NOVÉ HROZBY, NOVÁ KONCEPCIA, NOVÉ SPÔSOBILOSTI

NEW THREATS, NEW CONCEPTION, NEW COMPETENCE

Peter MARCHEVKA[1], Zuzana DIČEROVÁ[2]

SUMMARY:

The information and communication technologies (ICT) have for some time undergone turbulent developments. And it seems we have a period of turmoil ahead. The emergence of a new technology phenomenon brings with it people who will attempt to abuse it for committing crime. Likewise, the terrorists have developed new methods, forms and techniques of ICT, which led to cyber terrorism.
The paper aims to demonstrate that today the governments face a particular challenge as communication systems can be attacked in a split second impairing their vital functions. It also explores how the EU and NATO react towards this new threat. Being the member of both organizations, the Slovak Republic cannot afford to stand appart.

KEYWORDS: *cyber atac, cyber terrorism, information and communication technologies (ICT).*

ÚVOD

Počítače a internet sa stali neodmysliteľnou súčasťou každodenného života. Ich úlohou je uľahčiť život jednotlivcom, ale aj celej spoločnosti. Používajú sa na uchovávanie informácií, spracovávanie dát, posielanie a prijímanie správ, komunikáciu, na ovládanie strojov, kreslenie, písanie a v podstate sú použiteľné v každej oblasti života.

Obrovské možnosti počítačov podnecujú kriminálnikov a teroristov, aby ich používali ako hlavný nástroj na napadnutie cieľa. Internet poskytuje virtuálne „bojové pole“ pre krajiny, ktoré sú v konflikte s inou krajinou. Medzi príklady patrí Taiwan proti Číne, Izrael proti Palestíne, India proti Pakistanu, Čína proti Spojeným štátom americkým a mnoho ďalších.

Nové spôsoby a metódy terorizmu predstavujú jednu z najväčších hrozieb pre moderné demokratické spoločnosti. Predstavte si náboženských fundamentalistov, ktorí vedú svoju „svätú vojnu“ priamo zo svojho domova a všetko čo k tomu potrebujú, je počítač. Džihád cez internet? Ani zďaleka to nie je len hudba budúcnosti. Pokrok v oblasti informačných technológií so sebou už dnes prináša aj veľkú hrozbu. Je ňou kyberterorizmus.

Kyberterorizmus patrí k netradičným hrozbám, ktorým v súčasnosti čelí svet. Dnes je už možné, za relatívne nízke náklady, spôsobiť veľké škody pri minimálnom riziku odhalenia páchateľa. Kybernetický útok môže spôsobiť rozsiahle škody v ekonomike, infraštruktúre, ale môže ohroziť aj životy ľudí. Kyberterorizmus nepozná hranice štátov. Útoky na internet stále pribúdajú, a preto jednou z dôležitých úloh štátu je nájsť efektívny spôsob obrany a reakcie. V snahe bojovať proti takémuto terorizmu je potrebné vynaložiť veľa úsilia či už na úrovni jednotlivcov, krajín, regiónov alebo medzinárodnej úrovni.

Spoluautor britskej bezpečnostnej správy G. Day varuje pred kybernetickou hrozbou, ktorá môže vyústiť do kybernetickej vojny: „Vedenie konvenčnej vojny vyžaduje miliardy dolárov, pre vedenie kybernetickej vojny väčšina ľudí nájde zdroje veľmi ľahko.“

G. Day vo svojej správe považuje kybernetickú hrozbu za vážnejšiu ako jadrový úder. Platí tu zákonitosť, že čím modernejšie je krajina vybavená, tým nebezpečnejšiemu riziku je vystavená [12].

Skúsenosti s využitím praktík kybernetickej vojny získali Spojené štáty aj pri ochromení

[1] Peter MARCHEVKA, Ing., PhD., MO SR, Kutuzovova 8, Bratislava, e-mail: marchevkap@mod.gov.sk.
[2] Zuzana DIČEROVÁ, Ing., Mestský parkovací systém s. r. o., Biela 6, Bratislava, e-mail: dicerova.z@gmail.com.

irackej obrany v Iraku. Výhoda západnej vyspelej techniky má však aj slabé stránky. Chýba hlavne možnosť identifikácie nepriateľa.

