CENAA

Centre for European and North Atlantic Affairs

11. Slovenské strategické fórum

Kyberbezpečnosť na Slovensku: výzvy a príležitosti

Závery z 11. Slovenského strategického fóra,
ktoré sa konalo v dňoch 8. - 9. novembra 2013 v Beladiciach

PARTNER PODUJATIA

Atos

Úvod

Jedenáste Slovenské strategické fórum sa konalo v dňoch 8. a 9. novembra 2013 v Beladiciach, tentokrát ako súčasť programu **Globálne občianstvo v kybersvete (Global Netizenship in Cyber World)**, ktorým chce CENAA prispieť k rozvoju diskusie o kyberbezpečnosti na Slovensku. Téma bola zvolená vzhľadom na fakt, že prebiehajúce kyberútoky sa stále viac stávajú prostriedkom na dosahovanie politických cieľov. Aj z tohto dôvodu je potrebné angažovať národných a medzinárodných aktérov a využívať existujúce kapacity štátu a súkromného sektora. Cieľom fóra preto bolo predovšetkým kritické zhodnotenie stratégií a politík Slovenskej republiky, ako aj príležitostí pre spoluprácu štátneho a súkromného sektora v tejto oblasti. Fórum prebehlo v nasledujúcich štyroch paneloch, ktorých rozdelenie je zohľadnené v štruktúre tohto dokumentu.

- Kyberpriestor: aktuálne výzvy a príležitosti pre spoluprácu;
- Štátny vs. neštátny kyberterorizmus;
- Koordinácia v kyberbezpečnosti na národnej úrovni;
- Verejno-súkromné partnerstvo na boj proti kyberterorizmu.

Kyberpriestor: aktuálne výzvy a príležitosti pre spoluprácu

Ambíciou prvého panelu bolo definovanie základných problémov, ktoré súvisia s využívaním kybernetického priestoru a jeho nástrojov, ako aj potrieb na medzinárodnej a národnej úrovni v boji proti hrozbám, ktoré tento priestor generuje. Podľa mnohých odborníkov sa totiž hrozba kyberterorizmu môže stať v tomto tisícročí hlavnou bezpečnostnou výzvou, čo vyplýva z otvorenosti a bezhraničnosti kybernetického priestoru. Navyše kyberterorizmus je finančne pomerne nenáročný a často si vyžaduje len minimum nástrojov, ktoré sú v dnešnom svete voľne dostupné na trhu.

Kľúčovým problémom pri ochrane tohto priestoru je riziko obmedzenia slobody. Inými slovami, je zložité určiť správnu hranicu medzi zaistením bezpečnosti a zaistením slobody. Problémom je tiež výrazné prepojenie všetkých oblastí života práve cez informačné siete, či už ide o národnú úroveň prostredníctvom prvkov kritickej infraštruktúry alebo po individuálnu úroveň prostredníctvom jednotlivých domácností. Ohrozenie kyberpriestoru pritom spravidla prebieha tromi spôsobmi: Po prvé, plánovanou škodlivou činnosťou vo forme zámerných kyberútokov, špionáže, získavania osobných údajov a dát a podobne. Po druhé, neplánovanou činnosťou napríklad v dôsledku prírodných katastrof. A napokon, neúmyselnými ľudskými zlyhaniami, pri ktorých aj minoritná chyba môže spôsobiť rozsiahle škody.

Z charakteru kyberterorizmu pritom vyplýva zložitosť boja proti nemu, špeciálne na individuálnej úrovni. Je preto nevyhnutné využívať všetky

mechanizmy na úrovni štátu podporené efektívnou medzirezortnou a medzinárodnou spoluprácou a prepojením so súkromným sektorom. Je pozitívne, že táto problematika už v súčasnosti tvorí dôležitú súčasť agendy medzinárodných organizácií ako je NATO a EÚ. Na úrovni aliancie je pojem kybernetickej bezpečnosti akcentovaný najmä od kybernetických útokov proti Estónsku (2006), založenia Centra výnimočnosti v Talline (2008) či schválenia Strategickej koncepcie v Lisabone (2010). Potvrdzujú to samostatné rokovania ministrov obrany na túto tému na ich dvoch posledných stretnutiach, ale aj očakávaná agenda nadchádzajúceho summitu, ktorý sa uskutoční v septembri 2014 v Londýne. Existujú však rozdiely v chápaní miesta Aliancie v celej problematike, pričom názory sa pohybujú od koordinačnej úlohy až po jeho výrazné posilnenie smerom k potenciálneho zásahu na základe článku 5 Severoatlantickej zmluvy. NATO tiež nedávno zaviedlo vlastný systém boja proti zločinom v kybernetickom priestore. Reagovalo tak na štatistiku o počte takých incidentov, ktorý v rámci jej siete v roku 2012 presiahol číslo 7000.

