EUROOPA
KOMISJON

Strasbourg, 18.4.2023
COM(2023) 207 final

KOMISJONI TEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

Korvata küberturvalisuse valdkonna talendinappus edendamaks ELi konkurentsivõimet, majanduskasvu ja kerksust

(„Küberturbeoskuste akadeemia“)

Korvata küberturvalisuse valdkonna talendinappus edendamaks ELi konkurentsivõimet, majanduskasvu ja kerksust („Küberturbeoskuste akadeemia“)

1. Et vähendada kasvavaid riske, tuleks võtta kiiresti käsile töötajate puudulikud küberturbeoskused ja küberturbeoskustega töötajate nappus

Küberturvalisus on oluline osa kodanike, ettevõtjate ja liikmesriikide julgeolekust. Kuid ühtlasi eeldab see, et tagatud on ELi poliitiline stabiilsus, demokraatia stabiilsus ning ühiskonna ja ettevõtete õitseng. Küberturvalisuse **ohupilt** on viimastel aastatel palju muutunud. Sealjuures valmistab eriti muret see, et üha rohkem küberründeid on sihitud ELi elutähtsa sõjalise ja tsiviiltaristu vastu. Ohusubjektid on suurendanud oma suutlikkust ning esile on kerkinud uusi hübriid- ja emergentseid ohte, eriti seoses robotite ja tehisintellektil põhineva tehnoloogia kasutamisega[1]. Lunavararünded põhjustavad ettevõtetele ja asutustele pidevalt märkimisväärset rahalist ja mainekahju[2].

Suur hulk küberründeid on olnud sihitud ka liikmesriikide haldus- ja valitsusasutuste ning ELi institutsioonide, organite ja asutuste vastu[3]. Järjepidevalt on olnud sihikul rahandus-[4] ja tervishoiusektor,[5] mis on mõlemad ühiskonna ja majanduse selgrooks[6]. Küberohte on suurendanud ka geopoliitilised pinged, mida on tekitanud Venemaa agressioonisõda Ukraina vastu[7] ja mis võivad hakata Euroopa ühiskondi destabiliseerima. ELi **julgeolekut** ei saa tagada ilma selle **kõige väärtuslikuma varata, milleks on tema inimesed.** Et ennetada, tuvastada ja hoida ära ELi ja selle elutähtsat taristut ohustavaid küberründeid, kaitstes ELi ja suurendades selle elutähtsa taristu **kerksust**, on kiiresti tarvis sobivate oskustega pädevaid spetsialiste.

Euroopa **konkurentsivõime** ja **majanduskasv** sõltuvad suurel määral strateegilise digitehnoloogia (nt tehisintellekt, 5G ja pilvandmetöötlus) arendamisest ja kasutuselevõtust, kuid samas pärsib edusamme küberturvalisuse valdkonna talendinappus. Küberturvalisuse valdkonna vajalike oskustega tööjõud võimaldaks ELil jätkata tegutsemist olulise kõrgtehnoloogia pakkujana ülemaailmsel areenil.

---

[1] ENISA ohtude kaardistamise aruanne 2022 – ENISA (europa.eu)

[2] Europoli „Internet Organised Crime Threat Assessment (IOCTA) 2021“, (Internetipõhise organiseeritud kuritegevuse ohtude hindamise aruanne). Ohusubjektid tuginevad enamasti lunavara kui teenuse mudelile. Ettevõtjate aastased kulud ületasid 2022. aastal 18,4 miljardit eurot (Cybereasoni 2022. aasta aruanne lunavara tegelike kulude kohta).

[3] Vt näiteks ENISA ja CERT-EU ühisväljaanne, JP-23–01, „Sustained activity by specific threat actors“ (Mõningate ohusubjektide püsiv tegevus) TLP:CLEAR, 15. veebruar 2023.

[4] Näiteks Saksamaal moodustas 1. juunist 2021 kuni 31. maini 2022 teatatud e-kirjapettustest 90 % finantsandmete kogumine või rünnak finantssektori ettevõtte vastu. Nendesse on olnud segatud rohkem kui 20 000 nakatunud seadet 125 riigist, „The State of IT Security in Germany in 2022“ (IT-turbe olukord Saksamaal – 2022), Bundesamt für Sicherheit in der Informationstechnik (BSI), 1. jaanuar 2023.

