Source: Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki humanistyczne, społeczne i techniczne

Acta Scientifica Academiae Ostroviensis. Sectio A, Humanities, social and technical sciences

Location: Poland

Author(s): Pavel Nečas, Matúš GREGA

Title: Kybernetická obrana: strategická úloha severoatlantickej aliancie a jej národné implikácie

Cyber defence: strategic role of nato and its national implications

Issue: 1/2016

Citation style: Pavel Nečas, Matúš GREGA. "Kybernetická obrana: strategická úloha severoatlantickej aliancie a jej národné implikácie". Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki humanistyczne, społeczne i techniczne 1:306-322. https://www.ceeol.com/search/article-detail?id=561488

ARTYKUŁY NAUKOWE

ASO.A.7(1)/2016/306-322
ISSN 2300-1739

Pavel NEČAS •
Matúš GREGA ••

Kybernetická obrana: strategická úloha severoatlantickej aliancie a jej národné implikácie

Cyber defence: strategic role of nato and its national implications

Streszczenie: Informačná technika sa rozvíja mimoriadne významným spôsobom. Stala sa na jednej strane strategickým prostriedkom priemyslu, administratívy, bankového sektoru, ale napríklad aj ozbrojených síl. V posledných rokoch sa ukazuje, že hoci digitálny svet prináša obrovské výhody, je aj zraniteľný. Incidenty v rámci kybernetickej bezpečnosti , či už úmyselné, alebo náhodné, narastajú alarmujúcim tempom a mohli by narušiť poskytovanie základných služieb, ktoré považujeme za samozrejmé, ako je zásobovanie vodou, zdravotná starostlivosť, dodávka elektrickej energie alebo mobilné služby. Hrozby môžu mať rôzny pôvod – vrátane zločineckých, politicky motivovaných, teroristických alebo štátom podporovaných útokov, ako aj prírodných katastrof a neúmyselných chýb. Rozvoj informačných a komunikačných technológií má teda aj svoju tienistú stránku. Kybernetický priestor, tak ako svet fyzický, ponúkol možnosť realizácie sa negatívnej stránke človeka, ktorá má za následok vznik nových bezpečnostných hrozieb.

Słowa kluczowe: Informačná technika, kybernetický priestor, NATO, bezpečnostné výzvy, iregulárne hrozby, národné záujmy

Abstract. Information technology is developing extremely significant. It has become the one of the strategic means of industry, administration, banking sector, but also the armed forces. In recent years, it appears that although the digital world brings enormous benefits, is also vulnerable. Incidents within the cyber security, whether intentional or accidental, are increasing at an alarming rate and could disrupt the delivery of basic services that we take for granted, such as water supply, health care, power supply and mobile services. The threats may have different sources - including criminal and politically motivated terrorist or state-supported attacks as well as natural disasters and unintentional errors. The development of ICT has therefore without its drawbacks. Cyberspace as a physical world, offered the possibility of carrying out the negative side of man, which has resulted in the emergence of new security threats.

Key words: information technology, cyber space, NATO, cyber defence, cyber security, irregular threats

Received: 03.2016

Accepted 06.2016

• prof. Ing., PhD. Ústav občianskej bezpečnosti, Vysoká škola bezpečnostného manažérstva v Košiciach

•• kpt. Ing., Simulačné centrum, Akadémia ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši

Úvod

Sektor komunikačných a informačných technológií v súčasnosti predstavuje jednu z najrýchlejšie sa rozvíjajúcich oblastí spoločnosti. Výrazne sa premieta nielen do súkromnej a ekonomickej sféry, ale čoraz viac aj do štátnej a verejnej správy a tým aj do oblasti obrany a bezpečnosti [IVANČÍK 2012]. Vznik celosvetovej komunikačnej a informačnej siete, masívne využívanie počítačov, internetizácia spoločnosti, digitálne spracovanie informácií a obchodovanie s nimi, ako aj prenos dát a informácií prostredníctvom sietí na veľké vzdialenosti vedú k prehlbujúcej sa závislosti vyspelých štátov sveta a ich ekonomík na komunikačných a informačných technológiách, k zvyšovaniu vzájomnej prepojenosti i závislosti, a zároveň k "zmenšovaniu" vzdialeností medzi nimi. Tento technologický pokrok však prináša nielen nové príležitosti, výzvy a prosperitu, ale aj nové bezpečnostné riziká a hrozby. Preto sa čoraz dôležitejšou a naliehavejšou stáva ochrana kybernetického priestoru a kritickej informačnej infraštruktúry, čiže zaistenie kybernetickej bezpečnosti [IVANČÍK, KAZANSKÝ 2015].

Aj preto problematika kybernetickej bezpečnosti a obrany jednoznačne zaberá aj v rámci Severoatlantickej aliancie neustále prominentnejšiu úlohu. Je možné konštatovať, že Aliancia sa začala touto témou vážnejšie zaoberať až počas ostatných piatich rokov.

Ešte pred pár rokmi, boli kybernetické nebezpečenstvá a súvisiace bezpečnostné problémy a hrozby diskutované iba v úzkych kruhoch technikov a expertov. Aj NATO si však stále viac uvedomuje, že kybernetický svet znamená vážnu zraniteľnosť pre stále viac vzájomne prepojené spoločenstvá, Alianciu nevynímajúc. Kybernetické útoky patria medzi tie hrozby, ktorým budú štáty musieť čeliť v nasledovných rokoch stále výraznejšie. Kybernetické konflikty sa stávajú súčasťou tradične vedených konfliktov a „digitalizované" krajiny jednoducho musia pracovať na konkrétnych plánoch ako reagovať s cieľom ochrániť svoj kybernetický priestor, a tak aj svoje národné záujmy.