1. NOVÉ BEZPEČNOSTNÉ HROZBY

Bezpečnosť v oblasti informačných technológií je kľúčovým problémom v každom modernom národnom hospodárstve. Dokonalé počítačové systémy sú dnes veľkou konkurenčnou výhodou vyspelých krajín, bez ktorých nemôžu fungovať. Súčasne však tým predstavujú aj ich najzraniteľnejšie miesto. Ide o to, ako zneužiť, poškodiť alebo zničiť informácie, prípadne informačné systémy protivníka (konkurencie) a súčasne uchrániť pred napadnutím svoje:
V roku 1997 bolo celá riadiaca veža letiska v meste Worcester znefunkčnená. V tom istom roku skupina švédskych útočníkov napadla záchranný systém 911 na Floride.

V apríli v roku 2002 nastala kolízia špionážneho lietadla amerických národných síl a čínskeho bojového lietadla. Tento konflikt vyústil do DoS (denial of service) útokov na americké internetové stránky.

Koncom januára 2003 sa podarilo preniknúť do privátnej počítačovej siete jadrovej elektrárne v USA červovi Win32/SQL.Slammer11. Červ infikoval existujúci Microsoft SQL Server a následne vyradil z činnosti bezpečnostný monitorovací systém na približne päť hodín do časti podnikovej siete spoločnosti FirstEnergy Corp

Medzi najznámejšie prípady kybernetických útokov z posledného desaťročia patrí aj séria útokov na americké štátne a vojenské internetové stránky v roku 2003 - Titánový dážď.

Predmetom útoku hackerov v Estónsku sa v roku 2007 stalo približne milión počítačov napadnutých pirátskym softwarom. Na internetové stránky estónskeho prezidentského úradu, parlamentu, ministerstiev, politických strán, médií, najväčších bánk a firiem, ktoré sa špecializujú na komunikáciu, sa nebezpečne rozmnožili hackerské útoky. Internetové stránky boli zaplavené desiatkami tisícov návštevníkov. Takýto nápor nezvládli a v podstate ich to paralyzovalo. Útok prebiehal na dôležité webstránky prostredníctvom obrovského množstva distribuovaných odmietnutí služby. Estónci sú presvedčení, že útoky boli nariadené a koordinované z Ruska – s jasným politickým pozadím. Rusko obvinenie odmietlo a prehlasovalo, že útoky zdanlivo pochádzali z IP adries ruských vládnych úradov, išlo o niekoho snahu poškodiť Rusko. Do vyšetrovania prípadu sa vložilo i NATO, ktoré vyslalo do Tallinnu niekoľko svojich najlepších odborníkov na kybernetický terorizmus. Podobný útok sa odohral v roku 2008 proti litovskej štátnej správe.

V roku 2008 bol významný najmä kybernetický útok na počítačovú sieť Ministerstva obrany USA. Pri tomto útoku boli niektoré súčasti počítačovej siete nefunkčné viac ako týždeň. Americkí vojenskí odborníci predpokladajú, že útok uskutočnili čínski vojenskí experti - naverbovaní hackeri. V tom istom roku hackeri odstránili na deň webové stránky gruzínskeho prezidenta Saakašviliho.

V Českej republike koncom roku 2010 hackeri vyradili tisíckami fiktívnych objednávok objednávkový systém Českej pošty práve v dobe, kedy bola zahltená predvianočnými nákupmi.

V januári 2011 Rakúsko, Česko, Grécko, Estónsko a Poľsko museli kvôli útokom hackerov uzavrieť svoje národné registre emisných povoleniek. V Česku sídliacej firme Blackstone Global Venture zmizlo z účtu skoro pol milióna emisných povoleniek v hodnote 6,8 mil. eur.