Rovnako tak na úrovni Európskej únie bola na jar 2013 prijatá stratégia "Otvorený, bezpečný a chránený kybernetický priestor", ktorá predpokladá prijatie viacerých legislatívnych zmien členských štátov. K tomuto by mal napomôcť návrh smernice pripravený Európskou komisiou vo februári 2013, pričom počas nasledujúcich 18 mesiacov prebieha proces jej transpozície do národných legislatív. Okrem toho iniciátorom mnohých návrhov je aj Európska agentúra pre bezpečnosť sietí a informácií (ENISA) založená v roku 2004, ktorej hlavnou úlohou je zabezpečiť v EÚ potrebnú vysokú úroveň bezpečnosti sietí a prenášaných údajov.

Z hľadiska medzinárodnej úrovne tiež stojí za zmienku medzinárodná konferencia, ktorú od roku 2010 na túto tému organizuje Ruská federácia za účasti vysokých predstaviteľov bezpečnostného sektora z celého sveta (v júli 2013 za účasti 62 štátov). Ambíciou je pritom preniesť túto debatu do rámca OSN. V rámci Vyšehradskej štvorky sa spolupráca v tejto oblasti prehĺbila najmä počas predsedníctva Poľska v roku 2012, počas ktorého sa prvýkrát konalo aj stretnutie tajomníkov bezpečnostných rád, na ktoré neskôr nadviazali počas predsedníctva Maďarska. Kybernetická bezpečnosť sa dostala aj do záverečných dokumentov po stretnutí premiérov V4 v Budapešti v októbri 2013.

Na národnej úrovni predstavuje zatiaľ základný rámec v tejto téme Stratégia kybernetickej bezpečnosti z roku 2008, podľa niektorých hodnotení by však už bola žiaduca jej obnova. Nedostatkom je tiež absencia zákona o kybernetickej obrane. Problémom je i kompetenčné rozdelenie pri riešení tejto agendy, keďže na Slovensku sa prelínajú zodpovednosti ministerstva financií ako garanta tejto témy so zodpovednosťou ministerstva dopravy, pôšt a telekomunikácií ale aj Národného bezpečnostného úradu. Je pozitívom, že ministerstvu financií sa podarilo nadviazať bilaterálne i multilaterálne vzťahy a spôsob komunikácie s rôznymi subjektmi pôsobiacimi v tejto oblasti vrátane súkromných spoločností, tieto však často nie sú dostatočne formalizované

a vyplývajú skôr z osobných vzťahov a väzieb ako z inštitucionalizovanej spolupráce.

Štátny vs. neštátny kyberterorizmus

Diskusia v druhom paneli sa vrátila k definičnému zakotveniu pojmu kybernetický terorizmu a to jednak v rovine civilnej ale i vojenskej. Pri hľadaní definície kyberterorizmu spôsobuje komplikácie fakt, že už samotný pojem terorizmus je nejednoznačný, rôznym spôsobom interpretovaný a politicky i emociálne zaťažený. Z toho dôvodu častokrát vyvoláva pocit, že je zneužívaný štátnou mocou na obhajovanie svojich nelegitímnych aktivít, preto možno niekedy hovoriť o štátnom alebo skôr o štátom podporovanom terorizme. Podobná rôznorodosť platí i pri kyberterorizme, na ktorý možno nahliadať z užšieho i širšieho pohľadu. Kým v prvom prípade ide len o incidenty, ktoré ohrozujú životy, zdravie a majetky ľudí, v druhom prípade je to každá premyslená aktivita zameraná na narušenie informačných sietí a ich činností, napríklad aj s cieľom získavania informácií a údajov. Dnes sú síce fyzické následky a dopad kybernetického terorizmu na obyvateľstvo zatiaľ malé, potenciálne to však môžu zmeniť napríklad kybernetické útoky na zariadenia kritickej infraštruktúry.

