Informatsioon ja õigus

Eneken Tikk
Justiitsministeeriumi avaliku õiguse talituse nõunik,
kaitseministeeriumi küberjulgeolekustrateegia õigusekspertide töörühma juht

Informatsiooni j a õiguse puutepunktidest on mitu põhjust rääkida. Hiljuti ilmunud informatsiooni ja õiguse õpik[i] annab esmakordse võimaluse tutvuda laiema infoõiguse käsitlusega eesti keeles ning infosüsteemidega seonduvad õigusküsimused on vastuseks aprillis-mais toimunud küberrünnakutele muutunud Eesti ja paljude teiste riikide juristide, poliitikute, IT-spetsialistide ja isegi sõjandusasjatundjate seas atraktiivseks kõneaineks. Ehk praktilisim põhjus seisneb aga selles, et ühtse terminoloogiata ei ole võimalik Eesti kevadistele sündmustele ühtset õiguslikku hinnangut anda—ainuüksi ajakirjanduse pinnalt toimus siin ühtaegu rünne infosüsteemi vastu, küberterrorism, infoblokaad ja isegi kübersõda.

1. Informatsiooni ja õiguse kesksed mõisted: segadus juba rohujuuretasandil

Termini *informatsioon* näol on eeldatavasti tegemist sõnaga, mille kasutus on eesti keeles üldlevinud ja mis sellest tulenevalt seaduse tasandil eraldi avamist ei vaja. Samas muutub õiguse kontekstis teatud juhtudel oluliseks *informatsiooni* eristamine *andmetest*, seda kas või põhjusel, et näiteks isikuandmete kaitse korral ei pruugi seosetutel andmetel isiku eraelu kaitse seisukohalt vähimatki tähtsust olla. Aga niipea kui andmed omandavad seoses konkreetse füüsilise isikuga konteksti, kohaldub iga selliste andmetega tehtava toimingu suhtes korraga mitukümmend paragrahvi. Andmete legaaldefinitsiooni annab praegu veel kehtiv andmekogude seaduse[ii] (AKS) § 2 lõige 2: *Andmeteks loetakse igasuguseid üksteisest eraldatavaid informatsiooniühikuid.*

Omamoodi ajalugu on ka *andmekogu* ja *infosüsteemi* käsitustel Eesti õiguses. 1997. aastal jõustunud AKS-is käsitati andmekoguna *riigi, kohaliku omavalitsuse, avalik-õigusliku või eraõigusliku isiku peetavat korrastatud andmete kogumit, mille pidamisel kasutatakse automatiseeritud andmetöötlust või mida peetakse käsitsi ja korrastatud vormidel, mis või-maldavad andmetega lihtsat tutvumist või nende mehaanilist töötlemist*. Ka pealiskaudsel vaatlusel on see määratlus tänaseks ajale jalgu jäänud, eriti arvestades näiteks asjaolusid, et aastaks 2011 soovitakse kogu riigi dokumendihaldus muuta digitaalseks ning et staatilisi ehk üksnes ühe asutuse siseseks kasutamiseks mõeldud andmekogusid on äärmiselt vähe ja tänapäevane andmetöötlus seisneb suuresti andmekogudevahelises andmevahetuses. Seega saadi ligi kümme aastat hakkama Exceli faili sarnase andmekogu määratlusega[iii] ning andmekogude seaduse reformini jõuti seadusandja tasandil alles 2007. aastal.

Ka uues avaliku teabe seaduse (ATS) redaktsioonis, millesse andmekogude regulatsioon lülitati, ei ole mõnevõrra üllatuslikult loobutud termini *andmekogu* kasutamisest. Nii ongi õiguskeeles paralleelselt kasutusel nii *andmekogu* kui ka *infosüsteem* ning valdaval osal juhtudest mõistetakse nende all ühte ja sama nähtust.[iv] Kui aga hakata seletama, mis üks andmevahetussuutlik infosüsteem siis ikkagi on, lahknevad omakorda juristide ja IT-valdkonna spetsialistide selgitused.

Kehtivas õiguses on infosüsteemi mõiste avatud Vabariigi Valitsuse määruse[v] tasandil: *infosüsteem on andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talitluseks vajalike vahendite, ressursside ja protsessidega.* Sellest ilmneb, et infosüsteem on

oluliselt laiem mõiste kui andmekogu. Infosüsteem võib sisaldada ühte või mitut andmekogu, mis AKS-i § 2 lõike l kohaselt on ainult andmete kogum, mitte aga näiteks tark-ja riistvara, mida andmete töötlemisel kasutatakse, ega protsessid ja meetmed, mida andmete töötlemisel rakendatakse.

