TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Eleri Pilliroog

EUROOPA LIIDU KÜBERTURVALISUSE ÕIGUSLIKU RAAMISTIKU RAKENDAMINE COVID-19 KRIISI TINGIMUSTES

Magistritöö

Juhendaja
mag.iur. Liisi Adamson

Tartu
2022

SISUKORD

SISSEJUHATUS

2020. aasta alguses puhkes ülemaailmne kriis, mille Maailma Terviseorganisatsioon (WHO) kuulutas COVID-19 pandeemiaks.[1] Kaugtööst kaugõppeni sattus tehnoloogia inimeste ühenduses hoidmisel võtmerolli ning hüppeliselt kasvas kodanike sõltuvus digitaaltehnoloogiatest.[2] Selle kõige taustal tekkis aga tuli analüüsida, kuidas on tagatud turvaline ja usaldusväärne küberruum kriisi ajal oluliseks kujunenud valdkondades. COVID-19 kriisi ja küberturvalisust uurivates teadusartiklites on kirjeldatud, et mitmed rahvusvahelised agentuurid, näiteks Europol[3] ja Interpol[4], hoiatasid suurenevast ohust küberturvalisusele, kuid see ei takistanud juhtumite arvu tõusu ega ennetanud küberintsidente. Seega tekkis küsimus, kas riikide pingutused tugevdada küberturvalisuse nõudeid ja Euroopa Liidu (edaspidi EL või Liit) arendatud õiguslik raamistik olid piisavad, et aidata kaitsta olulisi infrastruktuure ja teenuseid kriisi ajal.[5]

Magistritöö eesmärgiks on analüüsida, kas EL-is vastu võetud asjakohased küberturvalisuse valdkonna õigusaktid, regulatsioonid ning loodud meetmed (edaspidi ühiselt ka küberturvalisuse õiguslik raamistik) suutsid COVID-19 kriisi ajal aidata liikmesriikidel tagada riiklikult olulise tähtsusega teenuste toimimise. Selle eesmärgi puhul on oluline hinnata ennetus- ja reageerimisvõimekusele seatud tingimuste täitmist, näiteks küberturvalisuse indeksite abil. Kuivõrd Liit loob ainult raamistiku, kuid ei taga ise antud teenuste toimimist, on oluline läheneda magistritöö probleemidele Liidu liikmesriikide perspektiivist. EL-i ülesanne küberturvalisuse valdkonnas on kehtestada riikideülesed õiguslikud, organisatoorsed ja tehnilised standardid, mille rakendamiseks on liikmesriikides üle võetud direktiivid ning loodud vastavad agentuurid rahvusvaheliseks koostööks.

Magistritöös on tõstatatud kaks põhilist uurimisprobleemi, millega on seotud omakorda alaprobleemid. Esimeseks probleemiks on liikmesriikide ettevalmistus ja ennetusvõimekus.

[1] Georgiadou, A., *et al*. Hospitals' Cybersecurity Culture during the COVID-19 Crisis. Healthcare, 9(10), 1335. 2021. lk 1.
[2] International Telecommunications Union. Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. 2022, lk 15. Kättesaadav arvutivõrgus: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/ (18.04.2022).
[3] Europol. How criminals profit from the COVID-19 pandemic. 27.03.2020. Kättesaadav arvutivõrgus: https://www.europol.europa.eu/media-press/newsroom/news/how-criminals-profit-covid-19-pandemic (7.02.2022).
[4] Interpol. Cybercriminals targeting critical healthcare institutions with ransomware. 2020. Kättesaadav arvutivõrgus: https://www.Interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware (19.04.2022).
[5] Georgiadou, A., *et al*. *Op cit*, lk 2.

Võimekuse hindamisel saab määravaks liikmesriikide kriisieelne õigusloome küberturvalisuse valdkonnas. Euroopa Liit on tänaseks vastu võtnud kaks olulist küberturvalisust käsitlevat õigusakti: võrgu- ja infosüsteemide direktiiv (edaspidi NIS direktiiv)[6], ja küberturvalisuse määrus. Antud EL-i õiguse instrumendid on põhiliseks allikaks liikmesriikide tegevuse hindamisel lisaks siseriiklikele õigusaktidele. Eelneval kümnendil Euroopa Liidus aset leidnud tõsised küberründed (WannaCry ja NotPetya; Yahoo andmelekked; DoS rünnakud Twitterile, Facebookile ja Soome infrastruktuurile; Saksamaa valitsuse pahavararünnak; kahtlustused, et Venemaa on sekkunud valimistesse ning luuranud kübervahenditega Norra, Taani, Hollandi ja Itaalia vastu)[7] oleksid pidanud andma nii Euroopa Liidule kui ka liikmesriikidele piisava eelhoiatuse, et kiiremas korras on tarvilik seada prioriteediks infrastruktuuride ja teenuste küberturvalisuse kaitse.

Teiseks probleemiks on Euroopa Liidu õiguslikust raamistikust tulenev reageerimisvõimekus ning EL-i küberturvalisuse valdkonna võimalikud uued suunad COVID-19 kriisi mõjul. Kodust töötamine ja e-õpe ei mõjutanud ainult üksikindiviide, vaid ka riigiasutusi, kes viisid oma töö koju. Selle tulemusel tekkis arvukalt olukordi, kus kasutati riskantseid turvaaukudega programme (näiteks Zoom), mistõttu ei olnud oluliste asutuste andmed täielikult kaitstud.[8] COVID-19 kriis andis ka tugeva surve tervishoiule ning oluliseks sai kiire teabevahetus. Seal, kus ennetusvõimekus ebaõnnestus, sai määravaks küberintsidentide kiire ja õigeaegne tuvastamine ning negatiivsete mõjude likvideerimine. Kuivõrd teadusartiklites on kriitiliselt hinnatud, et EL-i küberturvalisuse valdkonna seisukohad ei ole laias plaanis COVID-19 kriisi tulemusel muutunud, tuleb töös analüüsida ka seda, kas ja mis ettepanekuid tuleks kaaluda edasiseks EL-i küberturvalisuse õigusliku raamistiku arenguks.

Magistritöö esimene uurimisküsimus on, mil määral vastab liikmesriikide õigus Euroopa Liidu küberturvalisuse õiguslikule raamistikule. Uurimisküsimuse lahendamiseks tuleb aru saada, mis pädevused on Euroopa Liidul küberturvalisuse valdkonna reguleerimisel, millest koosneb EL-i küberturvalisuse õiguslik raamistik ning milliseid siseriiklike õigusakte on vastavalt loodud. Teine uurimisküsimus on, kas Euroopa Liidu küberturvalisuse õiguslik raamistik toetab

[6] 6. juuli 2016. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2016/1148 mis täpsustab meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. — ELT L 194, 19.7.2016, lk 1-30.

[7] Euroopa Kontrollikoda. ELi küberturvalisuse poliitika tõhusust mõjutavad probleemid. 2019, lk 12. Kättesaadav arvutivõrgus: https://www.eca.europa.eu/et/Pages/DocItem.aspx?did={DEA2082B-4296-43EE-A5C9-9D01D7C0A585} (24.04.2022).

[8] Pawlicka, A., *et al*. A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. Business Horizons, 64(6). 2021, lk 732. Kättesaadav arvutivõrgus: https://www.sciencedirect.com/science/article/pii/S0007681321001336. 2021.07.010 (7.02.2022).

liikmesriikide võimekust lahendada kriisi ajal küberohust tingitud probleeme riiklikult oluliste teenuste osutamisel. Selle küsimuse lahendamiseks tuleb mõista, mis mõju on COVID-19 kriisil olnud riiklikult olulistele teenustele, millised on seda valdkonna enim mõjutanud küberintsidendid ja kuidas need on sõltuvuses liikmesriikide küberturvalisuse võimekusega.

Magistritöös püstitatud hüpoteesid on järgmised:

1. Riiklikult oluliste teenuste tagamise häiritus on tugevas sõltuvuses riigi võimekusest rakendada olemasolevaid küberturvalisuse valdkonna meetmeid. Euroopa Liidu siseselt oli riigiti ettevalmistus ja vastupanuvõime küberturvalisusega seotud ohtude tõusule väga erinev.
2. Euroopa Liidu küberturvalisuse õiguslik raamistik ja loodud meetmed olid piisavad, et tagada ettevalmistus küberintsidentide teoreetiliseks ohjeldamiseks, kuid liikmesriigid ja erinevad asutused ei olnud võimelised neid vastavalt rakendama.
3. Euroopa Liit ei uuendanud COVID-19 kriisi mõjul küberturvalisuse valdkonnas kehtivaid seisukohti, vaid kiirendas varasemate ettepanekute elluviimist.

Magistritöös on tehtud mitmeid kitsendusi tulenevalt küberturvalisuse valdkonna suurusest ja antud uurimuse mahust. Esiteks lähtutakse küberturvalisuse õigusliku raamistiku hindamisel vaid kriitilist infrastruktuuri ja riiklikult olulisi teenuseid reguleerivatest õigusaktidest. Teiseks on valitud riiklikult oluliste teenuste puhul analüüsiks eelkõige COVID-19 pandeemiast enim mõjutatud sektorid nagu tervishoid ja elektrooniline kommunikatsioon. Ajalises mõttes puudutab analüüs enim statistikat ja küberintsidente alates 2020. aastast, kui pandeemia Euroopat enim mõjutama hakkas.

Magistritöö on kirjutatud õigusdogmaatilise võrdleva uurimusena, kus põhilisteks allikateks on õigusaktid, regulatsioonid, kirjandus ning erinevad valdkonnaga seotud teadusartiklid ja uurimused. Magistritöös koondatakse olemasolev informatsioon valdkonnaga seotud allikatest ja kõrvutatakse neid uurimistulemuste saavutamiseks. Võrdleva meetodi puhul analüüsitakse, mis ulatuses ning milliste erinevustega võeti siseriiklikkusse õigusesse üle Liidu küberturvalisuse õiguslik raamistik. Seejärel kõrvutatakse seda COVID-19 mõjuga ning riikide küberturvalisuse indeksite hinnangutega, et anda vastus uurimisküsimustele. Lisaks vaadeldakse grammatilise tõlgendamise abil, mis sõnastuses ja milliste erinevustega on üle võetud Liidu õigusaktid siseriiklikkusse õigusesse. Teleoloogilise tõlgendamisega selgitatakse küberturvalisuse põhimõtete ja seisukohtade kujunemist ning kasutusel on ka analüütiline meetod statistiliste andmete koondamiseks ja sünteesimiseks.

Magistritöös on valitud võrdleva analüüsi tarbeks EL-i liikmesriikide valimisse Eesti, Iirimaa ja Tšehhi. Kõik kolm riiki on näidanud hüppelist kasvu e-teenuste pakkumises ning arendamises ja riikide õiguskord soodustab rahvusvahelistel ettevõtetel samas valdkonnas tegutsemist. Samuti on kõikides valimiriikides üle võetud üks esimesi kõikehõlmavaid EL-i üleseid õigusakte küberturvalisusest ehk NIS direktiiv[9], mille eesmärk on Liidu üleüldise küberturvalisuse taseme tõstmine ja muuhulgas liikmesriikide ettevalmistus- ning reageerimisvõimekuse tagamine kokkupuutel küberohtudega. Magistritöös kasutatakse ka üleeuroopalist küberintsidentide statistikat COVID-19 mõju hindamiseks. Valimiriikide hinnangu täiustamiseks on esitatud iga riigi küberturvalisuse ametile küsimustik, eesmärgiga koguda informatsiooni, mis ei ole avalikult kättesaadav, ning kõrvutada ametkondade arvamust teoreetilise võimekuse analüüsiga. Ametitel paluti vastata Lisa 1-s täpsustatud küsimustele. Magistritöös on kasutatud lisaks kirjalikele allikatele ainult Eesti ja Tšehhi ametkondade poolt edastatud vastuseid. Iirimaa küberturvalisuse ametilt ei tulnud küsimustikule vastust, mistõttu antud riigi analüüsimisel kasutati vaid kirjalikke allikaid.

Magistritöö on jaotatud kolme suurde peatükki. Esimeses peatükis keskendutakse Euroopa Liidu küberturvalisuse õigusliku raamistiku selgitamisele ning tutvustatakse liikmesriikide valimi näitel õigusaktide rakendamist riigi tasandil. Lisaks kirjeldatakse, kuidas on kujunenud EL-i pädevus reguleerida küberturvalisuse valdkonda ja millised probleemid eksisteerivad mõiste „küberturvalisus“ kasutamisel. Teises peatükis defineeritakse riiklikult oluliste teenuste tähendus ja olemus liikmesriikide näitel. Lisaks tehakse ülevaade COVID-19 pandeemia negatiivsest mõjust eelnevalt mainitud teenuste küberturvalisusele. Kolmandas peatükis analüüsitakse Euroopa Liidu küberturvalisuse meetmete ja õigusaktide kohaldumist siseriiklikus õiguses ning võrreldakse seda nii küberturvalisuse indeksite kui ka juhtumite statistikaga, et hinnata liikmesriikide teoreetilist vastupanuvõimet COVID-19 kriisi tingimustes. See tähendab, et sünteesitakse eelnev informatsioon, koondatakse analüüsitulemused ja tehakse ettepanekud muudatusteks küberturvalisuse meetmete ja õigusaktide arendamiseks EL-i tasandil.

Tööd enim iseloomustavad märksõnad: küberturve, küberturvalisus, elutähtsad teenused, Euroopa Liidu õigus, infotehnoloogiaõigus.

[9] 6. juuli 2016. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2016/1148 mis täpsustab meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. — ELT L 194, 19.7.2016, lk 1-30.

1. Euroopa Liidu küberturvalisuse õiguslik raamistik

1.1. Küberturvalisuse kujunemine eraldiseisvaks poliitikavaldkonnaks Euroopa Liidu tasandil

Küberturvalisus kui eraldiseisev Euroopa Liidu poliitikavaldkond sai oma ametliku alguse 2013. aastal, kui vastu võeti Euroopa Liidu esimene ülevaatlik küberturvalisuse strateegia. Antud strateegia vastuvõtmine oli kauaoodatud, sest vajadus valdkonna-üleseks koordinatsiooniks EL-i tasandil tekkis juba aastaid varem. Küberruumiga kaasnevad negatiivsed mõjud olid ühiskonna osaks juba kümneid aastaid enne ametliku strateegia loomist. Seda alates ajast, mil arvuti kasutamine sai igapäevaseks põhivajaduseks ning teenused ja tooted olid kättesaadavad interneti vahendusel. Strateegia loomisega seati eesmärk, et küberruum oleks tulevikus kaitstud ning regulatsioonid ja meetmed harmoniseeritud terviklikult Liidu tasandil.[10]

Enne ametliku poliitikavaldkonna kujundamist loodi 2004. aastal Euroopa Võrgu- ja Inforturbeamet (edaspidi ENISA), mille eesmärk on tagada kõrge ja efektiivne tase võrgu- ja infosüsteemide kaitsmiseks Liidu ja liikmesriikide tasandil. Ameti loomisega sooviti anda panus tagamaks Euroopa Liidu kui ühtse majandusliku turu toimimine. ENISA oli algselt tähtajalise mandaadiga organisatsioon, kuid nähes ameti olulist, on selle organisatsiooni mandaati pikendatud mitmel korral. Koos 2013. aasta strateegiaga ning vastavate direktiividega tugevdati ENISA rolli ning kujundati ümber ameti struktuur, et see suudaks tugevdada usaldust erinevate võtmetähtsusega isikute jaoks küberturvalisuse valdkonnas.[11]

Lisaks rõhutas Euroopa Komisjon (edaspidi EK) 2009. aastal vajadust tagada efektiivne Euroopa majanduse ja ühiskonna kommunikatsiooni infrastruktuuride toimimine, mille raames oleks vaja kaitsta kriitilist infrastruktuuri ning tõrjuda küberründed. Euroopa Komisjoni hinnangul oli selleks vaja kaasata erinevaid võtmeisikuid nii avalikust kui ka erasektorist, et tagada ennetus- ja reageerimisvõimekus võimalike küberrünnete eest, mille eesmärgiks on kahjustada kriitilist infrastruktuuri. Näib, et vajadus kaitsta olulisi teenuseid ja infrastruktuuri

[10] Euroopa Kontrollikoda. *Op cit*, lk 12-13.
[11] Euroopa Komisjon. Digital Agenda: Commission proposal to strengthen and modernise European Network and Information Security Agency (ENISA) – frequently asked questions. MEMO/10/459, 2010. Kättesaadav arvutivõrgus: http://europa.eu/rapid/press-release_MEMO-10-459_en.htm?locale=en (09.04.2022).

on pikalt olnud Euroopa Liidu üks olulisemaid eesmärke küberturvalisuse valdkonnas. Selle küberturvalisuse eesmärgi saavutamiseks on vajalik erinevate sektorite koostöö.[12]

Üha kasvava digitaliseerimise ning kübersõltuvuse taustal tekkis eelnevalt nimetatud küberintsidentide mõjul[13] Euroopa Liidus oht küberturvalisusele, millega tegelemiseks astuti esimene suurem samm - Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum. 2013. aasta strateegia eesmärk oli ambitsioonikas, sest Euroopa Komisjoni soov oli muuta EL-i veebikeskkond maailma kõige turvalisemaks. 2013. aasta küberturvalisuse strateegia kolm olulist suunda olid:

- võrgu- ja infoturve, mis oli suunatud olulistele teenusepakkujatele ning kriitiliste digitaalsete infrastruktuuride tagajatele,
- elektrooniline kommunikatsioon ning privaatsus ja andmekaitse,
- küberkuritegevus.[14]

Käesoleva magistritöö raames on põhirõhk pandud suuresti esimesele valdkonnale ehk oluliste teenuste ja infrastruktuuride kaitsele küberturvalisuse valdkonnas. Kuigi järgnevalt käsitletakse ka elektroonilist kommunikatsiooni reguleerivaid õigusakte, jääb antud uurimusest välja põhjalik analüüs privaatsuse ja andmekaitse ning küberkuritegevuse regulatsioonidest Liidu tasandil ja siseriiklikus õiguses. Antud valik sai tehtud töös püstitatud uurimisküsimusele vastamiseks, sest oluliste teenuste operaatoritele kehtivad õigusaktid ja kriisi mõju saab uurida eelkõige strateegia esimese valdkonna abil. EL-i küberkuritegevust reguleerivate õigusaktide analüüs väljuks antud magistritöö mahuraamidest, sest nõuaks mitmete EL-i kriminaalõigust reguleerivate aktide sisu selgitamist.[15]

EL-i esimese strateegia vastuvõtmisega tunnistati Fuster ja Jasmontaite sõnul küberturvalisuse poliitikavaldkonnas seda, et küberrünnakud olid uus reaalsus ning sellistel rünnakutel võisid olla raskesti ennustatavad eskaleerivad mõjud. Nende koostatud analüüsi tulemusel järeldati, et strateegiaga nõuti küberrünnakute tõsiduse tunnustamist ja küberrünnakutega võitlemisel

[12] Giantas, H. D. Liaropoulus, N. A. Cybersecurity in the EU: Threats, frameworks and future perspectives. 2019, lk 13. Kättesaadav arvutivõrgus: https://www.researchgate.net/publication/335909463_Cybersecurity_in_the_EU_Threats_frameworks_and_future_perspectives (09.04.2022).
[13] Vt täpsem loetelu olulisematest küberintsidentidest käesoleva töö sissejuhatuses.
[14] Euroopa Komisjon. Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum. 2013. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52013JC0001 (09.04.2022).
[15] Seetõttu ei käsitleta töös GDPR-ist ning Euroopa Nõukogu Budapesti konventsioonist (arvukuritegevusvastane konventsioon) tulenevaid nõudeid liikmesriikidele.

tehtavat suuremat koostööd väljakujunenud võrgustike vahel. Ebatõhus küberturvalisuse poliitika võis takistada aga digitaalse ühtse turu tõrgeteta toimimist, millel omakorda oleks kahjulik rahaline mõju erinevatele osapooltele.[16]

EL-i küberjulgeoleku strateegia, kirjeldades valdkonnas valitsevaid põhimõtteid, kinnitas, et küberturvalisuse valdkonna meetmed peavad olema seotud EL-i üldiste väärtustega ja põhiõigustega nagu näiteks sõnavabadus ning isikuandmete ja eraelu puutumatuse kaitse. Kuigi küberturvalisust arendatakse strateegia loomisega eraldiseisvalt, on tegemist siiski multidistsiplinaarse valdkonnaga. Lisaks toodi strateegias välja, et internetile ligipääs tuleb tagada kõigile ning sellega peab kaasas käima interneti terviklikkus ja turvalisus. Strateegias räägiti nii ühisest vastutusest kui ka kõikehõlmavast koostöö- ja otsustusringist. Siinkohal peegeldus välja vajadus riikide ja erinevate valdkondade omavaheliseks koostööks, sest vastutust ei saa panna ainult ühele osapoolele. 2013. aastal vastu võetud strateegia oli oluline ka sellepoolest, et sõnastati edasised tegevused küberturvalisuse valdkonna arendamiseks. Esmapilgul oli ettenähtud tegevuste loetelu üsna optimistlik ning ehk veidi naiivne. Seda seetõttu, et küberturvalisuse valdkonna strateegilised eesmärgid nõudsid erinevate partnerite ning eelkõige riikide enda pingutusi.[17]

2017. aastal toimunud kaks suurimat EL-i kogukonda raputanud lunavararünnakut, mida tuntakse WannaCry ja NotPetya nimede all näitasid aga, et oli võimalik teha veel palju täiustusi, eelkõige seoses reageerimise ja koostööga erinevate küberturvalisusega tegelevate organisatsioonide vahel EL-i ja riiklikul tasandil.[18] Nendele rünnakutele järgnes samal aastal EL-i 2013. aasta küberjulgeoleku strateegia ajakohastamine. Uue versiooni eesmärk oli parandada Euroopa kriitilise infrastruktuuri kaitset ja suurendada EL-i digitaalset enesekehtestamisvõimet suhetes suurriikidega nagu Hiina, Venemaa ja USA, kelle arusaam küberturvalisusest võib ohustada demokraatiate stabiilsust. Reformitud strateegia jättis lahtiseks mitmeid küsimusi selle kohta, kuidas algselt püstitatud ambitsioonikat eesmärki – avatud, ohutut ja turvalist küberruumi – usaldusväärselt kaitsta. Piisavalt selgelt ei väljendatud ka seda, kuidas defineeritakse EL-i vastupanu- ja heidutusvõime või ületatakse institutsiooniline killustatus ja õigusliku volituse puudumine küberturvalisuse küsimustes. Vastuolulised teemad nagu kriminaalõiguse ühtlustamine või krüpteerimise kasutamine olid täielikult välja jäetud. Strateegia uuendus nägi vaid ette, et liikmesriigid oleksid pidanud

[16] Christen, M. *et al*. The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology vol 21, 2020, lk 99-100.
[17] Euroopa Komisjon. 2013. *Op cit*, lk 3-4.
[18] Christen, M. *et al*. *Op cit*, lk 99.

loobuma oma eraldiseisvatest jõupingutustest ja kiirendama küberturvalisuse õiguslikku reguleerimist EL-i tasandil.[19]

Uuendatud strateegia nägi ette viit suurt reformi: Euroopa küberturvalisuse uurimis- ja kompetentsikeskuse moodustamise; üleeuroopalise kriisidele reageerimise mehhanismi loomise, et tulla toime tulevaste suuremahuliste küberrünnakutega; küberturvalisuse hädaolukorra fondi loomise; sõjalise küberkaitse ühisprojektide arendamise alalise struktureeritud koostöö raames ja Euroopa Kaitsefondi abiga ning usaldust suurendavate meetmete ja riigivastutuse edendamise, et piirata küberriske kogu maailmas. Kõigi ettepanekute eesmärgiks oli saavutada EL-i vastupanuvõime suurendamine kübervaldkonnas. Strateegiast jäi välja aga keeruline küsimus sellest, kuidas tuleks võidelda interneti ja sotsiaalmeedia kuritegeliku sisuga. Enamik EL-i liikmesriike oli strateegia uuendamise hetkeks alla kirjutanud Budapesti konventsioonile ja seega nõustunud kohustusega võtta vastutusele isikud, kes panevad küberruumis kuritegusid toime. Sellegipoolest valitses Euroopa riikide vahel suur lahknevus selles osas, millised tegevused on digitaalvaldkonnas kuriteod. Peamine vaidluskoht oli hoopis sõnavabaduse ehk ebaseadusliku vihakõne määratluse üle.[20]

Euroopa Komisjoni retoorikat võis eelnevalt mainitud dokumentide pinnalt pidada soosivaks küberturvalisuse laiendatud visiooni kasutamiseks, et tagada EL-i väärtuste ja huvide järgimine. Rõhutati vajadust suurema koostöö ja programmide koordineerimise järele, mis käsitleksid julgeoleku-, piiri- ja rändehalduse infosüsteemide koostalitlusvõimet. EK viitas siinkohal ülemaailmsele küberrünnakutele ehk WannaCry juhtumile, millega näidati vajadust laiendada EL-i tegevust ja seega tunnustada pädevust küberturvalisuse valdkonnas. Samas viitas EK ka USA-st pärit lunavara käsitlevale statistikale, millega sooviti selgitada väidet küberrünnakute võimalike ohtude kohta EL-i erivaldkondades. EK sõnul pidi küberturvalisuse valdkond neid riske suutma käsitleda. Selline lai argumentatsioon võis aga olla vastuolus EL-i parema õigusloome poliitika loogikaga, mille järgi peab õigusloome eelkõige põhinema ühelt poolt parimatel saadaolevatel tõenditel ja teisalt sidusrühmade kaasamisel.[21]

[19] Bendiek, A., Bossong, R., Schulze, M. The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges. German Institute for International and Security Affairs. 2017, lk 1. Kättesaadav arvutivõrgus: https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf (09.04.2022).
[20] *Ibidem.*, lk 2, 5.
[21] Christen, M. *et al*. *Op cit*, lk 111-112;
Euroopa Komisjon. Commission staff working Document. Better Regulation Guidelines. 2015. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015SC0111 (09.04.2022).

Mõned küberturvalisuse valdkonda mõjutavad poliitikadokumendid pärinevad juba hilisemast ajast, näiteks 2021-2027 digitaalse hariduse tegevusplaan ja täiesti uus EL-i küberturvalisuse strateegia digitaalseks kümnendiks. Digitaalse hariduse tegevusplaan loodi eeldusel, et liikmesriikidel on vähene võimekus kaasata piisavas mahus digitaalseid eksperte, sealhulgas küberturvalisuse analüütikuid. Tegevusplaani eesmärk nägi ette kasvatada jõudsalt e-oskuste taset ning seega ka liikmesriikide kompetentsi küberturvalisuse valdkonnas. EL-i digitaalse kümnendi küberturvalisuse strateegia rõhutas samuti, et küberturvalisuse üldpädevused on madalad. Lisaks oli töötajate hulgas märkimisväärne puudus küberturvalisuse oskustest.[22]

Praegust küberturvalisuse suutlikkust ainuüksi strateegias püstitatud eesmärkide taustal on EL-i tasandil sellegipoolest raske mõõta; veelgi enam seda, kas selle tulemuseks on võimalikult turvaline veebikeskkond. Kuigi poliitika ja õigusaktide vahele jääv ruum on lai, võivad need strateegilised dokumendid anda aimdust EL-i edasistest plaanidest küberturvalisuse valdkonnas kehtestatavatele regulatsioonidele ning seda toetavatele meetmetele, mis kokku moodustavad tervikliku küberturvalisuse õigusliku raamistiku.

1.2. Euroopa Liidu õiguslikud pädevused küberturvalisuse valdkonna reguleerimisel

Euroopa Liidu küberturvalisuse valdkonna strateegia ja olulisemate õigusaktide taustal on oluline aru saada, mis pädevused ja õigused on Liidule omistatud, et selles valdkonnas tegutseda. Bendiek, Bossong ja Schulze seadsid Euroopa Liidu õiguslikud eesmärgid kahtluse alla, kui kommenteerisid Liidu tegevust 2013. aasta uuendatud küberturvalisuse strateegia valguses.[23]

EL-i küberturvalisus valdkond on hea näide sellest, kuidas omavahel on seotud sise- ja välispoliitika ning selle tarbeks on vaja ühendada ka Liidu erinevad õiguspädevused. Viimase kümnendi jooksul, kui Euroopa Liit alustas selle uue valdkonna reguleerimist, käivitasid samaaegselt ülemaailmsed julgeolekuohud sisepoliitika arengu. 2013. aasta EL-i strateegia vastuvõtmisega oli ühenduse eesmärk viia erinevad varasemad algatused terviklikult kokku,

[22] Euroopa Komisjon. The Digital Education Action Plan (2021-2027). Resetting education and training for the digital age. 2020. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0624 (09.04.2022);
Euroopa Komisjon. The EU's Cybersecurity Strategy for the Digital Decade. 2020. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN (09.04.2022).
[23] Bendiek, A., Bossong, R., Schulze, M. *Op cit*, lk 3.

mis peegeldasid soovi olla osa ülemaailmsete küberreeglite väljatöötamisel. Euroopa küberturvalisuse valdkond viidi ellu mitmetasandilise struktuurina, milles seadusandlus oli seotud nii rahvusvaheliste arengute kui ka siseriikliku õigusega liikmesriikides.[24]

Üllatusena võib tulla asjaolu, et küberturvalisust ei ole eraldiseisvalt EL-i aluslepingutes nimetatud valdkonnana, millega Euroopa Liit peaks tegelema. Wessel on kirjeldanud, et kõige sobivam valdkond, kus küberturvalisust oleks võinud mainida, on ühine julgeoleku- ja kaitsepoliitika (CDSP), mis on suures osas välja töötatud sõjalis- ja tsiviilkoostööna. Seda pädevust kasutatakse EL-i konsolideeritud lepingu art 42 põhjal, mis järgi Liidul on operatiivne tegutsemisvõime ja seda võib rakendada missioonidel väljaspool liitu rahuvalvamiseks, konfliktide ennetamiseks ja rahvusvahelise julgeoleku tugevdamiseks kooskõlas ÜRO põhikirja põhimõtetega.[25] Euroopa Liidu lepingu art 42(1) nimetatud missioonid ja art 43(1) sisalduv ülesannete täpsem loetelu ei sisalda aga viidet küberturvalisusele. Sama kehtib ka siseturgu käsitletavate ning vabadusel, turvalisusel ja õigusel rajaneva asutamislepingu sätete kohta, milles puudub viide küberturvalisusele. Küsimus säilib EL-i pädevusest küberturvalisuse valdkonda reguleerida, sest on arusaadav, et 2013. aasta strateegia vastuvõtmisega on sellest kujunenud Liidu jaoks üks olulisemaid prioriteete. Asjaolu, et EL-il puudub selgelt antud pädevus küberturvalisuse valdkonnas meetmete võtmiseks, on loonud olukorra, kus Liit kasutab oma õiguslikku pädevust teistes valdkondades või võtab vastu kergema mõjuga õigusakte ning meetmeid, et antud valdkonda reguleerida. Sellise killustatud lähenemisviisi puhul on raske aru saada, mida küberturvalisus täpselt hõlmab ning kuidas ja mille põhjal saab selle valdkonna ülesandeid ja vastutust jaotada.[26]

On võimalik väita, et Euroopa Liit oleks võinud võtta teistsuguse lähenemisviisi vastuseks eelnevalt mainitud küberrünnakutele ja küberohu kasvule. Näiteks soovitas Euroopa andmekaitseinspektori assistent Wiewiórowski, et kui oleks rakendatud andmekaitseseaduses nõutud asjakohaseid turvameetmed, oleks eelpool nimetatud küberründed Wannacry ja

[24] Tsagourias, N. Buchan, R. Wessel, A. R. Research Handbook on International Law and Cyberspace: Chapter 19: Towards EU cybersecurity law: Regulating a new policy field. 2015. Kättesaadav arvutivõrgus: https://www.elgaronline.com/view/edcoll/9781782547389/9781782547389.00032.xml (10.04.2022).
[25] Euroopa Liidu toimimise lepingu konsolideeritud versioon. ELT C 326, 26.10.2012, lk 47—390.
[26] Wessel, A. R. Cybersecurity in the European Union: Resilience through Regulation? The Routledge Handbook of European Security Law and Policy. 2019, lk 284-285. Kättesaadav arvutivõrgus: https://www.utwente.nl/en/bms/pa/research/wessel/wessel140.pdf (10.04.2022).

