**Izlaganje ministra Milice Pejanović-Đurišić na otvaranju okruglog stola na temu „Cyber security“**

Dame i gospodo,

Poštovani učesnici okruglog stola,

Zadovoljstvo mi je što imam priliku da govorim na otvaranju okruglog stola „Cyber security“, s obzirom da je riječ o izuzetno aktuelnoj temi koja svakim danom dobija na važnosti. Sigurna sam da će današnji direktan razgovor biti dobra prilika za razmjenu mišljenja o pitanjima od zajedničkog interesa. Svakako želim da se zahvalim našim domaćinima, kompaniji „Microsoft Montenegro“ na inicijativi i organizaciji ovog okruglog stola

Bezbjednost sistema zasnovanih na informaciono komunikacionim tehnologijama predstavlja sve veći globalni izazov. Svjedoci smo sve većeg broja cyber napada čime se osjetljivi podaci, kako lični tako i poslovni, mogu naći na otvorenim mrežama. Na taj način se stvaraju uslovi i za ometanje aktivnosti od društvenog značaja koje za posljedicu, često, imaju ogromne troškove u privredi, čime, posredno, negativno utiču i na svakodnevni život naših građana.

Podaci pokazuju da, u ovom vremenu ozbiljne krize, cyber kriminal predstavlja aktivnost čiji obim ima dvocifreni rast, kao što je to uostalom slučaj i sa drugim nelegalnim aktivnostima. Pri tome, za razliku od vremena prije nekih 15tak godina kad su većinu onih koji su hackovali sisteme ili napadali mreže i web sitove predstavljali tinejdzeri koji su to radili iz zabave ili potrebe socijalnog dokazivanja, danas je cyber kriminal mnogo ozbiljnija pojava motivisana vrlo često ne samo željom za sticanjem nelegalne finasijske dobiti. U tim uslovima, i efekti cyber kriminala postaju sve ozbiljniji za pojedince, za preduzeća pa i za vlade.

Upravo iz tih razloga potrebno je podići svijest, kako građana, tako i nadležnih državnih institucija o tome koliki je značaj uspostavljanja stabilne infrastrukture kojom ćemo zaštiti cyber-prostor. U tom kontekstu, neophodan je dodatni napor kako bi se što bolje upoznali sa različitim prijetnjama i izazovima koje u smislu ukupne bezbjednosti potiču od sve veće implementacije info-komunikacionih tehnologija , servisa i aplikacija.

U skladu sa naporima koji se ulažu na globalnom nivou, i Vlada Crne Gore se suočava sa potrebom dodatnog angažmana u pravcu uspostavljanja i dograđivanja adekvatnog zakonodavnog okvira sa ciljem postizanja većeg nivoa informacione bezbjednosti. Kako bi kreirali mehanizme za pravovremene i efikasne odgovore na potencijalno veoma štetne cyber napade, neophodno je postići visok stepen interkonektivnosti i interoperabilnosti na nivou državnih organa, uz izradu nacionalne strategije koja obuhvata mjere za postizanje cyber bezbjednosti, uključujući cyber odbranu, kao i mjere za odvraćanje potencijalnih napada. Pri tome je jasno da čisto nacionalne politike i strategije cyber odbrane ne mogu ni izdaleka biti dovoljne, s obzirom na činjenicu da je riječ o izazovima koji zaista imaju globalni karakter.

Polazeći od tih činjenica, Ministarstvo odbrane je u prethodnom periodu sa NATO partnerima dinamiziralo aktivnost na polju cyber odbrane, polazeći od usvojenog strategijskog koncepta fokusiranog na razvijanje sposobnosti država članica da koordinirano preveniraju, detektuju, da se odbrane i da se oporave od eventualnih cyber napada. Tako je, u ovoj fazi, konkretna saradnja pokrenuta kroz program „Nauka za mir i bezbjednost“ koji je namjenski osmišljen za Crnu Goru, Bosnu i Hercegovinu i Makedoniju.

Saradnja je intenzivirana kroz mogućnost participiranja na vježbama i radionicama u organizaciji NATO Alijanse, a naučene lekcije se koriste u cilju povećanja stepena nacionalne bezbjednosti.

U Ministarstvu odbrane nastojimo da razvijemo i unaprijedimo sposobnosti i vještine zaposlenih i pripadnika Vojske Crne Gore, uspostavljaju se potrebne organizacione cjeline, razvijaju se politike i uspostavlja saradnja, kako na nacionalnom tako, i na medjunarodnom nivou. Cilj je da budemo konstruktivan partner u procesu odbrane suvereniteta Crne Gore i u cyber-prostoru.

Naravno, kao i kod svih razvojnih projekata i ovdje se suočavamo sa izazovom finansiranja uspostavljanja i funkcionisanja projekata koji zahtijevaju i visok nivo ekspertskih znanja. Upravo zbog toga, želim naglasiti da siguran cyber-prostor nije imperativ samo ministarstava i Vlade. Sigurno je da i ostali segmenti javnog sektora, univerziteti prije svega, pa onda i privatni sektor imaju svoju ulogu i dio odgovornosti i u tom smislu svakako treba naći adekvatne modalitete saradnje i koordinacije budućih aktivnosti.

Upravo u tom kontekstu i ovu i slične manifestacije treba iskoristiti i kroz otvorenu diskusiju, identifikovati oblike buduće informaciono-bezbjednosne obrambene saradnje, prioritete u njihovoj realizaciji, i tako osigurati racionalnije trošenje vremena i sredstava na putu integracija u NATO i Evropsku Uniju. U očekivanju dalje saradnje, želim vam uspješan rad i zahvaljujem se na pažnji!