Lausa lõbus on otsida kehtivast õigusest vastet terminile *infoühiskond*. Ükski varasem inimkooslus pole end nimetanud infoühiskonnaks. Kunagi varem pole informatsioon ja sellele juurdepääsu võimaldamine olnud ühtaegu rahvusvahelise ja riigisisese poliitika prioriteet ning ükski ühiskond pole tuhandete aastate jooksul eriti juurelnud selle üle, millises ulatuses tuleks indiviidile tagada õigus informatsioonilisele enesemääratlemisele, mil viisil võiks kodumasin rikkuda inimeste privaatsust või millise osa sisemajanduse kogutoodangust moodustab avaliku teabe koguväärtus.

Informatsioonist on kujunenud majandusfaktor, kultuuriväärtus ja põhiseaduslikult kaitstav hüve, aga ka võimalik oht, kirjutab Saksa professor Stephan Lodde oma mahuka informatsiooniõigust käsitleva uurimuse eessõnas.[vi] Millist ohtu informatsioon, selle üleküllus või kätesaamatus ühiskonnas tekitada võib, sellest annavad aprillisündmused vaid ähmast aimu.

Eesti seadusandja ei ole infoühiskonna mõistet avades olnud ülemäära ratsionaalne, kui sedastab: *Infoühiskond on kõikehõlmav mõiste. See haarab kogu sotsiaalset reaalsust, milles me elame. Informatsiooni-ja kommunikatsioonitehnoloogia revolutsioon on muutnud ja muudab meie tänast maailma tunduvalt, kuigi paljusid eesolevaid ümberkorraldusi me veel täielikult ei hooma. Infoühiskond mõtestab uuesti lahti meie riigi geograafilise paiknemise iseärasustest tulenevad arengujooned, vähendades kaugusi nii riigisiseselt kui ka riikidevaheliselt, kaotades äärealasid ning ühtlustades eri piirkondade konkurentsivõimet. Tegeldes intensiivselt infoühiskonna rajamisega, astume ühte sammu Euroopa arenguga*.[vii]

Pole siis ime, et selle virvarri keskel nimetati kevadisi sündmusi eri nimetustega ning tänaseni pole selge, mis siis tegelikult toimus.

2. Mis juhtus aprillis: kas see oli arvutikahjurlus või kübersõda?

Kevadiste kübersündmuste järelkaja kestab IT-alase haavatavuse debatina kümnetes riikides. Eesti samme küberjulgeoleku tagamisel jälgib kogu maailm ning teema pole külmaks jätnud ka kohalikku avalikkust.

On tavapärane, et poliitikud teevad avaldusi enamasti juriidilises keeles ning tihti jätab juriidiliselt korrektne sõnavalik avalikkusele sõnumi lahtimõtestamiseks vähem või rohkem mänguruumi. Uskmatud võivad läbida mõtteharjutuse "üks maja kõik". Ehitised jagunevad seaduse kohaselt hooneteks ja rajatisteks. Seejuures on hoone katuse, siseruumi ja välispiiretega ehitis. Rajatis on ehitis, mis ei ole hoone.

Võimukandjate korrektse sõnavaliku eest hoolitseb arvukas nõuandjate eskaader, kelle ülesandeks on oma kompetentsivaldkonda kuuluv küsimus hoolikalt läbi analüüsida ja siis vastavuses poliitiliste suunistega vajalik avaldus koostada. Küberkaitse nõunikku pole isegi kaitseministril, rääkimata sise-, justiits- või peaministrist. Eesti IT-poliitika dokumentides pole küberjulgeolekut seni poole sõnagagi mainitud. Kui seda tahetaksid teha, ei saaks aluseks võtta ei Eesti ega rahvusvahelist õigust, sest õiguses pole teatavat tolerantsuspiiri ületavate arvutikuritegude eraldi defineerimisega lihtsalt tegeldud.

Nii olidki ministrid kevadiste sündmuste puhul lihtsalt loomulikust intelligentsist ühel meelel: seda, mis toimus, ei tohiks käsitada tavalise arvutikahjurlusena. Oma sõnumi kohaleviimiseks kasutasid nad võrdlusi, mis on praeguseks rohkesti juriidilist vastukaja tekitanud.

