Riikliku küberturvalisuse valdkonna (sh kriisijuhtimine) juhtimissüsteemi analüüsi küsimused

Struktuur	Vastuse mustand ITL 31.03.2022
1. Kuidas peaks/võiks olema/olla ülesehitatud küberturvalisuse korraldamine riiklikult? 2. Mil moel peaks jagunema küberturvalisuse vastutusala riiklikult?	1. Ühena esimestest küsimustest tuleb lahti mõtestada, millises osas saab käsitleda koos ja millises osas lahus tsiviilvaldkonna küberturvalisust ja küberjulgeolekut (kaitsevaldkonda). Praegu tundub, et neid aetakse läbivalt segi. ITL on seisukohal, et neid päris kokku panna ehk täpselt samamoodi juhtida ei saa. Kõiki kriise ei saa lahendada samasuguste meetmetega. Küsimuse all on põhiõigustesse sekkumise intensiivsus. Tsiviilkriisiks peavad selgelt olema ette nähtud leebemad meetmed kui sõjaliseks riigikaitsekriisiks ning see peab olema ITL-i hinnangul üks kriisijuhtimise aluspõhimõtteid. Teise küsimusena tuleks eristada infoturvet/küberturvalisust küber(vastu)ründe võimekusest. Küberturvalisus ja selle teadlikkus peaks olema ühiskonnas läbiv, mitte üksnes elutähtsa teenuse osutajatele kehtiv nõue. Oluline on ka defineerida, mida tähendab korraldamine: kas me peame silmas poliitikate/seaduste kehtestamist, millegi järelevalvamist või praktikas millegi ära tegemist (SOC funktsioon, turvadisain vm praktilist). Järelevalve osas tuleks kindlasti jälgida, et erinevad riiklikud asutused (CERT, RIA KII, RIA järelevalve, TTJA, FI, MKM, Eesti Pank jne) ei järelevalvaks samas domeenis pisut erinevate kriteeriumite alusel sama eesmärgiga mingeid funktsioone: see tekitab mõttetut dubleerimist ning suurendab halduskoormust. Siin tuleks efektiivsust otsida. Praktiliste tegevuste puhul tuleb analüüsida ja

	kokku leppida piirid, kuhu maale üks või teine organisatsioon midagi teeb: näiteks ei saa infoturbedisaini teha „äripoolest“ väga kaugelt (a’la MKM ütleb, kuidas PPA infosüsteem peab turvatud olema), küll aga peavad vastutuste piirid olema selged (nt „küberpettuste“ ja petukõnede lahendamise puhul on CERT täna liiga palju sõna võtnud PPA asemel, kes tegelikult pettuste menetlemisega tegeleb jne). CERT funktsioon on siiski midagi muud. Ehk siin on rollid ja ametijuhtide ambitsioonid pisut piire ületama hakanud. 2. Üks oluline küsimus küberturvalisuse vastutusala puhul on RIA roll ja ülesanded. RIA-l on hetkel topeltroll olles sisuliselt nii nõuete kehtestaja, täitja kui ka riiklik järelelvalvaja. ITL on seisukohal, et RIA ei tohi iseenda üle järelevalvet teha, mistõttu teeme läbipaistvuse ja rollide lahususe tagamiseks ettepaneku viia järelelvalve roll üle teise asutusse, nt TTJA-sse. Küberturvalisuse riiklik korraldamine s.h riigi CERT, kriitilise infra kaitse koordineerimine ja järelevalve peaks paiknema eraldi asutuses. Praegune olukord, kus tegemist on RIA ühe osaga, ei võimalda täielikku fokuseerimist küberturvalisusele ja sisaldab ka mitmeid rollikonflikte.
~~2.~~3. Kuidas peaks olema ülesehitatud riikliku küberturvalisuse korraldamine kriisijuhtimisel? ~~3.~~4. Kuidas peaks olema jaotatud riiklikult vastutusala kriisijuhtimisel?	3. Kriisijuhtimiseks peab kindlasti olema süsteem, s.h paigas peavad olema vajalikud käsuahelad ja vastutajad ja info edastamise kord. Seejuures on äärmiselt oluline, et ei lahendata eilset kriisi, vaid valmistutakse järgmiseks. Viimast on oluline arvestada ka mõistete defineerimisel, sest väga paljut ei saa seadusesse kirja panna, sest ühiskond, tehnoloogilised lahendused ja seega ka intsidendid muutuvad ajas. Pigem tuleb seejuures lähtuda kainest mõistusest ja kokkulepitud käsuahelast. Kriis on olukord, mis on uus ja ootamatu ning mida tuleb lahendama hakata vastavalt tegelikule situatsioonile ning teha otsused sõltuvalt

