a vzdelávanie personálu. NATO vynakladá značné úsilie na to, aby krajiny, ktoré uznávajú dôležitosť ochrany kritickej infraštruktúry vzdelávali personál, zodpovedných pracovníkov a obyvateľstvo o spôsoboch a metódach ochrany kritickej infraštruktúry v národných podmienkach a umožnili im túto činnosť vykonávať aj na spoločnom poli Aliancie.

Cieľom ochrany a obrany kritickej infraštruktúry v chápaní NATO je koordinácia plánovacieho procesu na zabezpečenie čo najefektívnejšieho použitia vojenských a civilných zdrojov pri kolektívnej podpore ochrany a obrany strategických objektov

Aliancie. Za plánovanie obrany kritickej infraštruktúry sú prioritne zodpovedné príslušné ústredné orgány štátnej správy na národnej úrovni a prostriedky orgánov verejnej správy zostávajú po celý čas nasadenia pod správou a kontrolou národných orgánov. Pre potreby NATO sa jednotlivé národné kapacity zlaďujú tak, aby vyžadované kapacity boli zabezpečené v požadovanej miere.

Ochrana kritickej infraštruktúry je v rámci Organizácie Severoatlantickej zmluvy v kompetencii Vyššieho výboru NATO pre civilné núdzové plánovanie (NATO Senior Civil Emergency Planning Committe - SCEPC), ktorý je zaradený v rámci organizačnej štruktúry v časti podriadených organizácií a agentúr, ako časť civilného núdzového plánovania (Civil Emergency Planning).

Na plnenie úloh ochrany kritickej infraštruktúry sú pod záštitou Vyššieho výboru NATO pre civilné núdzové plánovanie zriadené technické plánovacie výbory**,** ktoré združujú národných expertov jednotlivých krajín vyslaných vládnymi inštitúciami, priemyselnými spoločnosťami a vojenskými zástupcami. Jednotlivé výbory zodpovedajú za koordináciu krízového plánovania v oblasti:

- vnútrozemskej pozemnej dopravy
- námornej lodnej dopravy
- civilného letectva,
- potravinárstva a poľnohospodárstva
- priemyselnej výroby a zásobovania
- pôšt a telekomunikácií
- zdravotníctva
- civilnej ochrany a
- zásobovania a spracovania ropy.

Zabezpečenie dopravy, či už leteckej alebo vodnej, prevencia a samotné riešenie krízových situácii patrí medzi prioritné činnosti uskutočňované silami a prostriedkami NATO. Problematika je v kompetencii Výboru pre plánovanie civilného letectva (Civil Aviation Planning Committee - CAPC), Rady pre plánovanie oceánskej dopravy (Planning Board for Ocean Shipping - PBOS), Rady pre plánovanie európskej vnútrozemskej povrchovej dopravy (Planning Board for European Inland Surface Transport - PBEIST). Výbor pre priemyselné plánovanie (Industrial Planning Committee - IPC), Potravinársky a poľnohospodársky plánovací výbor (Food and Agriculture Planning Committee - FAPC) a ad hoc zvolávaný Výbor pre plánovanie zásobovania ropou a ropnými produktmi (Petroleum Planning Committee - PPC) má v kompetencii zabezpečovanie materiálovej podpory a dodávok. **Oblasť pôšt a telekomunikácií** je v kompetencii Výboru pre plánovanie civilných komunikačných systémov (Civil Communications Planning Committee - CCPC). Výbor koordinuje činnosť jednotlivých členských krajín na úseku harmonizácie štátnych komunikačných systémov a zvyšovanie ich odolnosti počas krízových situácií. **Oblasť zdravotníctva** je predmetom činnosti Spoločného zdravotníckeho výboru (Join Medical Committee - JMC).[2]

Riešenie úloh obrany kritickej infraštruktúry v NATO nie je reálne bez účasti radu ďalších vládnych a mimovládnych medzinárodných organizácií. Do procesu prípravy využiteľných opatrení a zdrojov, ako aj do samotného riešenia vzniknutých krízových situácií sú vo významnej miere zapojené aj Rada Európy, Európska Únia, Medzinárodný výbor Červeného kríža, Medzinárodná agentúra pre atómovú energiu, Organizácia OSN pre výchovu, vedu a kultúru (UNESCO), Úrad Vysokého komisára OSN pre utečencov (UNHCR), Detský fond OSN (UNICEF), Úradu OSN pre koordináciu humanitárnych záležitostí (UN-OCHA), Svetová zdravotnícka organizácia (WHO) a rad ďalších organizácií.