2.1. Karistusseadustiku terminid infotehnoloogiasõnastike vaatenurgast

Toimunu käsitamine *lihtsa arvutikuritegevusena* ei ole täpne, sest riigi infosüsteemide vastu suunatud ründed olid koordineeritud ja ajastatud ning iga robotvõrku[viii] kaasatud arvuti omanikku või valdajat pole mõtet otsida ja pokri panna. Sellest mõttekäigust sai tuule alla paralleel *terrorismiga*, mida iseloomustab eesmärk sundida riiki midagi tegema või tegemata jätma või tõsiselt häirida riigi poliitilist, põhiseaduslikku, majanduslikku või ühiskondlikku korraldust. Kehtiva karistusseadustiku (KarS) § 237 sätestab sellise tegevuse eest viie kuni kahekümne aasta pikkuse või eluaegse vanglakaristuse.[ix]

Arvutikuriteo eest saab selle toime pannud isikut karistada maksimaalselt kolmeaastase vangistusega ja sellegi eeldusena tuleb tuvastada olulise kahju tekkimine.[x]

KarS-i §-s 206 sätestatud *arvutikahjurluse* koosseis keelustab arvutis olevate andmete või programmi ebaseadusliku vahetamise, kustutamise, rikkumise või sulustamise, kui sellega on tekitatud oluline kahju, samuti arvutisse andmete või programmi ebaseadusliku sisestamise, kui sellega on tekitatud oluline kahju. Lõike 2 kohaselt on sama tegu karistatav ka juhul, kui see pannakse toime eesmärgiga takistada arvuti- või sidesüsteemi.

Arvuti mõiste tuleneb Euroopa Nõukogu arvutikuritegevusvastase konventsiooni[xi] artikli l punktist a. Selleks on seade, mis teostab vastavalt programmile arvutiandmete automaat-töötlust. *Arvutisüsteem* on arvutikuritegevusvastase konventsiooni artikli l punkti a kohaselt andmeid programmi järgi automaatselt töötlev seade või omavahel ühendatud seadmed. Artiklis l kasutatakse terminit *infosüsteem*, mis *on seade või omavahel ühendatud või seotud seadmete rühm, mille hulgast üks või mitu seadet teostavad vastavalt programmile arvutiandmete automaattöötlust; samuti nimetatud seadme või seadmete rühma salvestatud, töödeldud, välja võetud või edastatud arvutiandmed, mis on vajalikud kõnealuse seadme või seadmete rühma toimimiseks, kasutamiseks, kaitseks ja hoolduseks*. Termin *programm* on KarS-i kommentaarides määratletud tehnilistes standardites kasutatava definitsiooni kaudu: *süntaktiline üksus, mis vastab mingi programmikeele reeglitele ning koosneb tea-tava automatiseeritud andmetöötlusfunktsiooni täitmiseks vajalikest deklaratsioonidest ja lausetest või käskudest*.

Vahetamine tähendab andmete või programmi asendamist teiste andmete või programmidega. *Kustutamine* tähendab olemasolevate andmete või programmi kõrvaldamist. *Rikkumine* tähendab andmete või programmi muutmist viisil, mis raskendab nende otstarbelist kasutamist. *Sulustamine* on andmetele juurdepääsu sulgemine või selle takistamine. *Sisestamise* all mõistetakse arvutisse kandmist andmetöötlusprotsessiks või säilitamiseks.[xii]

Olulise kahju määratlus on fakti küsimus, mille tuvastamise alused tulenevad Riigikohtu praktikast. *Oluline/suur kahju* nõuab RKKK[xiii] otsuse nr 3-1-1-43-03 kohaselt sisustamist teo toimepanemise hetkel kehtinud miinimumpalgast lähtuvalt. Oluline kahju võib olla nii varaline kui ka mittevaraline (nt mainekaotus).[xiv] Näiteks juhul, kui rünnaku tagajärjel kaob usaldus konkreetse ettevõtja vastu, mis omakorda toob kaasa klientide ja tulu vähenemise.

Arvutivõrgu või arvutisüsteemi *ühenduse rikkumise* või tõkestamise eest karistatakse isikut KarS-i § 207 alusel. Rikkumise all mõistetakse andmesideühenduse võimaluse lubamatut täielikku katkestamist, tõkestamise all andmesidekiiruse lubamatut vähendamist. *Arvutivõrguna* mõistab KarS andmeside eesmärgil omavahel ühendatud arvutite võrku vastavuses tehniliste standarditega.