V auguste 2011 experti zo spoločnosti McAfee objavili doteraz najmasívnejší útok hackerov v histórii. Hackerom sa podarilo preniknúť do celkom 72 organizácií. Medzi obeťami boli napríklad Medzinárodný olympijský výbor, OSN, Svetový antidopingový výbor a rada veľkých firiem (zbrane, vývoj elektroniky...) a vládne organizácie (vlády USA, Vietnamu, Kanady, Tchaj-wanu...). Útok bol prekvapivo dlhodobý a prebiehal už od roku 2006. Spoločnosti McAfee sa podarilo zistiť detaily vďaka tomu, že sa dostali k jednému zo serverov, ktorý "zberal“ ukradnuté dáta. Cieľom útoku bolo zhromažďovať citlivé dáta štátneho tajomstva alebo obchodné informácie. Údaje boli zberané z rôznych zdrojov, napríklad z emailov, zdrojových kódov aplikácií alebo z vládnych sietí.

V posledný augustový týždeň bol vykonaný na internetový portál WikiLeaks kybernetický útok v čase, keď sa chystal zverejniť ďalšie tajné dokumenty americkej diplomacie.

V roku 2011 neznámi hackeri zaútočili na jednu z webových stránok Severoatlantickej

aliancie, ktorá však neobsahovala tajné informácie.

V poslednom období sa hovorí aj o záhadnom počítačovom víruse Stuxnet, ktorý napadol iránsky jadrový program a vážne poškodil odstredivky na obohacovanie uránu. Podľa západných počítačových odborníkov je tak vyspelý a účinný, že musel byť vytvorený v nejakom západnom štáte špeciálne pre Irán. Tak masívny útok totiž možno vykonať len so štátnou podporou. Odborníci sa zhodujú, že Stuxnet je najničivejší vírus, aký bol kedy vytvorený k útoku na priemyselné komplexy, reaktory a ich infraštruktúru. Je tak vyspelý a komplikovaný, že je mimo schopnosti obyčajných hackerov a mohli ho vytvoriť výlučne vojenskí počítačoví experti tak, aby napadol priemyselné kontrolné systémy vyrobené nemeckou firmou *Siemens* a preniesol tajné dáta do cudziny. Osobitosť a jedinečnú ničivosť vírusu potvrdilo aj počítačové oddelenie Pentagonu. Stuxnet trápi iránske systémy už dva mesiace a iránski experti zatiaľ netušia, ako proti vírusu bojovať. Irán preto tajne požiadal o pomoc predných svetových počítačových expertov. Nikto však zatiaľ svoje služby neponúkol, pretože Teherán odmieta oznámiť o víruse akékoľvek podrobnosti, rovnako ako spresniť miesto, kde by mali experti pracovať. Bezpečnostní analytici však dospeli k názoru, že vírus nakazil oveľa väčší počet počítačov a systémov, ako udáva Teherán (30.000), a to milióny. Ak by to bola pravda, išlo by o najväčší vírusový útok v dejinách.

Podľa správy spoločnosti McAfee sú veľké krajiny zapojené v „kybernetickej studenej vojne“ – navzájom sa špehujú a testujú svoje siete v pripravenosti na vojnu cez internet. Medzi tieto krajiny je možné zaradiť USA, Izrael, Rusko, Čínu a Francúzsko.

„Aj keď sme doposiaľ neboli svedkami ozajstnej kybernetickej vojny medzi veľkými krajinami, úsilie vytvárať schopné tímy expertov, ktorí by tieto útoky mohli podniknúť, je čím ďalej markantnejšie a naznačuje, že kybernetická studená vojna už začala,“ píše sa v správe *Virtually Here: The Age of Cyber Warfare* od McAfee. „V priebehu ďalších 20 až 30 rokov sa kybernetické útoky stanú bežnou súčasťou vojen,“ povedal William Crowell, bývalý vysoko postavený pracovník americkej štátnej Národnej bezpečnostnej agentúry - The National Security Agency - NSA. Bude hlavne chýbať rýchla možnosť identifikácie protivníka. Rovnako bezpečnostnú hrozbu predstavuje aj neregulovaná ekonomika a špekulatívne fungujúci bankový systém.[12]

2. EURÓPSKA ÚNIA

Aj v Európskej únii sa táto agenda dostala do ozornosti a postupne dobieha sklz v schopnostiach reagovať na kybernetické hrozby namierené na kritickú infraštruktúru jednotlivých krajín Únie.