	olukorrast ja asjaoludest. Seetõttu on oluline anda kriisi lahendavatele asutustele seadusega vajalikud volitused, kuid mitte kirjeldada lõpliku loeteluna kõiki meetmeid. Lisaks juhime tähelepanu, et kriisiks valmistumine, kriisi väljakuulutamine, lahendamine ja lõpetamine on erinevad asjad ja neid tuleb seaduses ka erinevalt käsitleda. 4. Oluline on paika panna, millal (millistest kriteeriumitest alates) kes ja mis valdkonda juhib. Kas see on siis minister, peaminister või Kaitseväe juhataja. Kriisi lahendamisel ja ka otsustamisel, kas tegu ikka on kriisiga, peab olema piisavalt osapooli. See on vajalik selleks, et kriisi lahendamise protsessi ei saaks liiga lihtsasti käivitada. Samuti selleks, et tagada laiemalt õiged otsused. Seetõttu palume hoiduda liiga kitsale ringile otsustusõiguse andmisest ning eelistada mitme tasandilist otsustusprotsessi. Väga oluline on tagada rollide lahusus, mis tähendab, et volituste andja/lõpetaja peab olema erinev volituste saajast. Kindlasti tuleb harjutada kriisi üleandmist. Pangaliidus korraldatud õppuse stsenaarium nägi ette, kuidas küberturvalisuse intsident (kriis) eskaleerus Elutähtsa teenuse toimepidevuse kriisiks. Õppuse ühe järelmina tõdesimegi, et tegelikult ei ole selge, kuidas jaguneb vastutus RIA CERT ja ETKA vahel ning kuidas toimub lahendamise üleandmine, kui „kriisi iseloom“ muutub. Peame oluliseks ka seda, et otsustusprotsess oleks võimalikult lihtne ja avalik, poolte (s.h erasektori osaliste) rollid ning ootused valmisoleku osas selged, käsuahelad asjaosalistele teada.
~~4.~~5. Milliste lepingute, koostöölepingute, aktide või muu sellisega peaks olema määratud vastutusalad?	Sellele küsimusele on hetkel raske vastata. Sõltub sellest, kes on osapoolteks. Kõigepealt peab kõik juhtimismudeli osapooled ühele skeemile panema ja siis vaatama, kus vastutusalad määrata.

	Oleme siiski seisukohal, et riigiasutustel ei ole vaja sõlmida omavahel lepinguid. Õigusaktidest peab tulema selged alused kes kellega mida teeb. Samuti see kellel, millal ja milliseid meetmeid on konkreetse sündmuse lahendamisel võimalik kohaldada. Kuna jutt on riigiasutustest, siis peaks funktsioonide kirjeldused tulenema kas vastava ministri määrusest või asutuse põhimäärusest.
~~5.~~6. Millised on teie hinnangul hetkeolukorra puudused küberturvalisuse ja kriisijuhtimise valdkonnas (vastusala, õiguste ja kompetentside vaatest), mida tuleviku juhtimissüsteem peaks arvestama?	Üks probleem on selles, et valdkonna juhtimine on killustunud, kuigi selle osas on viimaste aastate jooksul olnud siiski positiivseid arenguid. Rõhutame vajadust arvestada ka EL-i arengute ja uute õigusaktidega, sest Eesti küberturvalisuse juhtimismudel peab toimima koostöös EL-i mudeliga. Samas hetkel on EL-i loomisel uusi asutusi, nt Joint Cyber Unit, kelle roll ja vastused on meie teada veel lahtised. Seetõttu on äärmiselt oluline, et riigi tasandil panustatakse tugevate jõududega EL-i seadusloomesse. Teine suur probleem on selles, et ressurssi, kompetentse, on vähe. Kas on võimekust hallata pilveteenuste teemasid, AI tehnoloogiate, Cyber Resiliance, Ransomware jms teemasid. Tuleviku juhtimissüsteem peab arvestama sellega, et tekib üks ühine arusaam, kus on kompetentsid ja ressursid. Hetkel on RIA-s kujunenud arusaam, et neil on olemas kõik valdkondlikud kompetentsid ja nad oleksid küberintsidendi korral valmis üle võtma näiteks elektrijaama juhtimist. Meie leiame, et sel juhul on tegemist ülereguleerimisega, kui riik hakkab eraettevõtete eest kriisi juhtima või ka intsidente lahendama. Seetõttu on oluline läbi mõelda ja paika panna, kuidas kaasatakse vajadusel eraettevõtete ressurssi, s.h kuidas tagatakse eraettevõtete valmisolek ja võimalused panustada. Üks oluline aspekt siin juures on tänane töölepingu seaduses sisalduv valveaja regulatsioon (§§ 51, 52), mis seab olulised piirangud valveaja kasutamise võimalustele tehes telefonivalve korraldamise keerukaks ning ebaotstarbekaks kriitilise tähtsusega info- ja