KarS-i § 208 kohaldamise aluseks on arvutiviiruse levitamine, mille eest isikut karistatakse rahalise karistuse või kuni üheaastase vangistusega. Karistusmäär on kõrgem, kui sama tegevus kordub või sellega tekitatakse oluline kahju. Koosseisust ja selle kommentaaridest ei nähtu otseselt, kas karistatav on ka viiruse levitamine passiivse tegevuse või tegevusetusega (nt arvuti vajalikul määral turvamata jätmine). Tristan Ploom on seisukohal, et *seega peaks arvutispetsialist, kellele on andmeturbega tegelemine tööülesandeks, st õiguslikuks kohustuseks, nimetatud kohustuse täitmatajätmisel vastava koosseisu alusel vastutama*.[xv]

Arvutiviirusena käsitatakse KarS-i kontekstis kahjulikku (ingl *malicious*) arvutiprogrammi, mis on võimeline end omal algatusel või modifitseeritud kujul ise või teiste arvutiprogrammide abil arvutivõrgu kaudu edasi levitama ning häirima arvutite kasutamist, muutes või kustutades muu hulgas arvutis olevaid andmeid või programme, kasutades ära arvuti ressursse jne. Termin tähistab nii neid kahjulikke programme, mis levitavad end teisi programme muutes, kui ka neid, mis levitavad end teisi programme muutmata (uss, laviinkirjad). *Levitamine* on programmi edastamine vähemalt ühte arvutisse, mille valdaja ei ole selleks nõusolekut andnud.

KarS ei kriminaliseeri viiruse loomist, mistõttu võib juhtuda, et isik, kes on kahjuliku arvutiprogrammi loonud, "jätab" selle andmekandjal pahaaimamatu isiku kätte, kes omakorda teadmata, millega tal tegu, viiruse oma arvuti kaudu levima laseb.

KarS-i § 213 näeb ette karistuse varalise kasu saamise eesmärgil arvutiprogrammide või andmete ebaseadusliku sisestamise, vahetamise, kustutamise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise eest, kui sellega on mõjutatud andmete töötlemise tulemust. Arvutikuritegevusvastase konventsiooni artikli l punkti b kohaselt on *arvutiandmed* töötlemiseks sobivas vormis esitatud teave või programm, mille abil arvutisüsteem toimib. KarS-i kommentaaride kohaselt ei eelda sekkumine, et andmetöötlusprotsess oleks juba alanud (hõlmab ka lubamatut käivitamist). Säte on võrreldav nõudega sätestada kuriteona arvutiandmete sisestamine, muutmine, kustutamine või sulustamine, kui see pannakse toime tahtlikult ja ilma õigusliku aluseta ning kui selle tagajärjel saadakse mitteautentsed andmed, mida õiguslikel eesmärkidel kavatsetakse käsitleda või kasutada autentsetena olenemata sellest, kas need on otse loetavad ja arusaadavad.

KarS-i § 217 kriminaliseerib arvuti, arvutisüsteemi ja arvutivõrgu ebaseadusliku kasutamise, kui see toimub koodi, salasõna või muu *kaitsevahendi* kõrvaldamise teel. *Koodi* ja *salasõna* on kommentaaride kohaselt mõistetud kui andmeid, mida on vaja kasutaja kasutusõiguse tuvastamiseks ning mida peaks teadma ainult kasutusõigust omav isik.

2.2. Rünne arvutivõrgu vastu ehk mis aprillis-mais tegelikult juhtus

Tegelikkuses toimunu järgnev kirjeldus on IT-valdkonna juristile tavapärane lugemisharjutus: 27-29. aprillil toimusid DoS-[xvi] ja DDoS-ründed[xvii] valitsusasutuste ja uudisteportaalide veebilehtede vastu ning näotustamisrünne reformierakonna veebilehe vastu. 30. aprillist 3. maini jätkusid DoS- ja DDoS-ründed valitsusasutuste veebilehtede vastu. Lisaks rünnati

haridusasutusi, firmasid, kasutati suuremaid robotvõrke ning rünnati ka DNS-i[xviii] servereid. 4. mail toimus väga tugev DDoS-rünne (umbes 4-5 mpps) valitsusasutuste veebilehtede vastu. Elion ja Riigi Infosüsteemide Arenduskeskus filtreerisid liiklust, mistõttu sihtmärkideni jõuab umbes 7-8 kpps. 9. mail pandi toime väga tugev DDoS-rünne valitsusasutuste veebilehtede vastu (kestus umbes 2 päeva). 10. mail lisandus DDoS-rünne Hansapanga vastu (hanza.net maas umbes 2 tundi, pärast avatud osaliselt). 15. mail oli DDoS SEB Eesti Ühispanga vastu (seb.ee maas umbes 1,5 tundi, pärast avatud osaliselt). Pärast paari enam-vähem rahulikku päeva toimus 18. mail veel kord tugev DDoS-rünne valitsusasutuste veebilehtede vastu.