V decembri 2008 prijala Rada Európy **smernicu 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr (ECI)** a zhodnotení potreby zlepšiť ich ochranu. Predstavuje prvú fázu etapovitého prístupu k identifikácii a označeniu ECI a zhodnoteniu potreby zlepšiť jej ochranu. Smernica sa zameriava najmä na sektor energetiky a dopravy, ktorý ich následne 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 (IKT) a iné. Čo je však potrebné zdôrazniť, primárnu a konečnú zodpovednosť za ochranu ECI nesú členské štáty a vlastníci alebo prevádzkovatelia kritickej infraštruktúry.

V roku 2010 Európska komisia pripravila 41 opatrení na zvýšenie bezpečnosti občanov Európskej únie, ktoré sú rozdelené do piatich kapitol. Komisia ponúka medziiným aj efektívnejší boj proti terorizmu, v rámci ktorého sa chce sústrediť na kyberterorizmus. V záujme odolávať jeho hrozbám plánuje exekutíva EÚ zriadiť ústredie počítačovej kriminality do roku 2014. Päť oblastí dokumentu tvorí rozloženie medzinárodných kriminálnych sietí, prevencia terorizmu, zvýšenie bezpečnosti občanov a podnikov v kybernetickom priestore, posilnenie bezpečnosti prostredníctvom inteligentného riadenia hraníc, zvýšenie odolnosti voči krízam a nešťastiam.

"Vnútorná bezpečnosť EÚ sa doteraz nevyznačovala jednotným prístupom a zameriavala sa vždy iba na jednu oblasť. Teraz však prijímame spoločný postup, ako budeme reagovať na bezpečnostné hrozby a výzvy budúcnosti. Terorizmus, organizovaný zločin, cezhraničná trestná činnosť, počítačová kriminalita a tiež krízy a katastrofy sú oblasti, ktoré vyžadujú, aby sme v záujme zvýšenia bezpečnosti našich občanov, podnikov a spoločností vynaložili spoločné úsilie a spolupracovali v rámci celej EÚ. Táto stratégia načrtáva možné hrozby a opatrenia,

ktoré je potrebné prijať, aby sme proti týmto hrozbám boli schopní bojovať. Vyzývam všetky zainteresované strany, aby prevzali zodpovednosť za implementáciu týchto opatrení a tým aj za posilnenie bezpečnosti EÚ," povedala komisárka pre vnútorné záležitosti Cecilia Malmströmová.[12]

Výrazne sa zvýšili aktivity jednotlivých štátov Európskej únie v kybernetickej bezpečnosti. Napríklad v priebehu roku 2010 sa objavilo niekoľko tlačových správ o tom, že armáda Veľkej Británie, Nemecka, Poľska a ďalších štátov vytvárajú špeciálne kybernetické jednotky a vykonávajú nábor IT špecialistov. Na výstave EOROSATORY 2010 Francúzsko dokonca oznámilo, že zahájilo vývoj tzv. digitálnych zbraní.

Globálny rozmer kybernetickej hrozby a charakter protiopatrení, ktoré presahujú informačné územie jednotlivých štátov, si vynútili pre oblasť kybernetickej obrany Európskej únie zriadenie ***Európskej agentúry pre bezpečnosť sietí a informácií*** - ***European Network and Information Security Agency - ENISA***, ktorá sa zaoberá identifikáciou digitálneho protivníka. Podľa nových pravidiel má práve agentúra podporiť svojou činnosťou užšiu spoluprácu medzi krajinami v oblasti virtuálnej bezpečnosti a zároveň naďalej propagovať riziká, ktoré pre EÚ kybernetické útoky predstavujú.[6]

3. NOVÁ STRATEGICKÁ KONCEPCIA NATO

Nová Strategická koncepcia NATO hneď v úvode potvrdzuje, že čl.5 Washingtonskej zmluvy, teda spoločná obrana proti ozbrojenej agresii, je na prvom mieste, vrátane obrany proti novým hrozbám pre bezpečnosť občanov Aliancie.