	kommunikatsioonitehnoloogia teenuste ning taristu järjepideva toimimise tagamisel (vt selle kohta ITL-i ettepanekut õigusaktide osas). Samas võiks ka riigikaitseliste ametikohtade määramine elutähtsa teenuse toimimiseks olla käsitletud kasvõi viitena TLS-s, millisel juhul kehtib tavapärasest töö- ja puhkeajast erinev kord. Käsitletud võiks olla ka erasektrori puhul selged juhised prioriteetide osas, kui kriisiolukorrast tulenevad riigi poolt määratud kohustused ja roll ning elutähtsa teenuse osutaja kui erasektori poolt määratud roll riigikaitseliste ülesannete osas kattuvad. Lisaks toome välja järgmised puudused: • Õigusloome on ajale jalgu jäänud, õigusaktide sätted pole enam alati asjakohased ega baseeru ajakohastatud riskianalüüsidel. Näitena võib tuua HOS 41.2 teenuste paiknemise küsimuse. • Järelevalve kohmakus dubleeritus eri-riigiasutuste vahel. • Kriisijuhtimise üleandmine eriasutuste vahel
~~6.~~7.Kas teie hinnangul on hetkel katmata valdkondasid / funktsioone, millega ei tegeleta küberturvalisuse ja kriisijuhtimise valdkonnas? ~~7.~~8.Kas ja milliseid võimalusi näete nende valdkondade / funktsioonide parendamiseks?	7. Ettevõtted on kurtnud, et puudu on toimiv tagasisidestamise süsteem. Ettevõtted raporteerivad RIA-le intsidentidest, aga tagasisidet ei saa. Seega mureks on vähene diskussioon. Mureks on infovahetus ja selle kiirus, selged käsuahelad ja vastutajad. 8. Intsidentide osas võiks mõelda kaheastmelist infovahetust – esmane teavitus ka võimalike intsidentide osas, põhjalikum teavitus, kui intsidendi asjaolud ja mõju on selgunud. Viivitus, info jagamise kiirus võib olla küberturvalisuse seisukohalt olulise tähtsusega. Oluline on ka valmisolek ja kursis olek uute tehnoloogiate tulekuga seotud uutest võimalikest riskidest (nt pilveteenus). Vastutuse panemine turvariskide puudumise eest elutähtsa teenuse osutajale ei lahenda tegelikku probleemi.
Juhtimine	