NotPetya saanud ära hoida.[27] Euroopa Komisjon võib seda argumentatsiooni kasutades aga rõhutada pigem vajadust paremini reageerida küberohtudele, rakendades EL-i olemasolevast andmekaitseraamistikust tulenevaid nõudeid. Samas võttes arvesse küberturvalisuse valdkonna multidistsiplinaarsust näitas antud argumentatsioon vajadust ühtlustada erinevates õigusaktides olevaid turvanõudeid ja mitte ilmtingimata seda, et puudub vajadus uuteks küberturvalisust reguleerivateks aktideks.[28]

EL-i küberturvalisuse pädevuse küsimustes tõstatub esile pädevuse andmise põhimõte (*principle of conferral*). Tegemist on ühe Euroopa Liidu õiguse fundamentaalse printsiibiga, mis reguleerib Liidu pädevuse piire. Pädevuste kasutamist reguleeritakse aga subsidiaarsuse ja proportsionaalse põhimõtte järgi. Pädevuse andmise põhimõte sätestab, et EL-il võib vastu võtta õigusakte valdkondades, kus on sobivam seda teha Liidul, kui et liikmesriikidel eraldi tegutseda. Sellel juhul, mis tahes regulatiivse meetme kehtestamisel EL-i tasandil, sealhulgas küberturvalisusega seotud meetmete puhul, nõuab see seadusandjalt õiguslikku põhjendust, teisisõnu seaduslikku alust selle pädevuse omistamiseks. Eelkõige peab seadusandliku meetme ettepanek vastama Euroopa Liidu lepingu art 5 lg 3 sätestatud kriteeriumidele. Põhimõtteliselt tähendab see, et pädevuse määramiseks peab seadusandlik meede täitma ühe kahest eeldusest:[29]

1. Liikmesriigid ei suuda kavandatud meedet piisavalt saavutada ei piirkondlikul ega kohalikul tasandil.
2. Kavandatava meetme ulatuse või mõju tõttu on seda võimalik paremini ellu viia Liidu tasandil.[30]

Pädevuse andmise põhimõtte ja eelnevalt mainitud EL-i piiratud pädevuste tõttu julgeolekuküsimustes, laskus EK-l kohustus anda selgitus küberturvalisuse valdkonna õigusliku pädevuse omamiseks. See selgitus on antud NIS direktiivis, kus luuakse seos küberturvalisuse ja siseturu vahel. Fuster ja Jasmontaite sõnul meenutab see põhjendus suures osas arutluskäiku, mida kasutati 1995. aasta isikuandmete kaitse eeskirjade kehtestamisel.[31] Võrgu- ja infoturbe direktiivi põhjenduses 5 öeldakse, et liikmesriikide erinevad tavad seoses küberturvalisuse meetmetega takistavad tarbijatele ja ettevõtetele pakutavat kaitset ning

[27] Wiewiórowski, W. Privacy, security, and technology: the annual privacy forum. 2017. Kättesaadav arvutivõrgus: https://edps.europa.eu/press-publications/press-news/blog/privacy-security-and-technology-annual-privacy-forum-2017_en (10.04.2022).
[28] Christen, M. *et al*. *Op cit*, lk 111-112.
[29] Christen, M. *et al*. *Op cit*, lk 107.
[30] Euroopa Liidu lepingu konsolideeritud versioon. ELT C 326, 26.10.2012, lk 13—390.
[31] Christen, M. *et al*. *Op cit*, lk 107.

vähendavad sellest tulenevalt võrgu- ja infosüsteemide üldist turvalisuse taset.[32] Võrgu- ja infoturbe direktiiv võeti vastu liikmesriikide küberturvalisuse meetmetega seotud tavade ühtlustamiseks.[33] Seeläbi saavutatakse EL-i toimimise lepingu art 4 (2)(a) eeldused, mis annavad EL-ile jagatud pädevuse siseturu valdkonnas ja seega ka küberturvalisuse reguleerimiseks.

Kuigi EL-i pädevuse küsimus on sellega lahendatud, jääb valdkonna kiire areng pikas plaanis saavutamata, sest selged õiguslikud pädevused on jagatud ning kohati ebaselged. Lahenduseks saab olla, kas EL võtab tulevikus vastu selge seisukoha küberturvalisuse õiguslike pädevuste kohta EL-i lepingu muutmise läbi, mis on selgelt keeruline protsess või otsustab minna seni käidud teed pidi. EL on sellegipoolest võtnud vastu mitmeid poliitikadokumente ning õigusakte, mis on juba kaasa toonud osalise valdkonna fragmenteerituse. Õigusaktid on jaotunud nii siseturu, vabaduste kaitse, julgeoleku ning välispoliitika reguleerimise vahel, luues omaette väljakutse tulevaste meetmete ühtlustamise taustal. Järgnevalt keskendutakse küberturvalisuse valdkonda enim mõjutanud EL õigusaktidele Liidule antud pädevuste taustal ja kuidas need omavahel on seotud oluliste teenuste kaitsmise eesmärgil.[34]

1.3. Olulisemad küberturvalisuse õigusaktid ja kohalduvus liikmesriikides

Vaatamata mitmetele tõsistele küberrünnakutele, mille sihtmärkides olid Liiduga seotud riigid, kannatas EL küberturvalisuse küsimustes kuni 2016. aastani koostöö ja ühise seisukoha puudumise probleemides. Küberintsidentide sagedus, ulatus ja keerukus oli suurenenud ning ohustamas suures osas liikmesriikide üldist turvalisust ja majandust. EL-i liikmesriikide jõupingutused küberrünnaku raames teha koostööd kujunesid aga killustatud katseks ning ei suutnud tagada piisavalt järjepidevust, et küberprobleemidega toime tulla. 2016. aasta juulis, kui tehti ettepanek NIS direktiivi vastuvõtmisele, näitas Euroopa Liit märke kollektiivsemast lähenemisest küberturvalisuse probleemidele.[35]

Küberturvalisuse vastupanuvõime on jätkuvalt kriitilise infrastruktuuri kaitsmise peamine prioriteet Euroopa Liidus. Võrgu- ja infosüsteemid olid riiklike strateegiate ja võimete

[32] 6. juuli 2016. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2016/1148 mis täpsustab meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. — ELT L 194, 19.7.2016, lk 1-30.
[33] Christen, M. *et al*. *Op cit*, lk 107.
[34] Tsagourias, N. Buchan, R. Wessel, A. R. *Op cit*.
[35] Giantas, H. D. Liaropoulus, N. A. *Op cit*, lk 13-14.

killustatuse tõttu haprad, sest puudus ühine koordineerimine nõuete osas. Euroopa Komisjon soovis panustada tõhusa Euroopa mehhanismi loomisesse, et edendada koostööd ja teabe jagamist võrgu- ja infoturberiskide ja -intsidentide kohta. Seega EL-i küberturvalisuse strateegia elluviimise ühe osana tegi EK ettepaneku võtta vastu EL võrgu- ja infoturbe direktiiv teisisõnu NIS direktiiv.[36]

Olenemata, et tegemist on direktiiviga, omab antud õigus mõju siseriiklikule õigusele ja üksikindiviididele, mida saab vaadelda nii otsese kohalduvuse kui ka õigusmõju printsiipide alusel. Otsene kohaldatavus tähendab, et luuakse EL-i esmase õiguse ja liikmesriikide õiguse vahetu ühendus. Määrustel on otsekohalduvus, kuid EL-i direktiivid kohustavad liikmesriike looma siseriiklike õigusakte. Otsese õigusmõju puhul küsitakse, kas üksikisikud saavad siseriiklikes kohtutes tugineda EL-i õigusele. Otsest mõju on kahte tüüpi – vertikaalne ja horisontaalne. Vertikaalne otsemõju tähendab, et EL-i õigusakte saab kasutada liikmesriigi vastu ja horisontaalne tähendab, et EL-i õigusakte saab kasutada teise isiku vastu. Lepingud ja määrused on vertikaalselt ja horisontaalselt vahetult kehtivad. Lepingut või määrust saab liikmesriigi kohtus kasutada seadusena riigi või muu üksikisiku vastu. Erinevus seisneb selles, et direktiivid ei ole otseselt mõjuvad, seega neid ei saa kohtus kasutada enne, kui need on kehtestatud siseriiklike õigusaktidega.[37]

NIS direktiiv oli esimene horisontaalne siseturu instrument, mille eesmärk oli parandada Euroopa Liidu küberturvalisuse vastupanuvõimet. Direktiivi eesmärk oli suurendada küberturvalisust ning sellega seotud turvanõudeid kogu EL-is. Kuivõrd tegemist oli EL-i teisese õigusega vastavalt EL-i toimimise lepingu art 288 ehk direktiiviga, on pidanud iga liikmesriik õigusakti üle võtma siseriiklikku õigusesse. Seda kohustust kinnitas ka NIS direktiivi art 25. Üldjuhul annavad EL-i direktiivid teatud paindlikkuse, et võtta arvesse riiklikke olusid, näiteks olemasolevate organisatsiooniliste struktuuride taaskasutamiseks või kehtivate siseriiklike õigusaktidega vastavusse viimiseks.[38] NIS-direktiivil on kolm osa:

- Riiklikud võimekused: EL-i liikmesriikidel peavad olema teatud riiklikud küberturvalisuse meetmed, nt riiklik CSIRT, peavad tegema küberõppusi jne.

[36] Euroopa Komisjon. - Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665. 2021, lk 9.
[37] EKo C-26/62, *NV Algemene Transport- en Expeditie Onderneming van Gend en Loos vs. Netherlands Inland Revenue Administration*, ECLI:EU:C:1963:1.
[38] *Ibidem*; 6. juuli 2016. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2016/1148 mis täpsustab meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. — ELT L 194, 19.7.2016, lk 1-30; Euroopa Liidu toimimise lepingu konsolideeritud versioon. ELT C 326, 26.10.2012, lk 47—390.

- Piiriülene koostöö: piiriülene koostöö EL riikide vahel, nt operatiivne EU CSIRT võrgustik, strateegiline võrgu- ja infoturbe koostöörühm jne.
- Riiklik järelevalve kriitiliste sektorite üle: EL-i liikmesriigid peavad teostama järelevalvet kriitiliste üksuste küberturvalisuse üle.[39]

Tänaseks on võrgu- ja infoturbe direktiivis määratletud ülevõtmisega seotud ettekirjutused ja kohustused täidetud. NIS direktiivi on üle võtnud kõik 27 EL liikmesriiki. Ülevõtmise tulemusel on liikmesriigid võtnud oma siseriiklikesse õigusaktidesse nõuded riikide võrgu- ja infosüsteemide turvalisuse kohta koos üksikasjalike sätetega. Samuti on vastu võetud näiteks seadusi, eeskirju või suuniseid oluliste teenuste operaatorite ja digitaalsete teenuste osutajate identifitseerimiseks kasutatavate künniste määratlemise kohta.[40]

NIS direktiivis sisalduv on üheltpoolt mõeldud lähtepunktiks nii siseriiklike õigusaktide kavandamisel kui ka nende tõlgendamiseks vajalike definitsioonide ning põhimõtete loomisel. Näiteks loetletakse art 4 alusel üles kõik direktiivist arusaamiseks vajalikud mõisted. Võrgu- ja infosüsteemide defineerimiseks kasutatakse kolme kriteeriumit. Need on kas elektroonilised sidevõrgud direktiivi 2002/21/EÜ alusel; seade või omavahel ühendatud seadmete rühm, milles toimub mõne programmi digitaalsete andmete automaatne töötlemine või digitaalsed andmed, millega tehakse art 4(1)(c) loetelus märgitud toiminguid. Oluline on siinkohal märkida, et mainitud direktiiv 2002/21/EÜ on ka uue Euroopa elektroonilise side seadustiku loomise aluseks. Võrgu- ja infosüsteemide turvalisuse taset kirjeldatakse kui võimet vastu panna mis tahes tegudele, mis seaksid ohtu eelpool nimetatud andmetega seotud toimingud või nende süsteemide kaudu pakutavad teenused. Kokku selgitatakse lahti 19 erinevat direktiiviga seotud mõistet, kusjuures näiteks oluliste teenuse operaatorite (edaspidi OTO) ja digitaalsete teenuste osutajate (edaspidi DTO) puhul viidatakse direktiivi lisadele, kus on lahti kirjeldatud olulised üksused ning EL-i õigusaktid, mille alusel neid defineeritakse.[41]

[39] 6. juuli 2016. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2016/1148 mis täpsustab meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. — ELT L 194, 19.7.2016, lk 1-30.
[40] Euroopa Komisjon. 2021. *Op cit,* lk 11.
[41] 6. juuli 2016. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2016/1148 mis täpsustab meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. — ELT L 194, 19.7.2016, lk 1-30.

Direktiivis sisalduvad veel järgnevad kohustused: Esiteks art 1 alusel tuleb igal riigil luua vastav võrgu- ja infosüsteemide strateegia;[42] art 7 järgi peavad liikmesriigid määratlema strateegilised eesmärgid ja poliitilised ning regulatiivsed meetmed selleks, et strateegia abil toetada võrgu- ja infosüsteemide turvalisuse kõrge taseme saavutamist ja säilitamist; kolmandaks kohustuseks on CSIRT ehk küberturbe intsidentide lahendamise üksuse loomise nõue. Art 9, art 12 ja lisa 1-s käsitletakse täpsemalt CSIRT-ide loomisele ette nähtud nõudeid ja ühtse EL-i ülese CSIRT võrgustiku loomist. Lisaks CSIRT-ile tuleb art 8 järgi määrata ka üks või mitu riiklikku pädevat asutust, kes oleksid võrgu- ja infosüsteemide turvalisuse valdkonnas ühtseks kontaktpunktiks. Antud kontaktpunkt täidab sidepidamisfunktsiooni, et tagada asutuste piiriülene koostöö teiste liikmesriikidega, art 11 osutatud koostöörühma ja art 12 osutatud CSIRTide võrgustikuga. Artiklid ja lisad, mis käsitlevad oluliste teenuse operaatoreid analüüsitakse täpsemalt käesoleva uurimuse teises peatükis.[43]

NIS direktiivis on mainitud ka kohustus piiriüleseks konsultatsioonimenetluseks, mis mängib olulist rolli OTO ja DTO-dele võrdsete võimaluste loomisel kogu EL-is turva- ja teavitusnõuete osas, sest vastavalt direktiivi põhjendusele 44 on nendel teenuse osutajatel suurim vastutus nõuete täitmiseks.[44] 2021. aastal koostatud NIS direktiivi läbivaatamist toetav uuring selgitas, et põhimõtteliselt käsitletakse OTO-de kindlakstegemist riikliku küsimusena, kuigi liikmesriigid on kohustatud üksteisega nõu pidama piiriülese mõjuga OTO-de kindlakstegemisel. Siiski on vähesed liikmesriigid osalenud piiriüleses konsultatsioonis enne riigis tegutsevate OTO-de tuvastamise kriteeriumite määratlemist. 2018. aastaks oli vaid kaks liikmesriiki teiste liikmesriikidega ühendust võtnud. Vähesel määral on teised riigid kasutanud konsultatsiooni meetmeid struktureerimata viisil. Enamasti ei saa liikmesriigid konsultatsiooniprotsessi kahe liikmesriigiga korraga kooskõlastada.[45] Uuringus järeldatakse, et antud protsess viib selleni, et liikmesriigid võtavad olulise teenuse määratlemisel vastu väga erinevad lähenemised. Selle tulemuseks on ebaühtlane kübervastupidavus ja seega OTO-de loendi võrdlemine riigiti on keeruline.[46]

[42] Tuleb märkida, et kasutatakse sõna võrgu- ja infosüsteemid, mitte küberturvalisus. Riikide praktikast lähtuvalt on näha, et valdkonna laiemaks käsitluseks kasutatakse pigem küberturvalisuse mõistet, mida direktiivis ei ole lahti selgitatud.
[43] 6. juuli 2016. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2016/1148 mis täpsustab meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. — ELT L 194, 19.7.2016, lk 1-30.
[44] *Ibidem.*
[45] Euroopa Komisjon. Report From The Commission To The European Parliament And The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems. 2019.
[46] Euroopa Komisjon. 2021. *Op cit,* lk 14.

Uuringus mainitakse, et keskmiselt teatavad liikmesriigid 35 olulisest teenusest riigi kohta, kuigi liikmesriikide vahel on ka mitmeid erinevusi. Selliste erinevuste peamiseks põhjuseks on OTO-de tuvastamise kriteeriumite määratlemise protsess. Uuring toob näite, et olukorras, kus üks operaator on asutanud erinevates liikmesriikides filiaale, võivad riigid kohaldada operaatori suhtes erinevaid kriteeriume OTO-na tuvastamiseks. See omakorda põhjustab vastuolulist lähenemist järelevalvele ning täiendavat haldus- ja seadusandlikku koormust. Selle tulemusena võivad piiriülesed intsidendid, mis võivad kahjustada esmatähtsat infrastruktuuri, tekitada olulisel määral kahju. Näiteks energiasektorites tegutsevatel ettevõtetel või suurtel domeeniregistritel on piiriüleste teenuste osutajatena asjakohane osa siseturul ja neile oleks küberintsidendi korral märkimisväärne mõju.[47]

Võrreldes liikmesriikide algatatud meetmetega on võrgu- ja infoturbe direktiivi kõige ilmsem lisandväärtus ühtse õigusraamistiku loomine, et tagada võrgu- ja infoturbe kõrge tase kogu Liidus. Seetõttu pidi direktiiv tagama miinimumnõuete rakendamise kogu EL-is, mis põhinesid 2016. aastal kehtestatud siduvatel eeskirjadel. Iga liikmesriik pidi vastu võtma riikliku raamistiku ja kavandama riiklikud asutused, kes vastutaksid eelpool mainitud NIS direktiivi järelevalve ja rakendamise eest. On ebatõenäoline, et selline tulemus oleks saavutatud ainult riikliku poliitika või õigusaktidega.[48]

Tšehhi on olnud üks esimesi EL-i liikmesriike, kes on siseriiklikus õiguses vastu võtnud mitmeid komplekssseid küberturvalisust käsitlevaid õigusakte. Tšehhi küberturvalisuse seadus loodi juba enne NIS direktiivi vastuvõtmist ning mitmes aspektis kajastusid riigi õigusaktis reguleeritud administratiivsed ning institutsionaalsed meetmed ka hiljem direktiivis. Samas on peale 2016. aastat NIS direktiiv siseriiklikusse õigusesse üle võetud küberturvalisuse seaduse muudatusega.[49] Tšehhi on lisaks ühtsele küberturvalisuse seadusele loonud mitmeid toetavaid määruseid, mille abil antud valdkonda reguleeritakse. Mõned nendest on:

- 2011. aastal võeti vastu otsus luua CZ NSA riiklik asutus, mille vastutuseks sai küberturvalisuse valdkonna koordineerimine. Koos NSA-ga loodi ka riiklik küberturvalisuse keskus, mille ülesandeks oli uue õigusakti koostamine küberturvalisuse kohta.

[47] Euroopa Komisjon. 2021. *Op cit,* lk 14.
[48] Euroopa Komisjon. 2021. *Op cit,* lk 25.
[49] Polcák, R., *et al*. Cyber Law in the Czech Republic, third edition. 2020. Kättesaadav arvutivõrgus: https://books.google.ee/books/about/Cyber_Law_in_Czech_Republic.html?id=rubYDwAAQBAJ&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false (10.04.2020).

- 2014. aastal avaldati seaduste kogumikus küberturvalisuse seaduse nr 181/2014 rakendusmäärused:
    - määrus nr 316/2014 Coll. turvameetmete, küberturbeintsidentide ja reageerimismeetmete kohta.
    - määrus nr 317/2014 Coll. oluliste infosüsteemide kindlaksmääramise ja nende määramise kriteeriumide kohta.
    - valitsuse otsus nr 315/2014 Coll. millega muudetakse kriitilise infrastruktuuri elementide määramise kriteeriumeid.
- Alles 2015. aastal jõustus seadus nr 181/2014 Coll. küberturvalisuse kohta, mis jõustus koos rakendusmäärustega ja mida uuendati 2017. aastal.
- 2017. aastal võeti vastu määrus nr 437/2017 Coll. oluliste teenuste osutajate kriteeriumite määramise kohta. Samal aastal loodi ka Riiklik Küber - ja Informatsiooniturvalisuse Agentuur (NUKIB), millest sai põhiline riiklik üksus küberturvalisuse järelevalve teostamisel.
- 2018. aastal jõustus küberturvalisuse määrus nr 82/2018 Coll., mis võttis üle NIS direktiiviga seotud nõuded.[50]

On näha, et erinevate seaduste ja määrustega on tehtud palju selleks, et riigipoolselt reguleerida mitmeid küberturvalisuse aspekti. Tekib küsimus, kuidas on kõige efektiivsemalt võimalik nendes õigusaktides orienteeruda ning kas kõiki eraldiseisvaid määruseid on tarvis. Käesoleva töö raames saavad eelkõige oluliseks kolm erinevat õigusakti: 82/2018 Coll, 437/2017 Coll ja 181/2014 Coll., mille abil saab analüüsida riigis üle võetud EL-i küberturvalisuse õiguslikku raamistikku ja selle kohaldamist. Järgnevalt analüüsitakse, kuidas on Tšehhi küberturvalisuse määruste taustal NIS direktiiv üle võetud siseriiklikusse õigusesse.

Esimene oluline nõue on riikliku küberturvalisuse strateegia loomine. Tšehhi strateegia loodi enne NIS direktiivi vastuvõtmist aastatel 2015-2020 koos vastava rakendusplaaniga. Antud strateegias oli oluliste valdkondadena mainitud: asjakohaste struktuuride, protsesside ja koostöö tõhustamine küberturvalisuse tagamisel; kriitilise informatsiooni infrastruktuuri ja informatsiooni tehnoloogia turvalisuse kaitse; koostöö erasektoriga; tarbijate usalduse tõstmine; infoühiskonna arendamine; politsei suutlikkuse toetamine küberkuritegevuse menetlemisel; küberturvalisuse-alaste õigusaktide arendamine ehk õigusraamistiku väljatöötamine ja osalemine Euroopa ja rahvusvaheliste regulatsioonide loomises ja

[50] National Cyber and Information Security Agency (NÚKIB). Legislation. Kättesaadav arvutivõrgus: https://nukib.cz/en/cyber-security/regulation-and-audit/legislation/ (10.04.2022).

rakendamises. 2020. aasta lõpus kiitis Tšehhi valitsus heaks ka riikliku küberturvalisuse strateegia aastateks 2021–2025 koos rakendusplaaniga. Sellega suunatakse tähelepanu COVID-19 kriisist tulenevatele küberturvalisuse ohtudele ja kaasnevatele tagajärgedele. Uues strateegias käsitletakse ka toodete ja teenuste tarnijaid, kes on Venemaa ja Hiina häkkerite tegevuse tõttu sattunud küberohtu. Lisaks käsitletakse 5G võrku, IKT toodete sertifitseerimist ja sellega seotud küberturvalisuse väljakutseid.[51]

Teiseks nõudeks on CSIRT üksuste loomine. Tšehhis on sellised reageerimisüksuseid kaks: 1) valitsuse arvutihädaabimeeskond (GovCERT.ZE) ja 2) riiklik arvutiturbe intsidentidele reageerimise meeskond (CSIRT.CZ). GovCERT.ZE põhiülesanne on küberintsidentide aruannete kogumine määratud üksustelt, nende analüüsimine ja abi osutamine. CSIRT.CZ roll on teha koostööd ülemaailmse CERT/CSIRT-meeskondade kogukonnaga ning kogukonda toetavate organisatsioonidega – internetiteenuse pakkujad, sisupakkujad, pangad, turvaorganisatsioonid, akadeemilise valdkonna institutsioonid, riigiasutused ja muud institutsioonid. CSIRT.CZ pakub küberturvalisusega seotud teenuseid ka antud organisatsioonidele. Riiklik küber- ja infoturbeagentuur on osa Tšehhi riiklikust strateegiast. Konkreetne laiendamine on kavas ellu viia aastatel 2018-2023 eesmärgiga rajada uus labor, koolituskeskus ja andmekaitsekeskused ning suurendada büroo tööjõudu.[52]

Tšehhi jaoks on erinevad EL-i õigusaktid olnud tugevaks muutuste loojaks riigi küberturvalisuse õiguslikus valdkonnas. Seda on mõjutanud näiteks GDPR ülevõtmine ja NIS direktiiv. Sellegipoolest on kriitikat saanud Tšehhi riikliku CSIRT pädevused ja suutlikkus ning võimekus töödelda juhtumipõhist andmestikku, mis on seotud küberturvalisusega. Seetõttu on oodata, et lähitulevikus vaadatakse üle selle ameti tegevused ning tegeletakse küberintsidentides efektiivsema andmetöötlusega.[53]

Eesti puhul on põhiliseks lähtekohaks küberturvalisuse seadus (KüTS), milles on kokku koondatud kõik vajalikud nõuded, definitsioonid ning juhised võrgu- ja infosüsteemide

[51] National Cyber and Information Security Agency. National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020. 16.02.2015. Kättesaadav arvutivõrgus: https://www.nukib.cz/en/cyber-security/strategy-action-plan/ (7.02.2022);
National Cyber and Information Security Agency. National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025. 18.03.2021. Kättesaadav arvutivõrgus: https://www.nukib.cz/en/cyber-security/strategy-action-plan/ (7.02.2022).
[52] Euroopa Komisjon. Implementation of the NIS Directive in the Czech Republic. 2022. Kättesaadav arvutivõrgus: https://digital-strategy.ec.europa.eu/en/policies/nis-directive-czech-republic (10.04.2022); *Ibidem.*
[53] Polcák, R., *et al*. *Op cit*.

pidamiseks ning küberintsidentide lahendamiseks. KüTS-iga on terviklikult üle võetud NIS direktiiv ning isegi laiemalt, kui seda on nõutud. Eestis on sarnaselt Tšehhiga võetud vastu mitmeid varasemaid meetmeid küberturvalisuse valdkonna kaitsmiseks. Näiteks 2010. aastal anti Riigi Infosüsteemide Arenduskeskusele, uue nimega Riigi Infosüsteemi Amet (edaspidi RIA), volitused riigi IKT infrastruktuuri kaitse korraldamiseks ja infosüsteemide turvalisuse järelevalveks.[54] Enne NIS direktiivi kohaldumist oli Eestis vastu võetud küberjulgeoleku strateegia 2014-2017. Strateegia nimest lähtuvalt eksisteeris mõistete ühtlustamise vajadus, sest küberjulgeolek ja -turvalisus ei ole omavahel korrelatsioonis. Samas oli hilisemas küberturvalisuse strateegia dokumendis aastateks 2019-2022 jätkatud ühtsema küberturvalisuse mõiste kasutamisega, mis on kooskõlas vastuvõetud siseriikliku õigusaktiga.

Eesti küberturvalisuse strateegia 2019–2022 toob välja neli olulisemat eesmärki:

1. Jätkusuutlik digitaalne ühiskond, mis tagab tehnoloogilise vastupanuvõime ja valmisoleku kriiside ohjeldamiseks.
2. Innovaatiline, teaduspõhine ja globaalselt konkurentsivõimeline küberturbe sektori ettevõtlus ning teadus- ja arendustegevus.
3. Koostöö rahvusvaheliste partneritega.
4. Küberteadlik ühiskond ning küberturvalisuse valdkonna spetsialistide järelkasv.[55]

RIA, kui peamine küberintsidentidega tegelev riiklik ametiasutus ja kellest sai NIS direktiivi art 9 järgi CSIRT, teostab KüTS-i alusel nende intsidentide ennetamiseks üldist seiret ning analüüsib süsteemide turvalisust ohustavaid riske ja nende mõju. Samuti edastab küberintsidentide ennetamiseks ja lahendamiseks ohuteateid vastavalt KüTS § 12 ja § 13 alusel. KüTS § 5 järgi on RIA ühtne kontaktpunkt Eesti jaoks ning edastab vajaduse korral informatsiooni EL-i pädevatele asutustele. Lisaks on RIA riikliku ja haldusjärelevalve teostaja KüTS ja selle alusel kehtestatud õigusaktide osas.[56]

18. septembril 2018. aastal võeti vastu Iirimaa seadusandlik määrus nr 360, millega võeti üle NIS direktiiv siseriiklikusse õigusesse. Iirimaa riikliku küberturvalisuse keskuse sõnul oli tegemist olulise muudatusega, kuidas EL-i riigid küberturvalisusele lähenevad ja see hõlmab ametlikumat tüüpi regulatiivsete suheteid teatud võtmevaldkondades. Iirimaa tõi avalikus

[54] Majandus- ja Kommunikatsiooniministeerium. Küberjulgeoleku strateegia 2014-2017. Kättesaadav arvutivõrgus: https://www.mkm.ee/et/eesmargid-tegevused/kuberturvalisus (7.02.2022).
[55] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022. Kättesaadav arvutivõrgus: https://www.mkm.ee/et/eesmargid-tegevused/kuberturvalisus (7.02.2022).
[56] Küberturvalisuse seadus[1] – RT I, 22.05.2018, 1.

kommunikatsioonis välja ka selle, et NIS direktiivi ülevõtmine hakkab otseselt mõjutama mitmeid Iirimaa ettevõtteid ja kommunaalteenuseid. Riik määras hulganisti sellised ettevõtteid ja kommunaalettevõtteid oluliste teenuste operaatoriteks ning nende suhtes kehtivad NIS direktiivist üle võetud turvakohustused ja intsidentidest teatamise nõuded.[57]

Iirimaal on olnud kaks riikliku strateegiat küberturvalisuse valdkonna käsitlemiseks, 2015-2019 ning alates 2019. aastast kehtiv strateegia. Iirimaa esimeses riiklikus küberturvalisuse strateegias sätestati põhiliseks eesmärgiks küberturvalisuse keskuse arendamine (NCSC) ja rida meetmeid valitsuse andmete ja võrkude paremaks kaitsmiseks ning kriitilise tähtsusega riiklik infrastruktuur. Kehtivas strateegias kinnitatakse veelkord, et Iirimaa on üks EL-i suurimaid digitaalsete tehnoloogiate kasutusmääraga riike ning tehnoloogia mängib olulist rolli majandusliku ja sotsiaalse elu toimimises. Samas rõhutatakse, et sellise sõltuvuse tagajärjel on ilmsiks tulnud mitmeid keerulisi ohte, mis võivad kaasa tuua ka teenuste katkemise. Seega näeb uus strateegia ette mitmeid arengusuundi alates NCSC pädevuste ja võimekuste arendamisest, ühiskonna teadlikkuse tõstmisest kuni andmete haldamise ettevõtetele turvalisuse tegutsemiskeskkonna tagamiseni välja.[58] Strateegia on saanud ka teatud kriitikat, sest ei jaga piisavas mahus NCSC või riiklike asutuste võimekusi varasemate ohtudega toimetulemisel. Puudu on ka laiem käsitlus erasektori olulisusest ja nendega plaanitavast koostööst.[59]

Iirimaa puhul on kontaktpunktide ning CSIRT süsteemi vastutus mitme asutuse vahel laiali jaotatud, et vastava valdkonna pädevuses oleks konkreetsest oluliste teenuste üksustest tulenevad teenusepakkujad. Kuigi ühiseks kontaktpunktist on Iirimaa CSIRT, mis töötab NCSC all, on näiteks oluliste teenuste osutajate puhul vastutavaks ka keskpank. NCSC omakorda allub kommunikatsiooni, kliima ja keskkonna ministeeriumile. Kontaktpunktide ja CSIRT õigused on loetletud Iirimaa määruse nr 360 teises osas.[60]

[57] National Cyber Security Centre. Network and Information Security Directive. Kättesaadav arvutivõrgus: https://www.ncsc.gov.ie/nis/ (10.04.2022).
[58] Government of Ireland. National Cyber Security Strategy 2019-2024. Kättesaadav arvutivõrgus: https://www.ncsc.gov.ie/strategy/ (7.02.2022).
[59] BHConsulting. Analysis of the Irish National Cyber Security Strategy. 2020. Kättesaadav arvutivõrgus: https://bhconsulting.ie/analysis-of-the-irish-national-cyber-security-strategy/ (10.04.2022).
[60] Euroopa Komisjon. Implementation of the NIS Directive in Ireland. 2022. Kättesaadav arvutivõrgus: https://digital-strategy.ec.europa.eu/en/policies/nis-directive-ireland (10.04.2022); European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018– S.I. No. 360/2018.