Ründed muutis eriliseks nende kontekst: kõik Eesti valitsusasutuste ja avalike teenuste vastu suunatud ründed langesid pronkssõduri ümber tekkinud pingete kõrgaega.

Õiguslikku tähtsust omavad küberrünnete puhul (ehk küberründed muudavad õiguslikus mõttes eriliseks) järgmised asjaolud.

1. Automatiseeritus. Kure ja automaatne rünne on teostatav suurema tõenäosusega ning efektiivsemalt. Ka ründed, mis väljaspool küberruumi jääksid märkamata ja oleks õiguslikus kontekstis väheolulised, võivad küberruumi kontekstis olla ohtlikud. Seepärast muutub mõttekamaks ohtude tõrjumisse investeerimine - ignoreerimine läheb kallimaks kui lahendamine.

2. Tegutsemine distantsilt. Paljusid ründeid, milleks varem oli vajalik isiku füüsiline kohalolek, asendavad virtuaalsed rünnakud, mille kontekstis on kõik paigad maailmas üksteisest ühekaugusel. Areneb *jurisdiction shopping*,[xix] mis seab ohtu riigid, mille õigusruum võimaldab küberründeid tõrjuda ja süüdlasi vastutusele võtta. See oht lähtub vähem turvalistest ja vähem kvaliteetse õiguskorraga riikidest. Rahvusvaheline menetlemine on sellistel juhtudel äärmiselt keerukas ja aeganõudev. Tuletame meelde, mis kaasnes tšetšeenide veebilehe sulgemisega.

3. Teabe kiire levik. Ründed muudab tavapärasest edukamaks ja potentsiaalselt koormavamaks asjaolu, et ründajatel on võimalus ründe eri aspekte omavahel kiiresti ja väikeste kulutustega kooskõlastada, täiustada või teistele potentsiaalsetele ründajatele avalikustada. Vaid esimene ründaja peab ise välja mõtlema, kuidas seda teha, teised saavad kasutada detailset tee-seda-ise-oskusteavet.[xx]

Riigikaitse kontekstis on tähtis ka asjaolu, et ründe prognoosimiseks, avastamiseks, tõrjumiseks ja kõrvaldamiseks ei piisa üksnes avaliku võimu kandjate koostööst, sest suur osa kriitilise infrastruktuuri asutustest, kelle tegevuse halvamine võib riigi või elanikkonna heaolu mõjutada, on eraõiguslikud juriidilised isikud ning kohati ka välismaised juriidilised isikud. Muu hulgas ei ole võimalik selgepiiriliselt eristada rünnakuid riigi/ühiskonna ja konkreetse asutuse/isiku vastu.

2.1. Kübersõda? Kübersõda ... Kübersõda!!!

Termini *sõda* kasutamine on tekitanud elevust just sõja- ja riigikaitseõiguse kontekstis, kus sellega kaasneb NATO kollektiivse kaitse rakendumine[xxi], kohustus hoiduda teatud tsiviilühiskonnale eluliselt vajalike objektide ründamisest, mobiliseerimise ja sundkoormiste rakendamise vajadus. Siin tuleb igaühel teooria edasiarendamisel säilitada kaine mõistus, sest on raske ette kujutada efekti, mis saavutatakse sellega, et kõik küberrünnete toimepanijad kannavad selgelt eristatavaid eraldusmärke. Ometi võivad seosed sõjaõigusega ühel päeval ka

küberrünnete kontekstis asjakohased olla. Seda silmas pidades ongi vajalik võimalikud stsenaariumid ja tegevuskavad läbi mõelda ja üles tähendada.

Rahvusvahelise sõjaõiguse põhialused lähtuvad tavaõigusel põhinevast relvakonfliktide kodifikatsioonist Haagi ja Genfi konventsioonides. Ükski rahvusvahelise sõja- ja humanitaarõiguse instrument ei käsitle otseselt arvutivõrkude vastu suunatud ründeid. Seetõttu võib õiguskindlalt väita, et arvutivõrkude vastu suunatud ründed ületavad kehtivate õigusaktide piire ning rahvusvaheline õigus ei reguleeri vastavate rünnetega seonduvat.[xxii]

