Eva Kostrecová

Iniciatívy v rámci medzinárodnej spolupráce štátov a svetových inštitúcií pri ochrane elektronického priestoru

Elektronický priestor, nazývaný aj kybernetickým priestorom alebo jednoducho kyberpriestorom, je novým pojmom, ktorý bol zavedený do nášho každodenného jazyka spolu s počítačovými zariadeniami a službami, poskytovanými na báze informačných technológií. Elektronický priestor je novým spoločenským prostredím, ktoré zahŕňa globálnu počítačovú sieť, predstavujúcu prepojenie počítačových sietí celého sveta, ktorá spája ľudí, stroje a zdroje informácií vo svete, a cez ktoré sa môže každý ľudský jedinec „virtuálne" presúvať, komunikovať s inými ľuďmi, ale aj prezerať si údaje a informácie uložené na rôznych počítačových zariadeniach umiestnených po celej planéte.[1]

Zodpovednosť vládnych orgánov a inštitúcií za zabezpečenie dodržiavania ľudských práv a ochrany občanov, ktorá existuje vo fyzickom svete, je rovnaká aj v elektronickom priestore a pri používaní informačno-komunikačných technológií. Je teda možné povedať, že elektronický priestor nie je prázdnym prostredím, ale že ide skôr o spoločenskú arénu, v ktorej sa dejú veci medzi ľuďmi a majú na nich priamy dosah a kde faktory zraniteľnosti a rizík, ktoré existujú vo fyzickom svete, majú podstatne väčšie rozmery.[2] Strety a vzájomné pôsobenie aktérov v kyberpriestore ovplyvňujú samozrejme aj fyzický svet v podobe rôznych dôsledkov.

Vládni predstavitelia štátov celého sveta sú vyzývaní, aby prijímali opatrenia na ochranu ľudských práv v elektronickom priestore. Niektoré vlády už prijali v posledných rokoch zákony a normatívne texty a zaviedli do praxe systémy na ochranu svojich občanov v elektronickom priestore. Tieto iniciatívy sú však nepostačujúce, pretože elektronický priestor je celosvetový a neuznáva hranice štátov, a preto je potrebné na prijímaní ochranných opatrení spolupracovať na všetkých úrovniach tak politického spektra, ako aj hospodárskych a spoločenských inštitúcií. V minulom roku sa uskutočnili viaceré iniciatívy na vrcholovej úrovni. Niektoré z nich si priblížime v tomto príspevku.

1. Summit NATO o ochrane elektronického priestoru pod názvom „K posilneniu spolupráce v rámci NATO"

Šéfovia vojenských i civilných inštitúcií, majúcich v kompetencii ochranu elektronického priestoru, z 21 členských štátov NATO[3] sa stretli na Sumite v Paríži v dňoch 14. – 16. júna 2010. Tento summit, organizovaný francúzskou Národnou agentúrou pre bezpečnosť informačných systémov (ANSSI – Agence nationale de la sécurité des systèmes d'information), opätovne potvrdil význam spolupráce medzi NATO a členskými štátmi v oblasti ochrany elektronického priestoru.

---

[1] Definícia založená na vízii Williama Gibsona, autora sci-fi románov (http://pespmc1.vub.ac.be/cybspace.html)

[2] http://www.ecpat.net/ei/Publications/ICT/Cyberspace_FRE.pdf – Násilie proti deťom v kyberpriestore

[3] Belgicko, Bulharsko, Česká republika, Estónsko, Francúzsko, Holandsko, Chorvátsko, Kanada, Lotyšsko, Luxembursko, Maďarsko, Nórsko, Poľsko, Portugalsko, Rumunsko, Španielsko, Taliansko, Turecko, USA, Veľká Británia.

Počas dvoch dní rokovaní sa najvyšší šéfovia jednotlivých krajín, sprevádzaní príslušnými odborníkmi, navzájom podelili o svoje obavy v oblasti bezpečnosti informačných systémov a o zámery pri ochrane elektronického priestoru. 16. júna vo večerných hodinách bol summit ukončený prijatím spoločného vyhlásenia o základných princípoch spolupráce. Účastníci potvrdili, že je veľmi dôležité a v záujme všetkých občanov našej planéty podporiť úsilie NATO v oblasti ochrany elektronického priestoru. Z tohto dôvodu považujú za nevyhnutné formou spolupráce medzi NATO a členskými štátmi vypracovať jasnú a komplexnú víziu hrozieb spojených s elektronickým priestorom.

Účastníci summitu sa zhodli aj na potrebe viesť aktívnu a koordinovanú politiku ochrany sietí a informačných systémov NATO, aby bolo možné predchádzať týmto hrozbám. Počas rokovania sa sústredili na prevádzkové aspekty ochrany elektronického priestoru s cieľom, aby informačné a komunikačné systémy NATO boli plne a účinne k dispozícii intervenčným jednotkám a misiám nasadeným na akcie v teréne.