Toto má vplyv i na vojenstvo, kde sa výraz kybernetický začal chápať ako ďalšia z bojových dimenzií – tak ako sa v minulosti zdôrazňovala obrana námorného či vzdušného priestoru, dnes je potrebné pamätať aj na kybernetický priestor. Súčasťou tohto trendu bolo v Spojených štátoch amerických nedávne vytvorenie nového kybernetického veliteľstva, hoci tento krok vyvolal polemiku o jeho adekvátnosti. Novému charakteru tohto priestoru je však potrebné prispôsobiť aj ciele a nástroje jeho obrany. Na rozdiel od "konvenčných" útokov a spôsobov boja je boj v kyberpriestore sprevádzaný znižovaním času a možností na prípravu, keďže potenciálny útočník môže konať veľmi neštandardne, prekvapivo a bez možnosti odhadnúť jeho správanie.

V súvislosti s formami ochrany a obrany kybernetického priestoru na Slovensku sa preto objavuje viacero kľúčových otázok: sme pripravení eliminovať nebezpečenstvo identifikovaného a hroziaceho útoku (najmä zo strany neštátneho aktéra) na kritickú infraštruktúru preventívnym útokom?; bude obrana kyberpriestoru v kompetencii armády alebo budú pripravené nové štruktúry či jednotky na tento účel?; sú dostatočne známe a rozvinuté nielen nástroje a spôsobilosti ale najmä procesné súvislosti v prípade krízových situácií v dôsledku aktu masívneho štátneho či individuálneho terorizmu?; je súčasná slovenská legislatíva v tejto oblasti dostatočná? a podobne. Hodnotenia v jednotlivých aspektoch pritom ostávajú nejednoznačné.

Hoci je pravdou, že SR má najmä v zákonoch detailne spracovaný systém postupov a vzťahov jednotlivých prvkov systému, podľa niektorých hodnotení

tieto nie úplne reflektujú súčasné potreby štátu a jeho obyvateľov. Týka sa to nielen definovania základných úloh štátu na strategickej úrovni (rozdielne názory na aplikáciu článku 5 Severoatlantickej zmluvy či potrebu inovovania strategických dokumentov ako Bezpečnostná stratégia SR a Obranná stratégia SR), ale aj dôslednejšej koordinácie štátnych a súkromných aktivít v tejto oblasti (diskusie o kompetencii jednotlivých inštitúcií či zodpovednosti štátu za infraštruktúru).

Koordinácia v kyberbezpečnosti na národnej úrovni

Úlohou tretieho panelu bolo popísať súčasný stav na Slovensku z hľadiska siete inštitúcií a orgánov, ktoré sú zapojené do ochrany bezpečnosti v kybernetickom priestore. Ako už bolo zdôraznené v predošlých častiach, dianie v ňom zaznamenáva výraznú dynamiku, čo je dané obrovským množstvom zdieľaných informácií, uskutočňovaných transakcií a dostupnosťou hardvéru i softvéru. Tento pohyb je veľmi zložité dostatočne skoro detekovať, analyzovať a náležite predvídať, čo väčšinou robí kyberpriestor veľmi lukratívnym z hľadiska jeho využitia na nelegálne účely. K tomu sa pridávajú početné ľudské chyby, nedostatočná prevencia a automatizácia procesov, ktoré ešte vo väčšej miere zintenzívňujú možné ohrozenia tohto priestoru. Náročnou výzvou je ochrana počítačových systémov tak pri veľkých podujatiach (olympijské hry, summity a pod.), ako aj pri každodennej činnosti jednotlivých inštitúcií. Preto je nevyhnutné vytvárať tlak na potrebu zdieľania informácií a vedomostí nielen v špecializovaných inštitúciách, ale aj na národnej a medzinárodnej úrovni.

Na Slovensku sa situácia v tomto ohľade zatiaľ vyvíja pomerne pomaly, pričom štátny sektor zväčša reaguje na podnety iniciované v rámci Európskej únie prípadne iných zahraničných aktérov. Rozdelenie právomocí pri riešení tejto agendy rámcuje najmä tzv. kompetenčný zákon, pričom zatiaľ neexistuje špecializovaná inštitúcia, ktorá by riadila bezpečnostnú politiku v kybernetickom priestore. Zodpovednosť je tak rozdelená medzi viacerých aktérov. Okrem už spomínaných ministerstva financií, ministerstva dopravy pôšt a telekomunikácií a Národného bezpečnostného úradu, plnia špecializované úlohy v tejto oblasti najmä Národná agentúra pre sieťové a elektronické služby, CSIRT.sk (patriaci do pôsobnosti MF SR) a Úrad vlády SR, najmä prostredníctvom Kancelárie Bezpečnostnej rady SR a sekcie Riadiaci orgán pre Operačný program Informatizácia spoločnosti.

