Daamid ja härrad, sõbrad!

Tere tulemast Tallinna, väikesesse linna, millel on siiski huvipakkuv koht sõjakunsti ajaloos. 1219. aasta juunis lõid eestlased Toompeal lahingut taanlastega, ühega paljudest meie maad vallutanud rahvastest. Lahingu käik oli meile soodne, taanlaste käsi käis kehvasti ning eestlaste võit näis olevat käeulatuses. Kuid siis, hetkel, mil taanlased olid alistumas, langes taevast alla lipp – valge rist punasel taustal. Kuningas, olles püüdnud lipu kinni enne, kui see jõudis maad puudutada, tõstis selle kõrgele ning lehvitas oma julguse kaotanud sõjaväe ees, andes neile sel moel taas lootust ning viies nad võidule. Lipp, nimega Dannebrog, on ka tänapäeval Taani riigilipp, olles üks vanimatest kasutusel olevatest lippudest maailmas.

Tehnoloogia, sedakorda jumalik, kavaldas eestlased 1219. aastal üle. Hiljem sai Tallinnast linnamüüri ja vallikraaviga ümbritsetud linn; linnamüüri täiendasid tornid, vallid ja langevõredega väravad. Kõik need toimisid seni, kuni püssirohi nii meil kui ka mujal Euroopas kaitsemüüridest tugevamaks osutus.

Esmakordsed Talllinna külastajad avastavad peagi, et siin asub üks Euroopa suurimaid keskaegseid vanalinnu. Mitte küll seetõttu, et Tallinn ise oleks väga suur olnud, vaid tänu asjaolule, et ajal, mil suur osa Euroopa linnamüüridega ümbritsetud linnadest Teise maailmasõja õhurünnakutes hävitati, pääses Tallinn veidi kergemalt tänu asjaolule, et… 1944. aasta suures pommirünnakus osalenud lennukid ei tabanud märki.

Kõike seda räägin ma sissejuhatuseks seetõttu, et tahan öelda seda: tehnoloogia muutumise või ootamatu rakendamise korral muutuvad senised kaitsemehhanismid kasutamiskõlbmatuks.

Käesolev konverents leiab aset kaks ja pool aastat pärast 2007. aasta maikuus Eesti vastu suunatud DDoS (*Distributed Denial of Service*) küberrünnakuid. Mis veelgi olulisem, pärast 2007. aastat on sarnaseid rünnakuid toime pandud ka Leedu, Gruusia ja Kasahstani vastu. Rünnatud on ka USA, Saksamaa, Prantsusmaa ja Lõuna-Koera ministeeriume ja valitsusasutusi, sageli kaitsevaldkonnaga seotuid. See on aidanud küberrünnakutele

rahvusvahelises plaanis senisest rohkem tähelepanu juhtida.

Vaatamata sellele, et DDoS rünnakuid ei ole väga keeruka tehnilise olemusega, olid need siiski mitmel põhjusel väga olulised:

1) Rünnete eesmärgiks oli suurendada ühiskonna rahulolematust demokraatlikult valitud valitsuse sisepoliitika suhtes ning seega on need käsitletavad sekkumisena demokraatlikesse süsteemidesse, kasutades selleks uusi meetodeid, jätkates samas eelnevalt järgitud poliitika kohaldamist.

2) Vaatamata paljudele ajakirjanduses kajastamist leidnud mõttetustele olid rünnakud ilmselgelt organiseeritud. Need olid organiseeritud, kuna nende intensiivsus ei olnud stohhastiliselt juhuslik ega vastanud Gaussi ega ühelegi muule tavapärasele jaotusele. Nagu näitas CERT Eesti (*Computer Emergency Response Team*) koostatud DDoS rünnakute graafik, lõppesid need 9. mail täpselt kell 24.00, mis kahtlemata ei ole seotud nimetatud päeva ajaloolise tähendusega paljude riikide jaoks. Kui küsisin osakonna juhatajalt, kuidas on see võimalik, vastas tema: arvatavasti sai neil raha otsa.

3) On olemas tõendid, mille põhjal on alust arvata, et osaliselt sponsoreeriti rünnakuid riiklikul tasandil. Gruusia vastu suunatud küberkampaaniat uuriva USA Küberkuritegude vastase üksuse värskeima ettekande kohaselt olid nimetatud riigis asuvate kodulehekülgede vastu suunatud rünnakute korraldajad Venemaa sõjalistest kavatsustest eelnevalt teadlikud. Teisisõnu, rünnakuid oli ilmselgelt kooskõlastatud riigi sõjaväeliste ringkondadega ning seega võib neid käsitleda rahvusriigi suveräänsuse võimaliku rikkumisena; mis veelgi häirivam, need võivad illustreerida uut peatükki kübersõjariistade arengus. Kui lubate, siis koguni era- ja avaliku sektori partnerlust.

