Küberjulgeolekule teed rajades

Ene Ergma (RiTo 8), Riigikogu esimees, Ühendus Vabariigi Eest – Res Publica

Küberrünnakuid tuleb teadvustada tegeliku, aktuaalse ja ülisuure ohuna demokraatlikele riikidele ja rahvastele. Küberjulgeolek peab kujunema NATO ja Euroopa Liidu tiheda koostöö prioriteediks.

Mulle meeldib Tiiu Grünthal-Roberti mõte – kui on tagatud avalik kord, on võimalik demokraatliku diskussiooniga edasi minna (Eesti Päevaleht, 22. X 2007). Seda on hea meenutada, mõeldes sellele, et Eesti on esimene riik Euroopa Liidus ja NATO-s, mis sattus tänavu aprilli lõpupäevil suuremahuliste, keskselt koordineeritud küberrünnakute ohvriks. Küberründe sihtmärgiks oli võetud ei rohkem ega vähem kui kogu riigi elektrooniline infrastruktuur.

Küberrünnak Eesti riigi vastu algas 27. aprillil. Meie elektroonilised tõrjesüsteemid tegid ja teevad tõhusat kaitse- ja tõrjetööd. Ükski võtmetähtsusega üleriigiline süsteem (pangad, riiklikud andmebaasid, üleriigilised sidesüsteemid) pöördumatult kahjustada ei saanud. Kuid kuna enamik avalikke, riigihalduslikke ja äriteenuseid Eestis funktsioneerib elektrooniliselt (97% pangatoiminguist tehakse Eestis Interneti vahendusel; suuresti Interneti-põhine on koolide, kaitse-, teadus- ja tervishoiuasutuste, energeetiliste süsteemide töö, samuti riigi haldustegevus ja välissuhtlemine), siis puudutasid rünnakud otseselt või kaudselt iga Eesti elaniku turvalisust, iga ettevõtet, kokkuvõttes Eesti kui 21. sajandi moodsa ja avatud riigi eksistentsi.

Eesti vastu suunatud küberterrorism

Kuidas peaks parlament käituma kriisisituatsioonis? Põhiseadusega on Riigikogul ette nähtud võimalus välja kuulutada erakorraline seisukord. Hea on tõdeda, et siiani pole seda sätet kasutada vaja olnud. Mida oleks pidanud tegema Riigikogu aprillikriisi ajal? Riigikogu viis erakonda toetasid täielikult ja üks mööndustega valitsuse tegevust kriisi ajal, sellise raske olukorra reguleerimine ongi valitsuse pärusmaa. Riigikogu liikmete tegevus oli põhiliselt suunatud situatsiooni selgitamisele kolleegidele väljaspool Eestit – nii intervjuude kui ka otsekontaktide kaudu.

On küllalt põhjust järeldada, et küberrünnakud, mis algasid ühel ajal ülesässitatud sovetimeelsete jõukude märatsemisega Tallinnas aprilli lõpus, ei ole juhuslik kokkulangevus, vaid niisamuti süsteemne ja koordineeritud vaenutegevus. Kuigi küberründed võivad kulgeda meieni füüsiliselt kogu maailmas laiali paiknevate arvutite kaudu, on alust arvata, et nimetatud ründed Eesti vastu olid valdavalt organiseeritud ja koordineeritud meie suures, vastavat kapatsiteeti omavas idapoolses naaberriigis. Internetis levitati venekeelseid, kogunisti riigiasutuste serveritelt lähtuvaid üleskutseid ja üksikasjalikke instruktsioone Eesti riigi küberruumi ründamiseks.

Arvestades küberrünnete ulatust ja organiseeritust, sarnaneb neil päevil Eesti vastu suunatud rünne ka terrorismiga, antud juhul küberterrorismiga. On küllaldaselt viiteid, et rünnakutega

on teiste hulgas seotud organiseeritud kuritegelikud rühmitised, kes varustavad tegelikke ründajaid *botnet*'idega. (*Botnet* on "kaaperdatud" arvutite robotvõrk, mida kasutatakse rünnete korraldamiseks või rämpsposti levitamiseks.)

Me peame teadvustama küberrünnakuid reaalse, aktuaalse ja ülisuure ohuna demokraatlikele riikidele ja rahvastele. Paljud meist ei ole seda uut ohtu endale veel täie teravusega teadvustanud. Tõepoolest, küberrünnet ei iseloomusta tavarelvade plahvatusmüra, küberründe ajal ei pimesta meid valgussähvatus, ei raputa maapinna (seismiline) ega õhu võnkumine, ei uputa hiidlaine, me ei tunne lõhna ega maitset – kõigest hoolimata on hävitav küberplahvatus toimunud. Kuid tänapäeva elektroonika suudab küberrünnet, küberplahvatust fikseerida ja mõõta, see on väga sarnane tuumapommi plahvatusega.