On ka teaduslikke seisukohti, mille kohaselt tuleks rahvusvahelisi sõjapidamisreegleid arvutisõjas siiski põhimõtte tasandil kohaldada, sest need on tervikuna eesmärgistatud kaitsma füüsilist maailma sõjalise iseloomuga rünnete eest. Seega vajab esmatasandil diskussiooni küsimus, kas traditsioonilise sõjapidamise põhimõtted - vajadus, eristamine, proportsionaalsus ja rüütellikkus - on kohaldatavad ka arvutisõjas. Näitena võib küll kohaldada Genfi I lisaprotokolli[xxiii] artiklist 51 tulenevat sõjapidamise põhimõtet, mille kohaselt rünnak, mis käsitleb mitut ühes linnas, külas või muus tsiviilelanikkonna ja -objektide kontsentratsioonikohas asuvat eraldi paiknevat rünnakuobjekti ühena, on keelatud, ehk arvutivõrgu ründamisel tuleb vältida kahju tekitamist nn kõrvalistele võrkudele ja seadmetele, mis aga lähema selgituse ja õigusliku sisuta poleks praktiliselt järgitav.

Samas on sõjaasjanduse spetsialistid selle valdkonna õiguslikule käsitlusele mõnevõrra tähelepanu pööranud. Näiteks on infosõjana määratletud kriis või sõja ajal toimuv tegevus, mille eesmärk on saavutada informatsiooniline ülekaal, kahjustades informatsiooni, informatsioonil põhinevaid protsesse, infosüsteeme ja arvutivõrke.[xxiv]

Infosõda hõlmab operatsioonide turvamist, sõjakavaluste kasutamist, elektroonilist sõjapidamist, psühholoogilisi operatsioone, füüsilisi rünnakuid ning arvutivõrkude ründamist ja kaitset.[xxv]

Õiguslikud ja poliitilised argumendid arvutisõja kontseptsioonide kujundamiseks ning kasutamiseks on olulised, sest nendest sõltub tegeliku operatsiooni lubatavus ja ulatus. Senised teosed kübersõdade olemuse ja sellega seotud juriidiliste tagajärgede kohta on jäänud eeskätt teoreetilisteks tulevikuvisioonideks. Samas on üle maailma alustatud inforünnakute korraldamist ilma õiguslike juhisteta. Arvestades, et infosõdade osakaal üha suureneb, on õigusruumi vaja ka poliitikakujundajate ning rahvusvahelise õiguse advokaatide jaoks, kellel tuleb operatsioone kehtiva õiguse valguses õigustada.[xxvi]

Arvutite abil sõjapidamine ei allu seega rahvusvahelisele õigusele ega sõjapidamise reeglitele. Õigusprobleemide lahendamatus ei võimalda riikidel lähemalt uurida tehnoloogia mõju militaardoktriinidele ja kaitsestruktuuridele. Seega sõltub rahvusvahelise õigusliku baasi loomise kiirusest ka see, kas ja kui kiiresti saab infosõjast tunnustatud ja tõhus sõjapidamisviis, mis peaks võimaldama vältida inimohvreid.

Mis tahes rahvusvahelise õiguse instrumendi väljatöötamisele peaksid aga eelnema riigisisesed uuringud, katsetused ja teadustöö, mis võimaldaksid saavutada laiapõhjalise kvoorumi. Sellised uurimused ja nende tutvustamine partnerriikidele võiks olla loodava küberkaitse keskuse üks oluline tegevussuund. Ka juhul, kui rahvusvahelise instrumendi vastuvõtmiseni ei jõuta soovitud ajajooksul, võimaldab diskussioon eri riikide asjatundjate vahel luua tavaõigust.

Tegemist on valdkonnaga, kus head ja universaalset lahendusmudelit ei ole. Eri riikide haavatavus lähtub osalt kattuvatest (põhimõtteline sõltuvus info- ja kommunikatsioonitehnoloogiast), osalt erinevatest teguritest, nagu potentsiaalsed rünnete põhjused, riigi infosüsteemide ülesehitus. Seepärast saab Eesti kogemust kasutada just nimelt mudeli alusena-olgu selleks etalonturve, mudelseadus või lihtsalt koondatud seni parimad tavad.

3. Mõistmiseta ei saa olla regulatsiooni

Ei saa jätta tähelepanuta tõsiasja, et nii kaua kui pole selge, kes millest räägib, ei saa õiguslikust regulatsioonist juttu olla. Vaadates IT-õiguse senist arengut, on nii seadusandjad kui ka kohtud pidanud mitmel korral oma seisukohti kriitiliselt läbi vaatama, sest tehnoloogia arenguga sammu pidamine käib õigussüsteemile lihtsalt ülejõu. Seega omandavad IT-õiguse ja informatsiooni õiguskäibe reguleerimisel tähtsuse dünaamilised regulatsioonimehhanismid, nagu eneseregulatsioon, pehme ehk mittesiduva õiguse vahendid ja lepingulise iseloomuga instrumendid. Teisalt tuleb ka nende jaoks avada tee riigisiseses ja rahvusvahelises õiguses.