Napriek tomu, že SR je zatiaľ na začiatku procesu riešenia ochrany kybernetického priestoru z hľadiska ponúkajúcich sa možností a situácií, je známych niekoľko iniciatív, ktoré môžu byť pozitívnym príkladom do budúcnosti. K takým patrí patrí schválenie zákona o e-governmente, ktorý by mal napomôcť k zníženiu byrokracie pri komunikácii medzi občanmi, podnikateľmi a štátom, ako aj začiatok vydávania čipových občianskych preukazov plánovaný na 1. decembra 2013. Práve tento krok by mohol

predstavovať silný štartujúci element pre využívanie elektronických služieb na Slovensku. Pozitívny pokrok nastal za posledné roky aj pri sledovaní, analyzovaní a identifikovaní narušení informačných sietí.

Je evidentné, že potenciálny rozmach nových elektronických nástrojov musia sprevádzať aj kroky k adekvátnemu zaistenia ochrany údajov, ktoré sa dostanú do elektronického systému. K tomu by mohlo napomôcť aktualizovanie Stratégie kybernetickej bezpečnosti z roku 2008, zlepšenie modelu odovzdávania informácií medzi štátnym, súkromným a mimovládnym sektorom, či inovatívnejší postoj pri riešení partikulárnych problémov (najmä v spolupráci s väčšími štátmi), keďže Slovensko v tejto oblasti zastáva skôr reaktívny prístup. Dôležitou oblasťou záujmu by malo byť tiež zvyšovanie celkového povedomia obyvateľstva, napríklad formou digitálneho vzdelávania, výraznejším zapojením ministerstva školstva, vedy a výskumu pri tvorbe učebných osnov a celkovou intenzívnejšou spoluprácou štátnych orgánov a akademických inštitúcií.

Verejno-súkromné partnerstvo na boj proti kyberterorizmu

Jedným z dôkazov vysokej aktuálnosti otázky kybernetickej bezpečnosti je prijatie Cieľov NATO Slovenskou republikou v tejto oblasti so záväzkom splnenia v roku 2016. Toto je predpokladom pozitívneho rozvoja národných spôsobilostí, zároveň to však vytvára tlak a riziká pri realizácii jednotlivých úloh, keďže možnosti na úrovni štátu sú obmedzené tak na úrovni finančných, ale aj personálnych zdrojov. Pri plnení záväzkov v tomto sektore bude preto nevyhnutné dbať na znižovanie nákladov pri udržaní maximálnej efektivity výsledkov s využitím dostatočných znalostí aj súkromného sektora. V celom procese by mohli byť nápomocné verejno-súkromné partnerstvá (PPP), čím by mohlo byť zabezpečené optimálne zdieľanie rizika medzi verejným a súkromným sektorom a splnenie úloh v primeranom časovom horizonte. Zároveň by mohlo dôjsť k minimalizácii nedostatkov, ktoré sa objavujú na úrovni štátnej správy, akými sú nedostatočné skúsenosti v danej oblasti či rigidná flexibilita v rozhodovaní.

Pri modelovaní PPP je možné vychádzať zo skúseností niektorých iných krajín, kde táto debata pokročila o niečo ďalej. Inšpiráciou môže byť napríklad pomôcka vydaná agentúrou ENISA v roku 2011 pod názvom Good Practice Guide, ktorá je práve zameraná na tento typ projektov v kybernetickej bezpečnosti. Dobré príklady možno nájsť aj v Spojených štátoch, kde bola okrem iného pred časom spracovaná správa pre prezidenta o nevyhnutnosti realizovania PPP projektov v kybernetickej oblasti, ale aj v Nemecku, kde tento typ spolupráce prebieha pre účely rozvoja ozbrojených síl. Dostatočné skúsenosti v tejto oblasti však ponúkajú aj ďalšie krajiny, napríklad Francúzsko, Holandsko či krajiny Škandinávie. Vo všeobecnosti pritom platí, že zväčša je výhodnejšie prebrať overené riešenia ako prichádzať za každú cenu s novými.

Realizácia PPP projektov však so sebou prináša niekoľko obmedzení či potenciálnych ťažkostí. Jednak je to rad regulácií na rôznych úrovniach (EÚ, OECD, štát atď.), zložité financovanie a komplikované rozpočtovanie (výsledok by mal byť efektívnejší, ale nemusí byť vždy lacnejší), ale aj nedostatočné skúsenosti verejného sektora. Práve tie mnohokrát zdržujú celý proces, najmä v etape prípravy a výberu partnera. Rizikom je rovnako i nižšia miera flexibility pre následné zmeny, ktorých uskutočnenie je pomerne zložité, čo sa môže zdať najmä z finančného pohľadu nevýhodné. Faktorom, ktorý odrádza od takejto spolupráce je v neposlednom rade i vzájomné zdieľanie informácií, preto je nevyhnutné hneď v úvode nastaviť detailné pravidlá spoločného fungovania. A napokon veľmi relevantnou je tiež otázka transparentnosti, preto je potrebné dbať na otvorenosť a prehľadnosť všetkých procesov.