Vzhľadom na závislosť Severoatlantickej aliancie od jej informačnej a komunikačnej infraštruktúry prijali účastníci rozhodnutie, aby každý členský štát NATO zabezpečil reálne zdroje na podporu ochrany elektronického priestoru a prijal skutočné opatrenia, a to najmä v podobe zriadenia Centier operatívneho monitorovania a spracúvania informatických útokov (CERT – Computer Emergency Response Team).

2. Cvičenie Cyber Storm III – globálna koordinácia medzi verejným a súkromným sektorom pri ochrane elektronického priestoru

Iniciatíva praktickej „kybernetickej búrky“ pod názvom Cyber Storm III bola v dňoch 28. – 30. septembra 2010 zorganizovaná USA. Jej cieľom bolo zhodnotiť schopnosti účastníckych štátov a inštitúcií – pôsobiacich na území týchto štátov – spoločne čeliť celosvetovej informatickej kríze spôsobenej počítačovým útokom. Na cvičení koordinovanom americkým ministerstvom obrany sa aktívne zúčastnilo 13 štátov[4], ďalších sedem ministerstiev USA, Pentagon, 11 federálnych štátov USA a 60 súkromných spoločností.

Počas cvičenia bolo simulovaných 1500 útokov, proti ktorým museli účastníci „bojovať“ rovnakým spôsobom, ako keby išlo o skutočné napadnutia infraštruktúr a systémov neznámymi protivníkmi, resp. politickými odporcami. Toto cvičenie poskytlo reálny obraz o tom, čo sú kompetentní odborníci v rámci ochrany informačno-komunikačných technológií schopní vykonať a v čom musia urobiť nápravu. Cvičenie umožnilo otestovať schopnosť zoskupiť informácie pochádzajúce z mnohých zdrojov – tak z verejného, ako aj súkromného sektora, ako aj schopnosť zorganizovať globálnu reakciu. Overilo aj existujúce prijaté vládne programy a postupy pri medzinárodnej spolupráci a koordinácii s partnermi v procese riadenia informatickej krízy veľkého rozsahu.

Po prvýkrát v histórii bolo počas cvičenia možné overiť aj účelnosť a opodstatnenosť existencie a poslania nového Národného integračného centra pre ochranu elektronického priestoru a komunikácií (NCCIC – National Cybersecurity and Communications Integration Center), ktoré bolo v USA zriadené v roku 2009 a ktorého poslaním je koordinácia expertov z verejného a súkromného sektora pri ochrane kybernetického priestoru. Cvičenie potvrdilo zásadný význam tejto inštitúcie pri koordinácii reakcií na simulované útoky, pretože Centrum predstavuje organizačnú jednotku, ktorá združuje riadenie všetkých kapacít z jedného miesta.

Závery prijaté z tohto cvičenia potvrdzujú, že medzinárodná spolupráca je základom stanovenia jasnej a komplexnej vízie hrozieb, ktorým je nutné čeliť, ako aj nevyhnutnosť

[4] Austrália, Francúzsko, Holandsko, Japonsko, Kanada, Maďarsko, Nemecko, Nový Zéland, Švajčiarsko, Švédsko, Taliansko, USA, Veľká Británia

posilnenia tejto spolupráce medzi odborníkmi súkromného a verejného sektora z oblasti informačno-komunikačných technológií.

3. CyberEurope 2010 - Cvičenie o celoeurópskej spolupráci pri ochrane počítačových sietí

Pod záštitou Európskej agentúry pre bezpečnosť sietí a informácií (ENISA – European Network and Information Security Agency) sa 27 členských štátov Európskej únie, Island, Nórsko, Švajčiarsko a Európske združenie voľného obchodu (EFTA – European Free Trade Association) zúčastnilo 4. novembra 2010 v Aténach na prvom Paneurópskom obrannom cvičení proti počítačovým útokom. Na cvičení bol simulovaný masívny útok na európske prepojovacie body Internetu, ktorý paralyzoval siete a znemožnil elektronickú komunikáciu.

Cieľom tohto prvého paneurópskeho cvičenia bolo ukázať potrebu plynulej výmeny tokov informácií medzi členskými štátmi v reálnom čase v prípade útoku proti kritickým informačným infraštruktúram Internetu a nevyhnutnosť zintenzívnenia spolupráce pri riešení krízového stavu. Cvičenie bolo testom stresovej situácie, v ktorej sa ocitli štátne orgány Európy. Všetky členské štáty vyjadrili potrebu pokračovať v realizácii takýchto praktických cvičení na národnej i celoeurópskej úrovni. Rovnako sa zhodli v názore, že je nevyhnutné zapojiť do ďalších cvičení aj súkromný sektor a vymieňať si výsledky zistení i závery prijaté na takýchto národných i medzinárodných cvičeniach.