James Kraska ja Brian O'Donnelli arvates[xxvii]on kõige olulisem töötada välja kindlad lahingureeglid, mille aluseks peaks aga omakorda olema kehtiv õigus oma tavapärases hierarhias. KarS-i sätetest lähtuvate lahingureeglite väljatöötamine viiks praegu paratamatu läbikukkumiseni, sest juba teoreetiliselt tekib nende kohaldamisega palju küsimusi, millele vastuseid omamata ei saa ülemad oma käskude õiguspärasuses kindlad olla. Käsku andes peab ülem suutma ette näha selle kasu täitmise (tehnilisi, sõjalisi, õiguslikke jm) tagajärgi.[xxviii] Õiguskindlusetus pärsib valdkonna arengut, sest süsteemse käsitluse ja väljaõppe puudumise korral eelistavad ülemad tõenäoliselt sõjapidamise viise ja vahendeid, mis on neile tuttavamad.

Õiguslikult on oluline tagada ühtne mõistebaas, eristades seejuures üldist ja spetsiifilist mõistetasandit: esimese hulka kuuluvad infoõiguse ja kaitsetegevuste üldmõisted (nt isikuandmed, infosüsteem, rahuaeg, riigikaitselised koormised), teise gruppi aga küberkaitse kui seosvaldkonna mõisted (nt küberkaitse, küberrünne, infosõda jne). Arvestada tuleb, et õiguskindluse huvides peavad spetsiifilise mõistebaasi mõisted lähtuma üldmõistetest.

Nii kaua kui see töö on tegemata - arvestades, et õigusriigis toimub iga avaliku võimu (mille üks kandja on ka kaitsestruktuurid) tegevus õiguslikul alusel -, puudub praegu sisuliselt tegevuskava, mis võimaldaks kevadiste sündmustega õiguslikult korrektselt toime tulla.

Eestis on sellele vajadusele juba tähelepanu pööratud. Kevadiste sündmuste analüüsiks ning neile reageerimiseks, aga ka samasuguste juhtumite ennetamiseks ja nendega toimetulekuks on moodustatud küberjulgeoleku strateegia väljatöötamise töörühm, mis hõlmab ligi 30 eri valdkonna spetsialisti. Töörühma esimesi järeldusi ja ettepanekuid on oodata 2008. aasta alguseks.

---

[i] E. Tikk, A. Nõmper. Informatsioon ja õigus. Juura 2007.
[ii] Andmekogude seadus - RT11997,28,423.
[iii] Vrd nt terviseinfo süsteemi seadusemuudatuste paketi seletuskiri: *Kehtiv andmekogude seadus on suunatud eelkõige andmekogude asutamise reguleerimisele eesmärgiga tagada kontroll selle üle, kes ja milliseid andmekogusid tohib asutada.* Selline käsitlus oli aktuaalne 1990-ndate alguses, kui hakati