Za posledných necelých desať rokov, kedy sme boli svedkami prvých kybernetických útokov namierených proti určitým krajinám ako doplnok alebo súčasť politického a vojenského konfliktu. Príkladom kybernetických útokov ako súčasť politického boja možné uviesť Estónsko v roku 2007. Gruzínsko v roku 2008 bolo zasa príkladom využitia kybernetických útokov ako doplnok k útokom kinetickým počas rusko-gruzínskej vojny.

Aliancia schválila viacero dokumentov, ktoré stanovujú matricu ďalšieho vývoja a základné rámce politiky NATO v tejto oblasti. Dôležitá však bude najmä implementácia týchto dokumentov. Otázok zostáva nezodpovedaných viacero: Má NATO prevziať komplexnú zodpovednosť za siete svojich členských krajín? Má si Aliancia vypracovať plány reakcie na masívny útok v kyber priestore?

Cieľom tohto vedeckého článku je charakterizovať aktuálny vývoj v tejto agende v NATO, pokúsiť sa zodpovedať stanovené otázky a načrtnúť smer, ktorým by sa mala Aliancia uberať v nasledovných mesiacoch, najmä smerom k plánovaným summitom Aliancie. Cieľom je tiež upozorniť, aké kroky je potrebné vykonať na národnej úrovni v SR s cieľom priblížiť národné štandardy stanoveným postupom a opatreniam na úrovni NATO, EÚ či iných relevantných medzinárodných aktérov.

NOVÁ HROZBA (AJ PRE NATO)

Kybernetické ohrozenie je vo všeobecnosti považované za novú vznikajúcu hrozbu. Prvýkrát bola problematika kybernetickej obrany spomenutá až v Strategickej koncepcii Aliancie z roku 1999. Na Washingtonskom summite Severoatlantická aliancia vôbec po prvýkrát vo svojom oficiálnom dokumente zaradila „informačné systémy a závislosť NATO na nich, ako potenciálnu hrozbu pri eliminácii prevahy NATO v tradičných zbraňových systémoch“ [Strategická koncepcia NATO 1999, 5, http://www.mzv.sk].

Rok po dátume 11/9/2001, ktorý sa ukázal byť prelomovým vo vnímaní nových bezpečnostných hrozieb, vydala NATO dôležitú “výzvu k zdokonaleniu schopností nutných pre obranu proti kybernetickým útokom“ [http://www.nato.int/] v rámci záväzku k schopnostiam, vyhláseným počas summitu v Prahe, v novembri 2002. V nasledujúcich rokoch sa však Aliancia orientovala predovšetkým na implementáciu pasívnych ochranných opatrení, ktoré vyžadovali ozbrojené sily.

Až udalosti v Estónsku, na jar roku 2007, prinútili Alianciu k radikálnemu prehodnoteniu koncepcie kybernetickej obrany a k protiopatreniam nového formátu. Aliancia preto vypracovala dokonca po prvýkrát oficiálny dokument “Politika kybernetickej obrany NATO” [THEILER, http://www.nato.int], ktorý bol schválený v roku 2008, a ktorý stanovil tri hlavné piliere politickej koncepcie kybernetickej obrany Aliancie: 1) Subsidiarita, napr. asistencia je poskytovaná iba na žiadosť; inak je zachovávaná zásada vlastnej zodpovednosti zvrchovaných štátov; 2) Zamedzenie duplikácii, napr. predchádzanie zbytočnej duplikácie

štruktúr a schopností na medzinárodnej, regionálnej i národnej úrovni; 3) Bezpečnosť, napr. spolupráca založená na vzájomnej dôvere, so zreteľom na senzitivitu informačného systému, ktorý musí byť dostupný a na eventuálnu zraniteľnosť.

Táto koncepcia znamená veľký kvalitatívny krok vpred a zároveň otvorila cestu zásadnému rozhodnutiu z lisabonského summitu kontinuálne pokračovať v zdokonaľovaní kybernetickej obrany. NATO vypracovalo prvé mechanizmy a schopnosti kybernetickej obrany a koncipovalo osnovu Politickej koncepcie kybernetickej obrany.

Vývoj vo vnímaní kybernetickej obrany, ako dôležitej súčasti komplexnej obrannej mozaiky budovanej NATO, je zrejmý aj pri čítaní aktuálnej Strategickej koncepcie NATO prijatej v roku 2010 v Lisabone. Problematike kybernetickej bezpečnosti a obrany je tam venovaný výrazne väčší priestor, pričom okrem definovania kybernetických útokov ako novej hrozby v bezpečnostnom prostredí (paragraf 12) navrhuje Aliancia (paragraf 19) celú sériu opatrení, ktoré je nevyhnutné realizovať s cieľom odstrašiť a ubrániť Alianciu proti tejto hrozbe: „Zaistíme, aby NATO malo plný rozsah spôsobilostí potrebných na odstrašovanie a obranu proti akejkoľvek hrozbe voči bezpečnosti našich obyvateľov. Z tohto dôvodu budeme ďalej rozvíjať našu schopnosť prevencie, detekcie, obrany proti kybernetickým útokom a obnovy po nich, vrátane využitia procesu plánovania NATO na zlepšenie a koordináciu národných spôsobilostí kybernetickej obrany, zaistenia centralizovanej kybernetickej ochrany pre všetky orgány NATO a lepšieho integrovania kybernetickej informovanosti, varovania a reagovania členských krajín“ [Strategická koncepcia NATO 2010, 2-3, http://www.mzv.sk].