Hiljutiste rünnakute seisukohast on kõige olulisemad ilmselt teemad, mis nendega seoses päevakorrale kerkivad ning nõrgad kohad, mis nende tagajärjel nähtavaks saavad. Meil ei ole enam aega pikkadeks teoreetilisteks aruteludeks; reaalne igapäevaelu ootab meilt kiireid vastuseid ja tegevust.

Oleme tõdenud, et tehnilisest küljest muutuvad küberrünnakud järjest keerukamaks ning enam ei saa nende puhul rääkida suhteliselt lihtsatest DDoS rünnetest. On näha häirivaid märke, mille

kohaselt näitab küberrünnakute kasutussagedus nii avaliku kui erasektori poolt kahanemise asemel kasvutendentsi.

Kaasaegsed ühiskonnad sõltuvad internetipõhistest lahendustest. Neist on saanud meie igapäevaelu olulised komponendid – majandustegevuse, suhtlemisprotsesside, riigijuhtimise ja kodanike igapäevaste asjatoimetuste lahutamatu osa.

Riigi jaoks, mida esindan mina, on internet olnud üliolulise arengu- ja kaasajastamismootoriks; see on andnud meile võimaluse ületada ainsa hüppega kuristik nõukogudeaegse mahajäämuse ja tänapäevase tipptasemel tehnoloogia vahel.

Inimeste poolt tahtlikult või tahtmatult esile kutsutud küberkorratuste vastu suunatud reageerimisvõime arendamine nõuab märkimisväärset koostööd nii riikide siseselt kui ka *piiride üleselt*
; selleks on möödapääsmatu era- ja avaliku sektori rollikandjate laiapõhjaline koostöö ning riikidevaheline koordineeritud tegevus nii rahvusvahelisel kui ka regionaalsel tasandil.

Sooviksin esmalt käsitleda riiklikul tasandil rakendatavaid meetmeid.

Siinkohal tuleb keskenduda kolmele peamisele valdkonnale: avalikkuse küberturvalisuse ja -ohtude teemalise teadlikkuse tõstmine; avaliku- ja erasektori vaheline koostöö ja avalike haldusstruktuuride tugevdamine.

Esiteks, sihipärased jõupingutused üldsuse teadlikkuse suurendamiseks antud valdkonnas on tugevapõhjaliste otsuste aluseks. Inimesed peavad olema teadlikud materjalide kahtlastelt saitidelt allalaadimisega kaasnevatest ohtudest.

Samas ei tohiks me piirduda üksnes interneti ohutu kasutamise propageerimisega erasektoris. Meie püüdlused peaksid jõudma ka erinevate arvamusliidrite ja otsustajateni – poliitikute, ettevõtete juhtide ja ajakirjanikeni. Paljude riikide poliitikutel on vähe kogemusi arvutitehnoloogia uusimate arengute valdkonnas. Ettevõtlussektor ei pruugi huvituda IT arengutest, mis jäävad nende enda turunišis vajalikest rakendustest väljapoole.

Teisisõnu, küberjulgeolekuga seonduvatest teemadest peab saama rahvuslikku julgeolekut käsitleva diskursuse oluline komponent. Lõpuks muutuvad nimetatud teemad nii või teisiti peavooluküsimusteks, kuid meie huvides on ilmselgelt ise sündmuste käiku juhtida, laskmata sündmustel juhtida meid.

Teiseks, riiklikul tasandil on vajalik tegevuste senisest oluliselt parem koordineerimine nii erinevate riiklike ametkondade vahel kui siseselt, kaasa arvatud korrakaitseorganid, seadusandjad, kriisireguleerimisüksused ja sõjavägi.

Siinkohal tunnistan ausalt, et tunnen muret: paistab, et meil puudub antud valdkonnas võimekus, mis on vajalik vastutuse ja pädevuse adekvaatseks jagamiseks riiklikul tasandil. Mõned ametkonnad ei soovi kätte võidetust loobuda või pole lihtsalt huvitatud sellest, et keegi nende valdustesse trügib; teistel ametkondadel seevastu puudub võimekus, mis on vajalik selleks, et lahendada tänu kaasaegse tehnoloogiale neile kaela sadanud probleeme.

Teisisõnu, teatud tehnoloogilises kontekstis toiminud ülesannete ja kohustuste jagamine valitsusasutuste vahel ei pruugi täna enam sobivaks osutuda. Hetkel, mil sind pommitab Nõukogude armee (nagu see 1944. aastal juhtus), pole enam oluline, kes vastutab keskaegse linna vallikraavide, kaitserajatiste ja langevõrede eest.