[5] Mitmeid lunavararünnakud riiklike tervishoiuasutuste vastu on pandud toime Prantsusmaal. Näiteks Centre Hospitalier Sud Francilieni vastu korraldatud küberründe käigus sai ohusubjekt kätte 11 GB isiku- ja terviseandmeid, samuti personaliga seotud andmeid, ning avaldas need. Vt Panorama de la cybermenace 2022 (Küberohtude ülevaade 2022), Agence nationale de la sécurité des systèmes d'information (ANSSI), jaanuar 2023.

[6] ENISA ohtude kaardistamise aruanne

[7] Vt ka CERT-EU – Russia's war on Ukraine: one year of cyber operations (europa.eu); Venemaa küberoperatsioonid Ukraina vastu: kõrge esindaja poolt Euroopa Liidu nimel tehtud avaldus, 10. mai 2022; Kõrge esindaja poolt Euroopa Liidu nimel tehtud avaldus häkkerite ja häkkerirühmituste pahatahtliku kübertegevuse kohta seoses Venemaa Ukraina-vastase agressiooniga, 19. juuli 2022.

Et olla valmis uute ohtudega toime tulema ja edendada oma konkurentsivõimet, on EL küberturvalisuse poliitikat viimastel aastatel märkimisväärselt edasi arendanud ning võtnud vastu mitu olulist dokumenti, nagu teatis „ELi küberturvalisuse strateegia digikümnendi jaoks“,[8] küberturvalisuse 2. direktiiv,[9] valdkondlikud küberturvalisust käsitlevad õigusaktid,[10] ELi küberkaitsepoliitika teatis,[11] küberkerksuse määrus[12] ja kübersolidaarsuse määrus, mille komisjon esitas koos käesoleva teatisega. Kuid need dokumendid ei saavuta oma eesmärke, kui puuduvad nende rakendamiseks vajalike oskustega inimesed. Kuigi elanikkonna küberturvalisusalaseid alusteadmisi jagatakse algatuste raames, millega edendatakse ühiskonnaelus osalemiseks vajalikke üldoskusi,[13] on nii avalikus kui ka erasektoris ja nii riiklikul kui ka ELi tasandil, sealhulgas standardiorganisatsioonides, vaja pädevat tööjõudu, et käsitleda **küberturvalisusega seotud õiguslikku ja poliitilist olukorda**.

Seega sõltuvad ELi julgeolek ja konkurentsivõime küberturvalisuse valdkonna töötajate professionaalsusest ja oskustest. Siiski on EL jõudnud olukorda, kus vajalike oskustega küberturvalisuse spetsialistidest on väga suur puudus, mis seab ELi, selle liikmesriigid, ettevõtjad ja kodanikud suurde küberintsidentide ohtu. 2022. aastal oli Euroopa Liidus puudu **260 000**[14] **kuni 500 000**[15] küberturvalisuse spetsialisti (ELi koguvajaduseks hinnati 883 000 küberturvalisuse spetsialisti),[16] millest nähtub, et vabade töötajate pädevused ei vasta tööturu vajadustele. Küberturvalisuse valdkond kannatab ka oma tehnilise kuvandi tõttu ega suuda ligi meelitada **naisi**, kes moodustavad küberturvalisuse eriala lõpetajatest 20 %[17] ning info- ja kommunikatsioonitehnoloogia (IKT) spetsialistidest 19 %[18]. Selle probleemi lahendamiseks on **Euroopa digikümnendi poliitikaprogrammis 2030**[19] seatud eesmärgiks suurendada 2030. aastaks IKT-spetsialistide arvu 20 miljonini ja saavutada parem sooline tasakaal. Peale selle on ELi uue poliitika rakendamiseks vaja piisaval hulgal sobivate oskustega töötajaid.

---

[8] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberturvalisuse strateegia digikümnendi jaoks“ (JOIN(2020) 18 final).

[9] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv).

[10] Näiteks finantssektori puhul Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (digitaalse tegevuskerksuse määrus)

[11] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“ (JOIN(2022) 49 final).

[12] Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020 (COM(2022) 454 final).

[13] Elanikkonna üldisi digioskusi käsitlevate algatuste seas tuleks nimetada järgmisi: Euroopa sotsiaalõiguste samba tegevuskava ja digikompass, milles on seatud eesmärgiks, et 80 % elanikkonnast peab saavutama 2030. aastaks põhilised digioskused, digiõppe tegevuskava 2021–2027, digipädevuse raamistiku töövahend ning nõukogu soovituse ettepanek hariduses ja koolituses digioskuste õpetamise täiustamise kohta.