andmekogude seadust välja töötama, ning peegeldab andmekogude seaduse aluseks olnud riiklike registrite seaduse loogikat.
[iv] Infosüsteemi definitsiooni praegu seaduse tasandil avatud ei ole, kuigi seadused seda terminit käsutavad. Näiteks kasutatakse infosüsteemi mõistet andmekogu mõiste sünonüümina vereseaduses (RT12005,13,63; 2006,27,196).
[v] Vabariigi Valitsuse 12. augusti 2004. a määrus nr 273.
[vi] **S. Lodde.** Informationsrechte des Burgers gegen den Staat. Köln, Carl Heymanns Verlag KG, 1996
[vii] Riigikogu 13.05.1998 otsus "Eesti infopoliitika põhialuste heakskiitmine." - RT I, 1998, 47, 700.
[viii] Robotvõrk - pahavaraga nakatunud arvutite kogum, mida ründaja eemalt juhib.
[ix] Rahvusvahelise julgeoleku vastase, isikuvastase, elu või tervist ohustava keskkonnavastase või üldohtliku kuriteo toimepanemise, keelatud relva tootmise, levitamise või kasutamise või vara ebaseadusliku hõivamise või olulises ulatuses rikkumise või hävitamise eest, samuti selliste tegude toimepanemisega ähvardamise eest, kui see on toime pandud eesmärgiga sundida riiki või rahvusvahelist organisatsiooni midagi tegema või tegemata jätma või tõsiselt häirida riigi poliitilist, põhiseaduslikku, majanduslikku või ühiskondlikku korraldust või see hävitada või tõsiselt häirida rahvusvahelise organisatsiooni tegevust või see hävitada või tõsiselt hirmutada elanikkonda -, karistatakse viie- kuni kahekümneaastase või eluaegse vangistusega. (KarS § 237 - RT12001,61, 364).
[x] Nt KarS-i § 206 lõike l kohaselt võib isikut arvutikahjurluse ehk arvutis olevate andmete või programmi ebaseadusliku vahetamise, kustutamise, rikkumise või sulustamise eest, kui sellega on tekitatud oluline kahju, samuti arvutisse andmete või programmi ebaseadusliku sisestamise eest, kui sellega on tekitatud oluline kahju, karistada rahalise karistuse või kuni üheaastase vangistusega.
[xi] Arvutikuritegevusvastane konvensioon - RT n 2003, 9, 32.
[xii] Karistusseadustiku kommenteeritud väljaanne, lk 426.
[xiii] RKKK - Riigikohtu kriminaalkolleegium.
[xiv] Vt RKKK otsus nr 3-1-1-100-00, 3-1-1-138-03.
[xv] **T. Ploom.** Arvutikuritegude kvalifitseerimine. - Juridica Vm/200, lk 577.
[xvi] DoS - Denial of Service e teenusetõkestusrünne. Server või ühendus koormatakse üle mõttetute päringute või
infopakettidega ühest seadmest.
[xvii] DDoS - Distributed Denial of Service e hajus teenusetõkestusrünne. Sama mis DoS, kuid seda tehakse tavaliselt robotvõrgu abil.
[xviii] DNS - Domain Name Service e nimeteenus. Võimaldab kasutada veebiaadresse (www.mil.ee) IP-aadresside
asemel (127.0.0.1).
[xix] Jurisdiction shopping - tegevuse ülekandmine regulatsiooni või sanktsioonide poolest soodsasse õigusruumi
[xx] Lähemalt **B. Schneier**. Secrets and Lies: Digital Security in a Networked World. Wiley Computer Publishing 2000, Ik 21 jj.
[xxi] Washingtoni lepingu artikli 5 kohaselt: relvastatud rünnakut ühe või mitme NATO osalisriigi vastu Euroopas või Põhja-Ameerikas käsitatakse rünnakuna nende kõigi vastu ning sellest tulenevalt lepivad NATO liikmesriigid kokku, et niisuguse relvastatud rünnaku korral asub igaüks neist, rakendades Ühinenud Rahvaste Organisatsiooni harta artiklis 51 sätestatud õigust individuaalsele või kollektiivsele enesekaitsele, sel viisil rünnatud lepinguosalist või lepinguosalisi abistama, rakendades üksi ja koos teiste lepinguosalistega abinõusid, mida ta peab vajalikuks, sealhulgas relvajõudude kasutamist, eesmärgiga taastada ja säilitada Põhja-Atlandi piirkonna julgeolek.
[xxii] **Schmitt**. 'Wired Warfare', Bellum Americanum: The U.S. View of Twenty-first Century War and its Possible
Implications for the Law of Armed Conflict' (1998) 19 Michigan Journal of International Law 1051, 365.
[xxiii]12. augusti 1949 Genfi konventsioonide 8. juuni 1977 (I) lisaprotokoll rahvusvaheliste relvakonfliktide ohvrite kaitse kohta
[xxiv] Joint Chiefs of Staff, Joint Publication 1-02, DoD Dictionary of Military and Associated Terms (2001) 253.
[xxv] Joint Chiefs of Staff, Joint Publication 1-02, DoD Dictionary of Military and Associated Terms (2001) 253.
[xxvi] **B. T. O'Donnell, J. C. Kraska**. Humanitarian Law: Developing International Rules for the Digital Battlefield, Journal of Conflict & Security Law, April, 2003.
[xxvii] **B. T. O'Donnell, J. C. Kraska.** Humanitarian Law: Developing International Rules for the Digital Battlefield.
Journal of Conflict & Security Law, April, 2003.

[xxviii] **M. N. Schmitt** 'Wired Warfare', Bellum Americanum: The U.S. View of Twenty-First Century War and Its
Possible Implications for the Law of Armed Conflict' (1998), 19 Michigan Journal of International Law 1051, 368