Z analýzy a odporúčaní skupiny expertov k novej Strategickej koncepcii NATO vyplýva:
Ochrana pred nekonvenčnými hrozbami. Za predpokladu, že NATO si naďalej udrží ostražitosť, je šanca priameho vojenského útoku na hranice Aliancie malá, aspoň v predvídateľnej budúcnosti. V súčasnej dobe by sa mohli objaviť skôr 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.

Odozva na rastúce nebezpečenstvo kybernetických útokov. NATO musí zrýchliť svoje úsilie pri reagovaní na ***nebezpečenstvo kybernetických útokov*** ochranou svojich vlastných komunikačných a veliteľských systémov, pomáhať spojencom zlepšovať ich schopnosti predchádzať útokom a obnoviť prevádzku po útokoch a vyvinúť škálu spôsobilostí kybernetickej obrany, zameraných na účinné odhaľovanie a odstrašovanie.

Reakcia na netradičné hrozby. Diskutované sú predovšetkým reakcia NATO na terorizmus, *kybernetická zraniteľnosť*, energetická bezpečnosť a klimatické zmeny. Je možné, že budú potrebné nové spôsobilosti.

Spôsobilosti obrany proti kybernetickým útokom*.* Najbližší významný útok na Alianciu môže prísť cez optický kábel. Doterajšie ***kybernetické útoky proti systému NATO*** sa opakujú mnohokrát, ale najčastejšie pod prahom politického záujmu. Avšak, riziko útoku veľkého rozsahu na rozhodovacie a kontrolné systémy NATO alebo na energetickú sieť by si zasluhovalo konzultácie podľa článku 4 a mohlo by viesť k opatreniam kolektívnej obrany v zmysle článku 5. Efektívna kybernetická obrana požaduje prostriedky na prevenciu, odhaľovanie, reakciu na a obnovu po útoku. NATO podniká kroky na rozvoj týchto schopností prostredníctvom vytvorenia ***Úradu pre riadenie kybernetickej obrany, Centra výnimočnosti pre spoluprácu v oblasti kybernetickej obrany*** a ***Spôsobilosti reakcie na počítačové incidenty***. Napriek tomu pretrvávajú trhliny v systéme kybernetickej obrany NATO. Strategická koncepcia pripisuje veľkú prioritu riešeniu týchto zraniteľností, ktoré sú neakceptovateľné a čoraz viac nebezpečné.

Odporúčania:

NATO by malo pripustiť, že kybernetické útoky sú rastúcou hrozbou bezpečnosti pre Alianciu a jej členov. Preto:

- veľké úsilie by malo byť venované rozširovaniu monitoringu kritickej siete NATO a zhodnoteniu a náprave akéhokoľvek nedostatku, ktorý bude odhalený,

- centrum výnimočnosti by malo robiť viac, prostredníctvom výcviku a pomáhať členom zlepšovať ich programy kybernetickej obrany,
- spojenci by mali posilňovať spôsobilosti včasného varovania pomocou širokej siete monitorovacích uzlov a snímačov NATO,
- Aliancia by mala byť pripravená vyslať expertný tím každému členovi, ktorý je ohrozený kybernetickým útokom,
- časom by malo NATO naplánovať vytvorenie adekvátneho spektra spôsobilostí kybernetickej obrany, vrátane pasívnych a aktívnych prvkov. [7]