[14] (ISC)² andmed ENISA veebiseminaril „Assessing Cyber Skills on the basis of the ECSF“ (Küberturbeoskuste hindamine Euroopa küberturbeoskuste raamistiku alusel), 16. veebruar 2023.

[15] Euroopa Küberturvalisuse Organisatsiooni andmetel, nagu need on esitatud ühisteatises Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“ (JOIN(2022) 49 final).

[16] (ISC)² andmed ENISA veebiseminaril „Assessing Cyber Skills on the basis of the ECSF“ (Küberturbeoskuste hindamine Euroopa küberturbeoskuste raamistiku alusel), 16. veebruar 2023.

[17] Küberturvalisuse alane kõrghariduse andmebaas (CyberHEAD)

[18] Ainult 19 % ELi IKT-spetsialistidest on naised, vt Digitaalmajanduse ja -ühiskonna indeks (DESI) 2022 | Euroopa digitulevik (europa.eu). Selle kohta, kui suur osa liidu küberturvalisuse valdkonna töötajatest on naised, andmed puuduvad.

[19] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta otsus (EL) 2022/2481, millega luuakse digikümnendi poliitikaprogramm 2030, milles on ette nähtud seire- ja koostöömehhanism, et saavutada 2030. aasta digikompassis sätestatud Euroopa digiülemineku ühised eesmärgid ja sihid, sealhulgas oskuste vallas.

Näiteks rõhutab üle 42 % finantsteenuste sektori IT-valdkonna kõrgema tasandi juhtidest, et seoses kohustusega rakendada valdkondlikke küberturvalisuse instrumente, nagu digitaalse tegevuskerksuse määrus (DORA), on nende tegevuses küberkaitse ja -intsidentide haldamisel[20] peamiseks probleemiks küberturvalisuse valdkonna spetsialistide ja ekspertide puudus.

Tööjõu kättesaadavust piirab veelgi tööandjate kõhklus investeerida inimkapitali ja soov leida juba koolitatud ja kogenud töötajaid[21]. Tööjõu puuduse käes kannatavad igat liiki ettevõtjaid, sealhulgas väikesed ja keskmise suurusega ettevõtjad (**VKEd**), mis moodustavad 99 % kõigist ELi ettevõtetest[22]. Samuti on suured probleemid **haldusasutustel**, sest just nemad on kõige sagedamini küberrünnete sihtmärgiks ja peavad tegelema intsidentide tagajärgedega[23].

ELi küberturvalisuse valdkonna töötajate talendinappus on vaja seega kiiresti korvata, sest kaalul on ELi julgeolek ja konkurentsivõime.

2. Koostoime ja koordineeritud meetmete abil küberturbeoskuste nappuse vastu

ELi ja liikmesriikide algatusi, mida viivad läbi avaliku ja erasektori üksused, et tegeleda küberturvalisuse valdkonna tööjõupuudusega, on rohkelt. Jõupingutused on siiski olnud hajutatud ega ole suutnud olukorda päriselt muuta.

Raskusi on valmistanud juba seegi, kuidas jõuda ELis ühisele arusaamale küberturvalisuse valdkonna tööjõu koosseisust ja vastavatest oskustest, kuna sarnastel küberturvalisuse valdkonna ametikohtadel töötavatel inimestel peaksid olema samad oskused. Kuna valdkonna osalejad ei ole hakanud piisaval määral kasutama **Euroopa küberturvalisuse valdkonna spetsialistide ühist võrdlusraamistikku**, on raskendatud tööandjate, haridustöötajate ja poliitikakujundajate vaheline suhtlus ning küberturvalisuse valdkonna tööturu lünki ei suudeta mõõta ega hinnata. Lisaks takistab see kutsealal tegutseda soovijate jaoks haridus- ja koolituskavade koostamist ning poliitikale ja turu vajadustele vastavate karjäärivõimaluste loomist. **Tööjõu ümberõpe ja oskuste täiendamine** põhineb suurel määral küberturbekoolitustel ja sertifikaatidel, mida pakuvad erasektori teenuseosutajad. Töötajatel puudub seetõttu hea ülevaade pakutavate küberturbekoolituste ja nendega seotud sertifikaatide tasemest.