Na základe rozhodnutí summitu v Lisabone, v novembri 2010, Aliancia vytvorila úspešné predpoklady pre autonómne riadenie a konkrétne skúmanie kybernetickej obrany a pre vytvorenie konkrétnych opatrení na reakciu v prípade potreby. Následne boli vypracované a schválené základné dokumenty NATO pre kybernetickú obranu: Koncept kybernetickej obrany NATO (2011), Politika NATO v oblasti kybernetickej obrany (2011) a najmä Akčný plán pre kybernetickú obranu NATO (2011), ktorého implementácia má a v nasledovných rokoch bude mať reálny dopad na úroveň spôsobilostí NATO a jej členov v tejto oblasti.

SPEKTRUM HROZIEB

Aj napriek rastúcej použiteľnosti ofenzívnych kybernetických spôsobilostí v zločineckých sieťach či teroristických organizáciách, doposiaľ sú stále najnebezpečnejšími aktérmi v oblasti kybernetických agresií zvrchované štáty, ktorých aktivity sa vyznačujú vysoko sofistikovanou špionážou či sabotážou kybernetických sietí.

Ohrozenia pochádzajúce z kybernetického priestoru sú potenciálne širokospektrálne. Pri istej miere zjednodušenia môžeme hrozby existujúce v kybernetickom priestore rozdeliť do štyroch základných podskupín: a) kybernetické vedenie vojny, b) kybernetický terorizmus, c) kybernetická špionáž a d) kybernetická kriminalita, ktoré sa líšia svojimi cieľmi, postupmi a aj následnými možnými škodami. Z hľadiska sofistikovanosti a komplexnosti, vedci z Univerzity Georgetown definujú tri úrovne kybernetického ohrozenia: 1) Jednoducho štruktúrované: Spôsobilosť vykonávať základné útoky (hacky) proti jednotlivým systémom s využitím nástrojov vytvorených niekým iným. Útočiaca organizácia má malú cieľovú analýzu, velenie a riadenie a tiež nízku schopnosť učenia. 2) Pokročilo štruktúrované: Spôsobilosť vykonávať zložitejšie útoky rôznych systémov alebo sietí a prípadne upraviť alebo vytvoriť základné hackerské nástroje. Útočiaca organizácia má elementárnu cieľovú analýzu, velenie a riadenie a tiež elementárnu schopnosť učenia. 3) Komplexne koordinované: Spôsobilosť koordinovaného útoku, ktorý môže spôsobiť masové narušenie integrovanej heterogénnej obrany (vrátane šifrovania). Schopnosť vytvárať sofistikované hackerské nástroje. Veľmi schopný cieľ analýzy, velenie a riadenie a organizácia schopnosť učenia [DENNING, http://www.cs.georgetown.edu].

KYBERNETICKÉ VEDENIE VOJNY

Niet pochybnosti o tom, že niektoré štáty masívne investujú do kybernetických spôsobilostí, ktoré je možné aplikovať na vojenské účely. Na prvý pohľad sú závody v numerickom zbrojení založené na jasnej a nevyhnutnej logike, pretože kybernetické vedenie vojny poskytuje mnohé výhody: asymetrickosť, nízke náklady, celkové prednosti sú spočiatku na strane útočníka. Okrem toho, v kybernetickom vedení vojny neexistuje efektívne zastrašovanie, pretože už len identifikácia útočníka je extrémne ťažká a dodržovanie medzinárodných práv je zrejme neaplikovateľné [Nové hrozby- kybernetické dimenzie, http://www .nato.int]. Za týchto okolností je akákoľvek forma vojenských represálií veľmi

problematická, ako po stránke právnej, tak politickej. Ako už bolo uvedené, v nedávnej minulosti môžeme evidovať viacero konkrétnych príkladov kybernetických útokov ako doplnku symetrických útokov (napr. kosovský konflikt, konflikt Rusko-Gruzínsko).

KYBERNETICKÝ TERORIZMUS

Kybernetický terorizmus definuje webový portál ako použitie útokov na báze internetu v teroristickej činnosti, vrátane aktov úmyselného rozsiahleho narušenia počítačových sietí, najmä osobných počítačov pripojených k internetu, prostredníctvom nástrojov, ako sú počítačové vírusy a pod. Ciele takéhoto konania musia byť politické alebo ideologické.

Technika kybernetických útokov sa zreteľné rozvíja z bežných nepríjemností na vážne bezpečnostné hrozby pre informačné zariadenia a dokonca aj pre dôležité národné infraštruktúry (ekonomické či bezpečnostné). Príklad pre fyzické škody na majetku rozsiahleho charakteru a reálny kinetický kybernetický terorizmus veľkého rozsahu zatiaľ nie je verejne dostupný. Je však možné konštatovať, že je iba otázkou času, kedy niektorá z krajín bude musieť čeliť najvyššiemu ohrozeniu spojenému s kyber terorizmom.

KYBERNETICKÁ ŠPIONÁŽ

Kybernetická špionáž je akt získania tajomstva, resp. utajovanej skutočnosti, bez súhlasu pôvodného držiteľa takejto informácie. Tieto informácie môžu byť osobného, senzitívneho alebo oficiálne utajovaného charakteru. Môžu pochádzať od jednotlivcov, rôznych ekonomických či politických skupín alebo vlád. Záujem o ich získanie môže byť z dôvodov osobných, ekonomických, politických alebo vojenských. Tieto informácie sa získavajú pomocou použitia rôznych metód v sieti Internet alebo cestou využitia jednotlivých počítačových systémov (alebo mobilných telefónov) pomocou škodlivého softvéru, vrátane využitia trójskych koňov a/alebo spywarov.