NIS direktiivi ülevõtmisest tulenevate kohustuste täitmine ei ole tekitanud valimiriikides suuri probleeme. Seda ilmestab eelpool mainitud nõuete ajakohane täitmine koos vastavate strateegiate loomisega. Kuigi teatud erisusi võib leida näiteks pädevate asutuste määramisel, tuleb siin arvesse võtta eelkõige riigi enda finantsressursse ja võimekust mitmete asutuste vahel tööd koordineerida.

Lisaks NIS direktiivile on EL püüdnud reguleerida ka teisi küberturvalisuse valdkonda mõjutavaid aspekte. Näiteks 2004. aastal loodud ENISA on kuni direktiivi vastuvõtmiseni liikmesriikide puhul väheolulisuse mõjuga. Attströmi, Ludden ja Lessmann'i sõnul oli ENISA hääl ajakirjanduses, meedias ja avalikkuses nõrk ning seda ei võetud piisavalt kuulda. Ametil olid piiratud enesekehtestamisvõime ja puudulik pikaajaline visioon, sest see oli sõltuvuses tähtajalisest mandaadist. Olukorra tegid keeruliseks ka liikmesriikide erinevad soovid ja prioriteedid. Samal ajal oli ametil mitmeid struktuurilisi nõrkusi, mis mõjutasid nende töö tõhusust EL-i küberturvalisuse maastikul. Puudu oli piisavatest inim- ja rahalistest ressurssidest, et viia ellu soovitud tegevusi. Veel enam, kui väljaõppe ja oskuste tase ei ole piisavalt kõrge, ei ole võimalik täita tõhusalt kõiki määratud ülesandeid. Seega oli ENISA roll küberturvalisuses piiratud ja oma olemuselt üksnes toetav.[61]

Võrgu- ja infoturbe direktiivi rakendamisel ilmnes aga asjakohane oht, et järjepidevus on piiratud ja kõigi sidusrühmade jaoks tarbetult keerukas. Euroopa riikide erinevuste vähendamiseks anti ENISA-le uus alaline mandaat, see saaks täita uusi ülesandeid. Antud muudatus fikseeriti 2019. aasta juunis jõustunud EL-i küberturvalisuse seadusega. Riikide esindajatest, ENISA-st ja Euroopa Komisjonist koosnev koostöörühm andis strateegilised juhised ja oli aktiivseks partneriks CSIRT-ide võrgustikule, et tagada heade tavade edastamine ja vahetamine ning toetada liikmesriike direktiiviga seotud küsimustes.[62]

Eelnevalt oli ENISA mandaati pikendatud juba kahe määrusega, kuid selline limiteeritud tegevusperiood vähendas ameti võimalusi tegevuste pikaajaliseks planeerimiseks ning mõjus negatiivselt ENISA teenuste osutamisele. Lisaks leidus ENISA struktuuris vastuolusid ka NIS direktiiviga. Näiteks NIS direktiivi art 7 lg 2 annab liikmesriikidele võimaluse paluda ENISA abi riiklike võrgu ja infosüsteemide strateegiate loomisel, kuid ENISA pädevus selles osas oli piiratud. 2019. aasta küberturvalisuse määrus tegi lõpu ameti ajutisele iseloomule. Lisaks sellele, et enam ei vaja amet oma tegevuse kinnitamiseks mandaadi pikendamist, anti ENISA-

[61] Giantas, H. D. Liaropoulus, N. A. *Op cit*, lk 17-18.
[62] Euroopa Komisjon. 2021. *Op cit,* lk 10.

le ka mitmeid uusi õiguseid ning kohustusi, mis on seatud näiteks sertifitseerimise ja meetmete normaliseerimisega.[63]

2019. aastal võeti vastu EL-i küberturvalisuse määrus, mis viitab sellele, et kodanike küberturvalisuse-alase teadlikkuse tõstmiseks on vaja teha täiendavaid jõupingutusi. Määruses käsitletakse selle eesmärgi saavutamiseks järgnevaid teemasid:

- Liikmesriikides küberhügieeni edendamine, et teadlikkust tõsta.
- ENISA toetus liikmesriike küberturvalisuse alase teadlikkuse tõstmisel.
- ENISA peab aitama kaasa parimate tavade ja lahenduste edendamisele, sealhulgas küberhügieeni ja digioskuste valdkonnas kodanike, organisatsioonide ja ettevõtete tasandil.
- Avalike teabekampaaniate käigus tuleks levitada teadmisi selliste ohtude kohta nagu andmepüügirünnakud, robotvõrgud, finants- ja pangapettused ning andmepettuste juhtumid. Lisaks tuleks edendada turvameetodeid, sealhulgas mitmetasandilist autentimist, krüptimist, anonüümseks muutmist ja andmekaitset.[64]

Küberturvalisuse määrusega loodi ka raamistik, et tulevikus saaks tekkida ENISA juhtimise juurde Euroopa-ülene küberturvalisuse sertifitseerimise protsess ning juhis. Selle eesmärk oleks tagada adekvaatne küberturvalisuse tase IKT toodetele ja teenustele ning ennetada siseturu fragmenteeritust küberturvalisuse sertifitseerimise protsessi loomisel. Vastavalt EL küberturvalisuse määruse art 69-le on käesolev õigusakt vahetult kohaldatav kõikides EL liikmesriikides.[65]

Viimaseks oluliseks EL õigusaktiks antud peatüki raames on elektroonilise side seadustik (EECC), mille alusel uuritakse, kuidas on tagatud küberturvalisuse tingimuste täitmine elektroonilise kommunikatsiooni valdkonnas. COVID-19 negatiivne mõju oli lisaks tervishoiule ka elektroonilise kommunikatsiooni valdkonnas. Samas ei loetle NIS direktiiv oluliste teenuste operaatoritena näiteks kaabelleviteenuseid või elektroonilisi sideteenusepakkujaid. Ainuke viide oli art 4(1)(a), kus võrgu ja infosüsteemi alla kuulub ka

[63], 17. aprilli 2019. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) PE/86/2018/REV/1. ELT L 151, 7.6.2019, lk 15—69.

[64]*Ibidem.*

[65] Chałubińska-Jentkiewicz, K., *et al*. Cybersecurity in Poland: Legal Aspects. Springer. 2022, lk 91. Kättesaadav arvutivõrgus: https://doi-org.ezproxy.utlib.ut.ee/10.1007/978-3-030-78551-2 (10.04.2022).

elektrooniline sidevõrk. Sellega seoti osaliselt omavahel NIS direktiiv ja 2002/21/EÜ direktiiv. Saab nõustuda, et liikmesriikidele on tagatud teataval määral valikuvabadus ja pädevus ise otsustada, kas laiendada OTO-de loetelu, kuid sellegipoolest on üllatav, et NIS direktiivil puudub otsene viide elektroonilist kommunikatsiooni reguleerivatele õigusaktidele. Järgnevalt vaadeldakse, kuidas defineerib Euroopa Liit elektroonilise kommunikatsiooni teenusepakkujaid uuenenud EECC valguses ning mis küberturvalisuse juhiseid kehtestab Liit selles valdkonnas.

Telekommunikatsiooni tööstus seisab silmitsi märkimisväärselt muutunud õigusmaastikuga, sest 2020. aasta lõpuks tuli siseriiklikku õigusesse üle võtta uus elektroonilise side seadustik ehk direktiiv (EL) 2018/1972. Uus EECC lähtub võrreldes varasemate õigusaktidega funktsionaalsel lähenemisviisil ega põhine üksnes tehnilistel parameetritel, et defineerida elektroonilist kommunikatsiooni. See on suunatud pigem lõppkasutaja vaatenurgale.[66] EECC art 2(4) järgi on elektrooniline sideteenus määratletud kui teenus, mida tavaliselt osutatakse tasu eest elektrooniliste sidevõrkude kaudu ja mis hõlmab – välja arvatud teenused, mis pakuvad või teostavad toimetuskontrolli elektrooniliste sidevõrkude ja -teenuste kaudu edastatava sisu üle – järgmiste teenuste liike:

- internetiühenduse teenus määruse (EL) 2015/2120 art 2(2)(2) määratletud tähenduses;
- inimestevahelise suhtluse teenus;
- teenused, mis koosnevad täielikult või peamiselt signaalide edastamisest, nagu edastusteenused, mida kasutatakse masinatevaheliste teenuste osutamiseks ja ringhäälinguks.[67]

Sellest tulenevalt hõlmab elektrooniliste sideteenuste mõiste EECC-s ka muid sidet võimaldavaid teenuseid, mis koosnevad täielikult või peamiselt signaalide edastamisest.[68]

EECC raames võib erinevalt NIS direktiivist või küberturvalisuse määrusest leida mitmeid viiteid eelnevalt mainitud küberturvalisuse õigusaktidele. Näiteks EECC põhjendus 98 järgi

[66] EECC põhjenduses 15 rõhutatakse, et kuigi signaalide edastamine jääb oluliseks parameetriks direktiivi reguleerimisalasse kuuluvate teenuste kindlaksmääramisel, peaks määratlus hõlmama ka muid sidet võimaldavaid teenuseid, kuna lõppkasutaja seisukohast ei ole vahet, kas teenusepakkuja edastab signaale ise või side edastatakse Interneti-juurdepääsuteenuse kaudu.

[67] 11. detsembri 2018. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik. PE/52/2018/REV/1. ELT L 321, 17.12.2018, lk 36—214.

[68] Sein, K. Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector. Journal of Intellectual Property, Information Technology and E-Commerce Law. 2021, lk 172. Kättesaadav arvutivõrgus: https://www.jipitec.eu/issues/jipitec-12-2-2021/5298 (10.04.2022).

peavad pädevad asutused tagama üldkasutatavate elektroonilise sidevõrkude tervikluse ja käideldavuse säilimise. Leiab mainimist, et ka Euroopa Liidu Võrgu- ja Infoturbeamet peaks EECC järgi toetama elektroonilise side turvalisuse suurendamist, pakkudes muu hulgas oskusteavet ja nõu ning edendades parimate tavade vahetamist. Veel enam leiab EECC, et Euroopa Parlamendi ja nõukogu direktiiviga 2016/1148 loodud küberturbe intsidentide lahendamise üksused ehk CSIRT-id peaksid vajaduse korral abistama elektroonilise sideteenuste pakkujaid. Eeskätt võidakse nõuda, et CSIRT-id esitaksid pädevatele asutustele näiteks teavet, kuidas üldkasutatavate elektrooniliste sidevõrkude ja sideteenuseid mõjutavate riskide ja turvaintsidentidega toime tulla.[69]

EECC loetleb eraldi V jaotise turvalisuse peatükis ja art 40 abil nõuded, mis tuleb tagada, et maandatud oleks võrkude ja teenuste turvalisusega seotud riskid. Eriti ilmekas on EECC art 40 lg 1 esimene lause: "Liikmesriigid tagavad, et üldkasutatavate elektroonilise side võrkude ja üldkasutatavate elektroonilise side teenuste pakkujad võtavad asjakohased ja proportsionaalsed tehnilised ja organisatsioonilised meetmed". NIS direktiivi art 14 lg 1 esimene lause on aga järgnev: "Liikmesriigid tagavad, et oluliste teenuste operaatorid võtavad asjakohased ja proportsionaalsed tehnilised ja korralduslikud meetmed, et hallata riske, mis ohustavad nende töös kasutatavate võrgu- ja infosüsteemide turvalisust.". Kui vaadata terviklikult EECC art 40 võrdluses NIS direktiivi art 14 on märgata mitmeid sarnasusi. EECC on proovinud veidi laiemalt käsitleda turvaintsidendi mõju kindlakstegemise parameetreid, lisades juurde punktid: d) kui suures ulatuses on võrgu või teenuse toimimine mõjutatud ja e) majanduslikule ja ühiskondlikule tegevusele avalduva mõju ulatus.[70]

EECC art 41 (4) jõustab NIS direktiivi art 9 abil põhjendust 98, mille alusel peavad liikmesriigid tagama, et art 40 rakendamiseks ehk võrkude ja teenuste turvalisuse sätete täitmiseks on asutustel õigus CSIRT-idelt abi saada. Seda juhul, kui tegemist on küsimustega, mis kuuluvad CSIRTi ülesannete hulka vastavalt direktiivi (EL) 2016/1148 I lisa punktile 2. Kuigi mõni üksik viide NIS direktiivile on EECC-sse siiski lisatud, on kahe õigusakti otsene seos olematu. EECC kirjeldab rangemaid meetmeid küberturvalisuse tagamiseks ja NIS direktiivis ei kajastu otsene viide elektroonilise kommunikatsiooni teenuste osutajatele. Tegemist on laialivalguga ning

[69] 11. detsembri 2018. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik. PE/52/2018/REV/1. ELT L 321, 17.12.2018, lk 36—214.

[70] *Ibidem;* 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.

kohati segase õigusloomega, mis võib nii riikide kui ka teenuse osutajatele avaldada suuremat halduskoormust.[71]

Eelneva analüüsi toel saab kinnitust asjaolu, et EL-i küberturvalisust reguleerivate õigusaktidega moodustub Euroopa küberturvalisuse poliitika valdkonnas killustatud õigusraamistik ja see valdkond peab EL-i digitaalset sõltuvust arvestades jõuliselt edasi arenema. Wesseli soovituse kohaselt on küberturvalisus siiski suurepärane näide valdkonnast, kus tuleb ühendada erinevad poliitikavaldkonnad horisontaalse järjepidevuse nõude alusel ja kus tuleb võtta meetmeid nii EL-i kui ka liikmesriikide tasandil, mis omakorda nõuab vertikaalset järjepidevust.[72]

1.4. Küberturvalisuse mõiste ulatus ja probleemid

Küberturvalisus ehk *cybersecurity* kui eraldiseisev termin on Euroopa Liidu õiguslikus raamistikus lõpuni defineerimata ning seega võib mitmetes EL-i ja liikmesriikide õigusaktides otsetõlkena kohata segamini nii küberturvalisuse kui ka -julgeoleku sõnu. EL-i esimese strateegia ametlikus eestikeelses tõlkes on tegemist Euroopa Liidu küberjulgeoleku strateegiaga, kuigi ingliskeelne nimetus on siiski *cybersecurity*. Mõiste sisu avatakse strateegias järgnevalt: „Küberjulgeolek viitab tavaliselt kaitse- ja muudele meetmetele, mida saab nii tsiviil- kui ka sõjalises valdkonnas kasutada küberruumi kaitsmiseks ohtude eest, mis seonduvad selle üksteisest sõltuvate võrkudega ja infotaristuga või võivad neid kahjustada. Küberjulgeoleku eesmärk on tagada võrkude ja taristu käideldavus ja terviklus ning neis sisalduva teabe konfidentsiaalsus.“[73] Antud selgitusest nähtub, et põhirõhk küberjulgeoleku puhul on pandud kaitsmisvõime tagamisele. Selline kirjeldus on piisavalt lai, et ei anna konkreetseid järeldusi küberjulgeoleku ja küberturvalisuse eristamisel.

Strateegiaga kaasnenud 2016. aasta NIS direktiivis on samuti defineerimata mõiste küberturvalisus. Seda mainitakse dokumendis vaid ühel korral põhjenduses 34, kuid direktiivi ametlikus eestikeelses tõlkes kasutatakse sõna küberturve. Läbivalt kasutatakse mõistet võrgu-

[71] 11. detsembri 2018. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik. PE/52/2018/REV/1. ELT L 321, 17.12.2018, lk 36—214.
[72] Christen, M. *et al*. *Op cit*, lk 98.
[73] Euroopa Komisjon. 2013. *Op cit*, lk 3.

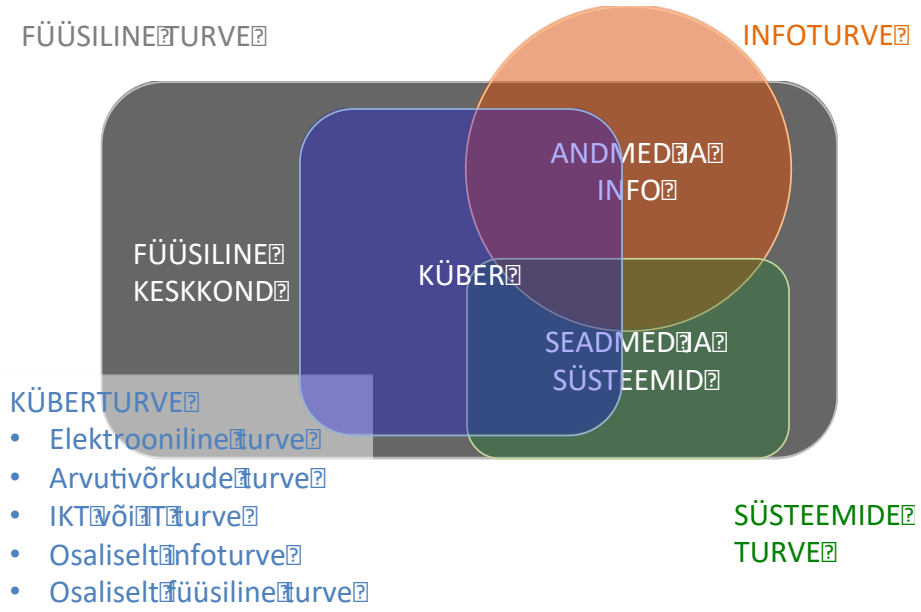
ja infosüsteemide turvalisus, mis on ka antud õigusakti art 4 (2) lahti selgitatud.[74] 2019. aasta EL-i määruses, mis käsitles ENISA-t ning IKT sertifitseerimist laiendatakse esimest korda küberturvalisuse mõistet EL-i õiguslikus raamistikus. Eestikeelses versioonis selgitatakse küberturvalisust kui tegevusi, mis on vajalikud kaitsmaks NIS direktiivis defineeritud võrgu- ja infosüsteeme, nende kasutajaid ja kolmandaid isikuid küberohtude eest.[75] 2013. aasta strateegias ja küberturvalisuse määruses on ühine osa küberturvalisuse piiritlemisel meetmetena, mille abil saab erinevaid süsteeme kaitsta. Samas NIS direktiivis määratletakse seda kui vastupanuvõime saavutamist. Järelikult ei ole EL-i tasandil järjepidavust antud mõiste defineerimisel.

Liikmesriikidel ei ole küberturvalisuse defineerimine kõige paremini õnnestunud. Eesti õiguskorda saab ühe positiivse näitena tuua. Kuigi algse terminina domineeris kahes esimeses küberturvalisust käsitlevas strateegias läbivalt küberjulgeolek, siis probleem mõistete defineerimisel ilmnes alles KüTS loomisel.[76] Probleemi lahendamisel oli seaduse loojatele lähtekohaks 2014-2017. aasta küberjulgeoleku strateegia lisa 2, kus tehakse Eesti õiguskorra jaoks selge ning põhjalik ülevaade mõistetest, mida oleks sobilik kasutada. Esimene oluline küsimus oli Majandus- ja Kommunikatsiooniministeeriumi (MKM) töögrupil selle kohta, kuidas defineerida eesliide „küber“. Teiseks väljakutseks olid põhihulgad, mis eesliitele järgnevad nagu näiteks rünne, oht, turvalisus jne. Need jäeti aga üheselt defineerimata, et anda võimalus uusi termineid kübervaldkonda juurde tuua. Veel enam rõhutas töögrupp, et ka nende põhihulkade tähendus võib valdkonniti erineda.

[74] 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.

[75] 17. aprilli 2019. aasta Euroopa Parlamendi ja nõukogu määrus 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus). – ELT L 151, 7.6.2019, lk 15-69.

[76] Kask, L. Küberturvalisuse seadusest. – Õiguskeel. 3/2018, lk 2. Kättesaadav arvutivõrgus: https://www.just.ee/oigusloome-arendamine/oiguskeel/ajakiri-oiguskeel#item-4 (7.02.2022).



Tabel 1. Eesti 2014–2017 Küberjulgeoleku strateegia lisa 2 valdkondlikus metoodikas sisalduv kübervaldkonna seosed infotöötluse vahenditega.

Eesti küberjulgeoleku strateegia lisas kaks välja toodud Tabel 1 näitab, kui ulatuslikust on seotud küber eesliide erinevate turvalisuse valdkondadega. Samuti seda, kuidas selle mõiste tähendus võib valdkondades muutuda. Töögrupi järeldus oli see, et eelkõige on eesliide küber sisalduv nii riistvara, tarkvara kui ka nendega seotud taristute valdkonnas. Töögrupp defineeris eesliite küber kui termini, „mis on seotud omavahel suhtlevate või suhtlemisvõimeliste infotöötlusvahenditega“.[77] 2019. aastal, kui vastu võeti uus Eesti küberturvalisuse strateegia, jälgiti sama loogikat eesliite ja põhihulkade selgitamisel, kusjuures eesliide küber on defineeritud kui võrgu- ja infosüsteemid. Selline definitsioon on täpsem kehtiva KüTS taustal.[78]

Selleks, et teha vahet küberturvalisusel- ja julgeolekul, tuleb esmalt aru saada, kuidas on eesti keeles kehtivates dokumentides eelpool nimetatud mõisteid kirjeldatud. MKM uue strateegia dokumendis on küberjulgeolek defineeritud kui seisund, kus riigi julgeolek on kaitstud süsteemides tekkivate ohtude eest. Küberturvalisuse all mõistetakse aga seisundit, kus süsteemid on kaitstud ohtude realiseerumise eest. Küberturbe puhul on tegemist sellesama turvalisuse tagamisega ehk tegevusega, kus rakendatakse meetmeid küberturvalisuse tagamiseks. Kuigi inglise keeles on küberturvalisuse ja -julgeoleku kirjapilt sama, on nendel mõistetel MKM sõnul konkreetne valdkondlik erinevus. Küberjulgeolek kehtib enamasti riiklikult oluliste kübervahendite terviklikkuse tagamisel, kuid küberturvalisus hõlmab laiemalt

[77] Majandus- ja Kommunikatsiooniministeerium. Küberjulgeoleku strateegia 2014-2017. Lisa 2 valdkondlik metoodika. *Op cit*, lk 4.
[78] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022. *Op cit*, lk 40.

erinevate kübervahendite turvalisust. Laura Kask kui üks KüTS loojatest on kirjeldanud, et NIS direktiivi ülevõtmiseks kaaluti seaduse pealkirjaks ka võrgu- ja infosüsteemide seadust, kuid see oli küberturvalisuse mõiste määratlusega kitsam definitsioon käsitledes pigem riist- ja tarkvara.[79] Järeldus on, et küberturvalisuse mõistet on kasulikum õiguskirjanduses kasutada selle laia määratluse tõttu, kohandades seda vastavalt teemale.[80]

Teine, kuid negatiivsem näide mõistete selgusetusest tuleb Poola näitel. 2018. aastal, kui Poola võttis siseriiklikusse õigusesse üle NIS direktiivi, jälgiti küberturvalisuse (*cybersecurity*) mõiste direktiivis antud võrgu- ja infosüsteemide turvalisuse definitsiooni. 2019. aastal, kui tuli välja otsekohalduv EL-i küberturvalisuse määrus, tekkis Poola definitsiooni ja EL määruse vahel vastuolu. Üks kirjeldas seisundit ning teine tegevusi. Poola muutis seejärel riiklikku küberturvalisuse seadust koos definitsiooniga, kus küberturvalisus tähistab meetmeid, mida on vajalik vastu võtta, et kaitsta infosüsteeme, nende kasutajaid ja kolmandaid isikuid küberohtude eest. Selline definitsioon järgib EL küberturvalisuse määruse selgitust. Seadusesse lisati juurde ka NIS direktiivist tulenev võrgu- ja infosüsteemide turvalisuse mõiste. Poola puhul ilmnes ka näiteid probleemidest EL-i ametlikes tõlgetes sarnaselt eestikeelsetele dokumentidele, kus julgeolek ja turvalisus on inglise keeles sama, kuid konkreetse riigi puhul erineva tähendusega.[81]

Probleem EL-i tasandil üheselt mõistetava küberturvalisuse definitsiooni loomisel on jätkuvalt relevantne. ENISA 2016. aastal tehtud uuringu alusel järeldati, et küberturvalisuse mõiste probleemiks on see, et ei ole võimalik luua mõistet, mis kataks kogu valdkonna raamistikku.[82] Kuigi iga riigi siseriikliku õiguse tõlgendamiseks tuleb esmalt vaadelda õigusakte ning toetavas materjalis välja toodud definitsioone, ei ole antud olukord EL-i õiguses kõige efektiivsem, kui igal riigil on erinev lähenemine. Seega kasvab üha enam vajadus EL-i õiguses luua katustermin küberturvalisuse selgitamiseks. Käesoleva töö raames tehtud analüüsi põhjal jääb küberturvalisus siiski põhiliseks terminiks kogu uurimuse ulatuses. Selle sisu saab olema eesti keelele sobivam, käsitledes seda kui seisundit, kus küberohtudest tulenevad riskid ei realiseeru.

[79] Kask. L. *Op cit.*
[80] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022. *Op cit*, lk 40.
[81] Szpor, G. The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland. Review of European and Comparative Law. 2021, lk 223-225. Kättesaadav arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?handle=hein.journals/recol46&id=219&collection=journals&index = (10.04.2022).
[82] Tallinna Ülikool, E-riigi Akadeemia SA. Riikliku küberturvalisuse indeksi metoodika analüüs. 2020, lk 8. Kättesaadav arvutivõrgus: https://ega.ee/wp-content/uploads/2020/05/NCSI_metoodika_audit_PDF.pdf (10.04.2022).

Küberturve aga meetmed, mida on vajalik kasutada selle seisundi saavutamiseks. Selline käsitlus on kooskõlas Eesti senise tegevusega küberturvalisuse valdkonna reguleerimisel ja sarnane NIS direktiivi võrgu- ja infosüsteemide turvalisuse selgitusele. Soovitus on edasiseks EL valdkonna ühtlustamiseks vaadata üle küberturvalisuse määruses selgitatud mõisted ning neid vajadusel viia vastavusse liikmesriikide praktikaga.

2. Riiklikult olulised teenused

2.1. Riiklikult oluliste teenuste olemus liikmesriikide näitel

Euroopa Liidu küberturvalisuse üheks olulisemaks eesmärgiks on aidata ennetada ja kaitsta liikmesriikide kriitilist infrastruktuuri ning olulise tähtsusega teenuseid. Selle ilmestamiseks on NIS direktiivis eraldi keskendutud nii oluliste teenuste operaatorite defineerimisele kui ka sätetele, mis räägivad operaatoritele kehtivatest tingimustest turvastandardite täitmisel.

Kuigi NIS direktiiv annab artikkel 5(2) alusel kriteeriumid oluliste teenuste operaatorite defineerimiseks, jääb lõplik loetelu koostamine siiski liikmesriikide enda pädevusse.[83] Lisaks kriteeriumitele on Euroopa Liit ka direktiivi lisas II välja toonud avaliku või erasektori üksused, millest saavad liikmesriigid lähtuda oluliste teenuste operaatorite loetelu koostamisel. NIS direktiivis defineeritakse olulise teenuse operaator art 4(4) kui direktiivi II lisas osutatud avaliku või erasektori üksusena, mis vastab art 5(2) sätestatud kriteeriumitele. Art 5(2) omakorda sätestab olulise teenuse operaatori defineerimiseks järgnevad kriteeriumid:

1) osutatakse teenust, mis on oluline elutähtsa ühiskondliku ja/või majandustegevuse säilitamisel;
2) teenuse osutamine sõltub võrgu- ja infosüsteemidest
3) intsidendil oleks oluliselt häiriv mõju nimetatud teenuse osutamisele.[84]

Siinkohal on oluline defineerida ning täpsustada teisi NIS direktiivi sätteid sh liikmesriikide siseriiklikusse õigusesse üle võetud mõiste “oluline häiriv mõju”. NIS direktiiv sätestab art 5(2)(c), et oluliste teenuste operaatori identifitseerimise üks kriteeriume on see, et küberturbeintsidendil oleks oluliselt häiriv mõju nimetatud teenuse osutamisele (st olulisele teenusele). Täpsemalt seda mõistet ei defineerita, kuid art 6 abil tuuakse välja tegurid, mille alusel seda kindlaks saab teha:

1) konkreetse üksuse poolt osutatavatest teenustest sõltuvate kasutajate arv;

[83] NIS direktiivis täpsustatakse ka digitaalsete teenuste osutajate (DTO) defineerimist ja neile kohalduvaid nõudeid. Kuivõrd elektrooniline kommunikatsioon ei lange DTO mõiste alla vastavalt direktiivi art 4(5), jääb antud tööst välja põhjalik analüüs digitaalsete teenuste osutajatele kehtivatest nõuetest.

[84] 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.

2) muude NIS direktiivi II lisas osutatud sektorite sõltumine üksuse poolt pakutavast teenusest;
3) intsidentide võimalik mõju majandus- ja ühiskondlikule tegevusele või avalikule julgeolekule;
4) üksuse turuosa;
5) intsidendist mõjutatud geograafilise ala võimalik ulatus;
6) üksuse tähtsus teenuse piisava kvaliteedi säilitamisel, võttes arvesse alternatiivide olemasolu kõnealuse teenuse osutamiseks.[85]

Käesoleva magistritöö eesmärgiks on analüüsida teenuseid ja sellega seonduvaid infrastruktuure, mida COVID-19 on enim mõjutanud. Võttes arvesse pandeemia olemust, jäävad enim haavatavateks valdkondadeks tervishoid ja elektrooniline kommunikatsioon. Näiteks raporteeris WHO 2021. aastal, et ligikaudu 90% riikidest teavitasid jätkuvatest häiretest olulistele tervishoiuteenustele.[86] On võimatu väita, et selle kriisi üks olulisemast pidepunktidest ei olnud tervishoiuteenustele pandud surve. Seega tuleb hinnata, kuidas on selle teenuse turvalisuse tagamine toiminud.

Tervishoiule kui üksusele, kus toimub olulise teenuse osutamine, viidatakse ka NIS direktiivi II lisas, et sinna kuuluvad: "Tervishoiuasutused (kaasa arvatud haiglad ja erakliinikud)" koos viitega EL-i direktiivile 2011/24/EL, mis omakorda täpsustab art 3(g) abil tervishoiuteenuse asutajaid, kes on füüsilised või juriidilised isikud või muud üksused, kes osutavad liikmesriigi territooriumil seaduslikult tervishoiuteenuseid. Tervishoiuteenuse sama direktiivi art 3(a) järgi on see teenus, mida tervishoiutöötajad osutavad patsientidele, et hinnata, säilitada või taastada nende terviseseisundit.[87] Seega on oluline NIS direktiivi vaadata koosmõjus teiste Euroopa Liidu õigusaktidega, mille abil defineeritakse või täpsustatakse olulise teenuse osutaja üksust ja annab mõisted nende defineerimiseks. NIS direktiiv defineerib ise vaid olulise teenuse osutaja.