Kuigi tööturu pakkumise poole tugevdamiseks on vaja parandada hariduse andmist ning karjäärivõimalusi, on praeguseni alahinnatud seda, mida saab tööjõu koolitamisel ja selle arenguga kohanemisel teha **nõudluse poolel**. Era- ja avaliku sektori tööandjatel on puudu ühisest foorumist, mis võimaldaks koondada ideid selle kohta, kuidas töötajaid kõige paremini koolitada ja kuidas **oskusi paremini hinnata**, eriti värbamisprotsessis. Kõige nõutumad on **tehnilised oskused**, mis on seotud küberturvalisusega,[24] näiteks tarkvara arendamine ja pilvandmetöötlus,[25] kuid põhjendamatult vähe võetakse endiselt arvesse **siirdeoskusi**. Tööandjad nõuavad ühe rohkem kriitilise mõtlemise ja analüüsioskust, samuti probleemide lahendamise ja enesejuhtimise oskust[26] ning kuni 2025. aastani[27] nende tähtsus ainult suureneb.

---

[20] S-RM, Cyber Security Insights Report 2022 (Küberturvalisuse aruanne 2022).

[21] Küberturbeoskuste arendamine ELis, ENISA, detsember 2019

[22] VKE määratlus (europa.eu)

[23] ENISA ohtude kaardistamise aruanne 2022 – ENISA (europa.eu)

[24] LinkedIn 2023 „Most In-Demand Skills: Learn the Skills Companies Need Most“ (Enim nõutud oskused: omandage oskused, mida ettevõtted kõige enam vajavad)

[25] ISACA küberturvalisuse olukorra 2022. aasta infograafik

[26] Näiteks Euroopa Kutseõppe Arenduskeskuse (Cedefop) töövahend: Skills-OVATE | CEDEFOP (europa.eu)

Praeguseks on loodud juba terve hulk avaliku ja erasektori küberturbeoskuste valdkonda investeerimise algatusi, mida **rahastatakse** ELi-üleste mehhanismidega eri instrumentide alusel[28]. Kuid oskustega töötajate jätkuv nappus ELis tekitab küsimusi selliste algatuste nähtavuse ja mõju kohta ning viitab sellele, et need ei pruugi alati vastata turu vajadustele, mis tuleks ELi tasandil kiiresti kaardistada. Lisaks toovad eri rahastamisallikad kaasa dubleerimisohu, mis ei võimalda suuremat edasiminekut ega lase avaldada ulatuslikumat mõju. Lisaks ei suuda need, kes vajavad investeeringuid, alati leida oma vajaduste jaoks kõige sobivamaid rahastamisallikaid.

Sidusrühmad on püüdnud leida lahendusi küberturbeoskustega töötajate nappuse keeruka ja mitmetahulise probleemi lahendamiseks. Euroopa Liidu Küberturvalisuse Amet (ENISA) töötab välja kõrgharidust ja ametikirjeldusi reguleerivaid instrumente,[29] küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus (ECCC)[30] on loonud küberturbeoskuste käsitlemiseks omaette töörühma, Euroopa Julgeoleku- ja Kaitsekolledž käsitleb tsiviil- ja sõjaväeliste töötajate küberturbeoskusi ühise julgeoleku- ja kaitsepoliitika raames,[31] eraorganisatsioonid otsivad omapoolseid lahendusi,[32] küberturvalisuse valdkonna sertifitseerijad töötavad oskuste nappuse leevendamiseks välja teekaarti ja koolituskavasid[33]. Liikmesriigid on püüdnud seda küsimust käsitleda ühelt poolt regulatiivsete algatustega,[34] teisalt on rajatud küberturbeoskuste akadeemiaid[35] ja küberlinnakuid[36], küberkuritegevuse tippkeskusi[37] ning avaliku ja erasektori partnerlusi[38]. Sageli on aga jäänud sidusrühmadel puudu tegevuse koordineeritusest ega ole saavutatud koostoimet. Samuti ei ole suudetud oluliselt muuta tööturgu, nagu näitab ELi küberturvalisuse valdkonna tööjõu süvenev nappus. Ühtlasi on vaja suurendada koostoimet küberkogukondade vahel, kuna vajalikud oskused küberturvalisuse säilitamiseks, **küberkuritegevuse** ohjeldamiseks ja **küberkaitsemeetmete** väljatöötamiseks on sageli sarnased.

