Kybernetická bezpečnosť jednou z tém Visegrad Youth Forum 2014

Na druhej panelovej diskusii, ktorá sa uskutočnila v rámci Vyšehradského mládežníckeho fóra na pôde Fakulty politických vied a medzinárodných vzťahov dňa 28. 11. 2014, vystúpili riaditeľka CSIRT.SK Petra Hochmannová, vojenský analytik z Inštitútu pre bezpečnosť a obranu Akadémie ozbrojených síl generála Milana Rastislava Štefánika Milan Hanko a Nikola Schmidt, ktorý pôsobí na Karlovej Univerzite v Prahe. Panelovú diskusiu moderoval Rastislav Kačmár z Euroatlantického centra.

Ako prvá začala Petra Hochmannová, ktorá okrem priblíženia činnosti CSIRT, krátko zhrnula históriu kybernetickej bezpečnosti. Zdôraznila, že v období, keď vývoj malwarov napreduje vysokou rýchlosťou, je nie len potrebné venovať pozornosť vzdelaniu v danej oblasti, ale aj bližšej spolupráci na medzištátnej a súkromnej úrovni. S ostatnými rečníkmi sa zhodli, že na dôsledky kybernetických útokov dopláca najmä civilné obyvateľstvo. Taktiež spomenula českú iniciatívu na vytvorenie platformy pre kybernetickú bezpečnosť v oblasti strednej Európy.

Major Milan Hanko, ktorý vystúpil ako druhý, ponúkol pohľad z perspektívy ozbrojených síl. Poukázal, že na poslednom summite NATO vo Walese sa zmenila stratégia a prístup, najmä v oblasti kybernetickej bezpečnosti. Dotkol sa aj témy diskutovaného článku číslo 5 Washingtonskej zmluvy. Vyjadril názor, že obrana kybernetického sektora neznamená primárne jeho militarizovanie, nakoľko najviac býva zasiahnutý súkromný sektor. Podľa jeho názoru niektoré krajiny ako napríklad Rusko a Čína venujú veľkú pozornosť prevencii, avšak Slovenskej republike chýba vypracovaná adekvátna stratégia.

Následne vystúpil so svojím príspevkom Nikola Schmidt, ktorý vysvetlil akademický postoj ku kyberpriestoru cez 3 diskurzy : vojenský, verejný a spravodajský. Poukázal na fakt, že poznatky potrebné na vývoj obranných systémov nie sú totožné s tými, potrebné na vývoj útočných kapacít. Taktiež z pohľadu medzinárodného práva, nemôžeme za kybernetické útoky viniť krajiny, pretože hlavný problém spočíva vo vytýčení hraníc štátov v kybernetickom priestore. Nie je ľahké určiť odkiaľ útok pochádza, keďže hackerské skupiny využívajú decentralizáciu sietí.

Po troch príspevkoch nasledovala diskusia, kde účastníkov zaujímala možnosť vytvorenia efektívnej ochrany pred kybernetickou kriminalitou, ako napríklad špeciálnej jednotky pre Slovenskú republiku. Diskutujúci poukázali na kapacity a možnosti NATO a vyjadrili názor, že vytvorenie jednotky s útočnými kapacitami a schopnosťami by bolo komplikované a zároveň by to nebolo v záujme štátov patriacich do vyšehradskej štvorky. Jednou z ďalších diskutovaných tém bola možnosť napadnutia a následného zneužitia Bitcoinu v kybernetickej vojne. Okrem toho boli spomenuté aj kybernetické útoky z Ruska, cielený útok na iránsky jadrový program, ako aj použitie nových typov útokov počas vojny v Iraku. Po skončení panelovej diskusie boli účastníci rozdelení do workshopových skupín, kde každý predstavoval ministra zahraničných vecí jednej z krajín V4. Okrem prezentácie vlastných názorov riešili konkrétne situácie, ktorým čelili krajiny v nedávnej minulosti. Jednou z nich bola napríklad prerušená dodávka elektrického prúdu v Poľsku, a to následkom hackerskej aktivity.

EAC - Euroatlantické centrum
Kuzmányho 3, 974 01 Banská Bystrica, Slovak Republic
tel./fax: +421 48 415 1689, e-mail: eac@eac.sk, web: www.eac.sk

Regional Office Bratislava
Campus of the University of Economics, Dolnozemská cesta 1, 852 35 Bratislava, Slovak Republic tel.
+421 2 6729 5164