Govor ministra za obrambo mag. Mateja Tonina na srečanju predsednikov odborov parlamentov EU za evropske zadeve, 19. julija 2021 – odpornost kritične infrastrukture in kibernetska varnost

Spoštovani gospod Lepassaar, dr. Svete, predsedniki in predstavniki parlamentov. Pozdravljeni tudi v mojem imenu.

V veselje mi je, da vas lahko nagovorim ob tej priložnosti. Današnji panel je v luči osrednje prioritete slovenskega predsedovanja Svetu EU zelo dobrodošel in aktualen. Odpornost je visoko na naši agendi, s sloganom »Skupaj. Odporna. Evropa.« pa opozarjamo tudi na pomen sodelovanja pri doseganju skupnih ciljev. Na področju zagotavljanja kibernetske varnosti je to še posebej pomembno.

Sodobna družba je vse bolj odvisna od neprekinjenega in zanesljivega delovanja komunikacijsko informacijskih sistemov in omrežij ter dobave električne energije. Razvoj novih tehnologij in hitra digitalizacija prinašata številne družbene koristi, po drugi strani pa porast ranljivosti, tveganj in groženj. V takšnih razmerah pride do pojava specifičnih izzivov, s katerimi se države in organizacije ne morejo več učinkovito soočati samostojno.

V tem kontekstu delovanje kritične infrastrukture že dolgo ni več samoumevno. Izpadi v delovanju kritične infrastrukture in zagotavljanju ključnih storitev lahko potencialno znatno ohromijo delovanje družbe, povzročijo ekonomsko škodo in ogrozijo suverenost države.

To je dodatno izpostavila pandemija COVID-19, v obdobju katere so bile v več državah številne bolnišnice in druge zdravstvene ustanove, energetska infrastruktura in drugi sektorji tarče kibernetskih napadov.

Ti nediskriminatorni in obsojanja vredni napadi so utrdili zavedanje, da moramo za tovrstno infrastrukturo zagotoviti posebno in celovito zaščito ter razviti učinkovite ukrepe za odpravo ranljivosti in okrepitev odpornosti naših družb.

Pridobljene izkušnje iz pandemije so nas opozorile tudi na medsebojno odvisnost, potrebo po usklajenem delovanju in odzivanju ter solidarnost. Integracija tovrstnih izkušenj je bistvenega pomena pri razvoju učinkovitih rešitev za zaščito kritične infrastrukture. Pri tem je potrebno izpostaviti tudi doprinos raziskovalnega dela in javno-zasebnih partnerstev ter medsebojno izmenjavo informacij in dobrih praks.

Glede na pomen kibernetske varnosti za odpornost kritičnih subjektov moramo nadaljevati z usklajenimi prizadevanji tudi na tem področju. Zagotovitev odprtega, zanesljivega, varnega in predvidljivega kibernetskega prostora je ključnega pomena za nemoteno delovanje družbe in države.

Na tej podlagi in v skladu z našimi prioritetami predsedovanja Slovenija pozdravlja predloga novih direktiv - revidirane Direktive o varnosti omrežij in informacijskih sistemov (NIS 2) in Direktive o odpornosti kritičnih subjektov (CER), ki sta skupaj z novo EU strategijo kibernetske varnosti pomemben del paketa krepitve odpornosti EU.

Direktivi urejata različne vidike, vendar sta povezani z vidika obsega bistvenih oziroma kritičnih subjektov. Ker se dopolnjujeta, moramo zagotoviti njuno medsebojno usklajenost, za kar si bomo še posebej prizadevali tekom našega predsedovanja. Glavno je, da direktivi zadostita dejanskim potrebam in v svojih področjih uporabe naslovita ključna vprašanja.

Pomemben vidik CER Direktive bo zagotovitev enotnega okvira za obravnavanje odpornosti kritičnih subjektov in odzivanje vseh držav članic. Potrebujemo dovolj prožen in pragmatičen pristop, ki bo državam članicam omogočal prilagoditve že vzpostavljenih nacionalnih sistemov, ne pa tudi konceptualnih sprememb. Pri tem se zavzemamo za opredelitev skupnih minimalnih pravil, ki bodo omogočala harmonizacijo CER Direktive z že vzpostavljenimi koncepti zaščite kritične infrastrukture.

Tveganja povezana s kibernetsko varnostjo bo medtem naslovila revidirana Direktiva o varnosti omrežij in informacijskih sistemov (NIS 2).

NIS direktiva predstavlja temelj evropske kibernetske odpornosti, zato bo delo na njeni reviziji ključnega pomena. Za Slovenijo in druge države članice je bila ta direktiva pomemben element krepitve nacionalne kibernetske varnosti in vzpostavitve medsebojnega sodelovanja.