Kybernetická špionáž môže byť páchaná on-line odborníkmi vo vzdialených krajinách alebo je realizovaná priamou infiltráciou domácich zariadení. Môže byť tiež dielom zlomyseľných amatérskych hackerov či programátorov. Cieľom je prístup k tajomstvu a utajovaným informáciám alebo ovládanie jednotlivých počítačov alebo celých sietí pre strategickú výhodu a psychologické, politické a fyzické podvratné činnosti a sabotáž.

Podľa zverejnených údajov [Nato suffered 2 500 cyber attacks in 2012. http://www.telegraph.co.uk] NATO čelilo v priebehu roku 2012 viac ako 2500 kybernetickým útokom, pričom „približne desať útokov mesačne" je možné považovať za koordinované a podporované cudzou mocnosťou s cieľom získať utajované informácie NATO.

KYBERNETICKÁ KRIMINALITA

Termínom kybernetická kriminalita sa označujú trestné činy zamerané proti počítačom alebo trestné činy páchané pomocou počítača. Ide o nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. Vo všeobecnosti evidujeme jej štyri najvýraznejšie prejavy: 1) Podvody, sprenevery – Predovšetkým sa týkajú finančnej sféry. Do tejto oblasti tiež patria prieniky do počítačových systémov a elektronického bankovníctva zvonku. 2) Falšovanie – najmä peňazí a dôležitých listín. K tomuto trestnému činu je potrebný len príslušný grafický software a kvalitnú tlačiareň. 3) Elektronická pomsta a ohováranie – jedným zo spôsobov prevedenia je šírenie nepravdivých informácií po internete, ktorého cieľom je pošpinenie cti určitej osoby alebo osôb, kedy môže dôjsť aj k zásahu do osobného alebo pracovného života. Ďalším spôsobom, ako sa niekomu pomstiť prostredníctvom internetu je zverejnenie osobných údajov. 4) Hoax – čiže nepravdivé varovanie. Obsahom týchto správ môže byť čokoľvek, dôležité je, aby svojim oznámením spôsobili obavy, resp. strach používateľov. Hoax je schopný ovplyvniť veľa používateľov a spôsobiť paniku a následné škodlivé konanie (napríklad problémy bánk, keď sa šíri hoax o krachu banky, ktorý má za následok masívny výber hotovosti).

AKTUÁLNY VÝVOJ V NATO

Je zrejmé, že problematika kybernetickej obrany sa v ostatných mesiacoch dostáva do absolútneho popredia agendy NATO. Estónsko sa pravidelne viac či menej úspešne snažilo dostať túto otázku na rokovanie vrcholných orgánov NATO už od udalostí z jari 2007, keď bola sieťová infraštruktúra krajiny komplexne napadnutá a tento útok spôsobil masívne škody. Následne bola schválená Politika NATO v kybernetickej obrane, ktorá definuje kybernetické hrozby ako potenciálny zdroj kolektívnej obrany, v zmysle článku 5 Washingtonskej zmluvy. Okrem toho, nová Politika NATO v kybernetickej obrane a Akčný plán jej implementácie, poskytuje členským štátom NATO príslušné direktívy a schválený zoznam priorít,

ktorých cieľom je pokrok Aliancie v kybernetickej obrane, vrátane zdokonalenia koordinácie medzi spojencami a s partnermi NATO.

V poslednom období sa k Estónsku snažiacemu sa povýšiť úroveň vnímania ohrozenia spojencov v NATO prostredníctvom kyber útoku pridali aj USA, Francúzsko či Veľká Británia, čo je možné zdôvodniť výrazne rastúcim počtom kybernetických útokov na tieto krajiny, ktoré pochádzajú pravdepodobne z Ruska, Číny, Iránu či Severnej Kórei. Dôsledkom prebiehajúcej intenzívnej diskusie v pracovných skupinách či výboroch bolo samostatné rokovanie ministrov obrany členských krajín NATO na tému kybernetickej obrany 4. júna 2013. Dôvodov bolo viacero: Ako už bolo spomenuté, viaceré krajiny a aj NATO samotné čelia kybernetickým útokom prakticky denne (v priemere viac ako 7 útokov na NATO denne [Nato suffered 2 500 cyber attacks in 2012. http://www.telegraph.co.uk]). Viaceré členské krajiny NATO majú vybudované veľmi limitované mechanizmy na potlačenie kybernetického útoku, a preto Aliancia po prvýkrát zaradila úlohy v oblasti budovania spôsobilostí v tejto oblasti medzi tzv. Národné ciele pre spôsobilosti.

ROZDELENIE ZODPOVEDNOSTI V OBLASTI KYBERNETICKEJ OBRANY

V zmysle Politiky NATO v oblasti kybernetickej obrany poskytuje Severoatlantická rada politický dohľad nad všetkými aspektmi jej implementácie. Rada je informovaná o závažných kybernetických incidentoch a útokoch. Výbor pre obrannú politiku a plánovanie zabezpečuje dohľad a poradenstvo na odbornej úrovni. Správna rada NATO pre kybernetickú obranu (CDMB) má na pracovnej úrovni zodpovednosť za koordináciu kybernetickej obrany medzi civilnými a vojenskými orgánmi NATO. Tento orgán pracuje pod záštitou Divízie NATO pre vznikajúce bezpečnostné výzvy.

Na technickej úrovni je dôležitá činnosť Rady NATO pre konzultácie, velenie a riadenie (NC3Board), ktorá je hlavným orgánom zodpovedným za konzultácie o technických aspektoch kybernetickej obrany.

Vojenské orgány NATO a Agentúra NATO pre komunikačné a informačné systémy (NCIA) nesú zodpovednosť za prevádzkové požiadavky, obstarávanie, implementáciu a prevádzkovanie spôsobilostí NATO v oblasti kybernetickej obrany. NCIA je prostredníctvom svojho technického centra NCIRC [NCIRC – NATO Computer Incident Response Capability] zodpovedná za poskytovanie technických a prevádzkových služieb kybernetickej bezpečnosti v celej NATO.