[85] 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.
[86] WHO. COVID-19 continues to disrupt essential health services in 90% of countries. 2021. Kättesaadav arvutivõrgus: https://www.who.int/news/item/23-04-2021-covid-19-continues-to-disrupt-essential-health-services-in-90-of-countries#:~:text=Among%20the%20most%20extensively%20affected,and%20services%20for%20other%20noncommunicable (11.04.2022).
[87] 9. märtsi 2011. aasta Euroopa Parlamendi ja nõukogu direktiiv 2011/24/EL, patsiendiõiguste kohaldamise kohta piiriüleses tervishoius. ELT L 88, 4.4.2011, lk 45—65.

Teiseks oluliseks analüüsi subjektiks on elektrooniline kommunikatsioon (sh telekommunikatsioon), sest riigi kohustus on kriisi ajal tagada nende teenuste turvalisus. Antud valdkonna abil saab ühiskond kriisi ajal kiirelt ja efektiivselt juhiseid ning teavet toimuvast. Vastasel juhul võib infopuudus olla tõrgete esinemise ajal eluohtlik ning kriisiga toime tulemisel laastava mõjuga.[88] Kuivõrd NIS direktiiv tuli üle võtta siseriiklikkusse õigusesse, vaadatakse lähemalt, kuidas kajastuvad olulise teenuse operaatori sätted siseriiklikus õiguses.

Eestis vastu võetud KüTS-iga võeti täielikult NIS direktiiv üle, kuid oluline on jälgida, mis täiendusi on tehtud seaduses teenuse (sh olulise) osutaja (edaspidi OTO) suhtes. NIS direktiivi jõustumisel tekkis Eesti õiguskorda uus termin "olulise teenuse operaator", mis defineeriti KüTS § 3 lõikes 1 abil. Samas ei ole olulise teenuse osutaja definitsioon võrdväärne hädaolukorra seaduses esitatud elutähtsa teenuse osutaja definitsiooniga, vaid see on laiem ning hõlmab ka teisi teenusepakkujaid, kelle teenused on ühiskonna ja majanduse toimimise jaoks olulised.[89] Näiteks loetleb küberturvalisuse seadus ette erinevaid teisi õigusakte, mille kaudu saab defineerida teenuse osutajat KüTS § 3 mõistes:

- lg 1 p 1 viitab hädaolukorra seadusele, kus on defineeritud elutähtsa teenuse osutaja,
- lg 1 p 5 viitab elektroonilise side seadusele, mille tähenduses on teenuse osutaja sideettevõtja (kaabelleviteenuseosutaja, kellel on 10 000 lõppkasutajat ja ringhäälinguvõrgu teenuse osutaja)
- lg 1 p 6 viitab tervishoiuteenuste seadusele, kus on üldterminina haiglavõrk (piirkondlik haigla, keskhaigla pidaja statsionaarse eriarstiabi osutamisel ja kiirabibrigaadi pidaja kiirabi osutamisel).
- lg 1 p 10 viitab Eesti Rahvusringhäälingule koos vastava ameti seadusega.[90]

Olulise teenuse operaatori viide on KüTS § 3 lg 2-s, kus eelneva loetelu all mainitud teenuse osutajad, kui nad asuvad NIS direktiivi II lisas mainitud sektoris, on nad selle direktiivi alusel defineeritud olulise teenuse operaatorina. KüTS seletuskirjas on ka põhjendatud, miks mainitakse ainult elutähtsaid teenuseid. Seletuskirjas öeldakse, et Eesti on olulised teenused määratlenud hädaolukorra seaduses elutähtsate teenustena. Hädaolukorra seaduse valdkondlik loetelu on NIS direktiivi lisa 2-st erinev, sest seal on näiteks teenuseid, mida Eesti veel ei osuta. Saab järeldada, et küberturvalisuse meetmete ja standardite rakendamiseks on Eesti teinud veidi

[88] CMS Law-Now. Communications as an essential service during Coronavirus (COVID-19) confinement. 2020. Kättesaadav arvutivõrgus: https://www.cms-lawnow.com/ealerts/2020/04/portugal-communications-as-an-essential-service-during-coronavirus (11.04.2022).
[89] Kask, L. *Op cit*, lk 4.
[90] Küberturvalisuse seadus[1] – RT I, 22.05.2018, 1.

laiema (sh kasutades eriseadusi) käsitluse küberturvalisuse seaduse alusel luues mõiste teenuse osutaja. KüTS-iga püüab Eesti laiendada vähemalt osaliselt küberturvalisuse tagamisel sätestatud nõudeid.[91]

Iirimaa on järginud seaduses S.I. No. 360/2018, NIS direktiivi eeskuju. Olulise teenuse operaator on defineeritud mõistes kui isik, kes on määratud selleks sama seaduse punkti 12 järgi. Konkreetne punkt sätestab kriteeriumid sarnaselt NIS-ile, millele vastamisel saab riigi vastav amet määrata isiku olulise teenuse operaatoriks. Nende kriteeriumite hulgas on näiteks järgmised punktid:

- isik osutab olulist teenust riigis,
- isikul on riigis registreeritud asutus,
- isik on 1. loendi veerus 3 sätestatud isik (sarnane loend NIS direktiiv lisa II, kus viited Iirimaal rakenduvatele eriseadustele),
- sektor ja vajaduse korral allsektor, milles põhiteenust osutatakse, on 1. loendis sätestatud sektor ja allsektor;
- põhiteenuse osutamine isiku poolt sõltub võrgust ja infosüsteemidest
- vahejuhtum, mis mõjutab isiku poolt põhiteenuse osutamist, avaldaks olulist häirivat mõju selle teenuse osutamisele riigis.[92]

Eelnevast nähtub, et kasutatud on põhilisi elemente olulise teenuse operaatori defineerimisel, mis sisalduvad ka NIS direktiivis. Ühtlasi ei kaldu ka Iirimaa seaduses definitsioon laiemaks, kui Eestis, kuid see viitab eriseadustele, mille raames saab määratleda sektorites olevaid olulise teenuse operaatoreid. Identifitseerimise kriteeriumid Iirimaa jaoks olid järgmised:

- Üksus peab pakkuma teenust, mis on oluline kriitilise ühiskondliku ja majandustegevuse säilitamiseks;
- Teenuse osutamine peab sõltuma võrgust ja infosüsteemidest;
- Turvaintsidendil oleks oluline häiriv mõju põhiteenusele.[93]

Tšehhi määrus No 437/2017 Coll. on välja toonud eraldi, millistele kriteeriumitele tuleb vastata, et määratleda teenuse osutaja olulise teenuse operaatoriks. Seaduse punktid on järgnevad:

[91] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse seaduse eelnõu seletuskiri. 2017, lk 9. Kättesaadav arvutivõrgus: https://www.koda.ee/sites/default/files/content-type/content/2017-10/seletuskiri_k%C3%BCberturvalisuse%20seadus.pdf (11.04.2022).
[92] 9. European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018– S.I. No. 360/2018.
[93] *Ibidem*.

- Valdkondlikud kriteeriumid määratakse teenuse tüübi, üksuse tüübi ja üksuse liigi erikriteeriumi järgi.
- Üksuse tüübi erikriteerium võtab arvesse üksuse tähtsust antud sektoris.
- Valdkondlikud ja mõjukriteeriumid on loetletud käesoleva määruse lisas.
- Konkreetsele sektorile või sektori teatud osale seatud mõjukriteeriumid on seotud teenuse liigi, üksuse liigiga ja käesoleva määruse lisas samal real märgitud üksuse liigi erikriteeriumiga.[94]

Lühikesele määruse sissejuhatusele järgneb põhjalik tabel olulistest sektoritest, kus määratakse millist tüüpi ettevõtjad on olulise teenuse operaatorid, mis on nendele kohalduv erikriteerium ning mõjukriteerium. Lisatud on ka viited Tšehhi eriseadustele, kus defineeritakse, millistele ettevõtetele määrus kohaldub. Tervishoiuteenuse pakkujate definitsioon tuleneb Tšehhi tervishoiuteenuse seaduse alusel, mille alusel erikriteeriumiks on see, et teenuse osutajal on kokku vähemalt 800 kiirravi voodikohta viimase kolme kalendriaasta jooksul või kõrgelt spetsialiseeritud traumaraviasutuse staatus vastavalt tervishoiuteenuste seadusele. Küberturbeintsidendi mõju infosüsteemis või elektroonilises sidevõrgus, mille toimimisest teenuse osutamine sõltub, võib olla järgnev:

1. teenuse liigi tõsine piirang, mis puudutaks rohkem kui 50 000 inimest;
2. mõne muu olulise teenuse tõsine piiramine/häire või kriitilise infrastruktuuri elemendi piirang/häire;
3. teenuse liigi kättesaamatus rohkem kui 1600 inimesele, mis on muul viisil asendamatu, kui ei teki liigseid kulutusi;
4. rohkem kui 100 kannatanut või 1000 vigastatut, kes vajavad arstiabi;
5. avaliku turvalisuse häirimine olulises osas laiendatud volitustega omavalitsuse haldusterritooriumist, mis võib nõuda pääste- ja likvideerimisoperatsioone integreeritud päästesüsteemi üksuste poolt;
6. rohkem kui 200 000 inimese delikaatsete andmete avalikustamine.[95]

Tšehhi ei ole üles loetlenud laiemat oluliste teenuse operaatorite loetelu, kust võiks leida elektroonilise kommunikatsiooni valdkonna teenuse osutajaid, mistõttu ei saa hinnata, kuidas NIS direktiiv neid teenusepakkujaid otseselt mõjutab. Jätkuvalt kehtib ka elektroonilise side seadustik rangemate turvanõuete osas. Tšehhi praktika on sellest tulenevalt pigem Iirimaa eeskujul NIS direktiivi minimaalne ülevõtmine ehk jäädud on direktiivi piiridesse ilma seda

[94] Decree on the criteria for the determination of an operator of essential service – 437/2017 Coll.
[95] *Ibidem.*

oluliselt laiendamata. Samas on Tšehhi kasutanud võimalust täpsustada mõju ning olulise teenuse sektorisse kuulumise erikriteeriumeid. Eriti oluline on markeerida, et lisaks sektorile on selgitatud ka spetsiaalsed kriteeriumid sektorisse kuulumiseks. Samuti on defineeritud mõjukriteerium, mille alusel saab analüüsida, kas küberintsident avaldas häirivat mõju sektoris oleva vajaliku teenuse toimimisele. See on aga huvitav aspekt määruses, sest mõjukriteerium erineb NIS direktiivis loodud olulise häiriva mõju definitsioonist. Martin Švéda NUKIB-ist kirjeldas, et selline täpsustus oli vajalik, sest nende arvates ei ole võimalik küberintsidendi tuvastamisel kohe identifitseerida, kas juhtum vastab NIS direktiivis välja toodud olulise häiriva mõju kriteeriumile. Seadusandja soov oli, et teenuse osutajaid raporteeriks kõiki kahtlaseid tegevusi küberturvalisuse valdkonnas. Seetõttu NIS direktiivi art 6 sisalduv loetelu olulise häiriva mõju teguritest ühildati Tšehhi määrus nr 317/2014 Coll-iga, mille tagajärjel täpsustati art 6(1)(a) kriteeriumit. Näitena saab vaadelda eelpool mainitud tervishoiusektori loetelu esimest mõjukriteeriumi.[96]

Vaadeldes riikide praktikat NIS direktiivi ülevõtmisel, siis järeldub, et rangemate reeglite sätestamine või teenuseosutajate laiem käsitlus on pigem erand ning vaid võimalus liikmesriikidel tagada kõrgem võrgu-ja infosüsteemide turvalisuse tase, mis on kooskõlas minimaalse ühtlustamise printsiibiga tulenevalt direktiivi art 3-st.[97] Seda võimalust on kasutanud eeskätt Eesti. Riigi Infosüsteemi Ameti õigusosakonna juhataja Silver Lusti sõnul oli see vajalik, sest Eesti riik on suures sõltuvuses e-teenustest ja seega eksisteerib ka kõrgendatud vajadus neid teenuseid kaitsta. Tšehhi kaalus riikliku kriisiseaduse alusel kriitilise infrastruktuuri kaasamist oluliste teenuste osutajate seadusandlusesse, kuid otsustas seda mitte teha riiklike regulatsioonide alusel. Iirimaa küberturvalisuse ametilt selles osas vastus puudub ning seaduse eelnõu seletuskiri ei ole kättesaadav, seetõttu on võimatu hinnata, mis põhjustel tehti sellised otsused NIS direktiivi ülevõtmisel siseriiklikusse õigusesse.[98]

Oluliste teenuste operaatorite defineerimisel ja nende mõistmisel on oluline aru saada, kuidas ja mis ulatuses rakenduvad neile kohustused tulenevalt NIS direktiivi ülevõtmisest siseriiklikusse õigusesse. Siinkohal on olulised direktiivi art 14 ja 15, mis räägivad oluliste teenuste operaatorite võrgu- ja infosüsteemide turvalisusest. Liikmesriigid peavad tagama, et oluliste teenuse operaatorid võtavad kasutusele asjakohased ja proportsionaalsed ning

[96] M. Švéda an E.Pilliroog. Brno. 11.04.2022. (kiri adressaadi valduses)
[97] 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.
[98] M. Švéda an E.Pilliroog. *Op cit*.

tehnilised korralduslikud meetmed, et toime tulla riskidega, mis ohustavad nende töös kasutatavate võrgu- ja infosüsteemide turvalisust. Liikmesriigid peavad tagama, et oluliste teenuste operaatorid võtavad kasutusele asjakohased meetmed, mille abil saab ennetada ja minimeerida oluliste teenuste osutamiseks kasutatavate võrgu- ja infosüsteemidele suunatud küberrünnakute mõju, et tagada eelnevalt mainitud teenuste järjepidevus. Liikmesriikide kohustuse hulgas on teavitamiskohustuse sätestamine oluliste teenuste operaatoritele ehk teenuste osutajad on kohustatud teatama juhtumitest, mis kuuluvad direktiivi reguleerimisalasse. Teatatav küberintsident on mis tahes juhtum, millel on oluline mõju oluliste teenuste operaatori pakutava olulise teenuse järjepidevusele. Antud kontekstis tähendab oluline mõju seda, et OTO pakutav põhiteenus katkeb ega toimi teatud aja jooksul. Teatatav intsident määratakse kindlaks direktiivis sisalduvate olulise mõju parameetrite abil. See tähendab, et põhjendamatu viivituseta peab operaator pädevale asutusele või CSIRT-ile teavitama intsidentidest, millel on oluline mõju nende poolt pakutavate oluliste teenuste järjepidevusele.[99]

KüTS § 7 sätestatakse eelnevalt mainitud teenuse osutajale kehtivad süsteemi turvanõuded, mida on vaja rakendada selleks, et küberintsidente ennetada ning lahendada. Lisaks tuleb tagada, et küberintsidendi toimumise ja tuvastamise korral oleks selle mõju teenuse toimepidevusele minimaalne.[100] Eriti oluline on arvesse võtta asjaolu, et kuivõrd Eestil on laiem käsitlus olulise teenuse operaatoritest, kui puhtalt direktiivis ettenähtud loetelu, siis laienevad ka kohustused suuremale hulgale subjektidele. Olulist saab KüTS-ist välja tuua järgnevat:

- Üldine kohustus rakendada organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid;
- Süsteemi riskianalüüsi koostamise kohustus;
- Kohustus dokumenteerida süsteemi riskianalüüs, turvaeeskirjad ja turvameetmed;
- Abinõude kasutusele võtmise kohustus küberintsidendi mõju ja leviku vähendamiseks;
- Korraline turvameetmete kontroll, tulemuste dokumenteerimine;
- Seoses süsteemi turvameetmete kirjelduse ja riskianalüüsiga on täpsemad nõuded dokumendile sätestatud ministri määrusega;
- Eraldi § kirjeldab ka kohustus ja täpset protseduuri, kuidas ja mis aja jooksul peab teenuse osutaja teavitama RIA-t küberintsidendist.

[99] 3. 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.
[100] Majandus- ja Kommunikatsiooniministeerium. 2017. *Op cit.*

Tšehhi ja Iirimaa õigusaktid kirjeldavad ühel või teisel moel sarnast protsessi ja kohustusi teenuse osutajatele. Ainus erinevus on see, et mõlema riigi puhul kehtivad need kohustused kitsamale ringkonnale.

Iirimaa näitel saab tuua ka eraldiseisva meetmena turvalisuse juhised, mis peaksid aitama oluliste teenuste operaatoritel seadusest tulenevate kohustuse täitmist. NCSC kirjeldab antud dokumenti eesmärki viie põhilise peatüki abil: identifitseerimine, kaitsmine, tuvastamine, reageerimine ja taastumine. Ühe osana kirjeldatakse oluliste teenuste operaatoritele kohalduvaid põhimõtteid, mille alusel peaksid teenuse osutajad turvameetmeid rakendama. Nende meetmeteks on:

- Tõhus oluliste teenuste operaatorite küberturvalisuse suurendamisel seoses ohumaastikuga praegu ja lähitulevikus.
- Kohandatud tagamaks, et jõupingutusi rakendatakse meetmetele, millel on oluliste teenuste operaatorite turvalisuse suurendamisel kõige suurem mõju.
- Ühildub valdkonnaüleste haavatavuste kõrvaldamiseks ja seda on täiendatud sektorile spetsiifiliste turvameetmetega.
- Proportsionaalne riskidega, rõhuasetusega oluliste teenuste aluseks olevate süsteemide kaitsmisel.
- Konkreetne ja hõlpsasti arusaadav, et tagada meetmete täielik rakendamine ja tõhustada aktiivselt küberturvalisust.
- Kontrollitav, et OTO saaks ministrile esitada tõendeid turvameetmete tõhusa rakendamise kohta.
- Kaasaarvatav, et tagada meetmete rakendamine kõigi viie teema (tuvastamine, kaitsmine, tuvastamine, reageerimine, taastamine) katmiseks.[101]

Kokkuvõttes on Iirimaa juhised hea tööriist oluliste teenuste osutajatele nii riskianalüüsiks, intsidendi tuvastamiseks aga ka selle negatiivse mõju vähendamiseks. Seaduse tasandil võib määruseid ja õigusakte olla tavapärasel kujul keeruline mõista, kuid lihtsas ja arusaadavas keeles loodud juhised, kui eraldiseisev meede, toimivad efektiivselt selleks, et aidata ettevõtetel järgida küberturvalisuse kohustusi ning tagada turvalisuse kõrge tase oluliste teenuste osutamisel.

[101] National Cyber Security Centre. NIS Compliance Guidelines for Operators of Essential Service (OES). 2019, lk 7. Kättesaadav arvutivõrgus: https://www.ncsc.gov.ie/pdfs/NIS_Compliance_Security_Guidelines_for_OES.pdf (11.04.2022).

Teenuste osutajad, kes riiklike regulatsioonide alusel ei ole määratud olulise teenuse operaatoriks ega ka digitaalse teenuse osutajaks, võivad siiski kasutada vabatahtlikku teavitamiskohustust vastavalt NIS direktiivi art 20-le ilma, et see piiraks art 3 kohaldamist. Vabatahtlikku teavitamiskohustust küberintsidentidest võivad kasutada kõik teenuste pakkujad, kellel on intsidendi tulemusel märkimisväärne mõju enda teenuse osutamise järjepidevusele. Nende teavituse töötlemisel tegutsevad liikmesriigid NIS direktiivi art 14 sätestatud korras. Vabatahtlikke teavitusi töödeldakse vaid juhul, kui selline töötlemine ei kujuta asjaomastele liikmesriikidele ebaproportsionaalset ega ülemäärast koormust. Samas ei too vabatahtlik teavitamine seda kasutanud teenuste osutajatele kohustusi, mida need teenuse osutajaid ei oleks pidanud järgima, kui nad ei oleks teavitamiskohustust kasutanud.[102]

Iseenesest on vabatahtlik teavitamiskohustus lisameede riikidele, kes on jälginud kitsamat teenuste osutajate mõistete defineerimist. Kuid kuna tegemist on vabatahtliku võimalusega, ei anna see kriisiolukorras sellist tugevat mõju mida ehk vaja oleks. Nii võib näiteks kriisi ajal tekkinud küberturvalisuse intsident jääda märkamatuks, kuid samaaegselt mõjutada suurel hulgal inimesi. Antud juhtumeid saab ennetada liikmesriikidele ette nähtud kohustuse järgi, kus oluliste teenuste operaatorite loetelu uuendamist teostatakse iga kahe aasta tagant, mida näeb ette NIS direktiivi art 5(5) alusel.[103]

Eelnevalt defineeriti läbi praktiliste näidete NIS direktiivi kohaldamine, mille alusel on Eesti, Iirimaa ja Tšehhi suutnud siseriiklikus õiguses rakendada olulise teenuse operaatoritele kohalduvaid sätteid. Nähes võimalusi erinevateks rakendusvõimalusteks nende kolme riigi näitel on põhiline suundumus pigem direktiivi minimaalne ülevõtmine ehk teenuse osutajate kitsam, kuid NIS direktiivile vastav definitsioon. Sellegipoolest on antud direktiivi ülevõtmisel seadusaktidesse kirjutatu üheselt kõrge kvaliteedi poolest arusaadav ja põhimõttelisi erinevusi riikide õigusaktides ei ole. Samuti näeme, et oluliseks saab vastavate pädevate asutuste juhendamine ning kaasuvad küberturvalisuse meetmed, mis aitavad erinevatel riiklikult oluliste sektorite esindajatel seadusega ettenähtud kohustusi täita. Kui tugi on minimaalne või olematu, võib tekkida probleeme valdkonna efektiivseks koordineerimiseks. Samas saab nende valimiriikide põhjal järeldada, et tehtud on enamatki, et oleks arusaadav, kellele ja mis ulatuses kohustused kehtivad küberturvalisuse kõrgete ja kvaliteetsete nõuete täitmiseks.

[102] 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.
[103] *Ibidem.*

2.2. COVID-19 kriisi mõju riiklikult olulistele teenustele

Olukorras, kus on defineeritud ja selgitatud riiklikult oluliste teenuste olemust, on oluline hinnata, kuidas COVID-19 avaldas survet nende teenuste toimimisele. Järgnevas peatükis kirjeldatakse üldist küberturvalisuse trendi kriisi ajal, olulisemaid küberintsidente ning tehakse kokkuvõtte negatiivse mõju ulatusest küberturvalisuse valdkonnas. Eriliselt keskendutakse tervishoiu ja elektroonilise kommunikatsiooni valdkonnale.

Riikide ja nende valitsuste meetmed alates 2020. aasta märtsist suurendasid digitaalsete rakenduste kasutamist enam kui 10% ja koos sellega tõid kaasa elanikkonna vähenenud kindlustatuse. COVID-19 oli andnud küberkurjategijatele vaba tee, et sotsiaalmeedia ja sõnumiplatvormide ärakasutamisega saavutada kerge juurdepääs potentsiaalsetele ohvritele (sh laste seksuaalselt kuritarvitamisele) ning suurendada meditsiiniga seotud petuskeemide aktiivsust.[104] Näiteks Facebooki kasutajaandmete taotluste kohaselt esitati sotsiaalmeediaplatvormile 2020. aasta esimese kuue kuu jooksul Euroopa Liidus kokku üle 150 000 õiguskaitseorgani päringu – üle 40 000 päringu rohkem kui 2019. aastal. Võrreldes 2019. aasta sama perioodiga sai Europol 2020. aasta samal perioodil riiklikult kadunud ja ära kasutatud laste keskuselt üha rohkem pöördumisi.[105]

Eurofund viitas sellele, et peaaegu 40% EL-is töötavatest inimestest läksid 2020. aastal täielikult kaugtööle. Rohkem kui 80% inimestest kogu maailmas julgustati kasutama kaugtöö võimalusi. Veelgi enam, küberrünnakute arv oli kõige suurem sotsiaalmeedia andmepüügirünnakute ja pahavara tõttu, mis saadeti vestluste, sotsiaalmeedia pettuste ja laste seksuaalse kuritarvitamise materjalide kaudu. Sotsiaalne manipuleerimine ja andmepüük muutus ja arenes kiiresti, sest platvormide kasutajad vajasid väga suurel hulgal ja peamiselt COVID-19 teemalist teavet.[106] Sotsiaalne distantseerumine ja igapäevaste toimingute tugev häiritus sundis inimesi internetist rohkem sõltuma, sh suurenes järsult ka pilvepõhise salvestusruumi kasutamine ning videokonverentside ja veebiostude arv.[107]

[104] Coman, I., Mihai, I. C. The Impact of COVID-19. Cybercrime and Cyberthreats. European Law Enforcement Research Bulletin, (SCE 5), 61–67. 2022, lk 61. Kättesaadav arvutivõrgus: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/489 (7.02.2022).
[105] *Ibidem.*
[106] *Ibidem*, lk 62.
[107] Pawlicka, A., *et al*. A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. Business Horizons, 64(6). 2021, lk 730–731. Kättesaadav arvutivõrgus: https://www.sciencedirect.com/science/article/pii/S0007681321001336. 2021.07.010 (7.02.2022).

Kõigist pandeemia mõjudest inimeste igapäevastele tegemistele on võib-olla kõige rohkem mõjutanud olukord, mille põhjustasid sulgemismeetmed, nagu näiteks ettevõtete ja hariduskeskuste sulgemine ning kodukontoritest töötamine. Nendel muudatustel olid ilmselged tagajärjed kodanike tegevusele internetis. Meetmed andsid eelkõige soodsama võimaluse ebaseaduslikule tegevusele ühendamaks potentsiaalsed sihtmärgid ja õigusrikkujad võrgus ja võrguväliselt. Näiteks kasutati rohkelt personaalarvuteid äriteabele juurdepääsuks, isiklikke kohtumisi asendasid veebikõned ning üha populaarsemaks muutus toodete ja teenuste ostmine e-poes. Pandeemiaga seotud täielik sulgemine mitmekordistas arvutivõrkude kasutamist äri- ja vaba aja veetmise eesmärgil. Selle tagajärjel suurenes ka tõenäosus, et kiiresti tulid ilmsiks uued viisid küberturvalisuse nõrkuste ärakasutamiseks.[108]

Suurbritannias läbi viidud uuringus järeldati, et COVID-19 kriis on seotud drastiliste, enneolematute muutustega küberkuritegevuse võimalustes. Märgiti, et enamik tänavakuritegusid vähenes ühiskonna täieliku sulgemise ajal, sest kurjategijatel ja sihtmärkidel vähenes võimalus füüsiliseks kohtumiseks. Teisisõnu kuna inimesed veedavad rohkem aega internetis ja vähem aega tänavatel, vähenevad tänavavägivalla- ja varakuritegude võimalused, kuid suurenevad küberkuritegude võimalused.[109]

Interpoli sõnul olid peamised küberkuritegevuse ja -rünnaku vormid COVID-19 ajal järgnevad:

- Veebipettused ja andmepüügid – kasutades COVID-19 teemalisi andmepüügimeile, mis sageli kehastavad valitsus- ja tervishoiuasutusi, meelitasid küberkurjategijad ohvreid esitama oma isikuandmeid ja laadima alla pahatahtlikku sisu. Interpolile teatasid ligi 2/3 organisatsiooni liikmesriikidest, et kasvas selliste COVID-19 teemaliste rünnakute hulk.
- Häiriv pahavara (lunavara ja DDoS) –häiriv pahavara, mis on suunatud kriitilise infrastruktuuri ja tervishoiuasutuste vastu. Interpoli tõi välja, et 2020. aasta aprilli esimese kahe nädala jooksul suurenes lunavara rünnakute arv mitmete küberkuriteo gruppide poolt, kes olid eelnevad kuud olnud suhteliselt mitteaktiivsed.
- Andmete kogumise pahavara – andmete kogumise pahavara, nagu kaugjuurdepääsu trooja programm, teabevargad, nuhkvara ja pangandustroojalased. Kasutades COVID-19-ga seotud teavet peibutisena, tungiti süsteemidesse, et tekitada võrkudes ohtu, varastada andmeid ja luua robotvõrke.

[108] Buil-Gil, D., *et al*. Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. European Societies, 23(sup1), S47–S59. 2021, lk 50. Kättesaadav arvutivõrgus: https://www.tandfonline.com/doi/full/10.1080/14616696.2020.1804973 (7.02.2022).
[109] *Ibidem*, lk 48, 55-56.

- Pahatahtlikud domeenid – kasutades ära suurenenud nõudlust COVID-19 kohta käiva teabe järele, suurenes juhtumite arv, kus registreeriti domeeninimesid, mis sisaldavad selliseid märksõnu nagu „koroonaviirus“ või „COVID“. Sellised veebisaidid toetavad aga suurt hulka pahatahtlikke tegevusi, sealhulgas C2-servereid, pahavara juurutamist ja andmepüüki. Interpoli teatel kasvas 2020. aastal pahatahtlike doomeninimede registreerimiste arv 569 %.
- Desinformatsioon – avalikkuse seas levis kiiresti suur hulk desinformatsiooni ja võltsuudiseid. Kontrollimata teave, ebapiisavalt mõistetavad ohud ja vandenõuteooriad hõlbustasid ka küberrünnakute sooritamist. Näiteks ühe kuu jooksul teavitati ainult ühes riigi 290 postitusest, millest enamik sisaldas varjatud pahavara. Samuti oli teateid desinformatsiooni kohta, mis oli seotud meditsiiniliste kaupade ebaseadusliku kaubandusega.[110]

Valeuudised COVID-19 kohta olid tõeliselt suur ning eetiline probleem. Võltsuudised võivad olla küberturvalisuse tagamise mõttes kasutu tegevus, kuid sellegipoolest ei tohiks neid lihtsalt kõrvale heita, sest need võivad olla äärmiselt eksitavad ja omada seega tõsiseid tagajärgi. Väidetavalt surid sajad inimesed, kuna nad uskusid võltsuudiseid erinevate kemikaalide allaneelamise ravivatest mõjudest seoses COVID-19-ga. Sarnaselt andmepüügi kampaaniatele, levitatakse enamasti valeteavet klikkide pärast. Pikemas perspektiivis ei ole tegemist ainult eetilise küsimusega, sest võib omada ka drastilisi tagajärgi oluliste teenuse osutamisel. Kuigi desinformatsioon kui selline ei ole otsesõnu kõikides EL liikmesriikides kehtestatud keelatud tegevusena, jääb selline turvaaukude ärakasutamise vältimine koostöös eraettevõtetega küberturvalisuse tagamisel oluliseks faktoriks, et limiteerida desinformatsiooni ohtrat levikut ning sellega kaasnevaid negatiivseid tagajärgi kriisi ajal.[111]

2020. aasta aprillis väljastas Interpol kõrgema hoiatuse ülemaailmse COVID-19 puhangule reageerimise esirinnas olevatele organisatsioonidele, kellest võivad saada lunavararünnakute sihtmärgid. Ametkonna sõnul oli rünnakute eesmärk lukustada organisatsioonid välja nende kriitilistest süsteemidest, püüdes seeläbi välja pressida rahalisi makseid. Interpoli küberkuritegevuse ohule reageerimise meeskond tuvastas lunavararünnakute arvu märkimisväärse tõusu viirusetõrjega seotud võtmeorganisatsioonide ja -infrastruktuuri vastu. Küberkurjategijad planeerisid kasutada lunavara haiglate ja meditsiiniteenuste digitaalseks

[110] Interpol. Interpol report shows alarming rate of cyberattacks during COVID-19. 2020. Kättesaadav arvutivõrgus: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (19.04.2022).
[111] Pawlicka, A., *et al*. *Op cit,* lk 733.