Kuidas riiki küberrünnakute eest kaitsta?

Kahjuks ei ole kübersõda enam kauge tuleviku teema ega põnev teoreetiline probleem. Me oleme oma demokraatlikult ja avatult arenevate ühiskondadega paradoksaalses olukorras, nii Euroopa Liidus kui ka NATO-s puudub küberkaitset käsitlev poliitika ning puuduvad seadused – rahvusvahelised konventsioonid ja kokkulepped –, mis sätestaksid reaalsed toimingud praktiliseks kaitse- või ennetavaks koostööks. Puuduvad seadused süüdlaste vastutuselevõtmiseks.

Me peame ühendama jõud Euroopa Liidus ja teistes rahvusvahelistes organisatsioonides, kaasa arvatud ÜRO Julgeolekunõukogu, et nii ruttu kui võimalik välja töötada elektroonilise infrastruktuuri kaitse ja infojulgeoleku globaalne süsteem. Euroopa Liit peab aktiivselt ja professionaalselt sekkuma kübertemaatikat käsitlevate probleemide lahendamisse, meie igapäevaellu tunginud küberohtude tõrjumisse.

NATO-s on suutlikkus kaitsta võtmetähtsusega (kriitilisi) infosüsteeme küberrünnakute vastu sätestatud ühe prioriteedina Riia tippkohtumise deklaratsioonis ja "Kõikehõlmavas poliitilises juhises" (*Comprehensive Political Guidance*, CPG). Praegused rünnakud Eesti vastu kinnitavad tähtsate (kriitiliste) infosüsteemide kaitse tugevdamise vajadust ning ühise poliitika ja ühtsete põhimõtete kujundamise olulisust Euroopa Liidus ja NATO-s. Vaja on:

1. õiguslikult fikseerida põhimõttelised seisukohad, mis sätestaksid küberrünnete olemuse: millal on tegu poliitilise vandaalitsemise, millal terrorismi ja millal rünnakutega riigi vastu ning vastumeetmed neile;
2. Euroopa Liidus ja NATO-s tuleb luua küberrünnete teavitussüsteem. Mõlemasse töösuunda tuleb kaasata ja nendega siduda kolmandad riigid.

Praegu jäävad vastuseta järgmised küsimused.

1. Kui ühe riigi sidekeskus hävitatakse raketilöögiga, siis on see ilmselt vaenulik sõjaline akt. Kui seda tehakse küberrünnakuga, siis mis see on?
2. Milline on küberründe definitsioon? Kust jookseb piir tavalise arvutihäkkeri huligaansuse ja organiseeritud küberrünnaku vahel? Kuidas tõestada, kes on rünnakute algataja? Küberruumis on ju edukalt võimalik jälgi peita.

3. Millist abi peaks küberründe alla langenud riigile osutama näiteks teised Euroopa Liidu või NATO liikmesriigid?
4. Kuidas eristada küberründe kompleksses nähtuses omavahel põimuvat rahvusvahelist kuritegevust, terrorismi ja ebasõbraliku riigi organiseeritavat (ründe)tegevust?
5. Kuidas kaasata küberterrorismi vastasesse rindesse ka Venemaa ja mitmed teisedki riigid?

On selge, et Euroopa Nõukogu 2001. aasta Küberkuritegevuse Konventsioonist (*Convention on Cybercrime*, Budapest, 23. XI 2001) meil siinjuures abi enam ei ole.

Küberrünnakute teema, nüüdisaegne küberjulgeolek peab kujunema NATO ja Euroopa Liidu edasise tihedama koostöö esmaeesmärgiks, seda tuleks käsitleda kõikehõlmava lähenemise (*comprehensive approach*) kaudu. Küberründed on väga kompleksne, üleilmne, pidevas muutumises ja arenemises olev nähtus. Seega peavad ka küberjulgeoleku nimel loodavad seadused ja konventsioonid olema eriti tõhusad: neid peab olema võimalik olukordade ja tehnoloogiate arenemise kohaselt kiiresti täiendada (*living convention*).

Globaalse küberjulgeoleku teema peab saama Riigikogu välissuhtluses prioriteediks.

Aprillisündmusi tuleb kindlasti Riigikogus laiemalt arutada, sest see puudutab väga paljusid ühiskonnaelu tahke.