Technické centrum NCIRC predstavuje hlavnú technickú a prevádzkovú spôsobilosť NATO a má kľúčovú úlohu v reakcii na kybernetickú agresiu proti Aliancii [Nové hrozby – kybernetické dimenzie. http://www.nato.int]. Threat Assessment Cyber Cell (CTAC) je tiež umiestnený spoločne s NCIRC.

Aliancia sa v súčasnosti venuje v oblasti kybernetickej obrany viacerým konkrétnym iniciatívam s cieľom komplexne vyskladať mozaiku konkrétnych opatrení a spôsobilostí potrebných v boji proti kybernetickým hrozbám. Medzi najhlavnejšie môžeme zaradiť nasledovné:

Integrácia kybernetickej obrany do procesu obranného plánovania NATO

V súlade s mandátom z lisabonského summitu bola v apríli 2012 kybernetická obrana začlenená do procesu obranného plánovania NATO (NDPP). NDPP je kľúčovým nástrojom Aliancie s cieľom poskytnúť rámec, v ktorom môžu byť národné a aliančné plánovacie činnosti harmonizované pri plnení cieľov v oblasti budovania spôsobilostí čo najefektívnejším spôsobom. Je zaujímavé spomenúť, že všetky členské krajiny, ktorým boli ciele v oblasti budovania spôsobilostí v kybernetickej obrane alokované, s nimi aj v plnej miere súhlasili.

Ciele v oblasti kybernetickej obrany boli tiež integrované do iniciatívy Smart defence. Inteligentná obrana je nový spôsob myslenia, ktorý umožňuje krajinám spolupracovať na rozvoji a udržiavaní spôsobilostí, ktoré si členské krajiny nemôžu dovoliť vyvíjať alebo obstarať samotné.

Výskum a odborné vzdelávanie

Keďže oblasť kybernetickej obrany sa neustále vyvíja, existuje potreba z dlhodobého hľadiska inštitucionalizovať spoločné vzdelávanie a výcvik v tejto oblasti. Z uvedeného dôvodu NATO spracovalo dokument Koncept NATO pre vzdelávanie a výcvik v oblasti kybernetickej obrany. Ide o záujem Aliancie zrýchliť svoje úsilie v oblasti vzdelávania a odbornej prípravy prostredníctvom existujúcich škôl a tiež Centra výnimočnosti pre oblasť kybernetickej obrany v Tallinne v Estónsku [NATO Center of Excellence for Cyber Defence. http://www.ccdcoe.org]. Toto centrum, ktoré bolo akreditované zo strany NATO aj EÚ v roku 2008, vykonáva výskum a odbornú prípravu pre kybernetickú obranu odborníkov z aliančných štruktúr, členských krajín oboch organizácií, vrátane odborníkov zo sponzorských a partnerských krajín.

Rovnako dôležitým ako zintenzívnenie a štandardizácia procesov vzdelávania a výcviku je tiež organizácia pravidelných cvičení krízového manažmentu [GREGA, BUČKA, 2012]. V novembri 2012 cvičenie NATO (CMX12) a koalície krajín (Cyber Coalition 2012) ponúklo vynikajúcu príležitosť na testovanie a konzultácie postupov pri riešení kybernetickej krízy. Podobné cvičenia sú plánované každý rok.

POMOC JEDNOTLIVÝM SPOJENCOM

Prioritou NATO v oblasti kybernetickej obrany je chrániť komunikačné systémy a siete vlastnené a prevádzkované Alianciou. Ochrana národných kritických infraštruktúr zostáva v právomoci členských štátov, čo si vyžaduje, aby národy investovali adekvátne zdroje (personálne a finančné) do rozvoja vlastných spôsobilostí. NATO pomáha spojencom v ich úsilí vybudovať adekvátnu národnú kybernetickú obranu prostredníctvom zdieľania informácií a osvedčených postupov a už spomínanou účasťou národných predstaviteľov na realizovaných medzinárodných cvičeniach.

Okrem uvedeného v súčasnosti prebieha na aliančnej pôde tiež diskusia o možnom nasadení kolektívnej aliančnej spôsobilosti, ako reakcie na kybernetický útok voči členskej krajine, ak táto o kolektívnu pomoc požiada. Ministri obrany členských krajín NATO sa na svojom rokovaní 4. 6. 2013 dohodli na pokračovaní tejto diskusie a výstupov jej následnej aplikácie.

V SPOLUPRÁCI S PARTNERMI A MEDZINÁRODNÝMI ORGANIZÁCIAMI

Spolupráca s partnermi NATO a medzinárodnými organizáciami, vrátane Európskej únie, je dôležitým prvkom politiky NATO v oblasti kybernetickej obrany. V súčasnosti prebiehajú diskusie spojencov o konkrétnych modalitách spolupráce. Každopádne by bolo iracionálnym riešením pre tie členské krajiny NATO, ktoré sú zároveň aj členmi EÚ [Ide celkovo o 23 z celkového počtu 28 členských krajín NAT], aby vypracovali duplicitné procedúry v oblastiach ako sú napr. krízové riadenie, vzdelávanie, školenie a výcvik, atď. Spolupráca teda musí prebiehať na základe spoločných hodnôt a spoločných prístupov s dôrazom na komplementárnosť a vylúčenie duplicít.