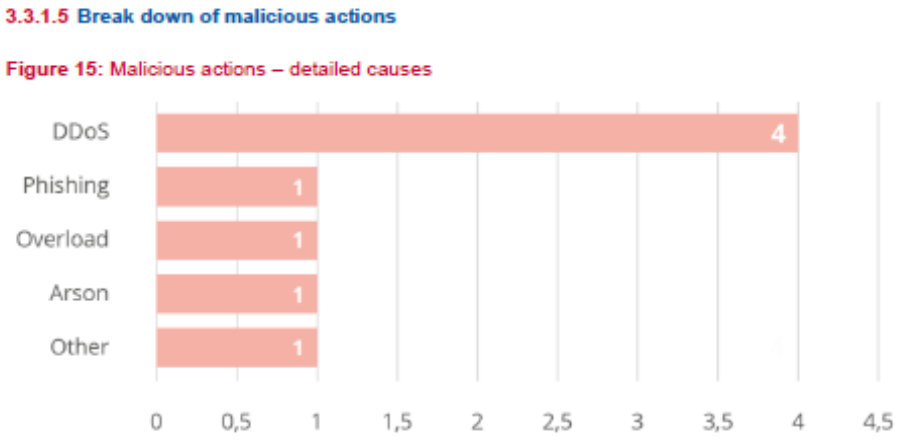
pantvangis hoidmiseks, takistades neil juurdepääsu olulistele failidele ja süsteemidele kuni lunaraha maksmiseni. Et toetada ülemaailmseid jõupingutusi selle kriitilise ohu vastu, väljastas Interpol ka kõrgendatud lunavaraohu hoiatuse politseiorganisatsioonidele kõigis oma 194 liikmesriigis. Ameti sõnul oli peamine plaanitav viis küberkuritegude toimepanemisel emailide kasutamine, kus väidetakse ekslikult, et tegemist on valitsusasutustelt saadud teabega või nõuannetega viiruse kohta. Sellise lähenemisviisiga julgustatakse adressaati klõpsama pahavaraga nakatatud lingil või manusel. Lisaks kõrgendatud ohuolukorrale lisas Interpol esmased juhised, kuidas vältida küberrünnaku ohvriks sattumist.[112]

COVID-19 puhang tõi kaasa Zoom-i ja teiste videokonverentsi platvormide populaarsuse tõusu, kuna süsteemi kasutati väga erinevate sündmuste korraldamiseks (nii töö- kui ka eraelutoimingud). Üsna pea selgus aga, et Zoom-i platvormil olid mõned turvanõrkused, millega seati ohtu miljonite inimeste privaatsuse ja heaolu. Kuigi teadmine turvanõrkustest eksisteeris juba aastaid, ei tegeletud nende kõrvaldamisega piisavalt efektiivselt. Ettevõte selgitas muuhulgas, et sellised veebikonverentsiprogrammid on väga keerulised, mistõttu ei pruugita mõningaid probleeme enne rakenduse kasutamist või küberintsidendi avastamist leida. Tegemist on aga olulise probleemiga, kui ettevõtted on teadlikud rakenduses eksisteerivatest vigades, kuid loodavad neid jooksvalt lahendada ilma ennetavate toiminguteta. Eraettevõtetel on selliseid tavasid lihtne omaks võtta, sest ühelt poolt ei ole tegemist otseselt ühegi seaduse rikkumisega, eriti olukorras, kus ettevõtte ei kuulu olulise teenuse operaatori üksusesse. Samas eetiliselt ja arvestades ka konkreetse platvormi laialdast kasutust on küsitav, et esiplaanil ei ole kasutajate turvalisus või miks taoline situatsioon on lubatav.[113]

Telekommunikatsiooni turvalisuse juhtumite raporti järgi pidid teenusepakkujad 2020. aastal ja eriti COVID-19 pandeemia algusest peale tegelema suurte tõusude ning muutustega kasutus- ja liiklusmustrites. See stabiliseerus järk-järgult selleni, mida praegu peetakse uueks normaalsuseks. Pandeemia üldine tunnus on see, et teenused ja võrgud on kriisi ajal olnud vastupidavad, hoolimata suurtest muutustest kasutuses ja liikluses. Siiski ei tohiks mainimata jätta, et mõned riigid juhtisid – seoses ENISA asjakohase teabe kogumisega riikide reguleerivate asutuste poolt võrkude seisundi kohta 2020. aasta esimestel kuudel – tähelepanu füüsilistele rünnakutele tugijaamadele, mastidele või muudele telekommunikatsiooniseadmete, mis võivad olla seotud levitatud vandenõuteooriatega ja ulatuslike

[112] Interpol. Cybercriminals targeting critical healthcare institutions with ransomware. 2020. Kättesaadav arvutivõrgus: https://www.Interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware (19.04.2022).
[113] Pawlicka, A., *et al*. *Op cit*, lk 732.

desinformatsioonikampaaniatega, et 5G on kahjulik ja isegi COVID-19 pandeemia eest vastutav.[114]



Tabel 2. ENISA ülevaade 2020. aastal enim toimunud küberrünnakutest telekommunikatsiooni ettevõtete vastu.

ENISA raporti järgi on välja toodud, et 2020. aastal põhjustasid telekommunikatsiooni valdkonnas ligikaudu 26% turvaintsidentidest inimlikud vead, mis on suuresti kooskõlas 2019. aasta trendiga (26%). Lisaks oli 61% telekommunikatsiooni intsidentidest süsteemirikked, mida on veidi rohkem kui 2019. aastal (56%). Tabel 2-st on näha, et telekommunikatsiooni vastu enim toime pandud pahatahtlikke küberintsidente olid seotud DDOS-idega ehk teenustõkestusründed, mille tagajärjel ei ole teenused või ressursid kättesaadavad ja kasutatavad. Samuti mõjutasid 2020. aastal pooled teatatud vahejuhtumitest EL-is mobiiltelefoni ja internetti.[115]

ENISA sõnul kasvas 2020. aastal ka tervishoiusektorile suunatud küberrünnakute arv nii intensiivsuselt aga ka ulatuse mõttes kordades. Erilistes näideteks olid Ryuk lunaraharünnak[116]; ja UVM Health Networki sulgemine[117]. Tervishoiuorganisatsioonid üldiselt ja eriti haiglad on olnud küberkuritegevuse peamiseks sihtmärgiks, seda eelkõige rünnakust saadavate andmete

[114] Gogou, V., Dekker, M. Telecom Security Incident 2020 – Annual report. ENISA. 2021, lk 5.
[115] *Ibidem*, lk 25.
[116] Salama, V. Several hospitals targeted in new wave of ransomware attacks. CNN. 2020. Kättesaadav arvutivõrgus: https://edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html (20.04.2022).
[117] Dyrda, L. Inside UVM Medical Center's randomware attack: 11 details. Becker's Health IT. 2020. Kättesaadav arvutivõrgus: https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html (20.04.2022).

väärtuse ja selle häiriva mõju tõttu. ENISA sarnaselt Interpolile hoiatas, et kriitilise infrastruktuuri ja teenustena tervishoiuorganisatsioonid, sealhulgas haiglad ja erasektori kliinikud, peavad olema selliste küberrünnakutega toime tulemiseks valmis, sest nende teenuste katkemine toob kaasa erakordselt drastilise mõju nii valitsustele kui ka elanikkonnale, eriti kriisi tingimustes.[118]

Teiselt poolt on tervishoiusektori näol tegemist üsna stabiilse ning ka pikaajalise arenguga sektoriga. ENISA on selgitanud, et vastuvõtlikkus küberrünnakutele tuleneb eelkõige tervishoiu tugevatest traditsioonidest. Tervishoiu operatsioonidel ja seadmetel on pikk kasutusiga (keskmiselt kuni 15 aastat) ning sellised seadmed ei ole tavapäraselt loodud pahatahtlike küberrünnakute vastu võitlemiseks. Sama ajal on ka infotehnoloogiatoodete elueatsüklid pidevalt lühenemas ja vajadus seadmete uuendamiseks kasvab.[119] COVID-19 kriisi tulekuga avaldus sektorile aga tugev surve, mille kaasnes aga soodne keskkond küberintsidentidele. Suurenev oht tõi kaasa selle, et haiglad ja haiglapersonali olid peamiseks sihtmärgiks, et toime panna lunavararünnakuid, teenuste katkestusi ning andmepüüki, mis omakorda tegi raskeks nii tervishoiukriisi ohjeldamise aga ka küberturvalisuse üldise tagamise.[120]

Tervishoiusektoris tehtud uuringu põhjal hinnati, kui hästi on haigla personal tegelikult valmis küberturvalisuse tagamiseks COVID-19 pandeemia ajal. Küsimustiku analüüs näitas, et IT-osakonnad said piisavalt aru kontseptsioonidest, nagu standardite rakendumine nende eeskirjades ja korduva riskianalüüsi kaasamise vajadusest oma tegevuste hulka. Samas oli uuringus vastuoluline järeldus, et andmepüügi sihipärase järelhindamise tulemuste kokkuvõtteks omistatakse madalaim keskmine tulemus IT-spetsialistidele, kuigi neilt võiks oodata paremat hinnangut. Eeldus on, et nad on kõige kvalifitseeritumad vastanutest ning need, kes on võimelised haigla personali juhendama ja nõustama kahtlaste meilidega seotud toimingutes.[121]

Arvestades eelnevalt kirjeldatud COVID-19 negatiivset mõju, võivad halbade asjaolude kokkulangemisel olla küberkuritegevuse tagajärjed tervishoiuteenuse osutamisele laastavad.[122]

---

[118] Baumann, A. A., *et al*. CSIRT capabilities in healthcare sector: status and development. ENISA. 2021, lk 6.
[119] *Ibidem*, lk 28.
[120] Pranggono, B., Arabo, A. COVID-19 pandemic cybersecurity issues. Internet Technology Letters, Volume 4, Issue 2. 2020. Kättesaadav arvutivõrgus: https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247 (22.04.2022).
[121] Georgiadou, A., *et al*. *Op cit*, lk 13.
[122] *Ibidem*.

27-st liikmesriigist on vaid mõned üksikud riigid andnud märku, et nad on, kas juba loonud või loomas tervishoiusektorile keskenduvat CSIRT-i. Kuigi selline asjaolu oleks turvalisuse aspektist kiidetav ja mõnes olukorras lausa vajalik, ei ole tegemist üldise kohustusega kõikidele liikmesriikidele. Hetkeseisuga ei ole valimiriikidest ei Eesti, Iirimaa ega Tšehhi loonud või planeerimas luua sellist üksust.

Kõige ilmekam näide COVID-19 mõjust on leitav ka meie valimiriikidest. NUKIB ehk Tšehhi küberturvalisuse riiklik agentuur teavitas vaid päev peale eriolukorra kehtestamist 2020. aasta märtsis, et COVID-19 puhangu keskel toimus küberrünnak Tšehhi suuruselt teisele haiglale. Küberründe tõttu pidi terve haiglavõrgu sulgema. Selle tulemusel pidi edasi lükkama nii operatsioone kui ka patsiente ümber suunama teistesse haiglatesse. Veelgi enam mõjutas antud olukorda kestev pandeemia, mis oli juba eelnevalt tõstnud haigla töökoormust.[123] Küberründe eesmärk oli kasutada *spear-phishing* meetodit[124], et saada juurdepääs haigla võrgule ja seejärel juurutada võrku lunavara, et krüptida haigla andmed.[125] Reaktsioon ründele oli kiire ning efektiivne. Suurema kahju ärahoidmiseks andis NUKIB välja reaktsioonimeetmed, mida peavad rakendama küberturvalisuse seaduse alusel tegutsevad tervishoiuteenuse osutajad. 2020. aasta aprillis avaldas amet ka siduva hoiatuse, et valmis tuli olla ähvardavaks küberrünnakuks Tšehhi digitaalsele infrastruktuurile, peamiselt suunatud tervishoiuteenuste osutajatele. Hoiatuse võttis muu hulgas murega teadmiseks ka Ameerika Ühendriikide välisminister. Selle ja mitmete sarnaste intsidentide tõttu kogu maailmas väljendasid oma muret ka EL ja NATO.[126]

Teine tõsine küberintsident tuleb Iirimaalt, kus 2021. aasta märtsis toimus lunavararünnak Iirimaa Tervishoiuteenuse Ameti vastu. Sisuliselt avas üks ametnik arvutustabeli, kuhu oli peidetud pahavara. Küberkuritegijad said ligi kaks kuud tervishoiuteenuse võrgusüsteemides tegutseda. Kuigi erinevaid märke rünnakust võis juba märgata, siis sellegipoolest ühtegi järeluurimist ellu ei viidud. 2021. aasta mais said kurjategijad lunavararünnaku aktiivseks teha.

---

[123] Bizga, A. Mysterious cyberattack cripples Czech hospital amid COVID-19 outbreak. Bitdefender. 2020. Kättesaadav arvutivõrgus: https://www.bitdefender.com/blog/hotforsecurity/mysterious-cyberattack-cripples-czech-hospital-amid-covid-19-outbreak (22.04.2022).

[124] *Spear-phishing* on emaili-põhine või elektroonilise kommunikatsiooni pettus suunatud üksikindiviidile, organisatsioonile või ettevõttele. Selle eesmärk on enamasti varastada andmeid või laadida alla pahavara kasutaja arvutisse. Kaspersky. What is Spear Phishing. Kättesaadav arvutivõrgus: https://www.kaspersky.com/resource-center/definitions/spear-phishing (22.04.2022).

[125] Botek, A. Brno University Hospital ransomware attack (2020). Kättesaadav arvutivõrgus: https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)#cite_note-7 (24.04.2022).

[126] *Ibidem*.

Ligikaudu 80% IT infrastruktuurides olid mõjutatud. Rünnaku tagajärjel kadusid mitmete oluliste patsientide informatsioon ja diagnostika andmed, sh avaldas see olulist mõju tervishoiuteenuste pakkumisele ja abi andmisele. Kõik arvutisüsteemid olid välja lülitatud ning haigla personal kaotas krüpteerimise tõttu juurdepääsu patsientide teabe, kliinilise hoolduse ja laborite süsteemidele. Süsteemid taastati alles sama aasta septembris. PWC tegi konkreetsest juhtumist analüüsi ning järeldas, et süsteemid on jätkuvalt haavatavad isegi rohkematele küberrünnakutele tulevikus.[127] Antud küberintsidendist võib leida mitmeid õppetunde, sest tegemist on nii administratiivse kui ka tehnilist tüüpi juhtumiga. Informatsiooni Turvalisuse Amet leidis näiteks, et puudu oli ametikohtadest, kes vastutaksid küberturvalisuse eest ning puudus ka küberturvalisust hindav komitee. Tugevad vead tehti rünnaku ennetamisel aga ka ohjeldamisel olenemata sellest, et küberründaja oleks olnud tuvastatav.[128]

Eestis tegutseva Riigi Infosüsteemi Ameti õigusosakonna juhataja Lusti sõnul ei esinenud riigis COVID-19 kriisist tulenevalt otseselt põhjuslikus seoses olevaid küberründeid. 2020. aasta suurimad intsidendid oli isikuandmete lekked kolmes ministeeriumi haldusalas ning 2021. aastal Log4j turvanõrkusega seotud intsidendid.[129] RIA kommenteeris 2020. aasta juhtumit järgnevalt: "On põhjust arvata, et samad kurjategijad pääsesid novembri lõpus ligi ka sotsiaalministeeriumi haldusalas 9158 inimese informatsioonile, mis seotud koroonaviiruse levikuga. Ajutise lahendusena hoiti neid andmeid ühe veebiserveri andmebaasis. Ründaja juurdepääs sellele elimineeriti samal päeval ning terviseamet teavitas neid inimesi, kelle andmetele kurjategija ligi pääses."[130] Teine kiirelt tähelepanu saanud intsident toimus Eesti Terviseametiga seonduvalt. Amet oli 8. märtsil 2020. aastal saatnud Eesti inimestele välja COVID-19 seotud infot. Vaid mõned päevad hiljem hakkasid levima petukirjad, mis matkisid nimetatud ameti algset emaili. Riigi Infosüsteemi amet selgitas: "Kirja lõpus oli link failile „Eeskiri.7z". Sellel vajutamise järel avanes ekraanil pealtnäha tavaline ennetusplakat, aga taustal paigaldati ohvri arvutisse pahavara, mis varastas brauseritesse salvestatud salasõnad ja pangakaartide andmed."[131] Kuigi RIA küberturbe intsidentide ülevaates perioodil 2020 märts kuni mai on näha mõningast rünnakute arvu suurenemist, ei saa sellest veel järeldada, et mõni

[127] Corera, G. Irish health cyber-attack could have been even worse, report says. BBC. 2021. Kättesaadav arvutivõrgus: https://www.bbc.com/news/technology-59612917 (22.04.2022).
[128] Health Sector Cybersecurity Coordination Center. Lessons Learned from the HSE Cyber Attack. 2022. Kättesaadav arvutivõrgus: https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf (22.04.2022).
[129] S. Lusti an E. Pilliroog. Tallinn. 14.03.2022. (kiri adressaadi valduses)
[130] RIA. Küberturvalisuse aastaraamat 2021. 2022, lk 14-15, 23. Kättesaadav arvutivõrgus: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2021.pdf (22.04.2022).
[131] RIA. *Op cit*, lk 22-23.

oluline teenus tervishoius või elektroonilise kommunikatsiooni valdkonnas oleks katkenud või mõjutanud tugevalt teenuse tarbijaid.[132]

Eelnevat kokku võttes näeme teatud erisusi riikide ettevalmistuses ja reageerimisvõimekuses, mis puudutab küberrünnete tõrjumist riiklikult oluliste teenuste suunas. Varasemalt on kindlaks tehtud, et Liidu turvalisuse nõuete ülevõtmine siseriiklikusse õigusesse toimus täies mahus mitu aastat enne COVID-19 kriisi. Veel enam on valimiriikidest Eesti ja Tšehhi näidanud üles initsiatiivi, et astuda ennetavaid samme, et kaitsta olulist infrastruktuuri ka enne ametlike Euroopa Liidu nõuete kehtestamist. Seadused on olemas, juhendid paigas ning võib väita, et ennetusvõimekus on seega tagatud.

COVID-19 negatiivne mõju on näidanud, et kõikide oluliste teenuste operaatorite süsteemid ei ole terviklikult kaitstud. Kõige ülevaatlikum näide tuleneb haiglates tehtud uuringust koosmõjus suuremate küberintsidentidega, mille tagajärjel saab hinnata nende teenuste osutajate personali võimekust tuvastada kahtlase sisuga meile ning hoida ära võimalikud lunavararünnakud. Tšehhi küberturvalisuse ameti õigusosakonna juhataja Martin Švéda mainis, et palju saab veel teha seoses kriisi juhtimisega, mille tagajärjel kannatas küberruum.[133] Järeldub, et kuigi teoorias on Euroopa Liidu kehtestatud sätted ja siseriiklikud õigusaktid piisavad, saab palju teha nende juhendite reaalses rakendamises ja eluliste olukordadega toime tulemisel. Asutuste võimekus neid rakendada on seatud kahtluse alla ning isegi mitmes situatsioonis tõestatult puudulik. Saame lükata ümber hüpoteesi, et liikmesriigid ei ole võimelised rakendama Euroopa Liidu küberturvalisuse õiguslikku raamistiku, kuid pidama jääb väide, et oluline probleem on asutuste ning erinevate operaatorite võimekus neid nõudeid järgida ning vastavalt rakendada.

[132] RIA. Olukord küberruumis 2020. aastal. 2022 Kättesaadav arvutivõrgus: https://www.ria.ee/et/kuberturvalisus/olukord-kuberruumis/olukord-kuberruumis-2020-aastal.html (22.04.2022).
[133] M. Švéda an E.Pilliroog. *Op cit.*

3. Liikmesriikide küberturvalisuse ennetus- ja reageerimisvõimekuse hindamine

3.1. Analüüs Euroopa Liidu küberturvalisuse õigusliku raamistiku rakendamisest COVID-19 kriisi tingimustes

Euroopas toimunud muudatused on saavutanud oma olemuslikult taotletud eesmärgi koordineerida küberturvalisust kui ühte olulist Liidu poliitikavaldkonda. Näiteks on Euroopa Liidu küberturvalisuse õigusliku raamistiku loomise tulemusel toimunud struktuurilised ning sisulised muudatused Euroopa Liidu küberturvalisuse ameti töös. Viimase üheksa aasta jooksul on loodud kaks pikaajalist strateegiat ja vastu võetud esimene Liidu-ülene küberturvalisuse nõudeid kehtestav ning praktilisi mõjusid omav võrgu- ja infosüsteemide direktiiv. Kõik see on toimunud enne 2020. aasta COVID-19 pandeemia algust, andes liikmesriikidele piisavalt aega, et teha ettevalmistusi selle ja teiste sarnaste kriisidega toimetulekuks. Selleks, et analüüsida liikmesriikide võimekust rakendada küberturvalisuse õiguslikku raamistiku COVID-19 kriisi ajal, tuleb mõista ja hinnata, milliste tingimuste täitmisega on kujunenud valimiriikide näitel nende küberturvalisuse tase. Seda saab teha kasutades kahte küberturvalisuse indeksit - globaalne ja riiklik küberturvalisuse indeks.

Globaalne küberturvalisuse indeks (GCI) on Rahvusvahelise Telekommunikatsiooni Liidu (ITU) algatus ja ÜRO IKT-le spetsialiseerunud agentuur. Seda kujundab ja täiustab erinevate ekspertide töö riikides ja teistes rahvusvahelistes organisatsioonides. GCI on usaldusväärne allikas, mis mõõdab globaalsel tasandil riikide pühendumust küberturvalisusele . Kuna küberturvalisusel on lai rakendusvaldkond, hinnatakse GCI abil iga riigi arengutaset viie indikaatori alusel – õiguslikud meetmed, tehnilised meetmed, organisatsioonilised meetmed, suutlikkuse/võimsuse arendamine ja koostöö. Need hinnangud koondatakse seejärel kokkuvõtlikuks tulemuseks.[134]

GCI hindamisindikaatorite sisu on järgnev:

- Õiguslikud meetmed, kus hinnatakse küberkuritegevuse ja küberturvalisuse-alaseid seaduseid ja määruseid.
    - Küberturvalisuse õigusaktid;
    - Andmekaitset käsitlevad õigusaktid;
    - Kriitilist infrastruktuuri käsitlevad regulatsioonid.

[134] International Telecommunication Union. *Op cit*.

- Tehnilised meetmed, kus mõõdetakse tehniliste võimaluste rakendamist riiklike ja sektoripõhiste agentuuride kaudu.
    - aktiivsete CIRT-ide olemasolu;
    - riik osaleb piirkondlikus CIRT-is;
    - Laste internetikaitsest teatamise mehhanismid.
- Organisatsioonilised meetmed, kus hinnatakse küberturvalisuse riiklikke strateegiaid ja nõudeid rakendavaid organisatsioone.
    - Riiklikud küberturvalisuse strateegiad;
    - Küberturvalisuse agentuurid;
    - Laste veebikaitse strateegiad ja algatused.
- Suutlikkuse/võimsuse arendamine, mis hindab teadlikkuse tõstmise kampaaniate, koolituste, hariduse ja küberturvalisuse suutlikkuse arendamise stiimuleid.
    - Riik viib läbi küberteadlikkuse tõstmise algatusi;
    - Küberturvalisuse uurimis- ja arendusprogrammide olemasolu;
    - Riiklike küberturvalisuse tööstuste olemasolu.
- Koostöö, mis hindab partnerlussuhete olemasolu agentuuride, ettevõtete ja riikide vahel.
    - Riigis on küberturvalisusega seotud avaliku ja erasektori partnerlussuhted;
    - Riigil on kahepoolsed küberturvalisuse lepingud;
    - Riigil on mitmepoolsed küberturvalisuse lepingud.[135]

ITU sõnul võib GCI olla pandeemia järel usaldusväärse ja turvalise küberruumi loomisel lähtekohaks, et mõista, kuidas pandeemia on mõjutanud küberturvalisuse-alaseid jõupingutusi ning kuidas töötavad riigid küberturvalisuse ja usalduse küsimustes. Näiteks teatasid mõned riigid ITU sõnul viivitustest seaduste heakskiitmisel ja jõustumisel, CIRT-de rakendamisel või täiustamisel, riiklike küberturvalisuse strateegiate väljatöötamisel või läbivaatamisel ning suutlikkuse arendamise elluviimisel. Isegi loodud koostöölepingud ei toonud kasu riikidevahelistele suhetele ning koostööle. Selle indeksi olulisus järeldub riikide ennetus- ja reageerimisvõimekuse hindamisel enne COVID-19 pandeemia algust.[136]

GCI-iga on seega loodud tõenduspõhine hindamismeetod võrdlemaks riike ja nende küberturvalisuse taset. Käesoleva magistritöö raames keskendutakse peamiselt õiguslike, tehniliste ning organisatsiooniliste meetmete hindamisele, kuid välistada ei saa ka COVID-19

[135] International Telecommunication Union. *Op cit*, lk 7.
[136] *Ibidem*.

raames relevantseks osutunud meetmeid nagu suutlikkus ja koostöö. Need valdkonnad on olulise koha leidnud ka NIS direktiivi nõuetes ja selle üldeesmärgis.

Teine hindamismeetod on riiklik küberturvalisuse indeks (NCSI), mis on ülemaailmne otseülekandena näidatud indeks. See tähendab, et erinevalt GCI-st täiendatakse riikide hinnanguid vastavalt jooksvatele muudatustele. NCSI eesmärk on mõõta riikide valmisolekut küberohtude ennetamisel ja küberintsidentide ohjamisel. NCSI hinnangud põhinevad avalikult kättesaadavatel tõendusmaterjalidel ning on samuti hea tööriist riikliku küberturvalisuse taseme tõstmiseks. Indeks keskendub järgnevatele valitsuste poolt rakendatavatele küberturvalisuse aspektidele:

- Kehtivad õigusaktid – õigusaktid, määrused, korraldused;
- Loodud üksused – olemasolevad organisatsioonid, osakonnad;
- Koostööformaadid – komisjonid, töörühmad jne;
- Tulemused – poliitikad, harjutused, tehnoloogiad, veebisaidid, programmid jne.[137]

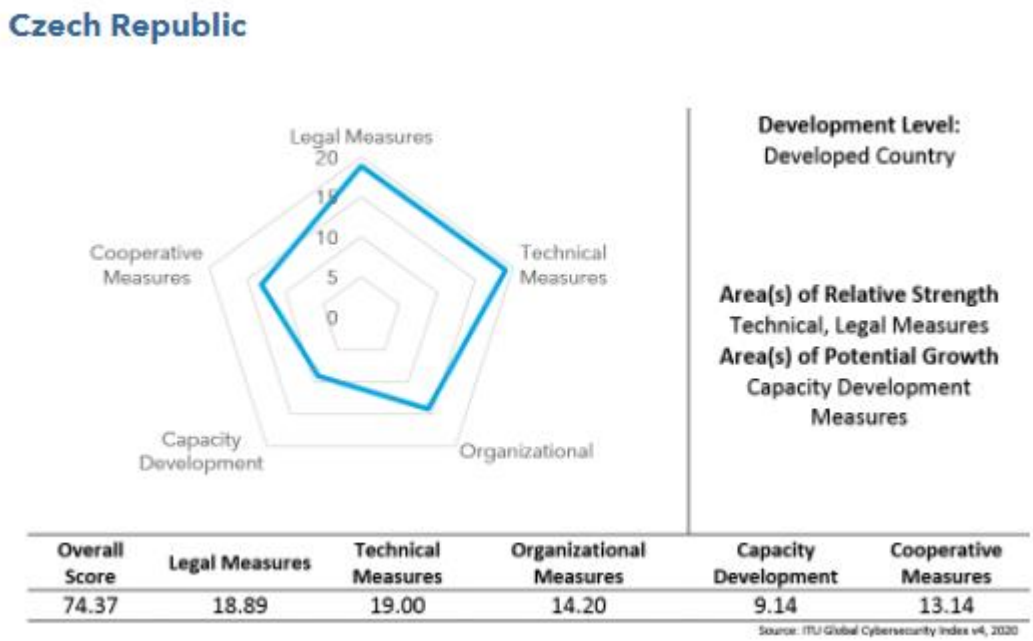
Täpsem NCSI indikaatorite loetelu on toodud välja käesoleva magistritöö Lisas 2. Analüüsi tarbeks on valitud kõige olulisemaks riigi taseme kirjeldamiseks järgnevad valdkonnad, mis on seotud EL-i küberturvalisuse õigusliku raamistiku rakendamisega: 1. küberturbepoliitika, 2. küberohtude analüüs, 5./6. digiteenuse ja oluliste teenuste kaitse, 9. küberintsidentidele reageerimine ja 10. küberkriisi juhtimine. Kuigi koguhinnang kujuneb 12 hindamiskriteeriumi kogusummas, analüüsitakse uurimuse raames riikide konkreetset suutlikkust täpsemalt eeltoodud kuue indikaatori alusel. See tähendab, et nendes valdkondades antud hinnangud ning järeldused on olulisema kaaluga, et analüüsida riikide toimetulekut COVID-19 kriisist tulenevate küberohtudega.

Sisuliselt on nii GCI kui ka NCSI metodoloogial mitmeid sarnasusi, eriti kui vaadata nende hinnatavate indikaatorite sisu. Samas on riikide hinnangud ning järjestustabel mõlema indeksi puhul erinev. Andmete päritolu võrreldes ilmneb, et NCSI kasutab informatsiooni, mis on vabalt kättesaadav riikide küberturvalisuse agentuuridelt ning õigusaktidest. GCSI-i metoodika järgi aga tehakse süsteemseid küsitlusi ning intervjuusid ka riikide kontaktpunktidega. Kuigi GCSI puhul on tegemist üldisemat sorti indeksiga, võivad sellest saadavad järeldused anda täpsemaid tulemusi metoodika tõttu. Järgnevalt analüüsitakse lähemalt riikide profiile ning

[137] National Cybersecurity Index. Kättesaadav arvutivõrgus: https://ncsi.ega.ee (24.04.2022).

hinnangute sisu kahe indeksi võrdluses, et koondada ühene järeldus riikide ennetus- ja reageerimisvõimekuse hindamiseks.

GCI tulemusel moodustub globaalne paremusjärjestus, kus valimiriigid on järgnevatel kohtadel: Eesti 3. kohal (99,48p), Iirimaa 46. kohal (85,86p) ja Tšehhi 68. kohal (74,37p). Euroopa regiooni-põhiselt muutuvad kohaasetused järgnevalt: Eesti 2. koht, Iirimaa 28. koht ja Tšehhi 35. koht. Kuigi Euroopa regioon on siinkohal laiem kui Euroopa Liit, saab puhtalt Liidu-põhiselt järeldada, et Eesti on esikohal küberturvalisuse ennetus- ja reageerimisvõimekuse tasandil.[138] NCSI järgi on valimiriikide globaalne paremusjärjestus järgnev: Tšehhi 4. koht (92,21p), Eesti 5. koht (90,91p) ja Iirimaa 42. koht (63,64p).[139]



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
74.37	18.89	19.00	14.20	9.14	13.14

Source: ITU Global Cybersecurity Index v4, 2020

Tabel 3. Tšehhi riigi hindamistulemus GCI alusel.