Z njeno revizijo bomo odpravili obstoječe pomanjkljivosti, postavili temelje za prihodnjo krepitev kibernetske varnosti in zagotovili večjo harmonizacijo med državami članicami. V času našega predsedovanja pričakujemo splošni pristop in morebitni pričetek trialoga z Evropskim parlamentom.

Poleg dela na NIS direktivi moramo skupna prizadevanja usmeriti tudi v izboljšanje koordinacije in sodelovanja na ravni EU z zagotovitvijo ustrezne povezave med državami članicami in relevantnimi institucijami, telesi in agencijami EU.

Napredek zadnjih nekaj let je očiten, vendar je prostora za rast še veliko. Če želimo ohraniti dosežke in jih nadgraditi, moramo nadaljevati s krepitvijo skupnega situacijskega zavedanja in kolektivne sposobnosti odzivanja. Pri tem kot pomemben element dopolnitve EU okvirja kibernetskega kriznega upravljanja pozdravljamo predlog Komisije glede Skupne kibernetske enote.

Delo na Svetu je usmerjeno v podrobno analizo predloga in oblikovanje skupnega stališča. Prizadevanja morajo temeljiti na obstoječih pobudah sodelovanja, ki že uspešno delujejo, in na obstoječih mandatih. Za uspeh pobude bo ključnega pomena, da se zagotovi ustrezna vključenost in vloga držav članic. Prav tako vidimo priložnost, da se skozi to pobudo naslovi delo na krepitvi kibernetske varnosti EU institucij. Pričakujemo, da se bo tesno sodelovanje med vsemi relevantnimi deležniki, ki so pomembni za okrepitev situacijskega zavedanja in koordiniranega odzivanja na ravni EU, nadaljevalo tudi v prihodnje.

Hkrati se kibernetski prostor vse bolj uveljavlja kot domena vojaškega delovanja, zato so z namenom izboljšanja celostnega kriznega odzivanja EU pomembna tudi naša prizadevanja na področju kibernetske obrambe,

vključno s krepitvijo mreže vojaških CERT. V tem kontekstu pa je vse bolj pomembno omogočanje in spodbujanje civilno-vojaškega sodelovanja.

Z aktualnimi in prihodnjimi izzivi kibernetskega prostora se bomo težko učinkovito soočali, če ne bomo razpolagali s sodobnimi zmogljivostmi in tehnologijami, zato so investicije in naložbe na tem področju nujne. Pri tem je potrebno izkoristiti mehanizme, ki jih v ta namen nudi EU.

Kljub najsodobnejšim zmogljivostim pa bo te izzive nemogoče naslavljati brez usposobljene in kvalificirane delovne sile. V tem kontekstu EU ponuja številne edinstvene priložnosti za profesionalni razvoj kibernetskih strokovnjakov držav članic. Nadaljnji razvoj izobraževanja, usposabljanja in vaj na EU in hkrati nacionalni ravni bo pripomoglo k pridobivanju in zadrževanju tovrstnih strokovnjakov. Upam, da si bomo tekom današnje razprave izmenjali več inovativnih idej za naslovitev te problematike, s katero se soočamo tudi v Sloveniji.

V okviru EU imamo države članice na razpolago različne instrumente in mehanizme za kolektivno odzivanje. Članice smo spodbujene k izmenjavi informacij, krepitvi sodelovanja, izgradnji skupnega situacijskega zavedanja in povezovanja različnih skupnosti, kar navsezadnje znatno prispeva h krepitvi medsebojnega zaupanja. To je osnova za učinkovito kolektivno delovanje. Mislim tudi, da pobude EU pomembno dopolnjujejo nacionalna prizadevanja za krepitev odpornosti. Zaradi naštetega moramo znotraj EU izkoristiti razpoložljiv potencial in poglabljati medsebojno sodelovanje, tudi z drugimi mednarodnimi organizacijami, zlasti z Natom.

Da bi dosegli te ambicije, moramo zagotoviti skladnost med mednarodnimi in nacionalnimi prizadevanji. Z nacionalnega vidika to vključuje visoko raven medresorske koordinacije na strateški in operativni ravni ter nenehne izboljšave sistema kibernetske varnosti. Na ministrstvu za obrambo te cilje zasledujemo z ustanovitvijo novega organa, ki bo zagotavljal učinkovitejše upravljanje kibernetske varnosti in izmenjavo informacij z ustreznimi organi.

Verjamem, da se bomo z vzpostavitvijo resnične kulture sodelovanja in s celovitim pristopom lahko kolektivno soočali z izzivi digitalne dobe, okrevali od morebitnih kriz in zagotovili gospodarsko prihodnost EU. V duhu našega slogana: »Skupaj. Odporna. Evropa.«

Hvala za pozornost.