1. Mil määral ning kuidas peaks olema kaardistatud riikliku küberturvalisuse korraldamisega kaardistatud riskid?	Muidugi peavad olema riskid kaardistatud ehk kellelegi teada. Need tuleb kaardistada tulevikku vaatavalt ehk selleks, et lahendada homseid probleeme ning neid ka ennetada. Hetkel tundub, et liiga kinni jäädakse eilse sõja näidetesse. Küberturvalisuse strateegia ja tegevusplaani koostamine ning järjepidev riskide hindamine ja kaardistamine on olulised. Riskide kaardistamise juures on oluline kaasata teadlased, tehnoloogia inimesed, nö eetilised häkkerid. Toetada olulisi teadussuundi, mille abil tekitada arusaama, kuhu areneb küberkurjategijate arsenal.
1. Kas oskate välja tuua mõjutegureid, mis võiksid mõjutada küberturvalisuse riikliku korraldamise (sh kriisijuhtimise) kujundamist? a. Millised on teie arvates olulised arengusuunad küberturvalisuses? b. Euroopa Liidu tugevale küberturvalisuse protsessijuhtimisele; c. tehnoloogia arengule (pilveteenused); d. suurematele küberintsidendidele välismaal (Iirimaa tervishoid). 2. b. Millised on olulisemad piirangud küberturvalisuses, näiteks Eesti halduskontekst ja limiteeritud ressursid?	Ilmselt EU õigusmuudatused eelkõige. Samas ka tehnoloogia areng ja võimalused. Info avalikkus ja võimalus jääda anonüümseks, jälitamise võimatus. Riikide ülene koostöö on rünnakute ja nende sooritajate avastamiseks oluline.
3. Millised on võimalike mõjutegurite mõjud riikliku küberturvalisuse juhtimissüsteemile teie seisukohast?	Riigil on vaja ressursse ja kompetentse mõjutegurite ja nende muudatustega operatiivselt kursis olla. Hea koostöö erasektoriga suurendab võimekust, mistõttu sanktsioonide ja järelevalve asemel võiks riik keskenduda juhtimissüsteemi võimalikult lihtsa ja läbipaistvana hoidmisele ning anda ise riigiasutustega eesotsas eeskuju + leida võimalused kogu ühiskonnas teadlikkuse tõstmisele küberturvalisuse osas (õppeprogrammid, e-riigi teenused ja kommunikatsioon) ja spetsialistide koolitamisele.

4. Kas ja mil määral võiks ITL olla kaasatud riikliku küberturvalisuse korraldamisel ja arendamisel (sh kriisijuhtimisel)?	ITL saab olla kaasatud kahest vaatest. Ühelt poolt oleme IKT ettevõtete koondaja ja eestkõneleja, teiselt poolt saame vahendada kontakte konkreetsete ettevõtetega. Kriisis ei sekku liit kindlasti konkreetse ettevõtte kriisijuhtimisse. Samuti ei saa me olema operatiivtasandi lüli kriisijuhtimises. Aga saame pakkuda võrgustikku, osaleda plaanide tegemisel ja ressursside kaardistamisel.
Tulemuste mõõtmine	
1. Milliseid mõõdikuid peaks riikliku küberturvalisuse korraldamise (sh kriisijuhtimine) tulemite mõõtmiseks kasutama?	Teatud mõõdikud on kirja pandud Digiühiskonna arengukavasse 2030. Kindlasti ei sobi meie hinnangul rahastuse protsent, sest kuigi kübertuvalisusesse panustatava rahastuse suurendamine on väga positiivne, ei näita raha suurus siiski seda, et seda õigesti kasutatakse. Suures pildis on meie hinnangul õige lähtuda nii avaliku kui ka erasektori teenuste kõrgest usaldatavusest. Kui teenuste turvalisusega on kõik korras, siis kasutajad usaldavad neid teenuseid. See mõõdik on tegelikult arengukavas ka olemas – „digiteenuste kasutamisest ei ole hoidutud turvariskide olemasolu kaalutlusel“ (lk 39). Kindlasti on oluline ka see, et oleks piisavalt infoturbe spetsialiste ja see, et arendamisel oleks tagatud *security by design*.
2. Millele tuginedes võiksid mõõdikud olla loodud? a. Millistel alustel peaks mõõdikuid looma teie seisukohalt?	Kõige parem indikaator on küberintsidentide arv ning ärahoitud küberrünnakute arv ehk nende ennetamise/ärahoidmise võimekus. Kindlasti annavad mingi pildi ka E-ITS rakendamise järel tehtavad auditid, kas ja kui edukalt suudavad riigiasutused, KOVid lisaks elutähtsa teenuse osutajatele seda rakendada.
3. Kas oskate välja tuua puudu olevaid mõõdikuid, mis võimaldaksid teha paremaid otsuseid riikliku küberturvalisuse parendamiseks?	Riik saab oma järeldused teha oma väiksemate ja suuremate intsidentide pinnalt, mis on puudujäägid ja arengukohad. Kõrvalt on raske hinnata, kui puudub ülevaade riigi küberturvalisuse täpsest seisukorrast.
Õiguslik analüüs	