Opatrenia na vytvorenie spôsobilosti

Najvyšší predstavitelia členských krajín NATO na **summite NATO v Lisabone v novembri 2010** vyzdvihli iniciatívu generálneho tajomníka NATO na budovanie nedostatkových spôsobilostí, ktoré sú potrebné pri odolávaní novým hrozbám s dôrazom na posilnenie kybernetickej obrany a na ochranu teritória a obyvateľstva európskych členských krajín a nasadených síl NATO proti tejto narastajúcej hrozbe.[4] Vytvorenie „***oddelenia pre nové bezpečnostné hrozby***" - „***emerging security challenges division – ESCD***" z podnetu generálneho tajomníka Andersa Fogha Rasmussena, nie je iba interným procesom, ale významným politickým posolstvom. NATO totiž po prvýkrát systematicky koordinuje svoju činnosť vo sférach, ktoré sa budú stúpajúcou mierou týkať bezpečnosti spojencov na oboch stranách Atlantiku: terorizmus, kybernetické útoky, ohrozenie energetických zdrojov a proliferácia zbraní hromadného ničenia.

Na prvý pohľad sa môže zdať, že tieto oblasti majú len málo spoločného. Avšak bližší pohľad na tento aspekt prezrádza, prečo k sebe patria z konceptuálneho hľadiska. Tieto hrozby zdieľajú totiž jednak určité spoločné charakteristiky, jednak konfrontácia s nimi vyžaduje zmenu koncepcie spojeneckej solidarity zo strany Aliancie a vzájomnú súčinnosť s medzinárodným spoločenstvom, zvlášť s civilnými aktérmi a súkromným sektorom.

Prvou ***spoločnou charakteristikou týchto nebezpečenstiev*** je skutočnosť, že nemusia nutne postihnúť všetkých spojencov rovnakým spôsobom. Teroristický útok na jedného spojenca môže vzbudiť kolektívne obavy, ale nemusí byť automaticky posudzovaný ako útok proti celej Aliancii. To sa zároveň týka kybernetických útokov na bankové systémy alebo útokov na energetické dodávky jednotlivých spojencov. Rozhodnutie, či je potrebné reagovať a akým spôsobom, záleží predovšetkým a jedine na štáte, ktorý bol napadnutý.

Na rozdiel od studenej vojny, kedy by útok Varšavskej zmluvy na niektorého spojenca NATO rozpútal kolektívnu odpoveď všetkých spojencov, dnešné hrozby by zrejme nedostali automatickú odpoveď. Spojenci NATO preto potrebujú úplne novú definíciu scenárov, ktoré budú predpokladom pre solidárnu pomoc Aliancie.

Druhou ***spoločnou charakteristikou týchto nových hrozieb*** je fakt, že nie vždy vyžadujú nevyhnutne vojenský zásah. Dobre orchestrovaný kybernetický útok môže paralyzovať celú krajinu spôsobom, ktorý mohol byť v minulosti dosiahnutý iba zahraničnou inváziou. V prípade, že by útočníkom bola napríklad niektorá nevládna organizácia, NATO by asi ťažko mohlo hroziť odvetnými vojenskými opatreniami.

Na druhej strane, proliferácia zbraní hromadného ničenia však môže vyprovokovať nasadenie nových vojenských obranných prostriedkov, napríklad riadených striel. Najlepším prístupom však naďalej zostáva stimulácia zmierňovania proliferácie riešením regionálnych bezpečnostných problémov a aplikáciou diplomaticko-ekonomickej metódy "biča a cukru". Stručne povedané, aj keď transatlantická spolupráca je nenahraditeľná pre konfrontáciu s novými bezpečnostnými hrozbami, "vojenský kufor s náradím" NATO už nestačí.

Tento aspekt vedie ***k tretej spoločnej charakteristike týchto nových hrozieb***: vzhľadom na to, že hrozby sú zahraničné i domáce, rovnako ako vojenské i ekonomické, vyžadujú holistický prístup. Konkrétne vyžadujú vybudovanie štruktúrovaných vzťahov medzi NATO a celou radou civilných aktérov.

To sa netýka iba ostatných najdôležitejších medzinárodných organizácií, ako sú OSN a Európska únia, ale taktiež nevládnych organizácií a súkromného sektoru, napríklad v oblasti energetiky a informačných technológií. Všetci títo aktéri sa musia stať partnermi v úsilí o riešenie bezpečnostných problémov vyprodukovaných globalizáciou. Vzhľadom na rozdiely v ich jednotlivých sférach pôsobnosti, kompetenciách a pracovných postupoch bude vybudovanie

dôvery a efektívnych vzťahov medzi nimi náročným procesom.