Tšehhi puhul ilmneb Tabel 3-st, et GCI-s on väga kõrged hinded antud juriidiliste ning tehniliste meetmete rakendamise kohta.[140] NCSI järgi on riik kõrged hinded saanud küberturbepoliitika väljatöötamise, küberohtude analüüsi ja teabe ning hariduse ja professionaalse arengu valdkonnas. Eelnevalt on kirjeldatud riigi õigusakte ning on järeldatud, et Tšehhi on teinud enamatki, et üle võtta EL-i õigusakte ning kohaldada Liidu-üleseid standardeid küberturvalisuse valdkonnas.[141] Samuti on riigil olemas kehtiv ning põhjalik küberturvalisuse

[138] International Telecommunication Union. *Op cit.*
[139] National Cybersecurity Index. *Op cit.*
[140] International Telecommunication Union. *Op cit.*
[141] Vt lähemalt käesoleva töö II ptk.

strateegia ning selle rakendamise plaan. Riigi tugevuseks on kindlasti EL-i regulatsioonide järgimine, sest oluliste teenuste kaitse ja küberintsidentidele reageerimise tulemused on NCSI alusel maksimummääraga hinnatud.[142]

GCI järgi on antud riigi puudulikud valdkonnad koostöö ja võimsuse arendamine. Võimsus iseenesest ei ole ainuke määrav faktor et järeldada, kas riik on suutnud valmis olla selliseks kriisiks nagu COVID-19 ning selle mõjudele küberturvalisuse valdkonnas. Üldpildis on tegemist üsna kõrge hinnanguga, kuid riigil on arenguruumi nii koostöö valdkonnas kui ka ühiskonna teadlikkuse tõstmisel. Viimane valdkond aitab kaasa sellele, et näiteks töövõimeline elanikkond suudab ka kaugtöövormis tööd teha ilma tööandja süsteeme ohtu seadmata ning võimalikuks küberintsidendi ohvriks langemata. Ühesõnaga suudavad sellised meetmed nagu elanike teavitamine ning pidev valdkonna arendamine tagada riikidele hea ning efektiivse ennetus- ja reageerimisvõimekuse küberturvalisuse tagamiseks kriisi ajal.[143]

NCSI puhul mõjutavad Tšehhi üldtulemust negatiivselt panus ülemaailmsesse küberturvalisusesse, digiteenuste kaitse, e-identifitseerimis- ja usaldusteenused ning küberkriisi juhtimine. Kõige olulisemad märksõnad on siinkohal digiteenuste kaitse ning küberkriisi juhtimise puudulikkus. Kui vaadata lähemalt nende indikaatorite täitmist, siis üldtulemust vähendavad kaks indikaatori alakriteeriumi. Esiteks, avaliku sektori digiteenuste pakkujad peavad rakendama küber-/IKT turvanõudeid, mis on määratletud õigusaktidega või laialdaselt tunnustatud turvastandardit. Teiseks, vabatahtlike kasutamise kord küberkriiside ohjeldamisel ei ole küberturvalisuse valdkonnas kehtestatud õigusaktidega.[144]

Ühelt poolt tuleb toonitada, et NIS direktiiviga nähakse ette turvanõudeid ka digitaalsete teenuste osutajatele, kuid võib eeldada, et direktiivi definitsioon ja nõuded võivad olla digitaalse teenuste osutajate kohta ebapiisavad. Hinnates nende puuduste olulisust kõigi kuue esile toodud indikaatori valguses, on tegemist alla keskmise negatiivse mõjuga riigi toimetulekule küberohtudega. Kokkuvõttes on Tšehhi riigi tulemus kahe indeksi hindamise taustal olnud pigem hea. Välja arvatud ühe erisusega, mis on seotud suure küberrünnakuga haiglale, on pandeemia kestel tuldud toime nii erinevate meetmete rakendamisega kui ka küberturvalisuse valdkonnas tekkinud või tekkida võiva kahju ärahoidmisega. Üldkokkuvõttes näitavad GCI ja NCSI kõrged hinnangud riigi suutlikkust efektiivselt küberohte ennetada ja nendega toime tulla.

[142] National Cybersecurity Index. *Op cit.*
[143] International Telecommunication Union. *Op cit.*
[144] National Cybersecurity Index. *Op cit.*

See tähendab, et Tšehhi eelnev töö küberturvalisuse valdkonna reguleerimisel on olnud hea, pannes paika piisaval määral õiguskaitseinstrumente.

Estonia (Republic of)

Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Organizational, Cooperative Measures

Area(s) of Potential Growth
Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
99.48	20.00	20.00	20.00	19.48	20.00

Source: ITU Global Cybersecurity Index v4, 2020

Tabel 4. Eesti riigi hindamistulemus GCI alusel.

Eestile antud hinnang on GCI Tabel 4. alusel ligilähedane maksimaalsele. [145] Täissumma on saadud nii juriidiliste, tehniliste, organisatsiooniliste kui ka koostöömeetmete rakendamise eest. Selle hinnangu põhjal võib järeldada, et riik on täitnud enamiku kui mitte kõik kriteeriumid, et tagada küberturvalisuse kõrge tase ning luua suutlikkus küberohtude laiapindseks ennetamiseks kui ka neile reageerimiseks. COVID-19 kriis ei toonud suuri mõjutusi olulise tähtsusega teenuste valdkonnas, mistõttu võib pidada riigi valmisolekut väga heaks. Üle on võetud kõik Euroopa Liidu küberturvalisuse õigusliku raamistiku direktiivid ning tehtud enamatki selleks, et kaitsta riikliku tähtsusega teenuste operaatoreid. Ainuke hinnangut mõjutav osa on võimsuse arendamine, mille puhul jäi maksimaalsest punktisummast puudu vaid 0,42 punkti. Sarnaselt Tšehhiga ei saa seda asjaolu pidada määravaks, sest hindamisindikaator ei ole kriisiga toime tulemise hindamisel kõige olulisem.

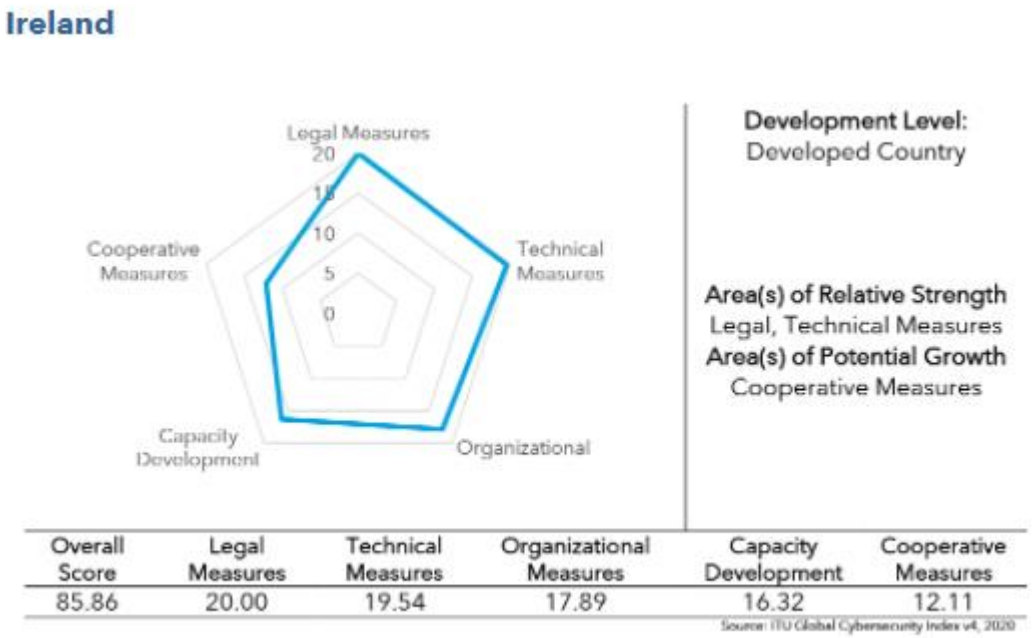
NCSI alusel on Eesti tulemus Tšehhist madalam. Eesti puhul on hindamistulemust negatiivselt mõjutanud järgnevad asjaolud:

- Ei ole koostatud riikliku tasandi küberturvalisuse strateegia rakendusplaani või muud samaväärset dokumenti.

[145] International Telecommunication Union. *Op cit.*

- Puudub doktorikraadi või samaväärse tasemega küberturvalisusele/elektroonilisele infoturbele keskendunud erialaprogramm.
- Puudub valitsusüksus, mille konkreetne ülesanne on võidelda küberkuritegevusega.[146]

Neid asjaolusid arvesse võttes on tegemist pigem vähesel määral mõju avaldavate hinnangutega. Eesti peamine miinus on see, et puudub küberturvalisuse strateegia rakendamisplaan, mida saaks edasiste strateegiate vastuvõtmisega lahendada. Teiselt poolt täidetakse küberturvalisuse strateegia olemasolu kriteerium. Lisaks on Eesti saavutanud kõigis kuues olulises valdkonnas maksimaalhinnangu. Kokkuvõttes võib Eesti tulemust kahe indeksi tulemusel pidada väga heaks. Väikeste muudatuste või ettepanekute puhul on tegemist siiski detailidesse langemisega. Üldpilt COVID-19 kriisiga toimetulemisel küberturvalisuse valdkonnas oli samuti väga heal tasemel. Suuremaid katkestusi oluliste teenuste toimimisel ei olnud ning on suudetud kiirelt reageerida ja kohaneda muutuvas olukorras. Eestile saab anda sama lõpphinnangu Tšehhiga ehk riigil on piisav võimekus ja suutlikkus küberohte ennetada ja nendega toime tulla.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
85.86	20.00	19.54	17.89	16.32	12.11

Source: ITU Global Cybersecurity Index v4, 2020

Tabel 5. Iirimaa riigi hindamistulemus GCI alusel.

Iirimaa olukord on veidi keerulisem ning kohati isegi vastuoluline. Tabel 5-st nähtub, et GCI alusel on antav hinnang pigem kõrge ja seda tagavad eelkõige juriidiliste ja tehniliste meetmete

[146] National Cybersecurity Index. *Op cit.*

täitmine.[147] NCSI indeksi puhul on riik maksimaaltulemuse saanud vaid küberintsidentidele reageerimise valdkonnas. Euroopa Liidu küberturvalisuse õigusliku raamistiku võttis riik täielikult üle ning kiidetavaks sai asjaolu, et loodud olid täpsemad juhised olulise teenuse operaatoritele küberturvalisuse nõuete täitmiseks. COVID-19 ajal aga ilmnes selge vastuolu ühe suurima tervishoiusektorit mõjutava küberrünnaku ohjeldamisel. Puudu oli nii personali teadlikkusest küberohtude ennetamisel kui ka oskustest reageerida, et kahjulikud tagajärjed kiirelt likvideerida. Tegemist oli küll konkreetselt ühe asutusega, kuid kriisi arvesse võttes märkimisväärse mõjuga riigi üleüldisele suutlikkusele. Indeksi alusel on riigil olemas põhjalik küberturvalisuse strateegia ning selle rakendamise plaan.

GCI järgi on Iirimaal puudused organisatsioonilistes meetmetes ning koostöö ja võimsuse arendamises. Eriti madal hinnang on saadud küberturvalisuse valdkonnas koostöö meetmete rakendamisel. NCSI indeksi puhul langetavad Iirimaa kokkuvõtlikku hinnangut miinused pea kõikides indikaatorites, välja arvatud isikuandmete kaitse ja küberintsidentidele reageerimise võimekus. NCSI kuue olulisema indikaatori alusel on välja toodud puudused järgnevad:

- Puudu on riikliku tasandi küberturbepoliitika koordineerimise komisjon, nõukogu, töörühm jne.
- Puudu on riikliku tasandi üksus, mis on spetsialiseerunud riiklikule strateegilisele küberohu olukorra analüüsile.
- Riikliku küberohu olukorra analüüsi avalikku osa ei avaldata vähemalt kord aastas.
- Avaliku sektori digiteenuste pakkujad ei rakenda küber-/IKT turvanõudeid või laialdaselt tunnustatud turvastandardit.
- Oluliste teenuste osutajad ei pea regulaarselt (vähemalt kord kolme aasta jooksul) esitama tõendeid küber-/teabeturbe poliitika tõhusa rakendamise kohta (nt auditi tulemus, dokumentatsioon, konkreetne aruanne).
- Valitsus ei ole kehtestanud suuremahuliste küberintsidentide jaoks kriisireguleerimisplaani.
- Valitsus ei ole viimase kolme aasta jooksul läbi viinud riikliku tasandi küberkriisiohje õppust või küberkomponendiga kriisireguleerimisõppust.
- Vabatahtlike küberturvalisuse valdkonna kasutamise kord ei ole kehtestatud õigusaktidega.[148]

[147] International Telecommunication Union. *Op cit.*
[148] National Cybersecurity Index. *Op cit.*

Kõik need on olulised asjaolud ja eeltingimused selleks, et riik suudaks küberturvalisuse kõrget taset hoida ka kriisi tingimustes. Iirimaa seadustes puudub nõue oluliste teenuste osutajatel viia läbi regulaarne audit. Eksisteerib vaid õigusaktis S.I. No. 360/2018 p 27. nõue turvalisuse hindamiseks, kus pädev asutus võib nende sektorite puhul, mille suhtes ta on määratud pädevaks asutuseks, läbi viia hinnangu, kas turvaauditi abil või muul viisil, oluliste teenuste osutaja poolt oma kohustuse täitmisest. Tegemist on pigem võimalusega kui kohustusega seda regulaarselt teha.[149]

Kokkuvõttes on Iirimaa tulemus kahe indeksi taustal riigi toimetuleku hindamisel pigem keskmine. GCI puhul ei saa üldiselt hinnangu üle suuri ja konkreetseid järeldusi teha, kuid koosmõjus NCSI-ga selgub, et puudujääke on mitmetes õigusaktides, kus oleks vajadus teatud nõuete lisamiseks. Samuti on strateegiliste tegevuste olematus tõenäoliselt halvendav riigi küberturvalisuse ennetus- ja reageerimisvõimekuse kvaliteedile. GCI ja NCSI hinnangud näitavad, et Iirimaal on suutlikkus küberohte ennetada ja nendega toime tulla, kuid selle tase on küsitav ning kohati etteaimamatult kehv, mõjutades seda, kas iga kriisi või küberohuga on võimalik siiski riigil lõplikult toime tulla.

Käesoleva magistritöö üks hüpoteesidest oli, et riiklikult oluliste teenuste tagamise häiritus on tugevas sõltuvuses riigi võimekusest rakendada olemasolevaid küberturvalisuse valdkonna meetmeid. Selles väites järeldus, et Euroopa Liidu siseselt oli riigiti ettevalmistus ja vastupanuvõime küberkuritegevuse tõusule väga erinev. Võib väita, et hüpoteesi sai osaliselt tõestada. Nimelt on läbi indeksites avaldatud hindamiskriteeriumite analüüsi tulemusel näha, mis osas on riigid nii Euroopa Liidu kui ka riiklike küberturvalisuse meetmeid rakendanud. Kuigi õigusaktid on normatiivsel kujul täielikult üle võetud, on näha teatud erinevusi riikide valikutes laiendada näiteks teenuse osutaja mõistet või luua kaasuvaid meetmeid, mis aitaks oluliste teenuste operaatoritel täita seadusest tulenevaid nõudeid. Veel enam saab oluliseks ka riikide strateegia ohjeldades COVID-19 ajal tekkinud küberründe. Selged erinevused on tulnud riikide ettevalmistuse kui ka reageerimise osas. Kuigi kriisieelne ja -järgne riikide õiguskord ning seega ka ettevalmistus ja vastupanuvõime ei olnud kõikides aspektides oluliselt erinev, on näha, et riiklikult oluliste teenuste häiritus on tugevas sõltuvuses sellest, mis meetmeid on vastu võetud ja mida lisaks kohaldatud.

[149] European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018– S.I. No. 360/2018.

Üldpildis on näha, et riigid tulevad toime Euroopa Liidu õiguslike regulatsioonide rakendamisega. Seda kinnitavad eelpool nimetatud siseriiklikud õigusaktid ning sellega kaasnevad meetmed. Siin on palju potentsiaali, kuidas vastav nõuete täitmine ning teadlikkus jõuaks kõikide olulisi teenuseid osutavate ettevõtete töötajateni. Olulist rolli hakkab siin lisaks õigusaktidele mängima ka riiklik strateegia ning võimekus koolitada küberturvalisuse spetsialiste, kelle ülesandeks on nõuete täitmisel tagada teenuste osutajate kõrge kvaliteet. Üldiselt on GCI ja NCSI indeksite koosmõjus paremusjärjestus järgnev: Eesti, Tšehhi ja Iirimaa. See tähendab, et riik, kus on olulised ja selged regulatiivsed meetmed ning ühtsed juhtimisstruktuurid, on näide tõhusast viisist oluliste teenuste küberturvalisuse kaitsmiseks COVID-19 ajal. EL saab anda endast parima, et luua õiguslik raamistik, kuid jagatud pädevuse kaudu on lõpptulemus liikmesriikide otsustada. See tähendab, et NIS direktiivi vastuvõtmisele pidid järgnema siseriiklikud õigusaktid, mis reguleerivad kõikehõlmavalt küberturvalisuse valdkonda. Selline lähenemine eeldab küberturvalisuse mõiste selget definitsiooni, oluliste teenuste kaitsmiseks kehtestatud piiritletud turvameetmeid ning laialdast koostööd erinevate küberturvalisuse sidusrühmade vahel riiklikul tasandil.

3.2. Euroopa Liidu küberturvalisuse õigusliku raamistiku vastupanuvõime ja areng peale kriisi

Euroopa Liidu küberturvalisuse õiguslik raamistik ja selle rakendamine on kollektiivsel tasemel vaid nii tugev, kuivõrd suudab nõrgim osapool piisava turvalisuse taseme saavutada. Selline väide on heaks lähtekohaks, millest tulenevalt hinnata Euroopa Liidu küberturvalisuse õigusliku raamistiku vastupanuvõimet COVID-19 kriisi ajal. Liit, mille ülesanne on määrata vaid riikide-ülesed nõuded küberturvalisuse valdkonnas, ei saa talle määratud pädevuste alusel siseneda otseselt iga riigi õigusesse selleks, et ette öelda, kuidas kohaldada ning rakendada antud õiguslikku raamistikku ning milliseid lisameetmeid vastu võtta. Jagatud pädevuse valdkonnas, kus Euroopa Liidul on vaid võimalus direktiivide näol valdkonda reguleerida, jääb liikmesriikidele palju otsustusruumi ja vastutust selleks, et tõestada küberturvalisuse õigusliku raamistiku vastupanuvõimet. Järgnevalt vaadeldakse, kas see raamistik toetas liikmesriikidel valimiriikide näitel ohjeldada kriisist tulenevat negatiivset mõju küberturvalisuse valdkonnas ning kas selle tagajärjel uuendati raamistiku põhimõtteid või seisukohti.

Euroopa Liidu õiguskaitsekoolituse agentuur väidab, et sobiva seisu loomiseks küberohtude tõkestamisel ehk piisava küberturvalisuse taseme loomiseks tuleb koostöös avaliku ja erasektoriga ning uurimisasutuste aktiivse ühistööga luua asjakohaste meetmete rakendamine

ja säilitamine. Selle eesmärk on nende sõnul varustada kaasatud institutsioonid, sh nende personal vahenditega, et tõkestada küberkuritegude katsete eskaleerumist ning arendada küberkaitsekultuuri. Vastuseks COVID-19 pandeemia ajal esinenud mustritele, peavad asjakohased õiguskaitse-alased koolitused tulevikus käsitlema uusi küberruumis esinevaid kuritegude toimepanemise viise nii pikas kui ka lühiajalises perspektiivis. Õiguskaitse seisab nende sõnul juba praegu silmitsi mitmete väljakutsetega seoses väljaõppesuutlikkuse puudumisega ning lünkade tõttu seadusandluses ja jurisdiktsiooni küsimustes. Ametlike õiguskaitseorganite raportite alusel esines pandeemia ajal tõrkeid küberkuritegude uurimise võimekuses, viibis kiire ja asjakohane teabevahetus ning lünklik oli kurjategijate õigeaegne tuvastamine.[150]

Seetõttu saavad eriti oluliseks eelmises alapeatükis käsitletud hindamisindikaatorid, mis käsitlevad erinevaid juriidilisi, tehnilisi ning organisatsioonilisi meetmeid ja võimekuste arendamist. Selleks, et teha üldistavaid hinnanguid Euroopa Liidu õigusliku raamistiku kohta, tuleb esmalt hinnata liikmesriikide võimekust läbi kolme aspekti. Esiteks, kas ja kuidas on üle võetud küberturvalisust käsitlevad Liidu õigusaktid. Teiseks, milliseid lisameetmeid on riigid loonud lisaks õiguslikule raamistikule. Kolmandaks, kas see õiguslik raamistik toetab seega kriisi ajal küberturvalisuse tagamist.

Vaadates riikide tegevusi seadusandluse muutmisel, mõjutas nende tegevust otseselt NIS direktiivi ülevõtmise kohustus siseriiklikusse õigusesse. Eelnevalt on selgitatud NIS direktiivis sisalduvad kohustuslikud elemendid ning direktiivi vastuvõtmise tagajärjel loodud õigusaktid valimiriikides. Veel enam hakkavad rolli mängima ka teiste oluliste sektorite direktiivid ning regulatsioonid Liidu tasandil. Käesoleva magistritöö raames oli näha erinevust elektroonilise kommunikatsiooni valdkonnas, kus sektorit käsitlev õigusakt lõi juurde rangemad või täpsemad normid siseriikliku õiguse täiendamiseks. Selline olukord peaks küberturvalisuse valdkonnas kindlasti erilist tähelepanu saama, et Liidu tasandil toimuks ühtlane koordineerimine küberturvalisuse nõuete määramisel. Antud soovituse taustal saaks NIS direktiiv olla nn katus kõikidele küberturvalisuse nõuetele sätestades, kas miinimumi või maksimumi, kuid otseselt piiramata valdkondlike täpsustuste tegemist. Vastupidine olukord, kus iga eraldiseisev õigusakt toob kaasa eraldiseisvad meetmed võib osutuda liikmesriikide jaoks nõuete rakendamise hetkel keeruliseks ning koormavaks.[151]

[150] Coman, I., Mihai, I. C. *Op cit*, lk 65-66.
[151] Vt lähemalt käesoleva töö I ptk.

Teisele küsimusele vastates ilmnevad teatud erisused lisameetmete kohaldamisel, kus mõni riik on otsustanud luua täiendavaid juhiseid või laiendada mõistete tähendusi. Kuivõrd EL-il ja liikmesriikidel on küberturvalisuse valdkonnas jagatud pädevus, on teatud erisused loogilised tekkima ja arusaadavad liikmesriikide perspektiivist. See tähendab, et soovitakse vastavalt riigi tasemele saavutada sobivaim õigusaktide kogum ning nõuete täitmine. Euroopa Liit peab aga suutma igakülgselt küberturvalisuse valdkonnas olulisi aspekte üheselt reguleerida, näiteks turvalisuse nõuete miinimumi, piiriülese koostöö ja mõistete ühtlustamise osas. Kui Liidul on soov küberturvalisust edaspidi eraldiseisva poliitikavaldkonnana käsitleda, on oluline võtta juhipositsioon valdkonna reguleerimisel. Antud põhimõtet EL-i üldisele lähenemisviisile toetab ka Eesti Majandus- ja Kommunikatsiooniministeerium. Fragmenteeritud turvanõuded või erinevad tõlgendused terminite osas võivad kaasa tuua valdkonna laialivalgumise ja seega jääb EL-i eesmärk valdkonna ühtsel reguleerimisel saavutamata.[152]

Kolmandas küsimuses on tähelepanu all eelnevalt mainitud ja täpsustatud õigusliku raamistiku olulisus liikmesriikide toetamisel küberturvalisuse valdkonna ohtudega tegelemisel olukorras, kus riike tabas COVID-19 kriis. Järeldus on, et kuivõrd NIS direktiivist tulenevad nõuded on saanud rakendust kriisi ajal, eriti vaadeldes sektoreid, kus toimus ulatuslikke küberründeid, on nii oluliste teenuse operaatoreid kui ka digitaalsete teenuste osutajaid käsitlevad nõuded saanud tähtsaks kriisi ajal liikmesriikide ennetus- ja reageerimisvõimekuse tagamisel. Siia lisanduvad NIS direktiivist tulenevad teised aspektid nagu CSIRT olemasolu eeldus, koostöö ja strateegiline valdkonna planeerimine riigi tasandil. “Küberrünnakud võivad olla demokraatiate ja majanduste stabiilsusele ohtlikumad kui relvad ja tankid. […] Küberrünnakud ei tunne piire ja keegi pole immuunne.” rõhutas Euroopa Komisjoni endine president Jean-Claude Juncker juba 2017. aastal. See on põhjus, miks EL ja liikmesriigid on küberturvalisuse väljakutsetele jõuliselt reageerinud. Loodud on mitmeid EL-i asutusi ning vastu võetud uusi õigusakte. See ei ole veel kõik, sest näiteks 2021. aastal lõi Euroopa Liit ka Liidu küberturvalisuse kompetentsikeskuse (ECCC), mis töötab koos riiklike koordineerimiskeskuste võrgustikuga (NCC). Selle peamine eesmärk on tugevdada Euroopa küberturvalisuse konkurentsivõimekust, et luua tugev võrgustik. Juurde tulevad mitmed teised direktiivid, mis tagavad Euroopa Liidu küberturvalisuse nõudeid ka teistes valdkondades (elektroonilise side seadustiku näitel) ning ENISA tegevuse tugevdamine, mille ülesanne on otseselt anda juhiseid riikidele ja ettevõtetele kriisi ajal küberohtudega toimetulemiseks. Seetõttu saab järeldada, et Liidu loodud ja riikide

[152] Majandus- ja Kommunikatsiooniministeerium. Sutt: EL küberturvalisuse tase peab vastama ohupildile. 2021. Kättesaadav arvutivõrgus: https://mkm.ee/uudised/sutt-el-kuberturvalisuse-tase-peab-vastama-ohupildile (16.04.2022).

poolt implementeeritud küberturvalisuse õiguslik raamistik on oluline lähtepunkt liikmesriikidele COVID-19 kriisist tulenevate küberohtude tõrjumisel ning seega toetab teoreetiliselt liikmesriike küberkriisidega toimetulemisel.[153]

Mis mõju aga avaldas COVID-19 kriis Euroopa Liidu edasisele tegevusele küberturvalisuse valdkonnas, mis puudutab õigusliku raamistiku tulevikku? Kuigi küberturvalisuse indekseid arvesse võttes suudeti anda teatav hinnang liikmesriikide ennetus- ja vastupanuvõimele kriisi hetkel, siis selle mõju ja ulatus võib kesta veel mitmeid aastaid. Seda kõike silmas pidades kerkib küsimus, kas COVID-19 on kaasa toonud ka ideelise muutuse EL-i küberturbepoliitikas või näeme selle asemel ideede ja poliitika järjepidevust tulevase küberkriiside ennetamisel. Carrapico ja Farrandi on jõudnud järeldusele, et kuigi pandeemial oli igapäevaelule ulatuslik mõju, ei toonud kriis kaasa toonud olulist diskursiivset nihet küberturvalisuses, vaid pigem tugevdas olemasolevaid narratiivseid suundumusi.[154]

Mis puudutab ühise küberturvalisuse valdkonna juhtimise võimalust riigiülesel tasandil, siis strateegiad, meetmed ja kavandatavad seadused, mis tõstavad esile EL-i kui küberturvalisuse valdkonnas aktiivse osaleja kasvavat potentsiaali, on märke EL-i ühisest otsusekindlusest ja pühendumusest, kirjeldavad Wolff ja Ladi. Eriti avaldub see potentsiaal küberturvalisuse teemade käsitlemisel EL-i kollektiivsel tasandil läbi demonstratsiooni, et EL ja selle liikmesriigid on huvitatud ja kaasatud ühistesse lähenemisviisidesse, koostöö- ja koordineerimisalgatustesse, sest päevakorras pannakse küberküsimustele üha enam rõhku. Wolff ja Ladi väidavad, et varasemate suundumuste kiirenemist võib märgata edasise integratsiooni (nt küberturvalisus) suunas, kuid see võib olla ka suurema natsionaliseerimise suunas (nt Schengen). COVID-19 kriis võimaldab aga ümber hinnata riigi rolli (nt hoolekande tagamisel ja rahvatervises). Seda võib vaadelda kui EL-i ja selle liikmesriikide vaheliste suhete küpsemist.[155]

Sarnane areng on suhete küpsemise näol toimunud ka küberturvalisuse valdkonnas, kus EL on teinud diskursiivse nihke sotsiaalmeedia platvormide ja nende rolli suhtes COVID-19

[153] Giantas, H. D., Liaropoulus, N. A. *Op cit*, lk 23-24.
[154] Carrapico, H., Farrand, B. Discursive continuity and change in the time of Covid-19: The case of EU cybersecurity policy. Journal of European Integration, 42(8), 1111–1126. 2020, lk 1. Kättesaadav arvutivõrgus: https://www-tandfonline-com.ezproxy.utlib.ut.ee/doi/full/10.1080/07036337.2020.1853122 (7.02.2022).
[155] Giantas, H. D., Liaropoulus, N. A. *Op cit*, lk 24; Wolff, S., Ladi, S. European Union Responses to the Covid-19 Pandemic: Adaptability in times of Permanent Emergency. Journal of European Integration, 42(8), 1025–1040. 2020. Kättesaadav arvutivõrgus: https://www.tandfonline.com/doi/full/10.1080/07036337.2020.1853120 (7.02.2022).

puudutava desinformatsiooni levitamisel. See diskursus on olnud kohal alates varasematest kriisidest, näiteks Cambridge Analytica skandaal, ja seega on see taas võetud endiste diskursuste kiirenemisena, mis on nüüdseks normaliseerunud.[156] Liidu tasandil ja sh liikmesriikides on äärmiselt oluline aru saada juba eelnevalt mainitud erinevate sektorite koostööst ja nende olulisusest võideldes küberkuritegevuse vastu. Kriisid peaksid suutma luua poliitilisi muutusi, eriti võttes arvesse COVID-19 kriisist ilmnenud küberohte. Ka need võivad põrkuda kuritegevuse ja eetiliste probleemide piiril. Konkreetselt desinformatsioon ei ole vastunäidustatud küberkuritegevuse sildi all, kuid see võib luua ohtlikke situatsioone, mis võivad kaasa tuua ulatuslikke ründeid võrgu- ja infosüsteemide vastu. Üks selline näide puudutas vandenõuteooriaid 5G ja COVID-19 seoste kohta, mis omakorda viis selleni, et sagenesid küberründed telekommunikatsiooni infrastruktuurile.[157]

Carrapico ja Farrandi järeldus on, et veebipõhise desinformatsiooni levik on kaasa toonud küberturvalisuse tagamisega seotud eri osalejate usalduse lõhenemise, sest sotsiaalmeedia platvormid ei jaga Liidu ametkondade arvates EL-i sõnavabaduse ja desinformatsiooniga seotud väärtusi. Erinevat lähenemisviisi sotsiaalmeedia platvormidele rõhutatakse ka 2020. aastal väljastatud Euroopa Liidu Nõukogu järeldustes meediapädevuse kohta pidevalt muutuvas maailmas. Siin liigitatakse veebiplatvormide pakkujad ekspertidest ja riiklikest ametiasutustest eraldi, kusjuures need platvormid on Nõukogu arvates osa desinformatsiooni ohust ja seetõttu esitatakse platvormidele rangemad nõuded läbipaistvuse ja vastutuse tagamiseks. EL-i küberturvalisuse valdkonna filosoofia ning sellest tulenevate programmide ja poliitikatasandite lahknevuste keskmes on seega muutuv arusaam erasektori ettevõtete rollist. COVID-19 puudutava desinformatsiooni suurenenud levik 2020. aastal loonud aluse pigem poliitika järjepidevusele kui katkemisele, suurendades muret seoses sotsiaalmeediaplatvormide rolliga ja rõhutades neid olevat ebakindluse allikaks võrreldes küberturvalisuse lahenduste erapakkujatega, keda peetakse jagavat EL-i huve ja väärtusi.[158]