Ciele na budovanie spôsobilostí v kybernetickej obrane boli začlenené tiež do približne 75% z dvojstranných programov spolupráce, ktoré boli dohodnuté s jednotlivými partnermi. Švédsko, Fínsko a EÚ sa zúčastnili tiež cvičenia CMX12,

viaceré partnerské krajiny sa zúčastnili tiež cvičenia Cyber Coalition 2012, Európska únia bola prítomná v úlohe pozorovateľa.

Spolupráca s priemyslom

Rozvoj partnerstva s priemyslom je zásadným krokom smerujúcim k zabezpečeniu účinnej kybernetickej obrany v rámci členských štátov NATO a tiež pre Alianciu samotnú. Partnerstvo s priemyselnou oblasťou by malo v čo najväčšej miere zahŕňať výmenu informácií, tzv. lessons learnt, spoluprácu v krízovom riadení, v plánovaní a tiež spoločnú participáciu na cvičeniach. Napriek istému pozitívnemu posunu je v tomto smere ešte výrazný priestor na zintenzívnenie spolupráce. CNAD [CNAD – Konferencia národných riaditeľov pre vyzbrojovanie v NATO] ako aj NIAG [NIAG – Skupina poradcov pre priemyselnú oblasť v NATO] by mali spoločne s predstaviteľmi priemyslu hľadať ďalšie konkrétne formy vzájomne prospešnej spolupráce.

Implikácie pre SR

Problematike kybernetickej obrany, resp. budovaniu národných spôsobilostí potrebných pre uskutočňovanie ofenzívnych a defenzívnych operácií v kybernetickom priestore, nie je v Slovenskej republike venovaná dostatočná pozornosť. Tento stav sa odzrkadľuje aj v nedostatočnom budovaní obranných a útočných spôsobilostí pre potrebu presadzovania národných záujmov. Na druhej strane je však potrebné priznať, že aj vďaka stále intenzívnejšiemu vnímaniu tejto témy zo strany medzinárodných organizácií, najmä NATO a EÚ, sa záujem zodpovedných organizácií v ostatnej dobe zvyšuje. Každopádne je možné konštatovať, že celková problematika je v relatívne počiatočnom stave svojho budovania. V podmienkach Slovenskej republiky je problematika bezpečnosti kybernetického priestoru rozpracovaná vo forme stratégií a koncepcií, tie sú však zamerané predovšetkým na informačnú bezpečnosť, rozvoj informačnej spoločnosti a ochranu kritickej infraštruktúry.

Význam kybernetického priestoru a jeho bezpečnosti bol prvýkrát v Slovenskej republike oficiálne zdôraznený v najvyššom strategickom bezpečnostnom dokumente Bezpečnostnej stratégii Slovenskej republiky z roku 2001, ktorá zadefinovala zneužitie informačných technológií, narušenie alebo úplné zlyhanie informačných systémov štátu v dôsledku terorizmu a pirátstva ako jednu z potenciálnych hrozieb pre bezpečnosť Slovenskej republiky [Bezpečnostná stratégia Slovenskej republiky 2001, http://www.merlin.ndu.edu]. O štyri roky

neskôr, Bezpečnostná stratégia Slovenskej republiky z 27. septembra 2005 bola vo vzťahu k hrozbám v kybernetickom priestore konkrétnejšia: „Miera informatizácie spoločnosti dosiahla vysoký stupeň a stále sa zvyšuje. Výkonnosť techniky, revolučné informačné a komunikačné technológie, nárast rýchlosti prenosu informácií a ich globálnej dostupnosti spôsobujú rýchlu globálnu premenu postindustriálnej spoločnosti na spoločnosť informačnú. Zraniteľnosť informačných a komunikačných systémov, ich preťaženie, neoprávnený prístup k informáciám, šírenie počítačových vírusov a dezinformácií sú rastúcou hrozbou pre SR [Bezpečnostná stratégia SR 2005. www.sfpa.sk/].

Za účelom efektívneho čelenia týmto nežiaducim hrozbám Slovenská republika prijala v roku 2008 Národnú stratégia pre informačnú bezpečnosť v Slovenskej republike (ďalej len NSIB), ktorá si stanovila za cieľ vytvoriť základný rámec informačnej bezpečnosti Slovenskej republiky. Súčasťou dokumentu je aj základný popis jednotlivých úloh s cieľom zabezpečiť ochranu celého digitálneho priestoru SR, mimo oblasti utajovaných skutočností, ktoré rieši NBÚ SR. NSIB a jej podporné dokumenty sa zameriavajú výhradne na oblasť neutajovaných informácií. Oblasť ochrany utajovaných informácií, teda priestor kybernetický spadá výhradne do kompetencie NBÚ, ktoré túto problematiku rieši vo vlastnej pôsobnosti v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

Ministerstvo financií Slovenskej republiky (ďalej len MF SR) ako ústredný orgán štátnej správy zodpovedný za túto oblasť a zastrešujúci orgán informačnej bezpečnosti vo vzťahu k ochrane neutajovaných údajov, do ktorého kompetencie spadá aj informačná bezpečnosť verejnej správy, pomocou svojich príslušných sekcií a odborov usmerňuje tvorbu koncepcií informačných systémov verejnej správy, vydáva štandardy a koordinuje oblasť bezpečnosti týchto systémov a správy internetu a vypracúva ďalšie materiály dotýkajúce sa informatizácie spoločnosti a verejnej správy; monitoruje, analyzuje a hodnotí stav bezpečnosti informačných systémov verejnej správy ako aj informačných systémov pracujúcich s osobnými údajmi a zastupuje SR v medzinárodných inštitúciách pre informačnú bezpečnosť [Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, 6]. Úlohou MF SR je zároveň vykonávať pravidelné prieskumy stavu informačnej bezpečnosti. V podmienkach MF SR bol zároveň zriadený poradný koordinačný výbor - Komisia pre informačnú bezpečnosť. Úlohou tejto komisie je

pripravovať návrhy a stanoviská pre oblasť ochrany a bezpečnosti informačných systémov verejnej správy, vyjadrovať sa k bezpečnostným štandardom, navrhovať a skúmať návrhy právnych noriem a relevantných materiálov týkajúcich sa informačnej bezpečnosti a zriaďovať pracovné skupiny pre plnenie stanovených úloh.

