Bucureşti, 24 noiembrie 2015

„Protecția infrastructurii cibernetice: provocări și oportunități”

Asociaţia **New Strategy Center**a organizat marţi, 24 noiembriea.c., la Cercul Militar Naţional, dezbaterea cu titlul: **„Protecția infrastructurii cibernetice: provocări și oportunități”**. Această dezbatere face parte din seria evenimentelor dedicate securității cibernetice, prin care **New Strategy Center** își propune să pună la dispoziția invitaților săi expertiza unor personalități din țară și din străinătate și să ofere o platformă de dialog pentru instituțiile cu responsabilități în domeniul securității cibernetice, companii de profil și experți din mediul academic.

Noile amenințări care apar în mod constant în spațiul cibernetic, corelate cu vulnerabilitățile sistemelor IT&C, preocupă din ce în ce mai mult statele din spațiul euroatlantic și nu numai. În ultimii ani, atacurile cibernetice la adresa infrastructurilor critice ale unor state s-au dovedit extrem de periculoase, afectând deopotrivă instituțiile guvernamentale și mediul de afaceri.

Atât la nivelul NATO, cât și la nivelul UE s-au depus eforturi pentru elaborarea unor strategii și politici destinate creșterii nivelului de protecție a infrastructurilor cibernetice, în special a celor care susțin infrastructurile critice naționale. Preocuparea pentru infrastructura critică cibernetică a relevat importanța realizării unui larg parteneriat public-privat, sectorul privat dovedindu-se adesea mai dinamic și mai eficient decât instituțiile publice în dezvoltarea de soluții protective și în construcția de sisteme reziliente. Pe baza Strategiei de Securitate Cibernetică, România urmărește păstrarea unui mediu virtual sigur, precum și creșterea gradului de reziliență a infrastructurilor cibernetice naționale, care să constituie suportul pentru securitatea națională, precum și pentru protejarea mediului de afaceri și a societății românești.

Una dintre temele discutate s-a referit la amenințările la adresa infrastructurii cibernetice și mijloacele de contracarare. Astfel, în domeniul cibernetic există 4 mari categorii de amenințări, fiecare cu caracteristicile sale. Cele mai periculoase și mai sofisticate astfel de amenințări sunt cele **statale** și cele ale **criminalității** organizate. Acestea prezintă un înalt grad de sofisticare, iar capabilitățile tehnice folosite sunt de cel mai înalt nivel. Celelalte două tipuri de amenințări cibernetice sunt cele **teroriste** și cele **extremiste**. Acestea nu prezintă un real pericol datorită nivelului tehnic foarte redus. Până în acest moment, astfel de acțiuni s-au manifestat prin realizarea unor **defacement-uri** ale site-urilor instituțiilor publice. S-a mai discutat și despre nevoia unei legislații în domeniul cibernetic care să susțină acțiunile de contracarare unor atacuri din acest domeniu.

Un alt subiect al dezbaterii a fost nevoia cooperări dintre sectorul public și cel privat. Acest lucru este absolut necesar în condițiile în care o mare parte a infrastructurilor critice este deținut de mediul privat. În cazul unui atac asupra acestor infrastructuri critice ce ar avea ca efect distrugerea lor, statul va fi considerat vinovat. Astfel de atacuri nu îi vor afecta doar pe cei direct vizați, ci vor afecta întreaga populație/societate. Din acest motiv o colaborare strânsă între cele două medii este absolut necesară.

În cadrul dezbaterii, ca o completare la punctele mai sus menționate, a fost abordat și subiectul protecției datelor și sistemelor informatice utilizate în cadrul infrastructurilor critice. În acest caz, s-a reiterat nevoia unei mai bune colaborări între sistemul sectorul public și cel privat, precum și necesitatea unor stimulente financiare pentru cei ce activează în domeniul IT.

O alta temă importantă care a fost dezbătută în cadrul acestei dezbateri s-a referit la cadrul legislativ necesar susținerii activității de protecție a infrastructurii cibernetice. În acest sens, în România nu există o lege a securității cibernetice. Principiul ce trebuie avut mereu în vedere este identificarea unui echilibru între a folosi cele mai bune tehnici și practici și respectarea drepturilor fundamentale ale omului. Astfel legea securității cibernetice trebuie să asigure atât combaterea amenințărilor cât și protecția intimității populației.

În cadrul aceleiași dezbateri s-a mai discutat și despre dezvoltarea unui standard național de protecție cibernetică care să creeze o cale spre un spațiu cibernetic mai sigur. A mai fost abordat și subiectul educației care ar trebui să joace un rol important în formarea acelor comportamente care să susțină securitatea cibernetică, începând, mai ales, cu copiii din ciclul gimnazial.