EL-i kohanemisvõime kriisidega on poliitikavaldkondade lõikes erinev, näidates seega erineval määral suutlikkust või isegi vajadust poliitikat muuta. Kohanemisvõimet on määratletud kui valitsuste võimet muuta poliitikat, kui seda peetakse vajalikuks. Kriisi ajal hinnatakse sageli poliitika kohanemisvõimet, kuid stabiilsust võib mõnikord pidada selliste institutsioonide, näiteks EL puhul oluliseks võimeks olla vastupidav. Kriisidega silmitsi seistes võib teatav

[156] Carrapico, H., Farrand, B. *Op cit*, lk 2.
[157] Gogou, V., Dekker, M. *Op cit*.
[158] Carrapico, H., Farrand, B. *Op cit*, lk 9-11.

järjepidevus rahustada erinevaid sidusrühmi, kuid pidev muutus tekitada segadust. Näiteks pole pärast COVID-19 kriisi puhkemist EL-i kliimapoliitikas suuri samme astutud, kuid seda poliitika järjepidevust võib pidada positiivseks arenguks, kuna kliima- ja keskkonnapoliitika seisukohtades taandutakse sageli kriiside ajal. Euroopa rohelise kokkuleppe tugevdamist pandeemiaga võitlemisel võib vaadelda kui head kohanemisvõimet kriisiga. Sellest on järeldatud, et COVID-19 ei ole häirinud küberturvalisuse kihistumise protsessi. See tähendab, et EL-i küberturvalisuse õigusliku raamistiku kujunemine alates ühtse kaitse- ja julgeolekupoliitikast kuni eraldiseisva EL-i küberturvalisuse poliitikani on üles ehitatud ideede ja õigusnormide järkjärgulise arenguga. Kuigi küberturvalisuse alusfilosoofia tasandil muutusi toimunud ei ole, on aga tegemist olulise nihkega, mis tuleneb enne COVID-19 kriisi tõusnud küberturvalisuse ohu tasemest.[159] EL on läinud üle formaalsemale õiguse reguleerimisele, mida iseloomustab siduvate vahendite ja spetsiaalse poliitikavaldkonna loomine. Selline õiguslike meetmete abil loodud küberturvalisuse valdkonna kaitse aitas EL-i sõnul näiteks kiirendada sotsiaalmeedia partnerite tuvastamist osana probleemidest, kuigi selle tagajärjel ei toimunud suurt diskursiivset nihet küberturvalisuse valdkonna reguleerimisel.[160]

Ühiskonna arenev digitaalkeskkond ja COVID-19 kriis on aga esile toonud EL-i küberturvalisuse valdkonnas ka uusi väljakutseid. Üks peamisi probleeme, mis on ilmnenud seoses oluliste teenuste osutajatega, on suur sõltuvus digitaalsetest infrastruktuuridest ja võrgusüsteemidest ning tungiv vajadus tagada tarneahelate vastupidavus ja usaldus, kuna sellel on suur mõju riiklikule ja majanduslikule julgeolekule, rahva tervisele ja ohutusele. Lisaks muudavad üha enam ühendatud IKT-infrastruktuurid, IoT ja tööstus 4.0 kaudu ühendatud seadmete arv, 5G võrkude kasv ja andmekeskne maailm tarneahelad üha globaalsemaks. Kodanikud ja ettevõtted peavad saama usaldada nende poolt kasutatavaid tooteid, mis omakorda loob vajaduse kehtestada tarneahela küberturvalisuse juhtimisega seotud riiklikuid regulatsioone. Tarneahela haavatavused võivad avaldada astmelist mõju mitmetele kriitilistele infrastruktuuridele ja teenustele. Eesti riigi küberturvalisuse taset ja Euroopa Liidu uusi suundi kommenteerides ütles RIA õigusosakonna juhataja Silver Lusti järgmist: “Kuivõrd COVID-19 andis tugeva tõuke digitaliseerimise suunas ja lahendusi oli vaja leida väga kiirelt, ilma pikemate analüüsideta, tingis see paljudel juhtudel ka pigem kehva küberturvalisuse taseme. Eesmärk on endiselt tõsta EL-i üleselt küberturvalisuse baastaset ja hetkel selle nimel palju

[159] Vt lähemalt käesoleva töö I ptk.
[160] Wolff, S., Ladi, S. *Op cit*, lk 1034; Carrapico, H., Farrand, B. *Op cit*, lk 5.

keskendutaksegi tarneahelatele ja laialdasemalt NIS 2.0 vaates skoobi laiendamisele, et rohkem sektoreid oleksid kohuslased."[161]

Et reageerida digitaliseerimisest tulenevatele kasvavatele ohtudele ja küberrünnakute arvu suurenemisele esitleti 16. detsembril 2020. aastal EL-i uut küberturvalisuse strateegiat koos kahe seadusandliku ettepanekuga: võrgu- ja infosüsteemide turvalisust käsitleva direktiivi 2016/1148 (NIS2) läbivaatamine ja uus direktiiv kriitiliste üksuste vastupidavuse kohta (CER). 2021. aastal esitas Euroopa Komisjon konkreetse õigusliku ettepaneku asendada NIS direktiiv, et seeläbi tugevdada turvanõudeid, käsitleda tarneahelate turvalisust, ühtlustada aruandluskohustusi ja kehtestada rangemad järelevalvemeetmed ja jõustamisnõuded, sealhulgas ühtlustatud sanktsioonid kogu EL-is. Komisjoni sõnul on NIS2 tulekuga olulist rolli mänginud COVID-19 pandeemia, mis vallandas digitaalsete harjumuste ümberkujundamise ja selle ettenägematu kiirenemise ühiskondades üle maailma. Kuid see on süvendanud ka olemasolevaid probleeme, nagu digitaalne lõhe, mis aitas kaasa küberturvalisuse intsidentide ülemaailmsele kasvule.[162]

Komisjon avalikustas NIS direktiivi hindamisel järeldused mitmeid probleemseid järeldusi. Näiteks ei anna õigusakt piisavalt selgust OTO-de ulatuse kriteeriumite või riiklikku pädevuse osas. See on viinud nende sõnul olukorrani, kus teatud tüüpi üksusi pole mõnes liikmesriigis tuvastatud ja seetõttu ei pea nad võtma kasutusele turvameetmeid ega teatama küberintsidentidest. Näiteks mõnes liikmesriigis ei kuulu suuremad haiglad direktiivi reguleerimisalasse ja seega ei pea rakendama turvameetmeid. Olgugi, et pea iga tervishoiuteenuse osutaja kuulub NIS direktiivis välja toodud olulise teenuse üksusesse. Samuti andis direktiiv liikmesriikidele turvalisuse ja vahejuhtumite nõuete kehtestamisel laia kaalutlusõiguse OTO-de aruandlusnõuete järgimisel. Hindamine näitas, et mõnel juhul on liikmesriigid neid nõudeid rakendanud oluliselt erineval viisil, tekitades täiendava koormuse rohkem kui ühes liikmesriigis tegutsevatele ettevõtetele. Probleeme leiti ka direktiivi järelevalve- ja jõustamisrežiimil ning liikmesriikide-vahelises koostöös.[163]

[161] Euroopa Komisjon. - Study to support the review of Directive (EU) 2016/1148. 2021, *Op cit*, lk 24; S. Lusti an E. Pilliroog. *Op cit*.
[162] Euroopa Parlament. The NIS2 Directive: A high common level of cybersecurity in the EU. Briefing. 2021, lk 6. Kättesaadav arvutivõrgus: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (24.04.2022).
[163] *Ibidem*.

NIS 2-s on seega kaalutud ettepanekute hulgas järgmised kolm põhiteemat:

1. Soov suurendada paljude EL-is tegutsevate ettevõtete kübervastupidavuse taset kõigis olulistes sektorites sh kehtestades eeskirjad, mis tagavad, et kõik avaliku ja erasektori üksused kogu siseturul, mis täidavad olulisi majanduse ja ühiskonna kui terviku jaoks vajalikke funktsioone, peavad kasutusele võtma piisavad küberturvalisuse meetmed.
2. Vähendada vastupanuvõime ebakõlasid siseturul direktiiviga juba hõlmatud sektorites, ühtlustades veelgi *de facto* kohaldamisala, turvalisuse ja intsidentidest teatamise nõuded, siseriiklikku järelevalvet ja jõustamist reguleerivad sätted ning liikmesriikide asjaomaste pädevate asutuste võimalusi.
3. Parandada ühise olukorrateadlikkuse taset ning kollektiivset ettevalmistus- ja reageerimisvõimet. Võttes vastu meetmeid pädevate asutuste vahelise usalduse suurendamiseks. Jagades rohkem teavet ning reeglite ja protseduuride kehtestamine ulatusliku intsidendi või kriisi korral.[164]

Ettepanekud on igati asjakohased, sest ka käesolevas uurimuses on täheldatud NIS direktiivi erinevat rakendamist ning seetõttu turvanõuete kohaldumiste erinevusi. Toetuda puhtalt NIS kehtivas direktiivis loetletud oluliste teenuse operaatorite üksustele vajab kiiresti muutuva kübermaailma mõistes uuendamist. Vajalik oleks rohkem ühtlustada kaitset elektroonilise kommunikatsiooni ettevõtetele, kaasates neid oluliste teenuste operaatorite loetelus. Kuigi elektroonilise side seadustik püüab turvalisuse elemente täpsustada rangemalt, ei ole tegemist ühtse Liidu-tasandi lähenemisega. Mitmel juhul viitabki NIS2 muude õigustekstide sätetele, nagu näiteks direktiiv 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (EECC). Mõned selle direktiivi sätted on uue NIS2-ga tunnistatud kehtetuks, näiteks EECC artiklid 40 ja 41 turvalisuse kohta. Kavandatav direktiiv tunnistaks seega kehtetuks vastavad EECC turvasätted ja reguleeriks täielikult elektroonilise kommunikatsiooniteenuse pakkujate turvalisust.[165]

Üheks plaanitavaks muudatuseks oleks ka ENISA vastutusvaldkondade laiendamine, sest ametil on oluline roll NIS direktiivi rakendamise järelevalves. Esiteks tehakse ametile

[164] Euroopa Parlament. The NIS2 Directive: A high common level of cybersecurity in the EU. Briefing. 2021, lk 7.

[165] Opinion of the European Economic and Social Committee on 'Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 and Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities' (COM(2020) 823 final lk 286/175. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020AE5749&rid=8 (24.04.2022) ; Euroopa Parlament. *Op cit*.

ülesandeks koostada iga kahe aasta järel aruanne küberturvalisuse olukorra kohta EL-is ja pidada Euroopa haavatavuse registrit. Registri eesmärk oleks pakkuda juurdepääs teabele, mis on seotud IKT-toodete ja -teenuste haavatavuste kohta, mille tagavad vabatahtlikkuse alusel hädavajalike ja oluliste teenuste üksused ja nende IKT-tarnijad. Teiseks oleks ENISA kohustatud looma ja haldama ka registrit, kuhu kuuluvad üksused nagu näiteks domeeninimesüsteemi teenusepakkujad, tipptaseme domeeninimede registrid, pilvandmetöötlusteenuse pakkujad, andmekeskuse teenusepakkujad, sisuedastusvõrgu pakkujad, veebiturud, veebiotsingumootorid ja suhtlusvõrgustikud. Sellises üksused peavad ametile teatama informatsiooni sellest, millises EL-i liikmesriigis nad on asutatud. Selle eesmärk on tagada, et eelpool nimetatud asutused ei peaks silmitsi seisma mitmete erinevate õiguslike nõuetega, võttes arvesse asjaolu, et nad osutavad suurel määral piiriüleseid teenuseid.[166]

NIS2 taustal on aga veel käsitlemata, milliste meetmete abil saaks paremini kaitsta alaealisi, eriti olukorras, kus nende igapäevane sõltuvus internetiteenustest on märgatavalt suurenenud. Näiteks on ITU maininud GCI 2020. aasta raportis, et laste võrgus kaitsmise mehhanismide väljatöötamine peab olema riikide elutähtsate prioriteetide hulgas. Kuigi internet toob laste haridusele ja kasvule märkimisväärset kasu, loob see neile võimaluse ka kokku puutuda võrguriskidega. Enamik riike on võtnud kasutusele algatusi laste võrgukaitse toetamiseks, näiteks luues veebisaite ja sotsiaalmeediakanaleid spetsiaalsete õppematerjalide, teabemängude ja juhenditega lastele, vanematele ja õpetajatele. Välja on pakutud ka riiklike küberturvalisuse teadlikkuse strateegiad, mis saaksid olla osa NIS direktiivis nõutud küberturvalisuse strateegiast. Äärmiselt oluline on, et strateegilised meetmed oleksid mingil kujul turvanõuetena rakendatud ka ettevõtete suhtes, kes oma digitaalseid teenuseid alaealistele suunavad.[167]

Euroopa Liidu majandus- ja sotsiaalkomisjon ütles olulised märkused kommenteerides 2019. aasta küberturvalisuse määruse vastuvõtmist. Komisjon mainis, et ükski õiguslik raamistik pole suutnud kaasas käia digitaalse innovatsiooni arengu kiirusega, mistõttu probleeme lahendatakse ükshaaval õigusaktide kaupa. Selline näide tuleneb hästi välja, kui vaadelda Euroopa Liidu tegevust. Vastu on võetud erinevad õigusmõjuga ning otseselt või kaudselt küberturvalisust

[166] Euroopa Parlament. *Op cit*, lk 8.
[167] International Telecommunication Union. *Op cit*, lk 23; AlShabibi, A., Al-Suqri, M. Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. 2021 22nd International Arab Conference on Information Technology (ACIT), 2021. Kättesaadav arvutivõrgus: https://ieeexplore-ieee-org.ezproxy.utlib.ut.ee/document/9677117 (24.04.2022).

käsitlevaid õigusakte: elektroonilise side seadustik, GDPR, NIS direktiiv, e-IDAS määrus[168]. Komisjon andis sellega kriitilise hinnangu EL-i küberturvalisuse õiguslikule raamistikule ning võimekusele ka edaspidi toime tulla suuremahuliste küberrünnakutega. Selle probleemi lahenduseks saab pidada uusi põhjalikke õiguslikke meetmeid ning liikmesriikide suhtes tehtavat süvaanalüüsi EL-i meetmete rakendamisest. Positiivne on, et selline tegevus näitab EL-i tsentraliseeritud lähenemist küberturvalisuse reguleerimisele, mille mõjul saab saavutada edaspidi liikmesriikide efektiivse vastupanuvõime küberohtudele ja sellega saaks jätkuvalt tagada ka EL-i lepingu art 13 ja art 21 alusel õigusliku järjepidevuse ning efektiivsuse seadusandlike aktide vastuvõtmisel.[169]

Euroopa Komisjon soovib eelnevalt välja toodud NIS2 muudatustega suurel määral täiendada senist Euroopa Liidu küberturvalisuse õiguslikku raamistikku. Hetkel on aga tegemist vaid ettepanekutega ning reaalsed läbirääkimised on veel ees. Lõplike tulemuste puhul saab määravaks nii liikmesriikide enda ettepanekute mõju ja üldise konsensuse saavutamine. Kindlasti tuleb suurel määral arvestada õigusliku raamistiku täiendamisel ka COVID-19 kriisist tulenevaid õppetunde ja seada eesmärgiks, et uued meetmed kajastuksid loodavates õigusmuudatustes. Olenemata, et teatud eelarvamused säilivad erasektori rollist küberturvalisuse tagamisel, on EL siiski astunud sammu edasi ja püüdnud kasvõi osaliselt kriisist tulenevaid mõjusid kajastada NIS2 muudatustes. Kuigi juriidiliste muudatustega võetakse üks suund turvalisuse taseme tõstmiseks, saab palju veel teha seoses elanikkonna harimisega küberohtude mõjust. Euroopa Liidu ülesanne on seda valdkonna püüda võimalikult üheselt mõistetavalt koordineerida ning samaaegselt abistada liikmesriike nendele pandud ülesannetes. Vaid selliselt saab tagada võrgu- ja infosüsteemide kõrge kaitse ning vastupidavuse küberruumis kriisiolukorras.

[168] eIDAS on e-identimise ja e-tehingute jaoks vajalike usaldusteenuste määrus, mille eesmärk on lihtsustada piiriülest e-teenuste kasutamist.

[169] Edegbeme- Belaz, A. The changing role of the EU in cybersecurity. ResearchGate. 2019, lk 25. Kättesaadav arvutivõrgus: https://www.researchgate.net/publication/334173763_The_changing_role_of_the_EU_in_cybersecurity (24.04.2022).

KOKKUVÕTE

2020. aastal alanud ülemaailmne COVID-19 kriis ei piirdunud vaid majandusliku või ühiskonna negatiivse mõjutamisega. Iga eluvaldkond ning süsteem sai proovile pandud seoses suurenenud digitaalkasutusega ning ulatuslike sulgemismeetodite rakendamisega. Magistritöö eesmärk oli uurida, kuivõrd mõjutas kriis küberturvalisuse valdkonna süsteeme ning eelkõige riikliku tähtsusega teenuste osutamissuutlikkust, analüüsides Euroopa Liidu liikmesriikide ennetus- ja reageerimisvõimekust.

Enne COVID-19 kriisi algust võttis Euroopa Liit vastu mitmeid õigusakte ning meetmeid, luues esimese selletaolise küberturvalisust käsitleva õigusliku raamistiku. Kuivõrd Euroopa Liit käsitleb võrgu- ja infosüsteemide direktiivis oluliste teenuste kaitsmist ja tugevdab läbi küberturvalisuse määruse Liidu-ülest koostööd, sai oluliseks hinnata liikmesriikide enda panust ning võimekust tõrjuda kriisi ajal esinenud küberintsidentide kasvu. Liikmesriikide analüüsi valimisse kuulusid kolm riiki: Eesti, Tšehhi ja Iirimaa.

Magistritöös analüüsiti esimese uurimisprobleemina liikmesriikide õiguse vastavust Euroopa Liidu küberturvalisuse õigusliku raamistikule. Euroopa Liit on loonud mitu strateegiat, mille üheks eesmärgiks on luua ühtne küberturvalisuse õiguslik raamistik. NIS direktiivi ja küberturvalisuse määruse loomisega on Euroopa Liit kindlustanud oma rolli võtmemängijana küberturvalisuses luues liiduüleseid nõudeid võrgu- ja infosüsteemide kaitseks võimalike küberohtude eest. Enne COVID-19 kriisi olid need õigusaktid võetud liikmesriikide poolt üle siseriiklikusse õigusesse. See tähendab, et riikidel oli piisavalt aega, et valmistada ette meetmed hädavajalike teenuste kaitsmiseks küberohtude korral.

Käesoleva magistritöö peamine analüüs viidi läbi tervishoiu ja elektroonilise kommunikatsiooni sektori osas. Selle käigus leiti, et COVID-19 kriis mõjutas neid sektoreid ulatuslikult. Haiglate vastu toime pandud küberrünnakud ning desinformatsiooni kampaaniad panid küberturvalisuse jaoks loodud õiguskaitsevahendid proovile. On järeldatud, et liikmesriigid võtsid NIS direktiivi täielikult üle siseriiklikusse õigusesse vähemalt minimaalse ühtlustamise põhimõtte alusel. Liikmesriikide puhul on nähtav erinevus selles, kuidas on lähenetud küberturvalisuse reguleerimisele siseriiklikus õiguses. Eesti puhul valiti küberturvalisuse reguleerimiseks kõikehõlmav viis. See tähendab, et küberturvalisuse seadus on peamine allikas turvanõuete jaoks ning antud akt loob otsesed seosed teiste õigusvaldkondadega. Kuigi näiteks elutähtsate teenuste käsitlemiseks on loodud teisi seaduseid, on seda siiski käsitletud ka küberturvalisuse seaduses. Oluline on mainida, et kaasnevad

meetmed on liikmesriikidel aidanud direktiivi paremini üle võtta, näiteks Tšehhi puhul põhjalik mõjukriteeriumite määratlus ja Iirimaa puhul NIS-i vastavusjuhised oluliste teenuste osutajate määratlemisel. Kokkuvõttes saab väita, et liikmesriikide siseriiklik õigus vastab Euroopa Liidu poolt loodud küberturvalisuse õiguslikule raamistikule.

Teiseks uurimisprobleemiks oli, kas eelnevalt nimetatud Euroopa Liidu küberturvalisuse õiguslik raamistik toetab liikmesriikide võimekust lahendada kriisi ajal küberohust tingitud probleeme riiklikult oluliste teenuste osutamisel. Probleemi lahendamisel tehti kõigepealt ülevaade valimiriikide oluliste teenuste osutajatele kehtivatest nõuetest ja uuriti, kas oli ka mingeid konkreetseid erinevusi NIS direktiivi ülevõtmisel siseriiklikusse õigusesse. Kuivõrd kõik direktiivi olulised elemendid olid kohaldatud, nagu näiteks oluliste teenuste osutajate defineerimise eeltingimused, neile kehtivad turvanõuded, küberintsidentidest teavitamise nõuded ja regulaarse riskianalüüsi teostamine, siis järeldub, et on tehtud piisavalt küberturvalisuse ennetusvõimekuse saavutamiseks. Kui seda kõrvutada COVID-19 kriisi reaalse mõjuga ning suuremate intsidentidega järeldus, et kuigi Euroopa Liidu küberturvalisuse õiguslik raamistik toetab liikmesriike teoreetiliselt küberohtude tõrjumisel, siis esinevad probleemid oluliste teenuste operaatoritele kehtestatud nõuete täitmisel. Siin esines näiteid nii puudulikust personalist ja spetsialistidest ning ka võimekusest küberintsidente tuvastada ning neile vastavalt reageerida. Seega ei ole probleem niivõrd liikmesriikide õigusaktides kuivõrd nende kohases rakendamises.

Teise uurimisprobleemi raames kontrolliti ka kahe hüpoteesi vastavust eeldustele. Selgus, et riiklikult oluliste teenuste tagamise häiritus on tugevas sõltuvuses konkreetse riigi võimekusest rakendada olemasolevaid küberturvalisuse valdkonna meetmeid. Paika ei pea väide, et riikide ettevalmistus ja vastupanuvõime küberturvalisuse ohu tõusule oli väga erinev. Seda seetõttu, et kõikidele valimiriikidele kehtivad ühesugused nõuded. Tõepoolest, teatud erinevusi võis märgata siseriiklike õigusaktide kohaldamisel, kuid need erinevused rakendamises ei olnud määravad oluliste teenuste tagamisel. Esitatud oli ka hüpotees, et Euroopa Liidu küberturvalisuse õiguslik raamistik oli piisav, et tagada ettevalmistus küberintsidentide teoreetiliseks ohjeldamiseks, kuid liikmesriigid ja erinevad asutused ei olnud võimelised neid küberturvalisuse nõudeid vastavalt rakendama. Töö käigus selgus, et esitatud hüpotees osutus tõeseks, kuid erinevus tekkis liikmesriikide ja erinevate asutuste võimes küberturvalisuse nõudeid rakendada. Siinkohal on liikmesriigid teinud juba piisavalt, et nõudeid rakendada, kuid näiteks oluliste teenuste operaatorite puhul on küsitav, kas esiteks, nad on teadlikud sellest, et nad kuuluvad antud klassifikatsiooni alla ning millised nõuded neile sellest tulenevalt

kohalduvad. Ka NIS direktiivi rakendamist käsitlenud uuring selgitas, et näiteks mõned haiglad ei suutnud ennast defineerida olulise teenuse osutajana, kuigi tervishoiusektor on selleks üksuseks nimetatud. Olulist rolli mängisid ka riikide küberturvalisuse indeksite hinnangud, mis osutasid puudujääkidele küberkriisidega toime tulemisel.

Lisaks oli töös esitatud hüpotees, et Euroopa Liit ei uuendanud kriisi mõjul küberturvalisuse valdkonnas kehtivaid seisukohti, vaid kiirendas varasemate ettepanekute elluviimist. Antud hüpotees pidas vaid osaliselt paika. Töös järeldati, et säilinud on Euroopa Liidu hoiakud erasektori suhtes, eriti mis puudutab sotsiaalmeediaettevõtteid. COVID-19 kriisiga tõusis küberruumis esile desinformatsiooni negatiivne mõju, mis avaldus nii virtuaalses kui ka füüsilises ruumis ning võis seada ohtu inimeste elusid ja tõkestada kriitiliselt tähtsa informatsiooni edastamist. Samas on Euroopa Liidul teatud eeldus usaldada vaid otseselt küberturvalisuse teenuseid osutavaid ettevõtteid, kuigi näiteks desinformatsiooniga võitlemisel oleks pidanud tegema suuremat koostööd sotsiaalmeediaettevõtetega. Hüpotees ei pidanud aga paika NIS direktiivi muutmise valguses. Hetkel Euroopa Liidus arutlusel olev NIS2 on näidanud, et proovitakse käsitleda ka COVID-19 kriisist tulenevaid negatiivseid mõjusid. Siinkohal on eriti oluliseks lähtepunktiks liikmesriikide enda kogemused, näiteks tarneahelate haavatavuste käsitlemine, oluliste teenuste loetelu ülevaatamine elektroonilise side seadustiku vastuvõtmise osas, küberintsidentidest teavitamise nõuded ja tugevamad järelevalvemeetmed.

Lisaks hüpoteesidele ilmnevad ka probleemid, kui uurida EL-i kompetentsi küberturvalisuse valdkonna reguleerimisel. Seda valdkonda ei ole otseselt mainitud Euroopa Liidu eraldiseisva pädevusena, vaid see tuleneb kaudselt hoopis Euroopa Liidu lepingu ühisest välis- ja julgeolekupoliitikast või vabadusel, julgeolekul ja õigusel rajaneval alast, sest Euroopa Liidu lepingu artiklites pole küberturvalisust otseselt mainitud. Euroopa Liidu ainus võimalus on kasutada pädevuse andmise põhimõtet ning seega peab igas õigusaktis olema kindel selgitus selle kohta, miks Euroopa Liit on antud küsimuses kompetentsem tegutsema kui liikmesriigid eraldi. On selge, et antud olukord tekitab suurema probleemi, sest küberturvalisuse õiguslikul raamistikul on sellises olukorras suur oht killustuda. Ettepanek on küberturvalisuse *expressis verbis* määratlemiseks Euroopa Liidu lepingus. Selline käik võiks olla vastuseks mõningatele kujunenud probleemidele. Kuigi tegu on keerulise protsessiga, on see vajalik samm pidevalt muutuvas digitaalses maailmas loomaks ühtset küberturvalisuse õigusliku raamistikku. Vastasel juhul saab Euroopa Liit jätkata ainult senisel viisi, kasutades teistes valdkondades olevaid pädevusi ning võttes vastu nn pehmeid seaduseid.

Samuti on ebaselge küberturvalisuse määratlemine nii Euroopa Liidu õigusaktides kui ka liikmesriikide sisemiselt. NIS direktiivi abil määratles Euroopa Liit võrgu- ja infosüsteemide turvalisuse. Küberturvalisust on mainitud ainult seetõttu, et see on rahvusvahelise koostöö jaoks olulise tähendusega. Kuigi küberturvalisuse määrus, mis defineerib küberturvalisuse mõistet, võeti vastu 2019. aastal, pole see kooskõlas NIS direktiivis käsitletava turvalisuse selgitusega. Näiteks kasutasid mõned liikmesriigid NIS direktiivi, et reguleerida küberturvalisuse valdkonda laiemalt, piirdumata ainult võrgu- ja infosüsteemidega. Erinevus seisneb selles, et ühe puhul käsitletakse turvalisust seisundina, kus süsteemid suudavad tekkinud ohtudele vastu seista ning teise puhul on tegu süsteemide kaitsmiseks vajalike tegevustega. Lahenduse antud probleemile võib leida Eesti näitel, kus on võimalik eristada küberturvalisust ja küberturvet. Eesti keeles lähtub termin küberturvalisus direktiivis mainitust ning termin küberturve küberturvalisuse määrusest. Mõlemad terminid on üksteisest läbi põimunud ning üks ei pruugi välistada teist. Ingliskeelsetes tõlgetes on sellist erinevust raske välja tuua, sest küberturvalisus ja -turve on sama kirjapildiga, kuid arvestades mõistete selget seost, pole see võimatu. Õigusselguse huvides on terminite ühtlane defineerimine vajalik.

Magistritöö tulemusel selgus, millised probleemid esinevad küberturvalisuse mõiste käsitlemisel ja Euroopa Liidu õiguslikes pädevustes. Kuigi töös sai pakutud Eesti näitel üks võimalus küberturvalisuse mõiste sisustamiseks, on eelkõige oluline, et selline algatus tuleneks Euroopa Liidu õigusaktidest. Töös esitleti ka võimalusi, kuidas saab rakendada praktiliselt küberturvalisuse indekseid, et arendada riigi võimekusi antud valdkonnas, mille raames tuleb muuta ka siseriiklikke õigusakte. Käesoleva magistritöö järeldusest võiks kasu olla ka NIS2 direktiivi läbirääkimistel, pöörates eriliselt tähelepanu oluliste teenuste operaatoritele kehtivate normide täiustamisele. Samuti tuleks lähemalt veel uurida oluliste teenuste osutajate võimekusi ja puudujääke konkreetselt küberturvalisuse nõuete rakendamise osas läbi erinevate sektoripõhiste uuringute. Eelkõige seetõttu, et globaalsed kriisid võivad ettearvamatult avaldada tugevat survet erinevatele sektoritele, nagu näitas COVID-19 pandeemia.

The implementation of the European Union cybersecurity legal framework during the COVID-19 crisis

Abstract

In the beginning of 2020 when WHO declared COVID-19 as a pandemic, technology became an important part of keeping people connected.[170] This raised the question if the cyberspace is as safe and trustworthy as we expect it to be. When researching the connection between the COVID-19 crisis and cybersecurity, scientific articles have described the rise of cyber threats. The aim of this thesis is to analyze whether the cybersecurity acts, regulations and measures adopted by the European Union supported the Member States in ensuring the provision of essential services during the COVID-19 crisis. The analysis will investigate prevention and response capabilities of Member States through the use of cyber security indexes such as the global and national cybersecurity index. As the European Union provides only a legal framework and not the particular services it is important to analyze the problems through the perspective of the Member States. The goal of the European Union is to create overall legal, technical and organizational standards and measures on a wider scale and Member States can adopt these measures into national law via directives.

The thesis explores two main research problems. The first problem analyzes the Member States' capability for prevention of cyber threats. It is crucial to assess the legislation adopted before the crisis in the field of cybersecurity. The European Union had adopted two important cyber security legal acts beforehand: the network and information systems directive (in short NIS directive)[171] and the cybersecurity act[172]. These are the main sources used for analyzing the European Union law. Considering substantial cybersecurity attacks such as WannaCry, NotPetya, Yahoo data breaches etc., the EU as well as Member States should have had a clear understanding of the importance of protecting critical infrastructure along with essential services prior to the COVID-19 crisis.[173]

[170] Georgiadou, A., *et al*. *Op cit*, lk 1.
[171] 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.
[172] 17. aprilli 2019. aasta Euroopa Parlamendi ja nõukogu määrus 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus). – ELT L 151, 7.6.2019, lk 15-69.
[173] Euroopa Kontrollikoda. *Op cit*, lk 12.