Konkreetsemalt, eriti suure tähtsusega on horisontaalne koostöö majanduslike ja ühiskondlike institutsioonide ja korrakaitseorganite vahel. Ja kolmandaks, erasektori kaasamine on täiesti möödapääsmatu. Ilma avaliku- ja erasektori partnerlusteta ei ole tõhusate või toimivate lahenduste leidmine võimalik.

Adekvaatse strateegia väljatöötamise võtmeks on siiski rahvusvahelise tasandi tegevused. Lõppeks on küberründed, küberkuritegevus ja küberterrorism, *a priori*, piiriülesed probleemid. Pahatahtlike küberrünnakute eest vastutavad isikud vajavad juriidilisi piire, mille taga end varjata. Riigisisest võimekust arvestades peaks küberterrorist, kes otsustab rünnata omaenda riigis asuvaid ametkondi, olema üsna rumal.

Oluliseks teemaks, millele tähelepanu pöörata, on rahvusvaheline koostöö kriitiliste

infoinfrastruktuuride kaitsmise valdkonnas.

Me oleme tunnistajaks olnud tervele reale edukatele algatustele: Euroopa Nõukogu küberkuritegevuse konventsioon ja terrorismi ennetamise Euroopa konventsioon, mis võeti vastu Euroopa Nõukogu heakskiidul, on siinkohal suurepärasteks edunäideteks. Ka Euroopa Liit on vastu võtnud rea olulisi määrusi.

Nimetatud lepped ei ole mitte üksnes üle-euroopalised, vaid neis võivad osaleda ka muud riigid. Konventsiooni on ratifitseerinud USA; Küberkuritegevuse Konventsioonile on alla kirjutanud Kanada, Jaapan ja Lõuna-Aafrika; enam kui sada maailma riiki kasutab seda asjaomaste õigusaktide väljatöötamisel juhendmaterjalina.

Riikide soov täita Euroopa Nõukogu küberkuritegevuse konventsioonist tulenevaid kohustusi on käsitletav omamoodi lakmuspaberina, mis kajastab riigi valmisolekut antud valdkonnas koostööd teha.

Selles valguses on eriti kahetsusväärne asjaolu, et Venemaa on otsustanud nimetatud konventsiooniga mitte ühineda.

On neid, kes väidavad, et reguleerimissüsteem on praeguse seisuga nõrgalt arenenud ning adekvaatne kaitse on tagatud üksnes täiendavate piirangute kehtestamise korral.

Teisalt on ka neid, kes kinnitavad, et täiendavate regulatsioonide kehtestamine pole vajalik, pooldades mitteametlikku ehk isereguleeruvat süsteemi – eks ole ju interneti tegelikuks eesmärgiks tõkete kõrvaldamine vaba infovahetuse teelt, mitte nende püstitamine. Suure tõenäosusega on mõlemal vastasleeril osaliselt õigus.

Rahvusvahelise reguleerimissüsteemi tugevdamisel tuleb olla ettevaatlik ning vältida ülepeakaela välja töötatud lahendusi, mis osutuvad töökõlbmatuteks või ei võta arvesse reguleeritava võrgustiku keerulist olemust. Uusi õiguslikke reguleerimismehhanisme välja pakkudes tuleb hoiduda vaba infovahetuse ja sõnavabaduse hävitamist internetis.

Ja nüüd, mu daamid ja härrad, tuleb esitada järgmine küsimus: milline on selles kõiges NATO roll?

Me kõik oleme lähimineviku tõttu teadlikud asjaolust, et poliitikast motiveeritud küberrünnakutel on erinevad vormid; neil on erinev keerukusaste ja sihtmärgid. Nimetatud rünnakute tagajärjel on mitmed riigid oma küberstrateegiad üle vaadanud ning hakanud omakorda rõhutama vajadust koostöö kui tõhusa küberkaitse olulise osa järele.

Artiklis 5 on sätestatud ülim rahvusvaheline kaitsemehhanism, mida rakendatakse NATO riikide vastu suunatud relvastatud ründe korral. Hiljuti aset leidnud küberintsidendid ei ole vähemalt otsustajate seisukohast (veel) ületanud relvastatud ründele kehtestatud piire, kuid tekitavad rahvusvahelisele kogukonnale siiski märkimisväärset peavalu. Teisisõnu, rünnakud on endast kujutanud tõsist probleemi, kuid ei ole tekitatud kahju pinnalt lähtudes veel samaväärsed konventsionaalse kallaletungiaktiga. Samas tuleks neile küsimustele siiski mõelda, kuna raketi või viiruse poolt rivist välja löödud elektrivõrk jääb siiski rivist väljalöödud elektrivõrguks. Esimene variant on päris kindlasti käsitletav Artiklis 5 kirjeldatud olukorraga, teine mitte. Selleks, et asja veelgi ebamäärasemaks ajada, mõelgem taktikalist tuumarelva kasutades antud EMP impulssi, mille ainsaks eemärgiks on riigi side- ja elektrivõrgustike rivist väljalöömine. Vahendit, mida selleks kasutatakse – ja mis on tegelikult pahavaraga samaväärne – on käsitletud Artiklis 5.