1. Millistes õigusaktides peaks olema reguleeritud küberturvalisuse tagamiseks vajalikud asjaolud?	Horisontaalsed reeglid peavad olema ühes kohas – küberturvalisuse seaduses, kriisijuhtimise teemad valmisolekuseaduses. Samas leiame, et kui konkreetses valdkonnas on põhjendatud erinõuded, siis need peavadki olema valdkondlikus õigusaktis, et sellega seotud inimesed nendega kursis oleks. Kui uus mudel saab paika, siis tuleb hoolikalt üle kontrollida, et üheski õigusaktis ei ole dubleerivaid sätteid ja ülekatteid. Kindlasti tuleb arvestada kõikvõimaliku EL-i ja rahvusvahelise õigusega. Näiteks kriitilise infrastruktuuri vastupanuvõime direktiiv, mida EL-is menetletakse samal ajal uue küberturvalisuse direktiiviga. EL-i õigusest on tulemas üha rohkem ja rohkem otsekohalduvaid akte, mistõttu pilt on väga keeruline. Eriti ettevõtete jaoks. Eesti tasandil on oluline analüüsida ja lahti kirjutada küberturvalisuse ja valmisolekuseaduse seosed, sest need mõlemad seadused on mõeldud olema üldseadused, kuigi küberturvalisuse seadus on tegelikult kitsam.
2. Millistes õigusaktides võiks olla reguleeritud: - intsidendiks valmisolek; - intsidendi tuvastamine; - intsidendi lahendamine; - normaalse olukorra taastamine?	Üldpõhimõtted peaksid tulenema ikkagi valmisolekuseadusest. Edasine sõltuvalt intsidendist – kui on küberintsident, siis tundub loogiline, et eriregulatsioon on küberturvalisuse seaduses, andmekaitsega seotud intsidendid andmekaitse seaduses jne.
3. Millised küberturvalisuse tagamiseks olulised asjaolud on teie seiskukohast õigusaktides reguleerimata?	Tänases töölepingu seaduses sisalduv valveaja regulatsioon (§§ 51, 52) seab olulised piirangud valveaja kasutamise võimalustele tehes telefonivalve korraldamise küberturvalisuse tagamisel keerukaks ja ebaotstarbekaks. Seetõttu tuleb muuta töölepingu seadust selliselt, et see võimaldaks rakendada teatud töötajatele paindlikumat ja nende töö iseloomu arvestavat valveaega. Selline erand peaks puudutama neid töötajaid, kes peavad tagama süsteemide 24/7 toimimise ja kellel on vaja reageerida eriolukordadele (süsteem või selle osa on maas või ei toimi korrektselt) väljaspool tööaega. Puudu on töölepingu seadusest ka riigikaitseliste ametikohtade sisu ja olemus ning sellega seotud erisused ja ülesannete andmine.

	Õigusaktides on kajastamata ka isikuandmete töötlemise reeglid kriisihalduseks. Suurte kriiside lahendamisel võib tekkida olukordi, kus on vaja tavaolukorrast erinevat andmete töötlemist, aga sellele tuleb ennetavalt mõelda ja reeglid paika panna.
4. Kas oskate tuua välja küberturvalisuse tagamise asjaolusid, mis on tänastes õigusaktides „üle reguleeritud“?	Peame ülereguleerimiseks dubleerivaid kohustusi ettevõtetele. Näiteks pangandussektoris, kus tuleb auditeid esitada nii finants- kui ka küberturvalisuse järelevalvele. Oht on ka NIS2 direktiivist tulenevalt, et küberintsidente, mis hõlmavad endas ka isikuandmetega seotud intsidenti, hakatakse menetlema kahe seaduse järgi, võimalik et ka sanktsioneeritakse siis topelt, kui järelevalve asutused üksteisest eraldiseisvalt asju menetlevad.