Lisaks on vahendid, mida ELil on võimalik kasutada **küberturvalisuse valdkonna tööturu olukorra ja arengu** ning oma tööjõu oskuste hindamiseks, piiratud. Liikmesriigid ja ELi institutsioonid, organid ja asutused saavad praegu tugineda kas eraõiguslike asutuste kogutud andmetele või laiemalt IKT-spetsialiste käsitlevatele andmetele, mida ELis on kogunud eelkõige Eurostat[39] ja Euroopa Kutseõppe Arenduskeskus (CEDEFOP)[40]. Teisisõnu on ELil

---

[27] „The Future of Jobs Report“ (Aruanne töökohtade tuleviku kohta), oktoober 2020, Maailma Majandusfoorum

[28] Näiteks: küberturbeoskuste ühendus – Euroopa uus visioon – projekt „REWIRE“ (rahastatud programmist „Erasmus+“); küberturvalisuse valdkonna pädevuskeskust toetavad projektid (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (rahastatud programmist „Horisont 2020“), projekt „Cybersecpro“ (rahastatud programmist „Digitaalne Euroopa“).

[29] Näiteks: Euroopa küberturbeoskuste raamistik (ESCF); CYBERHEAD – Küberturvalisuse alane kõrghariduse andmebaas; küberõppuste platvorm (CEP); Euroopa küberturvalisuseteemaline võistlus; Euroopa küberturvalisuseteemaline kuu.

[30] Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik.

[31] Eelkõige küberkaitsehariduse, -koolituse ja -õppuste ning hindamise (ETEE) platvorm

[32] Näiteks Euroopa Küberturvalisuse Organisatsiooni 5. töörühm „Haridus, koolitus, teadlikkus, küberharjutusväljad, inimtegurid“; organisatsioon DIGITALEUROPE

[33] Näiteks SANS Institute, (ISC)², ISACA.

[34] Näiteks riiklikes haridus- ja küberturbestrateegiates.

[35] Näiteks Portugali C-Academy

[36] Näiteks Prantsusmaa Campus Cyber

[37] Näiteks Leedu küberkuritegevuse alane koolituse, teadusuuringute ja hariduse tippkeskus(L3CE)

[38] Näiteks Microsofti küberturbeoskuste algatus.

[39] IKT-spetsialistid tööhõives – Statistics Explained (europa.eu)

[40] Näiteks Euroopa Kutseõppe Arenduskeskuse (Cedefop) töövahend: Skills-OVATE | CEDEFOP (europa.eu)

oma vajadustest osaline ja killustatud ülevaade, mis ei ole lubanud luua tervikpilti küberturvalisuse valdkonna tööturu olukorrast.

3. Küberturbeoskuste akadeemia – ELi-ülene koordineeritud tegevus

3.1.Eesmärk

Küberturbeoskuste käsitlemisega seotud raskuste ületamiseks ja tööturu nõudluse rahuldamiseks loob komisjon Euroopa oskuste aasta kontekstis **küberturbeoskuste akadeemia**, nagu teatas Euroopa Komisjoni president oma 2022. aasta Euroopa Liidu olukorda käsitlevale kõnele lisatud kavatsusavalduses[41], [42].

Küberturbeoskuste akadeemia (edaspidi „akadeemia“) näol luuakse ühtne **kontaktpunkt ja koostoimekeskus**, mille abil arendada küberturvalisuse valdkonnas hariduse ja koolituse pakkumist ning rahastamisvõimalusi ja erimeetmeid küberturbeoskuste arendamise toetamiseks. Sellega hoogustatakse sidusrühmade algatusi sellise tasemeni, mis võimaldab tuua muutusi tööturul, sealhulgas kaitsevaldkonnas. Suurema mõjukuse saavutamiseks kujundatakse akadeemia tegevus ühiste eesmärkide ja valitud tulemusnäitajate järgi.

Akadeemia tegevuse keskmes hakkab olema **küberturvalisuse spetsialistide** õpetamine. Akadeemia tegevusest lähtutakse ELi küberturvalisuse poliitika kujundamisel, aga see peab andma sisendi ka haridussüsteemi ja elukestvasse õppesse. Koos käesoleva teatisega esitas komisjon kaks nõukogu soovituse ettepanekut, ühe digiõppe ja teise digioskuste kohta[43].