Niektorí spojenci možno váhajú priznať NATO dôležitejšiu úlohu na úseku energetickej bezpečnosti alebo proliferácie nukleárnych zbraní z dôvodu nadmernej militarizácie niektorých oblastí, ktoré majú zostať v politickom rámci. Iní môžu byť znepokojení nebezpečenstvom, že konfrontácia s týmito novými bezpečnostnými problémami môže odvracať pozornosť Aliancie od jej hlavného poslania - kolektívnej obrany. Tieto problémy môžu byt riešené a rozptýlené iba za predpokladu, že Aliancia bude venovať viac času jednaniu o nových hrozbách.

Je potrebná nová rovnováha medzi súčasnosťou a budúcnosťou: NATO musí zdokonaliť kultúru politickej diskusie, ktorá nie je obmedzená na problémy týkajúce sa priamo NATO po vojenskej stránke, ale ktorá zahrňuje zároveň problémy "výhradne" politického významu. Pokiaľ bude každá diskusia v NATO posudzovaná ako príprava vojenskej operácie, akákoľvek prezieravá a racionálna diskusia o nových hrozbách 21. storočia nebude seriózna. Aj úlohou oddelenia "***Nové bezpečnostné hrozby***" je prispievať k rozvoju tejto novej kultúry diskusie. Za použitia strategických analýz bude skúmať spektrum všetkých hrozieb, ktoré by sa mohli dotknúť bezpečnosti spojencov. Tento postup pomôže stimulovať diskusiu medzi spojencami a posilniť jedinečnú hodnotu NATO ako hlavné fórum pre bezpečnostné konzultácie medzi Európou a Severnou Amerikou, najsilnejšími spoločenstvami rovnako zmýšľajúcich národov.[8]

ZÁVER

Ako vyplýva z informácií o priebehu a výsledkoch **summitu NATO v Lisabone** konaného v **novembri 2010,** aj v rámci Slovenskej republiky bolo potrebné určiť garanta pre plnenie bezpečnostných cieľov Slovenskej republiky v oblasti kybernetickej obrany.[4] Slovenská republika má vyčleneného jedného príslušníka Ozbrojených síl Slovenskej republiky štruktúrach ***Centra výnimočnosti pre spoluprácu v oblasti kybernetickej obrany***.

Vzhľadom na to, že ochrana kyberpriestoru sa nedá vykonávať samostatne, bude musieť aj Slovenská republika získať spôsobilosti na jeho ochranu ako člena Európskej únie a NATO.

Vo svojom vystúpení na konferencii **Bezpečnostné fórum 2011** v Banskej Bystrici zástupca náčelníka Generálneho štábu ozbrojených síl Slovenskej republiky generálporučík Jaroslav Vývlek povedal, že „kybernetické útoky sú stále častejšie a sú lepšie organizované. Štáty NATO sa zatiaľ nedohodli, ako postupovať v tejto oblasti. Viaceré z nich majú možno „morálne" zábrany pri aplikácii nepopulárnych opatrení, ako napríklad obmedzenie občianskych práv pri používaní počítačov a internetu. Z histórie však dobre vieme, že nové zbrane najskôr používali zlodeji, ilegálne živly a potom našli „vládne pochopenie". Preto sa treba rýchlo spamätať a urýchlene budovať spôsobilosti kybernetického vojska. Príslušníci takéhoto vojska budú experti na programovanie a operácie a budú disponovať zručnosťami, akými dnes disponujú."

Ako zabezpečiť, aby príslušníci ozbrojených síl Slovenskej republiky takéto spôsobilosti získali a dokázali ich využiť aj v podmienkach kybernetickej vojny?

Doteraz sme poznali štyri dimenzie vojny – zem, more, vzduch a kozmos, ktoré sú štandardnými plánovacími faktormi pre vojnovú kampaň. Teraz pribudla piata dimenzia vo vojnovom umení – kybernetický priestor.