Pre úspech spolupráce verejného a súkromného sektora na Slovensku je dôležité, aby sa upustilo od súčasného konkurenčného vzájomného vnímania oboch strán a skôr sa zdôrazňovala myšlienka partnerstva a obojstrannej výhodnosti. To je však pomerne zložité v prostredí, kedy štátny sektor len s ťažkosťami udržiava vysokokvalifikovaný personál, ktorý častokrát nachádza svoje uplatnenie práve v súkromnom sektore. Existuje však i opačný problém a to nedostatočné možnosti prístupu kvalitných ľudí do verejného sektora (zlý výber, otázka klientelizmu).

V súčasnosti sa na Slovensku ukazuje niekoľko oblastí, v ktorých možno PPP projekty uplatniť. Široké možnosti ponúka hlavne oblasť informatizácie spoločnosti (e-government, e-health), ktorá sa už rozbieha niektorými konkrétnymi aktivitami. Ale aj oblasti ako outsourcing databáz a IT-postupov, finančných tokov, archívov, výskumných technológií a kybernetickej bezpečnosti ako takej. V tejto súvislosti možno spomenúť i rozsiahle príležitosti na úrovni NATO, keďže ročný obrat v oblasti informačných technológií sa v ňom pohybuje na úrovni cca 300 mld. EUR. Tieto sú však zatiaľ slovenskými súkromnými spoločnosťami využívané len vo veľmi obmedzenej miere (len 2 spoločnosti).

Pre zvýšenie dynamiky v týchto procesoch je potrebné rozvinutie širokej expertnej diskusie s cieľom prinášať skutočné riešenia pre spoluprácu verejného a súkromného sektora. V súčasnosti totiž táto debata prebieha len na úrovni niekoľkých odborných združení a mimovládnych organizácií. Je potrebné, aby aj súkromné spoločnosti samotné prichádzali s vlastnými štúdiami a návrhmi a aby sa tieto dostávali na najvyššiu úroveň rozhodovania. Na strane súkromných spoločností totiž prevláda presvedčenie, že sú schopné ponúknuť atraktívne riešenia postavené na relevantných príkladoch. Je však dôležité, aby prebiehala vzájomná informovanosť o potrebách a možnostiach a aby bola na strane štátu prekonaná prílišná opatrnosť a obavy z realizácie takýchto partnerstiev.

Odporúčania

- *Prehodnotiť aktuálnosť základného strategického a legislatívneho rámca SR v oblasti kybernetickej bezpečnosti, ako aj adekvátnosti rozdelenia kompetencií medzi orgánmi ústrednej štátnej správy.*

- *Prehlbovať spoluprácu s Európskou úniou a Severoatlantickou alianciou, v tejto problematike a to nielen formou pasívneho prijímania ich rozhodnutí, ale aj generovaním vlastných návrhov a iniciatív. Súčasne zintenzívniť spoluprácu s ďalšími krajinami, ktoré sú z politického i odborného hľadiska lídrami na tomto poli.*

- *Na národnej úrovni formalizovať multilaterálne vzťahy a spôsob komunikácie medzi jednotlivými subjektmi pôsobiacimi v tejto oblasti vrátane súkromných spoločností.*

- *Usilovať o zintenzívňovanie diskusie a zvyšovanie povedomia o téme kybernetickej bezpečnosti a to tak na strategickej ako aj expertnej úrovni. V rámci toho posilňovať prepojenie štátnych inštitúcií, súkromných spoločností a mimovládneho sektora.*

- *Rozvíjať iniciatívy zamerané na informatizáciu spoločnosti (e-health, e-government). Pritom dbať na dostatočnú ochranu zdieľaných údajov a informácií.*

- *Spracovať štúdiu udržateľnosti pre realizáciu verejno-súkromných partnerstiev a identifikovať strednodobé ciele a oblasti hlavného záujmu štátu.*

- *Posilniť zapojenie slovenských spoločností do obchodných aktivít v rámci Severoatlantickej aliancie a zvýšiť tak ich pripravenosť pre zapojenie do projektov na národnej úrovni.*

CENAA
Tolstého 9
811 06 Bratislava
E-mail: office@cenaa.org