Podpora prípravných cvičení pre ochranu elektronického priestoru v rámci Európskej únie sa stala jednou z priorít politík EÚ, najmä v podobe Digitálneho programu pre Európu[5]. Aj závery a odporúčania prijaté účastníkmi cvičenia Cyber Europe 2010 potvrdzujú túto prioritnú politiku. Cvičenie splnilo všetky svoje ciele a jeho scenár zohľadňoval potrebu vyváženosti medzi zabezpečením technických a komunikačných potrieb. Všetky zúčastnené strany sa zhodli, že neexistujú dostatočné celoeurópske opatrenia na prípravu takýchto paneurópskych testov. Ich neexistencia odráža skutočnosť, že mnoho členských štátov sa snaží zlepšiť svoje národné opatrenia na ochranu kybernetického priestoru bez toho, aby zvážili možnosti spolupráce pri riešení problémov na celoeurópskej úrovni.

Cvičenie bolo len prvým krokom k budovaniu dôvery a k posilneniu spolupráce a výmeny informácií v rámci paneurópskeho elektronického priestoru. Všetky zúčastnené štáty odporučili, aby ENISA bola poverená úlohou organizovať a riadiť budúce cvičenia, ktorých príprave by mal byť venovaný dlhší čas, a aby bola koordinovaná na medzinárodnej úrovni a v spolupráci so súkromným sektorom.

4. Cyber Coalition 2010 – Civilno-vojenské koordinačné cvičenie NATO zamerané na ochranu elektronického priestoru

Zástupcovia 24 členských štátov Severoatlantickej aliancie, 12 priamych účastníkov[6] a 12 pozorovateľov[7] a inštitúcie NATO zodpovedné za ochranu elektronického priestoru sa stretli v dňoch 16. – 18. novembra 2010 v Shape, neďaleko belgického mesta Mons, na civilno-vojenskom medzinárodnom a transdisciplinárnom koordinačnom cvičení zameranom na ochranu elektronického priestoru. Cyber Coalition 2010 bolo už tretím cvičením NATO

[5] http://ec.europa.eu/information_society/digital-agenda

[6] Česká republika, Estónsko, Francúzsko, Grécko, Litva, Nemecko, Nórsko, Poľsko, Taliansko, Turecko, USA, Veľká Británia

[7] Belgicko, Bulharsko, Dánsko, Holandsko, Chorvátsko, Lotyšsko, Maďarsko, Portugalsko, Rakúsko, Rumunsko, Španielsko

s cieľom riešiť stresovú situáciu spojenú s hrozbami a útokmi na kybernetický priestor a reakciami na incidenty. Prvé cvičenie v novembri 2008 bolo určené len pre inštitúcie NATO. Na druhé v roku 2009 boli už pozvané všetky členské štáty Severoatlantickej aliancie.

Scenár cvičenia simuloval situáciu humanitárnej intervencie síl NATO v oblasti, kde prichádza k etnickým a náboženským konfliktom. Útoky teroristickej skupiny na komunikačné prostriedky a informačné systémy Aliancie ohrozovali spojenecké sily podieľajúce sa na intervencii, ale aj kritické informačné systémy členských štátov. Pri riešení krízového stavu museli účastníci pristúpiť k medzinárodnej civilno-vojenskej spolupráci a trénovať si situácie, ako prekonať technické problémy a výzvy spojené so šírením škodlivých počítačových kódov.

Cyber Coalition 2010 bolo procedurálnym cvičením obrany elektronického priestoru, ktoré však preverovalo aj celý rad technických prvkov. Na tomto cvičení aktívne riešili úlohy národné ministerstvá obrany členských štátov a ich inštitúcie kompetentné pre ochranu elektronického priestoru, Koordinačný a riadiaci výbor NATO a tímy riešiace incidenty tak z NATO, ako aj z členských krajín. Koordinačný a riadiaci výbor riadil cvičenie zo Shape v Belgicku, zatiaľ čo ostatní účastníci plnili praktické úlohy cvičenia zo svojich krajín a miest, kde riešia každodenné povinnosti pri zvládaní incidentov.

Hlavnou devízou tohto cvičenia pri riešení kritickej situácie bolo spojenie rôznych aktérov, ktorí hľadali východiská spoločnými silami. Bolo príležitosťou pre všetky krajiny a ich odborníkov riešiť problémy so svojimi partnermi z NATO a ministerstiev obrany ostatných štátov pri riadení a využívaní kybernetických nástrojov na zvládnutie stresových stavov spojených s ohrozením kritických infraštruktúr a informačných systémov. V záveroch prijatých po realizácii praktických aktivít cvičenia sa účastníci zhodli na pravidelnejšom organizovaní kybernetických obranných cvičení, na ktorých budú testovať reakcie na možné útoky a incidenty v elektronickom priestore, medzinárodnú spoluprácu kompetentných národných inštitúcií a procesy strategického rozhodovania NATO a jeho členských štátov.

Použité zdroje:

http://www.ssi.gouv.fr
http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf
http://fr.canoe.ca/techno/internet/archives/2010/09/20100930-090447.html
http://www.nato.int/cps/en/natolive/news_68205.htm?selectedLocale=en

RNDr. Eva Kostrecová, PhD.
Fakulta Elektrotechniky a informatiky
STÚ v Bratislave
Katedra aplikovanej informatiky a výpočtovej techniky
e-mail : eva.kostrecova@stuba.sk