Akadeemia toetub neljale sambale: 1) **haridus- ja koolituspõhine teadmusloome**, milleks töötatakse välja küberturvalisuse valdkonna ametikirjelduste ja nendega seotud oskuste ühine raamistik, tugevdatakse tööturu vajaduste rahuldamiseks haridus- ja koolitusvõimaluste pakkumist Euroopas, luuakse tööturu pakkumise poole tugevdamiseks karjäärivõimalusi ja muudetakse küberturvalisuse valdkonna koolituskavad ja sertifikaadid nähtavamaks ja selgemaks; 2) olemasolevate **rahastamisvõimaluste** täpsem suunamine ja suurem nähtavus oskustega seotud tegevuste mõju maksimeerimiseks; 3) sidusrühmade **algatused**; 4) näitajad, mille abil **jälgida turu arengut** ja olla valmis hindama tegevuste tulemuslikkust.

Akadeemia elluviimist toetatakse 10 miljoni euroga programmist „Digitaalne Euroopa“[44].

3.2.Akadeemia juhtimine

Et pakutav taristu saaks toimida akadeemiliste ringkondade, koolitajate ja ettevõtete vahel koostööd võimaldava **ühtse kontaktpunktina**, mis tooks koolitamise otstarbel kokku ELi küberturvalisuse ökosüsteemi pakkumise ja nõudluse poole esindajad, peaks akadeemia võtma **Euroopa digitaristu konsortsiumi (EDIC)**[45] vormi. See instrument võimaldaks liikmesriikidel teha ühiseid samme küberturbeoskuste nappuse kõrvaldamiseks, teha igaühe volituste ja pädevuse piires tihedat koostööd komisjoni, Euroopa Liidu Küberturvalisuse Ameti (ENISA) ja küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskusega (ECCC) ning koondada ühise eesmärgi saavutamiseks kõik

[41] 2022. aasta Euroopa Liidu olukorda käsitlevale kõnele lisatud kavatsusavaldus, mis on adresseeritud Euroopa Parlamendi presidendile Roberta Metsolale ja Tšehhi peaministrile Petr Fialale

[42] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“ (JOIN(2022) 49 final).

[43] Ettepanek võtta vastu nõukogu soovitus edukat digiõpet ja -koolitust võimaldavate peamiste tegurite kohta ning nõukogu soovitus hariduses ja koolituses digioskuste õpetamise täiustamise kohta..

[44] Euroopa Parlamendi ja nõukogu 29. aprilli 2021. aasta määrus (EL) 2021/694, millega luuakse programm „Digitaalne Euroopa“ ja tunnistatakse kehtetuks otsus (EL) 2015/2240

[45] Euroopa digitaristu konsortsiumid on sätestatud Euroopa Parlamendi ja nõukogu 14. detsembri 2022 otsuses (EL) 2022/2481, millega luuakse digikümnendi poliitikaprogramm 2030; artikkel 13 jj.

asjaomased sidusrühmad ning Euroopa tasandi, liikmesriikide ja erasektori otseinvesteeringud. Selleks võiksid huvitatud liikmesriigid esitada komisjonile 30. maiks 2023 eelteate oma kavatsuse kohta asutada digitaristu konsortsium. Vabatahtlik eelteade lubaks komisjonil esitada Euroopa digitaristu konsortsiumi asutamise taotluse kohta esialgseid kommentaare, mis võimaldaks taotlust täiustada ja selle ametlikku esitamist kiirendada. Kogu protsessi jooksul ja liikmesriikide soovitavas ulatuses tegutseb komisjon mitut riiki hõlmava projekti kiirendajana ja hõlbustab Euroopa digitaristu konsortsiumi taotluse ettevalmistamist. Pärast seda, kui komisjon on taotlusele andnud positiivse hinnangu ja digikümnendi programmikomitee on selle heaks kiitnud, teeb komisjon otsuse Euroopa digitaristu konsortsiumi asutamise kohta ja aitab seejärel koordineerida Euroopa digitaristu konsortsiumi elluviimist[46].

Sel ajal, kui Euroopa digitaristu konsortsiumit ametlikult asutatakse, tõhustab komisjon Euroopa küberturvalisuse kogukonna toetusprojektis (ECCO) osalejate toel[47] **digioskuste ja töökohtade platvormi**,[48] et luua ühtne virtuaalne kontaktpunkt.