Tekitades „Küberartikli 5” kohaldamiseks vajalikku valmisolekut (millest saab, vastandina Euroopa Liidule või Euroopa Nõukogule, NATO „nišš” globaalse küberjulgeoleku alaste päevakorraliste küsimuste lahendamisel), on oluline näha kollektiivkaitset küberrünnakute tõrjemehhanismi osana laiemas plaanis (kaasates korrakaitseorganeid, infoinfrastruktuuride pakkujaid ja infoühiskonna sidusgruppe).

Seega on Artikli 5 rakendamine rahvusvahelise rahu ja sõbralike suhete tagamisel küberkeskkonnas tihedalt seotud sellega, kuidas riigid korraldavad „Artiklis 4 viidatud valmisoleku” tagamise – st üldise koostöö küberkuritegevusega võitlemisel, info vahetamise võimalike ohtude ja kaitsemeetmete kohta, jne. Kollektiivkaitse on üles ehitatud individuaalsele kaitsele. Individuaalsed kaitsemehhanismid (riikide, organisatsioonide, üksuste tasandil) peavad olema koordineeritud ja kooskõlastatud, vältimaks halle alasid seadusandluses, mis lubaksid „kurikaeltel” (antud juhul niinimetatud „patriootlikel häkkeritel” või lausa spioonidel) seadusest tulenevast vastutusest pääseda.

Kollektiivseid kaitsemehhanisme ei saa käiku lasta „vigade parandamiseks” või riiklikul tasandil tehtud ettevalmistuste puudumise tõttu. Seega tuleb igal rahval mõelda oma osa täitmisele küberjulgeolekualases seadusandluses ja poliitikas, mis võib omakorda viia rahvusvaheliste arenguteni antud valdkonnas.

Selles kontekstis on Artikli 5 rakendamine tihedalt seotud Artikli 4 rakendamisega. Niipea, kui küberkonflikt ületab reaalselt Artiklis 5 sätestatud künnise (ja siinkohal juhiksin tähelepanu asjaolule, et mingeid eriti keerulisi prognoose ei ole siin vaja anda – kui see juhtub, oleme sellest nii või teisiti teadlikud), hakkavad kõige olulisemat rolli mängima rahuajal välja töötatud ja Artiklis 4 sätestatud koostöö tagamiseks rakendatavad õiguslikud ja poliitilised mehhanismid.

Ma ei taha sugugi väita seda, et NATO ja liikmesriigid ei peaks mõtlema Artikli 5 kohandamistingimustele. Teisisõnu, läbi mõtlema, milline on NATO kaasamise künnis; millised „kodutööd” tuleb ründe objektiks sattunud riigil kõigepealt ära teha, jne. Infoarhitektuuri olemusest tingitult on sõjaliste struktuuride võimalused efektiivsete meetmete rakendamiseks piiratud – eriti juhul, kui ründed on suunatud eraomandis olevate ja kriitiliste infrastruktuuride või potentsiaalselt kaheotstarbeliste objektide vastu.

Seega algab Artikli 5 kohaldamiseks vajalik valmisolek Artiklist 4 tuleneva valmisoleku tagamisest – otsustamisest, milliseid vastumeetmeid on potentsiaalselt võimalik rakendada riigis ja riikidevahelises mastaabis, milline on sõjaliste ning muude struktuuride vaheline tasakaal konflikti lahendamisel. Lisaks tuleb arvesse võtta ka niisuguseid aspekte, nagu vastulöögi proportsionaalsus, liitlaste konsensus NATO poolset reaktsiooni eeldava ründe tõsiduse ning rakendatavate jõumehhanismide ja meetmete osas.

Rääkimata küsimusest, mille lahendamisega on NATO-l pärast 9/11 aset leidnud sündmusi juba olnud vaja tegeleda: Kes on vastutav? Kuidas me otsustame, kes on vastutav? Ja mida teha siis, kui NATO ei jõua vastutuse osas kokkuleppele, nagu see väga vabalt juhtuda võib.

Lõpetuseks sooviksin tänada NATO kooperatiivse küberkaitse kompetentsikeskust ürituse korraldamise eest ning tervitada teid kõiki Tallinnas ja Eestis, kohas, mis pole mitte üksnes Jumala poolt taanlastele kingitud riigilipu, vaid ühtlasi – ja sugugi mitte juhusliku kokkusattumuse tõttu – Skype’i ja e-valimiste sünnikohaks ja kindlasti mitte juhuslikult ka esimene suveräänne riik maailmas, mille vastu on toime pandud dokumenteeritud

küberrünnakuid.

Tänan tähelepanu eest!