Nová dimenzia, možno hovoriť aj o virtuálnom priestore, súvisí s informačným vekom a poskytuje pre plánovanie želateľných stavov nové príležitosti a strategické voľby. Počítače ako unikátny „zbraňový nástroj" môžu pomôcť štátom dosiahnuť svoje strategické ciele bez fyzického ničenia. Piata dimenzia vo vojenskom umení musí rozširovať pole pre tvorbu koncepcií, resp. pohľadov do budúcnosti, pretože počítače sú nekonvenčnými bojovými nástrojmi. Útok na počítačovú sieť môže byť použitý na uľahčenie dosiahnutia strategických, operačných a taktických cieľov. Ďalej, pretože fyzická deštrukcia pri útokoch v kyberpriestore je zriedkavá, tvorcovia rozhodnutí ju našli ako atraktívnu voľbu v situácii krátkeho vojenského konfliktu. V súvislosti s novými informačnými a komunikačnými technológiami ide o rozvoj stratégie, ktorá zahŕňa: ochranu vojenských cieľov, informačných systémov, finančných stredísk, letovej prevádzky, energetických podnikov, energotrás a pod.[13] Tu vidím priestor pre akademickú obec pre realizáciu vo vzdelávacom procese.

LITERATÚRA

[1] BALABÁN, M., RAŠEK, A.: *Divoké karty v budoucím vývoji světové bezpečnosti: Trendy do roku 2040*. Vojenské rozhledy 2/2008, s. 3-17.
[2] BALABÁN, M., RAŠEK, A.: *Energetický kolaps*. The Science for Population Protection, 2/2009, s. 7-18.
[3] CLINTON, H. R.: *Prejav ministerky zahraničných vecí USA, seminár ku strategickému konceptu NATO*, 22.február 2010, Washington D.C..
[4] DI PAOLA, G.: *Globálne bezpečnostné výzvy a reakcia NATO, prejav predsedu vojenského výboru NATO*, Konferencii Silk Road, 2010, Turecko.
[5] GOLDGEIER J.: M.: *Budúcnosť NATO*, Špeciálne hlásenie výboru č.51, Výbor pre zahraničné vzťahy, február 2010.
[6] NIŽŇANSKÝ, J.: *K niektorým aspektom kybernetických útokov*, LÍDER č.1/2010, Účelová publikácia určená pre vnútornú potrebu ozbrojených síl Slovenskej republiky, OdVCD ŠbO GŠ OS SR, Bratislava 2010.
[7] RAŠEK, A.: *Divoké karty jako varovné prognózy aneb Jak by to jinak mohlo být*. Sondy, 22/2007, s. 15.
[8] SHARMA A.: *Kybernetické vojny: Vzorový prechod od prostriedkov k výsledkom, z knihy The Virtual Battlefield: Perspectives on Cyber Warfare*, vydané Cooperative Cyber Defence Centre of Excellence, Tallinn, Estónsko, 2009, ISBN 978-1-60750-060-5.
[9] Deklarácia hláv štátov a vlád NATO, november 2010, Lisabon.
[10] Informácia o priebehu a výsledkoch summitu NATO v Lisabone v dňoch 19. – 20. novembra 2010.
[11] Nariadenie Európskeho parlamentu a Rady ES č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sieti a informácií.
[12] NATO 2020: zaistená bezpečnosť; dynamické zapájanie sa. Analýza a odporúčania skupiny expertov pre nový strategický koncept NATO, Analýza a odporúčania skupiny expertov pre nový strategický koncept NATO, skupina expertov pod vedením Madeleine K. Albright.
[13] Strategická koncepcia pre obranu a bezpečnosť členov Severoatlantickej zmluvy, november 2010, Lisabon.
[14] Zdroj: CNET, *http://news.cnet.com/8301-27080_3-10399141-245.html*.
[15] Zdroj: *www.euractiv.sk/.../eu-stupnuje-boj-proti-kybernetickym-utokom-015969*.