Problematika ochrany utajovaných skutočností v kybernetickom priestore spadá do kompetencie NBÚ SR ako ústredného orgánu štátnej správy pre ochranu utajovaných skutočností, šifrovú službu a elektronický podpis.[1] Problematika ochrany utajovaných skutočností a informácií je vo vládnych dokumentoch vyčlenená z digitálneho priestoru a tvorí samostatný kybernetický priestor. Ochranu utajovaných skutočností upravuje Koncepcia ochrany utajovaných skutočností v SR z roku 2007 a Koncepcia šifrovej ochrany informácií v SR z roku 2008 spolu s Návrhom opatrení pre zabezpečenie kybernetickej ochrany v SR, vypracované NBÚ SR.

Keďže je v záujme ochrany digitálneho priestoru potrebné rozvinúť bližšiu spoluprácu v oblasti ochrany utajovaných skutočností a informačnej bezpečnosti celého digitálneho priestoru Slovenskej republiky, Uznesením Bezpečnostnej rady SR č. 218 z roku 2008 bol NBÚ SR učený ako národná autorita pre riadenie kybernetickej ochrany, a teda poverený riešením otázok spadajúcich do tejto oblasti a určený za kontaktný bod pre spoluprácu s NATO. NBÚ ako národná autorita pre kybernetickú ochranu zaisťuje taktiež ochranu elektronicky vymieňaných utajovaných skutočností. Vo februári 2009 podpísal Národný bezpečnostný úrad, ako jeden z prvých národných bezpečnostných autorít členských krajín s NATO Memorandum o kybernetickej obrane s cieľom rozvoja vzťahov a výmeny skúseností na expertnej úrovni v tejto oblasti. V tom istom roku vzniklo v podmienkach NBÚ špecializované pracovisko počítačovej bezpečnosti a reakcie na incidenty SK CSIRC s cieľom koordinovať kybernetickú obranu, zvyšovať bezpečnosť informačných systémov a podieľať sa na medzinárodnej spolupráci [Národný bezpečnostný úrad 2001- 2011, 23]. Medzi ďalšie kritické oblasti z pohľadu kybernetickej bezpečnosti patria ochrana osobných údajov a elektronický podpis. Na základe platnej legislatívy spadá ochrana osobných údajov do kompetencie Úradu na ochranu osobných údajov Slovenskej republiky

[1] § 70, Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

(ďalej len ÚOOÚ SR) a oblasť elektronického podpisu do kompetencie NBÚ. Problematika elektronického obchodu patrí do pôsobnosti Ministerstva hospodárstva Slovenskej republiky (ďalej len MH SR). Počítačová kriminalita patrí do pôsobnosti Ministerstva spravodlivosti Slovenskej republiky a Ministerstva vnútra Slovenskej republiky (MS SR, MV SR), existujúca legislatíva pokrýva aj túto oblasť.

Napriek vyššie uvedenému členeniu zodpovednosti za rôzne aspekty kybernetickej bezpečnosti v podmienkach Slovenskej republiky absentuje ucelená koncepcia informačnej bezpečnosti Slovenskej republiky, ktorá na jednej strane podchytí národné záujmy v tejto oblasti a na strane druhej zabezpečí realizáciu politických cieľov. Mala by jasne stanovovať aký druh spôsobilostí SR potrebuje na zabezpečenie svojich národných záujmov. Vláda musí brať pri jej komplexnej príprave do úvahy množstvo svojich bezpečnostných záujmov, ktoré niekedy môžu byť tiež v kontradikcii [CZOSSECK, PODINS 2010]. Slovenská republika si síce uvedomuje dôležitosť obrany kybernetického priestoru, však k dnešnému dňu absentuje všeobecná právna úprava jednoznačne riešiaca stav a ambície Slovenskej republiky v oblasti obrany kybernetického priestoru a jeho bezpečnosti. Problematickou oblasťou v Slovenskej republike, ktorú v dostatočnej miere nepokrývajú strategické a politické dokumenty je spolupráca na národnej úrovni a jej nástroje, zapojenie súkromného a priemyselného sektora ako aj širokej verejnosti do zaistenia kybernetickej bezpečnosti [PITÁKOVÁ, 2010, 69].

Ako už bolo spomenuté, ciele na budovanie spôsobilostí v rámci tzv. Národných cieľov NATO boli zahrnuté do úloh pre viaceré členské krajiny, Slovensko nevynímajúc. Národnou autoritou zodpovednom za splnenie požiadaviek NATO je NBÚ SR. V najbližších rokoch zrejme spojenci budú musieť komplexne vybudovať národné stratégie a procedúry vychádzajúc z Politiky NATO pre kybernetickú obranu. Bude nevyhnutné jasne stanoviť národnú riadiacu štruktúru v tejto oblasti, autoritu pre strategické plánovanie či vybudovať operačné centrum. Spravodajské služby by mali rozvíjať spôsobilosti jednak na detekciu hrozieb (tzv. situačné povedomie, situational awareness), ale tiež na aktívne rozviedne operácie (kybernetická špionáž).