The second problem analyzes the response to the growing threat to cybersecurity as well as possible changes in EU law. COVID-19 crisis revealed that there were multiple times when people used risky and non-secure programs and that helped to provide a suitable environment for malicious attacks. Even though many agencies such as Europol[174] and Interpol[175] issued warnings about the growing threat to cybersecurity, states and businesses were not left untouched by these cyber-attacks. This begs the question if and what went wrong with the implementation of EU cybersecurity norms.

The EU has created several strategies outlining the path towards a unified cybersecurity legal framework. With the adoption of the NIS directive and the cybersecurity act, it strengthens its role as a key player in regulating cyber security and creating EU-wide requirements to protect network and information systems from the potential cyber security threats. Before the beginning of the COVID-19 crisis these legal acts were transposed to the national law in Member States. This would mean that the countries should have had enough time to prepare and adopt measures for the protection of essential services.

The first research question is: to what extent does Member States' law correspond to the European Union legal framework for cybersecurity? To answer this question, it must be understood what legal competences the European Union has in regulating cybersecurity, what regulations make up the legal framework and what national laws have been enacted accordingly. The second question posed is: does the European Union's legal framework for cybersecurity support the Member States competences in providing essential services when dealing with cybersecurity issues during the COVID-19 crisis?

The hypotheses set out in the master's thesis are the following:

1. Disruption of the provision of essential national services is highly dependent on the ability of the state to implement existing measures in the field of cybersecurity. Within the European Union, preparedness and resilience to the growing threat posed by cyber security varied greatly from country to country.
2. The European Union's legal framework for cybersecurity and the measures put in place were sufficient to prepare for the theoretical containment of cyber incidents, but the Member States and the various authorities were unable to implement them accordingly.

[174] Europol. *Op cit*.
[175] Interpol. Cybercriminals targeting critical healthcare institutions with ransomware. *Op cit*.

3. As a result of the COVID-19 crisis, the European Union did not update its current agenda in the field of cybersecurity but accelerated the implementation of previous proposals.

Several restrictions have been made in the master's thesis due to the broadness of the field of cybersecurity and the scope of this study. First, the assessment of the legal framework for cybersecurity is based solely on legislation governing critical infrastructure and services of national importance. Secondly, for services of national importance, the sectors most affected by the COVID-19 pandemic, such as health and electronic communications, have been selected for analysis. In terms of the time period, the analysis focuses on statistics and cases from 2020 and onwards.

This master's thesis was written as a comparative study of legal dogma, where the main sources are legislations, regulations, literature and various scientific articles and research related to the field. The master's thesis gathers existing information from sources related to the field and compares them to achieve research results. The comparative method analyzes the extent to which, and the differences between, how the Union's legal framework for cybersecurity has been transposed into national law. It is then compared with the impact of COVID-19 and estimates of national cyber security indexes to answer research questions. The wording and the differences between the transposition of European Union law into national law are further examined through a literal interpretation. Teleological interpretation explains the development of cyber security principles and positions and uses an analytical method to compile and synthesize statistics.

Estonia, Ireland, and the Czech Republic were selected for the comparative analysis in the master's thesis. All three countries have shown a rapid increase in the provision and development of e-services, and the national legal order encourages multinational companies to operate in the same field. One of the first comprehensive EU-wide cyber security laws has also been transposed in all sample countries. This is the network and information systems security directive (NIS directive), which aims to increase the overall level of cybersecurity in the Union and to ensure, inter alia, the preparedness and response capacity of Member States to deal with cyber threats. The master's thesis also uses pan-European cybersecurity incident statistics to assess the impact of COVID-19. A questionnaire has been submitted to each country's cybersecurity agency to improve the assessment of the sample countries. The aim was to gather information that is not publicly available and to compare the opinion of the authorities with the

analysis of theoretical capability. Also, to understand whether the country had cyber-attacks that have not been disclosed to the public.

For the purpose of this thesis the main analysis was carried out in concern to the health and electronic communication sectors. It was presented that COVID-19 highly impacted service providers in these sectors. During the cybersecurity attacks against hospitals as well as a large presence of disinformation campaigns, all the cybersecurity legal remedies were put to test.[176] It is concluded that the Member States by way of at least minimal harmonization adopted the NIS directive fully into their national law. The visible difference is the approach to regulate cyber security in the national law. In the example of Estonia, the choice was to regulate in a comprehensive manner. This meant that the cybersecurity act would be the main source of security requirements and creating a direct link to other fields of the law. Even though other acts concerning vital services exist this was all addressed in the cybersecurity act. It is important to mention that the accompanying measures, for instance Czech Republic's thorough definition of the impact criteria and the Ireland's NIS compliance guidelines for operators of essential services, have also helped the Member States to transpose the directive. In analyzing the first research problem it is concluded that through the creation of a joint legal framework on cybersecurity, the European Union plays a major role in regulating this policy area. The NIS directive as well as the cybersecurity regulation affect member states' national law directly. In the sample countries all these EU legal acts have been adopted or otherwise transposed into the national law. All in all, this means that Member States' law is in fact corresponding to the legal framework for cybersecurity in the European Union.

The second research problem investigated the EU legal framework on cybersecurity and how this helped member states to combat threats during the rise of cybersecurity incidents due to the COVID-19 crisis. In solving this problem, it was important to get an overview of how the sample countries regulated cybersecurity standards for the providers of essential services. As the focus was mainly on the health end electronic communications sector, this part went into detail in order to understand which norms and regulations were adopted as well as what differences could be found in comparing national laws. All mandatory norms and standards from the directive were applied and this meant that enough was done to prevent cybersecurity incidents. The second part of analyzing this research problem focused on the relevant cybersecurity incidents and their impact on member states. In this overview it was concluded

[176] Baumann, A. A., *et al*. CSIRT capabilities in healthcare sector: status and development. ENISA. 2021.

that even though on a theoretical scale the legal framework supports the member states in countering cyber threats, not enough was done to combat the problems in concern to providers of essential services. There were many examples of not having enough qualified personnel as well as capabilities to detect, deter and respond to major cybersecurity incidents. This doesn't mean that national regulations are faulty, but a lot can be done to achieve an effective level of applying those laws.

Problems arise when analyzing the legal competences that the EU has in regulating cybersecurity. As this field is not directly mentioned as a separate competence for the EU and instead derived from the TEU's common foreign and security policy or area of freedom, security and justice, no word of cybersecurity is mentioned in the TEU's articles. The EU has the only option to use the principle of conferral and thus in every legal act there must be a clear explanation as to why it is better for the EU to act on this matter than the Member States. Clearly this creates a much more substantial problem, as the dangers of the cybersecurity legal framework to be fragmented is high. It is proposed that the *expressis verbis* mentioning of the cybersecurity in the TEU could answer some of the problems. This is a difficult process, but nevertheless in a changing digital world a necessary step in creating a unified legal framework for cybersecurity. Otherwise, the EU can only continue to do what it has been doing under the principle of conferral, with using competences in other fields and adopting the so-called soft laws.[177]

Another substantial problem is the definition of cybersecurity in EU legal acts and corresponding Member States' law. With the NIS directive, the EU gave a definition for the security of network and information systems. Cybersecurity is only mentioned as this is important for international cooperation. Even though the cybersecurity act adopted in 2019, is defining the term but this does not correspond to the NIS directive's security explanation. For instance, some Member States used the directive to follow a wider approach to regulate the field of cybersecurity and not limiting it only to network and information systems. The difference being that one is considering security to be a state when the systems can resist threats and the other being activities necessary to protect the systems. A solution can be found in the example of Estonia, where there is a possibility to distinct cybersecurity and cyber security. In Estonian, the term cybersecurity follows the example of the directive and the term cyber security the

[177] Wessel, A. R. Cybersecurity in the European Union: Resilience through Regulation? The Routledge Handbook of European Security Law and Policy. 2019, lk 284-285. Kättesaadav arvutivõrgus: https://www.utwente.nl/en/bms/pa/research/wessel/wessel140.pdf (10.04.2022).

cybersecurity act. Both terms are intertwined, and one does not necessarily exempt the other. Of course, in English translations this is quite difficult to achieve, but considering the clear relation these terms have, not impossible, and for legal clarity a necessary change.[178]

In conclusion, it was found that disruption to the provision of nationally essential services is highly dependent on a country's ability to implement existing cybersecurity measures. The claim that Member States' preparedness and resilience to the growing threat of cybersecurity varied widely is incorrect. This is because the same requirements apply to all member states. Indeed, some differences could be observed in the application of national legislation, but these differences in implementation were not decisive for the provision of essential services. The EU legal framework for cybersecurity was sufficient to prepare for the theoretical containment of cyber incidents, but Member States and various authorities were not able to implement these cybersecurity requirements accordingly. The work revealed that there was a difference in the ability of Member States and different authorities to implement cyber security requirements. Here, Member States have already done enough to implement the requirements, but it is questionable, for example, for operators of essential services whether, firstly, they are aware that they fall under this classification and what requirements apply to them as a result. A study on the implementation of the NIS Directive also found that, for example, some hospitals were unable to define themselves as an essential service provider, although the healthcare sector had been identified as such. Assessments of national cybersecurity indexes pointed to shortcomings in dealing with cyber crises.

In addition, the paper concluded that the European Union did not renew its current position in the field of cyber security as a result of the crisis but accelerated the implementation of previous proposals. The European Union's attitude towards the private sector has been maintained, especially with regard to social media companies. The COVID-19 crisis highlighted the negative effects of disinformation in cyberspace, both in virtual and physical space, which could endanger people's lives and prevent the transmission of critical information. At the same time, the European Union has a certain precondition to trust only companies that provide cybersecurity services directly, although, for example, there should have been greater cooperation with social media companies in the fight against disinformation.[179] However, in light of the amendment to the NIS Directive, NIS2 has shown that it is also trying to address the negative effects of the COVID-19 crisis. A particularly important starting point is the

[178] Szpor, G. *Op cit*.
[179] Carrapico, H., Farrand, B. *Op cit*.

Member States' own experience, such as addressing supply chain vulnerabilities, reviewing the list of essential services for the adoption of the Electronic Communications Code, cybersecurity incident reporting requirements and stronger surveillance measures.[180]

As a result of this thesis, it became clear what problems exist in dealing with the concept of cyber security and in the legal competences of the European Union. Although the proposed example of Estonia provided an opportunity to incorporate the concept of cybersecurity, it is especially important that such an initiative stems from the legislation of the European Union. The paper also presented ways in which cybersecurity indexes can be used in practice to develop national capabilities in this area, which will also require changes to national legislation. The conclusion of this thesis could also be useful in the negotiations of the NIS2 Directive, with a special focus on improving the standards applicable to operators of essential services. The capabilities and gaps of key service providers in the specific implementation of cyber security requirements should also be further explored through various sector-specific studies. Especially because global crises can put unpredictable pressure on various sectors, as the COVID-19 pandemic has shown.

[180] Euroopa Parlament. *Op cit*.

LÜHENDITE LOETELU

CSIRT	Küberturbe intsidentide lahendamise üksused
DTO	Digitaalse teenuse osutaja/operaator
ECCC	Euroopa Liidu kübeturvalisuse kompetentsi keskus
EECC	Elektroonilise side seadustik
EK	Euroopa Komisjon
ENISA	Euroopa Võrgu- ja Inforturbeamet
EUROPOL	Euroopa Politseiamet
IKT	Info- ja kommunikatsioonitehnoloogia
INTERPOL	Rahvusvaheline Kriminaalpolitsei Organisatsioon
IoT	Asjade internet (*Internet of Things*)
ITU	Rahvusvaheline Telekommunikatsiooni Liit
NCC	Riiklikud koordineerimiskeskused
NIS	Võrgu- ja infosüsteemide direktiiv
OTO	Olulise teenuse osutaja/operaator
TEU	*Treaty of the European Union*

KASUTATUD MATERJALID

Kasutatud normatiivallikad

1. 9. märtsi 2011. aasta Euroopa Parlamendi ja nõukogu direktiiv 2011/24/EL, patsiendiõiguste kohaldamise kohta piiriüleses tervishoius. ELT L 88, 4.4.2011, lk 45—65.
2. 6. juuli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv 2016/1148, meetmete kohta, millega tagatakse võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu Liidus. – ELT L 194, 19.7.2016, lk 1-30.
3. 11. detsember 2018. aasta Euroopa Parlamendi ja nõukogu direktiiv 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik – ELT L 321, 17.12.2018, lk 36-214.
4. 17. aprilli 2019. aasta Euroopa Parlamendi ja nõukogu määrus 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus). – ELT L 151, 7.6.2019, lk 15-69.
5. 17. mai 2019. aasta Nõukogu otsust (ÜVJP) 2019/797, piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberründe id. ST/7299/2019/INIT. ELT L 129I , 17.5.2019, lk 13—19.
6. Decree on the criteria for the determination of an operator of essential service – 437/2017 Coll.
7. European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018– S.I. No. 360/2018.
8. Euroopa Liidu lepingu konsolideeritud versioon. ELT C 326, 26.10.2012, lk 13—390.
9. Euroopa Liidu toimimise lepingu konsolideeritud versioon. ELT C 326, 26.10.2012, lk 47—390.
10. Küberturvalisuse seadus[1] – RT I, 22.05.2018, 1.

Kasutatud kohtulahendid

11. EKo C-26/62, *NV Algemene Transport- en Expeditie Onderneming van Gend en Loos vs. Netherlands Inland Revenue Administration*, ECLI:EU:C:1963:1.

Kasutatud kirjandus

12. AlShabibi, A., Al-Suqri, M. Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. 2021 22nd International Arab Conference on Information

Technology. 2021. Kättesaadav arvutivõrgus: https://ieeexplore-ieee-org.ezproxy.utlib.ut.ee/document/9677117 (24.04.2022).

13. Baumann, A. A., *et al*. CSIRT capabilities in healthcare sector: status and development. ENISA. 2021.
14. Bendiek, A., Bossong, R., Schulze, M. The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges. German Institute for International and Security Affairs. 2017. Kättesaadav arvutivõrgus: https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf (09.04.2022).
15. BHConsulting. Analysis of the Irish National Cyber Security Strategy. 2020. Kättesaadav arvutivõrgus: https://bhconsulting.ie/analysis-of-the-irish-national-cyber-security-strategy/ (10.04.2022).
16. Bizga, A. Mysterious cyberattack cripples Czech hospital amid COVID-19 outbreak. Bitdefender. 2020. Kättesaadav arvutivõrgus: https://www.bitdefender.com/blog/hotforsecurity/mysterious-cyberattack-cripples-czech-hospital-amid-covid-19-outbreak (22.04.2022).
17. Botek, A. Brno University Hospital ransomware attack (2020). Kättesaadav arvutivõrgus: https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)#cite_note-7 (24.04.2022).
18. Buil-Gil, D., *et al*. Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. European Societies, 23(sup1), S47–S59. 2021. Kättesaadav arvutivõrgus: https://www.tandfonline.com/doi/full/10.1080/14616696.2020.1804973 (7.02.2022).
19. Carrapico, H., Farrand, B. Discursive continuity and change in the time of Covid-19: The case of EU cybersecurity policy. Journal of European Integration, 42(8), 1111–1126. 2020. Kättesaadav arvutivõrgus: https://www-tandfonline-com.ezproxy.utlib.ut.ee/doi/full/10.1080/07036337.2020.1853122 (7.02.2022).
20. Chałubińska-Jentkiewicz, K., *et al*. Cybersecurity in Poland: Legal Aspects. Springer. 2022, lk 91. Kättesaadav arvutivõrgus: https://doi-org.ezproxy.utlib.ut.ee/10.1007/978-3-030-78551-2 (10.04.2022).
21. Christen, M., *et al*. The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology vol 21, 2020.
22. CMS Law-Now. Communications as an essential service during Coronavirus (COVID-19) confinement. 2020. Kättesaadav arvutivõrgus: https://www.cms-lawnow.com/ealerts/2020/04/portugal-communications-as-an-essential-service-during-coronavirus (11.04.2022).

23. Coman, I., Mihai, I. C. The Impact of COVID-19. Cybercrime and Cyberthreats. European Law Enforcement Research Bulletin, (SCE 5), 61–67. 2022. Kättesaadav arvutivõrgus: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/489 (7.02.2022).
24. Corera, G. Irish health cyber-attack could have been even worse, report says. BBC. 2021. Kättesaadav arvutivõrgus: https://www.bbc.com/news/technology-59612917 (22.04.2022).
25. Dyrda, L. Inside UVM Medical Center's randomware attack: 11 details. Becker's Health IT. 2020. Kättesaadav arvutivõrgus: https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html (20.04.2022).
26. Edegbeme- Belaz, A. The changing role of the EU in cybersecurity. ResearchGate. 2019, lk 25. Kättesaadav arvutivõrgus: https://www.researchgate.net/publication/334173763_The_changing_role_of_the_EU_in_cybersecurity (24.04.2022).
27. Euroopa Komisjon. Digital Agenda: Commission proposal to strengthen and modernise European Network and Information Security Agency (ENISA) – frequently asked questions. MEMO/10/459, 2010. Kättesaadav arvutivõrgus: http://europa.eu/rapid/press-release_MEMO-10-459_en.htm?locale=en (24.04.2022).
28. Euroopa Komisjon. Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum. 2013. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52013JC0001 (09.04.2022).
29. Euroopa Kontrollikoda. ELi küberturvalisuse poliitika tõhusust mõjutavad probleemid. 2019. Kättesaadav arvutivõrgus: https://www.eca.europa.eu/et/Pages/DocItem.aspx?did={DEA2082B-4296-43EE-A5C9-9D01D7C0A585} (24.04.2022).
30. Euroopa Komisjon. Commission staff working Document. Better Regulation Guidelines. 2015. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015SC0111 (09.04.2022).
31. Euroopa Komisjon. Implementation of the NIS Directive in Ireland. 2022. Kättesaadav arvutivõrgus: https://digital-strategy.ec.europa.eu/en/policies/nis-directive-ireland (10.04.2022).
32. Euroopa Komisjon. Implementation of the NIS Directive in the Czech Republic. 2022. Kättesaadav arvutivõrgus: https://digital-strategy.ec.europa.eu/en/policies/nis-directive-czech-republic (10.04.2022).

33. Euroopa Komisjon. Report From The Commission To The European Parliament And The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems. 2019.
34. Euroopa Komisjon. - Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665. 2021.
35. Euroopa Komisjon. The Digital Education Action Plan (2021-2027). Resetting education and training for the digital age. 2020. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0624 (09.04.2022).
36. Euroopa Komisjon. The EU's Cybersecurity Strategy for the Digital Decade. 2020. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN (09.04.2022).
37. Euroopa Parlament. The NIS2 Directive: A high common level of cybersecurity in the EU. Briefing. 2021. Kättesaadav arvutivõrgus: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (24.04.2022).
38. Europol. How criminals profit from the COVID-19 pandemic. 27.03.2020. Kättesaadav arvutivõrgus: Kättesaadav arvutivõrgus: https://www.europol.europa.eu/media-press/newsroom/news/how-criminals-profit-covid-19-pandemic (7.02.2022).
39. Georgiadou, A., *et al*. D. Hospitals' Cybersecurity Culture during the COVID-19 Crisis. Healthcare, 9(10), 1335. 2021. Kättesaadav arvutivõrgus: https://www.mdpi.com/2227-9032/9/10/1335/htm (7.02.2022).
40. Giantas, H. D. Liaropoulus, N. A. Cybersecurity in the EU: Threats, frameworks and future perspectives. 2019. Kättesaadav arvutivõrgus: https://www.researchgate.net/publication/335909463_Cybersecurity_in_the_EU_Threats_frameworks_and_future_perspectives (24.04.2022).
41. Gogou, V., Dekker, M. Telecom Security Incident 2020 – Annual report. ENISA. 2021.
42. Government of Ireland. National Cyber Security Strategy 2019-2024. Kättesaadav arvutivõrgus: https://www.ncsc.gov.ie/strategy/ (7.02.2022).
43. International Telecommunication Union. Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. 2022.
44. Interpol. Cybercriminals targeting critical healthcare institutions with ransomware. 2020. Kättesaadav arvutivõrgus: https://www.Interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware (19.04.2022).

45. Interpol. Interpol report shows alarming rate of cyberattacks during COVID-19. 2020. Kättesaadav arvutivõrgus: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (19.04.2022).
46. Kask, L. Küberturvalisuse seadusest. – Õiguskeel. 3/2018. Kättesaadav arvutivõrgus: https://www.just.ee/oigusloome-arendamine/oiguskeel/ajakiri-oiguskeel#item-4 (7.02.2022).
47. Kaspersky. What is Spear Phishing. Kättesaadav arvutivõrgus: https://www.kaspersky.com/resource-center/definitions/spear-phishing (22.04.2022).
48. Majandus- ja Kommunikatsiooniministeerium. Küberjulgeoleku strateegia 2014-2017. Kättesaadav arvutivõrgus: https://www.mkm.ee/et/eesmargid-tegevused/kuberturvalisus (7.02.2022).
49. Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022. Kättesaadav arvutivõrgus: https://www.mkm.ee/et/eesmargid-tegevused/kuberturvalisus (7.02.2022).
50. Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse seaduse eelnõu seletuskiri. 2017. Kättesaadav arvutivõrgus: https://www.koda.ee/sites/default/files/content-type/content/2017-10/seletuskiri_k%C3%BCberturvalisuse%20seadus.pdf (11.04.2022).
51. Majandus- ja Kommunikatsiooniministeerium. Sutt: EL küberturvalisuse tase peab vastama ohupildile. 2021. Kättesaadav arvutivõrgus: https://mkm.ee/uudised/sutt-el-kuberturvalisuse-tase-peab-vastama-ohupildile (16.04.2022).
52. M. Švéda an E.Pilliroog. Brno. 11.04.2022 (kiri adressaadi valduses).
53. National Cyber and Information Security Agency. Legislation. Kättesaadav arvutivõrgus: https://nukib.cz/en/cyber-security/regulation-and-audit/legislation/ (10.04.2022).
54. National Cyber and Information Security Agency. National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020. 16.02.2015. Kättesaadav arvutivõrgus: https://www.nukib.cz/en/cyber-security/strategy-action-plan/ (7.02.2022).
55. National Cyber and Information Security Agency. National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025. 18.03.2021. Kättesaadav arvutivõrgus: https://www.nukib.cz/en/cyber-security/strategy-action-plan/ (7.02.2022).
56. National Cybersecurity Index. Kättesaadav arvutivõrgus: https://ncsi.ega.ee (24.04.2022).
57. National Cyber Security Centre. Network and Information Security Directive. Kättesaadav arvutivõrgus: https://www.ncsc.gov.ie/nis/ (10.04.2022).

58. National Cyber Security Centre. NIS Compliance Guidelines for Operators of Essential Service (OES). 2019. Kättesaadav arvutivõrgus: https://www.ncsc.gov.ie/pdfs/NIS_Compliance_Security_Guidelines_for_OES.pdf (11.04.2022).
59. Opinion of the European Economic and Social Committee on 'Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 and Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities' (COM(2020) 823 final. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020AE5749&rid=8 (24.04.2022).
60. Pawlicka, A., *et al*. R. A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. Business Horizons, 64(6), 729–734. 2021. Kättesaadav arvutivõrgus: https://www.sciencedirect.com/science/article/pii/S0007681321001336. 2021.07.010 (7.02.2022).
61. Pranggono, B., Arabo, A. COVID-19 pandemic cybersecurity issues. Internet Technology Letters, Volume 4, Issue 2. 2020. Kättesaadav arvutivõrgus: https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247 (7.02.2022).
62. Polcák, R., *et al*. Cyber Law in the Czech Republic, third edition. 2020. Kättesaadav arvutivõrgus: https://books.google.ee/books/about/Cyber_Law_in_Czech_Republic.html?id=rubYDwAAQBAJ&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false (10.04.2020)
63. RIA. Küberturvalisuse aastaraamat 2021. 2021. Kättesaadav arvutivõrgus: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2021.pdf (22.04.2022).
64. RIA. Olukord küberruumis 2020. aastal. 2022 Kättesaadav arvutivõrgus: https://www.ria.ee/et/kuberturvalisus/olukord-kuberruumis/olukord-kuberruumis-2020-aastal.html (22.04.2022).
65. Salama, V. Several hospitals targeted in new wave of ransomware attacks. CNN. 2020. Kättesaadav arvutivõrgus: https://edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html (20.04.2022).
66. Sein, K. Interplay Of Digital Content Directive, European Electronic Communications Code And Audiovisual Media Directive In Communications Sector. Journal of Intellectual

Property, Information Technology and E-Commerce Law. 2021. Kättesaadav arvutivõrgus: https://www.jipitec.eu/issues/jipitec-12-2-2021/5298 (10.04.2022).

67. S. Lusti an E. Pilliroog. Tallinn. 14.03.2022 (kiri adressaadi valduses).
68. Szpor, G. The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland. Review of European and Comparative Law. 2021. Kättesaadav arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?handle=hein.journals/recol46&id=219&collection=journals&index= (10.04.2022).
69. Tallinna Ülikool, E-riigi Akadeemia SA. Riikliku küberturvalisuse indeksi metoodika analüüs. 2020. Kättesaadav arvutivõrgus: https://ega.ee/wp-content/uploads/2020/05/NCSI_metoodika_audit_PDF.pdf (10.04.2022).
70. Tsagourias, N. Buchan, R. Wessel, A. R. Research Handbook on International Law and Cyberspace: Chapter 19: Towards EU cybersecurity law: Regulating a new policy field. 2015. Kättesaadav arvutivõrgus: https://www.elgaronline.com/view/edcoll/9781782547389/9781782547389.00032.xml (10.04.2022).
71. Wessel, A. R. Cybersecurity in the European Union: Resilience through Regulation? The Routledge Handbook of European Security Law and Policy. 2019. Kättesaadav arvutivõrgus: https://www.utwente.nl/en/bms/pa/research/wessel/wessel140.pdf (10.04.2022).
72. WHO. COVID-19 continues to disrupt essential health services in 90% of countries. 2021. Kättesaadav arvutivõrgus: https://www.who.int/news/item/23-04-2021-covid-19-continues-to-disrupt-essential-health-services-in-90-of-countries#:~:text=Among%20the%20most%20extensively%20affected,and%20services%20for%20other%20noncommunicable (11.04.2022).
73. Wiewiórowski, W. Privacy, security, and technology: the annual privacy forum. 2017. Kättesaadav arvutivõrgus: https://edps.europa.eu/press-publications/press-news/blog/privacy-security-and-technology-annual-privacy-forum-2017_en (10.04.2022).
74. Wolff, S., Ladi, S. European Union Responses to the Covid-19 Pandemic: Adaptability in times of Permanent Emergency. Journal of European Integration, 42(8), 1025–1040. 2020. Kättesaadav arvutivõrgus: https://www.tandfonline.com/doi/full/10.1080/07036337.2020.1853120 (7.02.2022).

LISAD

Lisa 1. Valimiriikide küberturvalisuse ametitele esitatud küsimustik

Eestikeelne versioon:

1. Mis ulatuses ning miks sellisel kujul otsustas riik võtta üle EL direktiivi (NIS direktiiv)?
2. Kuidas hindate ja mille alusel riigi võimekust COVID-19 kriisi ajal tagada küberturvalisust?
3. Teie arvates riigi õppetunnid COVID-19 kriisist küberturvalisuse valdkonnas? Mis ettepanekuid olete kaalunud, mida võiks EL tasandil küberturvalisuse valdkonnas edaspidi reguleerida tulenevalt kriisist?
4. Mis on EL senised uued suunad COVID-19 kriisist tulenevalt küberturvalisuse valdkonnas?
5. Mis on olnud riigi suurimad ja olulisemad küberturvalisuse juhtumid COVID-19 kriisi ajal, mis mõjutasid riiklikult olulisi teenuseid (elutähtsaid teenuseid) või kriitilist infrastruktuuri?

Ingliskeelne versioon:

1. To what extent did your country decide to transpose the EU Directive (NIS Directive)?
2. In this light, could you further explain how the impact criteria of DECREE No 437/2017 Coll.of December 8, 2017 was defined in the relevant sectors?[181]
3. How do you assess and on what basis the country's ability to ensure cyber security during the COVID-19 crisis?
4. In your opinion, what lessons have you marked from the COVID-19 crisis in the field of cyber security? What proposals have you considered for further regulation amendments at EU level in the field of cyber security as an afterthought of the crisis?
5. Would it be possible to share your country's largest and most important cyber security incidents during the Covid-19 crisis, which affected nationally important services (vital services) or critical infrastructure?

[181] Antud küsimus esitati vaid Tšehhi küberturvalisuse ametile.

Lisa 2. National Cybersecurity Index indikaatorite loetelu

1. Küberturbepoliitika väljatöötamine
    1.1. Küberturbepoliitika üksus
    1.2. Küberturbepoliitika koordineerimise formaat
    1.3. Küberturvalisuse strateegia
    1.4. Küberturvalisuse strateegia rakendusplaan
2. Küberohtude analüüs ja teave
    2.1. Küberohtude analüüsi üksus
    2.2. Avalikud küberohuaruanded avaldatakse igal aastal
    2.3. Küberohutuse ja -turvalisuse veebisait
3. Haridus ja professionaalne areng
    3.1. Küberohutuse pädevused alg- või keskhariduses
    3.2. Bakalaureusetaseme küberturvalisuse programm
    3.3. Magistritaseme küberturvalisuse programm
    3.4. PhD tasemel küberturvalisuse programm
    3.5. Küberturvalisuse erialaliit
4. Panus ülemaailmsesse küberturvalisusesse
    4.1. Küberkuritegevuse konventsioon
    4.2. Esindatus rahvusvahelistes koostööformaatides
    4.3. Rahvusvaheline küberturvalisuse organisatsioon, mida majutab riik
    4.4. Küberjulgeoleku suutlikkuse suurendamine teiste riikide jaoks
5. Digiteenuste kaitse
    5.1. Digiteenuste pakkujate küberturvalisuse vastutus
    5.2. Küberturbe standard avalikule sektorile
    5.3. Pädev järelevalveasutus
6. Oluliste teenuste kaitse
    6.1. Oluliste teenuste osutajad on kindlaks tehtud
    6.2. Küberturbe nõuded oluliste teenuste operaatoritele
    6.3. Pädev järelevalveasutus
    6.4. Turvameetmete regulaarne jälgimine
7. E-identifitseerimis- ja usaldusteenused
    7.1. Ainulaadne püsiidentifikaator
    7.2. Nõuded krüptosüsteemidele
    7.3. Elektrooniline tuvastamine
    7.4. Elektrooniline allkiri

7.5. Ajatempel

7.6. Elektrooniline registreeritud kohaletoimetamise teenus

7.7. Pädev järelevalveasutus

8. Isikuandmete kaitse

8.1. Isikuandmete kaitse seadusandlus

8.2. Isikuandmete kaitse asutus

9. Küberintsidentidele reageerimine

9.1. Küberintsidentidele reageerimise üksus

9.2. Aruandluse vastutus

9.3. Rahvusvahelise koordineerimise ühtne kontaktpunkt

10. Küberkriisi juhtimine

10.1. Küberkriiside ohjamise plaan

10.2. Riikliku tasandi küberkriiside ohjamise õppus

10.3. Osalemine rahvusvahelistel küberkriisi õppustel

10.4. Vabatahtlike operatiivne toetus küberkriisides

11. Võitlus küberkuritegevuse vastu

11.1. Küberkuriteod on kriminaliseeritud

11.2. Küberkuritegevuse üksus

11.3. Digitaalne kohtuekspertiisi üksus

11.4. Ööpäevaringne rahvusvahelise küberkuritegevuse kontaktpunkt

12. Sõjalised küberoperatsioonid

12.1. Küberoperatsioonide üksus

12.2. Küberoperatsioonide õppus

12.3. Osalemine rahvusvahelistel küberõppustel[182]

[182] National Cybersecurity Index. Kättesaadav arvutivõrgus: https://ncsi.ega.ee (24.04.2022).