ZÁVER

Zámerom úprav kritickej infraštruktúry na úrovni Európskej únie je v európskom rámci úprava takých podmienok, ktoré by na všeobecnej aj oblastne explicitne stanovenej rovine riešili otázku identifikácie, kategorizácie a ochrany kritickej infraštruktúry. V súčasnosti je Európska únia integrátorom národných snáh, pričom sa snaží byť v čo najväčšej možnej miere aj navrhovateľom vhodnej právnej úpravy. Z celoeurópskeho aspektu sa zaoberá otázkami riešenia možných ohrození, ktorých zničenie alebo narušenie by pri takom množstve infraštruktúr, ktoré sa na teritóriu členských krajín nachádzajú, mohlo mať nielen národné, ale aj cezhraničné účinky.
Pri transpozícii smernice na podmienky Slovenskej republiky bude potrebné zamerať úsilie na zabezpečenie správnej transpozície, aby sa neporušila jej celistvosť pri samotnej transpozícii a vykonávaní v právnom systéme a nedošlo k vytváraniu neistoty. Je dôležité, aby Slovenská republika dôkladne preskúmala svoj právny systém s cieľom zabrániť možnému prekrývaniu pravidiel prijatých pri transponovaní smernice s už existujúcimi ustanoveniami platného právneho poriadku Slovenskej republiky a tým zabezpečila väčšiu transparentnosť a pochopiteľnosť

transponovanej smernice. Transponovaná smernica by mala doplniť metódy a prostriedky ochrany kritickej infraštruktúry v Slovenskej republike a súčasne by mala zabezpečiť celoplošnú kontrolu, ako nový nástroj na kontrolu a presadzovanie vykonávania právnych predpisov v oblasti kritickej infraštruktúry. Malo by ísť o systematickú kontrolu, ktorú vykonávajú príslušné orgány Slovenskej republiky, zodpovedné za vynucovanie aplikácie práv predpisov a mali by sa vytvoriť účinnejšie nástroje na monitorovanie vykonania práv predpisov a tým by mohli byť napr. celoplošné kontroly a testovania. Ale o tom v budúcom čísle.

LITERATÚRA

[1] NOVÁK, L. a kol.: Plánovanie zdrojov na riešenie krízových situácií – vysokoškolská učebnica. Bratislava, VŠMEVS 2010. 308 s. 40%. ISBN 978-80-970272-4-7.
[2] Bezpečnostná stratégia EÚ. EK Brusel, Belgicko, 2003.
[3] NATO Handbook, NATO – Public Diplomacy Division, 1110 Brussels, ISBN 92-845-0178-4, Belgium, 2006.
[4] New NATO´s Strategic Concept, Slovak Atlantic Commission, 2010.
[5] Oznámenie Komisie Rade a Európskemu Parlamentu - Ochrana najdôležitejšej infraštruktúry v boji proti terorizmu KOM/2004/0702 v konečnom znení.
[6] Predbežné stanovisko k návrhu smernice Rady o identifikácii a označení európskej kritickej infraštruktúry a o zhodnotení potreby zlepšiť jej ochranu - EÚ tlač: 2006/0276 (CNS).
[7] Príručka NATO (slovenský a český preklad). NATO, Bratislava 2001.
[8] Smernice Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ, L 345/75, 23.12.2008).
[9] Zmluva o založení Európskeho spoločenstva.
[10] Zelená kniha o európskom programe na ochranu najdôležitejšej infraštruktúry, KOM(2005) 576, Brusel, 2005.
[11] Critical Infrastrukture Protection in a NATO/EAPC Civil Emergency Planning context, Directorate 1110- Brussels, Belgium 2007.