Členovia NATO budujú kybernetické tímy na boj aj obranu a inšpirujú tým zrejme aj MO SR. O vlastnej kybernetickej útočnej spôsobilosti preto aktuálne uvažuje aj Slovensko. „V členských štátoch NATO vznikla potreba mať podobné

tímy pripravené na okamžitý zásah pri obrane štátu samostatne alebo s inými štátmi. Teraz je o tom predčasné hovoriť, keďže všetko závisí od našich finančných možností", potvrdila hovorkyňa MO SR v júni 2013 a zároveň potvrdila, že ministerstvo zvažuje financovať vlastnú vojenskú jednotku na riešenie počítačových incidentov (CSIRT). Takýto tím už u nás funguje na ministerstve financií, no nie je útočný. Stráži funkčnosť dôležitých vládnych sietí, telekomunikačných operátorov či serverov elektrární [Slovensko chce kybernetickú armádu. Denník Sme. 26.6.2013; BUČKA, GONOS 2013].

ZÁVER

Kybernetický priestor je novou a mimoriadne dynamickou doménou. Severoatlantická aliancia a jej členské štáty ešte len začínajú objavovať všetky výhody, ale aj hrozby, ktoré táto doména prináša. Na rozdiel od konvenčných zbraní však kybernetický priestor dáva relatívne veľké možnosti aj stále viac aktívnym neštátnym aktérom. Medzinárodné kybernetické „hry", ktoré sú plné rôznorodých „hráčov" prinášajú stále nové otázky o tom, čo to vlastne bezpečnosť a obrana znamená, a to ako z národného, tak aj z medzinárodného hľadiska, NATO a iné medzinárodné organizácie nevynímajúc. Je viac ako pravdepodobné, že hľadanie adekvátnych opatrení na zamedzenie existujúcich kybernetických hrozieb bude v nasledovných rokoch vyžadovať zásadné zvýšenie úrovne priority, ktoré tejto agende doposiaľ členské krajiny NATO, ale aj Aliancia samotná prikladali.

Je možné konštatovať, že aj Slovenská republika si uvedomuje dôležitosť bezpečnosti kybernetického priestoru. Toto uvedomenie, okrem iných vplyvov, je tiež výsledkom rastúceho tlaku zo strany najmä NATO a EÚ, ktoré vyvíjajú viaceré iniciatívy na budovanie obranných spôsobilostí v tomto priestore. Napriek existencií viacerých stratégií, koncepcií a právnych úprav jednotlivých elementov kybernetického priestoru v podmienkach Slovenskej republiky, však k dnešnému dňu absentuje kvalitatívna všeobecná právna úprava jednoznačne riešiaca stav a ambície Slovenskej republiky v oblasti obrany kybernetického priestoru a jeho bezpečnosti a tiež jasné vymedzenie zodpovedností a právomocí, čo bude potrebné riešiť vo veľmi krátkom časovom horizonte.

Je dobré, že o tejto agende sa začína písať čoraz častejšie a že si ju začínajú všímať okrem odborníkov aj politici. Na zabezpečenie adekvátnych spôsobilostí bude jednoznačne potrebné vyčleniť personálne aj finančné zdroje. Aliancia si to

uvedomuje, a to aj kvôli tomu, že viacerí jej členovia cítili následky kybernetických útokov vo svojich krajinách. Je potrebné využiť ich existujúce skúsenosti a zabrániť výrazným škodám, ktoré by mohli vzniknúť kvôli šetreniu na nesprávnom mieste. Tak ako v každej oblasti, v ktorej je NATO zodpovedné za našu spoločnú obranu, aj a najmä tu platí, že Aliancia je len taká silná, ako silná je jej najslabšia súčasť.

SPIS LITERATURY

CLARKE, R.A., KNAKE, K.K.: *Cyber war – The next threat to national security and what to do about it.* New York, NY: Harper Collins Publishers. 2010. 261 s. ISBN 978-0-06-196223-3

CZOSSECK, C., PODINS, K.: Conference on Cyber Conflict. NATO CCD COE. Tallinn. ISBN: 978-9949-9040-1-3

BUČKA, P., GONOS, M.: *Bezpečnosť priemyselných sietí v prostredí moderných kybernetických hrozieb.* In: Acta Scientifica Academiae Ostroviensis [elektronický zdroj]: Sectio A: Nauki humanistyczne, społeczne i techniczne. - ISSN 2300-1739. - č. 1 (2013), online, s. 101-127.

Plný text: http://zn.wsbip.edu.pl/wydania/zeszyt2/sekcjaA/zeszyt_a.pdf

DENNING, D.: *Cyberterror.*http://www.cs.georgetown.edu/denning/infosec /cyberterror.html

GREGA, M., BUČKA, P.: *Blended simulation - not only as an effective military training commanders and staffs in ICM operations*. In: Výstavba, rozvoj a použití AČR 2012. - Brno: Univerzita obrany, 2012. - ISBN 978-80-7231-909-1. S. 1-11.

IVANČÍK, R.: Kybernetická bezpečnosť – neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti. In *Národná a medzinárodná bezpečnosť 2012 : zborník príspevkov z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika. 2012. s. 173-182. ISBN 978-80-8040-450-5.

IVANČÍK, R. – KAZANSKÝ, R.: Kybernetická bezpečnosť. In *Bezpečnostné fórum 2015, zborník vedeckých prác z 8. medzinárodnej vedeckej konferencie*. Banská Bystrica : Vydavateľstvo Univerzity Mateja Bela – Belianum, s. 78-85. ISBN 978-80-557-0849-2.

MAZANEC, B. M.: *The Art of (Cyber) War*, The Journal of International Security Affairs, Spring 2009 – Number 16.

Národný bezpečnostný úrad: *10 rokov Národného bezpečnostného úradu*, Bratislava: Tlačiareň Ministerstva vnútra Slovenskej republiky, 2011. 92 s.