Euroopa Liidu Küberturvalisuse Amet aitab kooskõlas ameti eesmärkidega[49] kaasa akadeemia elluviimisele ja osutab eelkõige abi küberturvalisuse alase hariduse ja koolituse valdkonnas, võttes arvesse küberturvalisuse 2. direktiivi kohast aruandluskohustust[50]. **Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus** lähtub küberturbeoskuste akadeemia elluviimise toetamisel oma strateegilisest tegevuskavast. Eelkõige rakendab küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus programmi „Digitaalne Euroopa“ 3. strateegilist eesmärki (Küberturvalisus). Seda tegevust toetab komisjon, samuti liikmesriigid oma **riiklike koordineerimiskeskuste** kaudu. Vajaduse korral kutsutakse kokku küberturvalisuse 2. direktiivi[51] alusel loodud **koostöörühm**. Kokkuvõttes on vaja ühendada jõud **ettevõtlus- ja akadeemiliste ringkondadega**, et saavutada akadeemia eesmärk korvata küberturbeoskuste nappus.

4. Teadmusloome ja koolitus: ELi küberturbekoolituse ühine lähenemisviis

Küberturbeoskuste akadeemia teadmusloome ja koolituse sambas töötatakse välja struktureeritud lähenemisviis, millega suurendada küberturbeoskustega inimeste **arvu** ELis, kohandada koolitusi paremini **turuvajadustega** ja muuta **karjäärivõimalused** nähtavamaks.

4.1. Rääkides ühte ja sama keelt: küberturvalisuse valdkonna ametikirjelduste ja nendega seotud oskuste ühtlustamine

[46] Samas, artikkel 12.

[47] Vt Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ja võrgustik: uus ELi rahastatud projekt küberkogukonna toetamiseks (europa.eu). 2022. aasta detsembris allkirjastas Euroopa Komisjon küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse raames 3 miljoni euro suuruse lepingu ELi küberkogukonna toetamiseks. Selle projektiga aidatakse saavutada ELi kogukonnaloome ja suutlikkuse suurendamise eesmärke küberturvalisuse uuringute, innovatsiooni, omaksvõtu ja tööstusbaasi valdkonnas.

[48] Avaleht | digioskuste ja töökohtade platvorm (europa.eu)

[49] „ENISA toetab suutlikkuse ja valmisoleku arendamist kogu liidus sellega, et aitab liidu institutsioonidel, organitel ja asutustel ja liikmesriikidel ning avaliku ja erasektori sidusrühmadel arendada küberturvalisuse valdkonna oskusi ja pädevusi.“ Küberturvalisuse määruse artikli 4 lõige 3.

[50] Küberturvalisuse 2. direktiivi artikkel 18

[51] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv).

Euroopa Liidu Küberturvalisuse Amet on juba alustanud Euroopa küberturbeoskuste raamistiku (**ECSF**) kaudu[52] tööd küberturvalisuse spetsialistide ametikirjelduste kindlaksmääramiseks. Sellest tuleks kujundada alus, millele tuginedes määrab akadeemia kindlaks asjakohased oskused ja hindab neid, jälgib oskuste nappuse arengut ja annab teavet uute vajaduste kohta. Igale Euroopa küberturbeoskuste raamistiku[53] kohasele ametikirjeldusele on lahutamatu osana lisatud vastav Euroopa e-pädevuste raamistiku[54] element.

Seetõttu vaatab Euroopa Liidu Küberturvalisuse Amet Euroopa küberturbeoskuste raamistiku läbi ning teeb kindlaks küberturvalisuse valdkonna töötajate **kasvavad vajadused ja lüngad**, kasutades muu hulgas täiustatud tehnoloogiat (nt tehisintellekt, suurandmed,[55] andmekaeve). Sel eesmärgil teeb Euroopa Liidu Küberturvalisuse Amet Euroopa digitaristu konsortsiumi (kui see on loodud) ja küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse juhtimisel koostööd riiklike koordineerimiskeskuste, komisjoni, Euroopa küberturvalisuse kogukonna toetusprojektis osalejate ja turuosalistega[56]. Küberkaitse valdkonna töötajate puhul võtab Euroopa Liidu Küberturvalisuse Amet nõuetekohaselt arvesse Euroopa Julgeoleku- ja Kaitsekolledži tehtud tööd. Samuti võtab Euroopa Liidu Küberturvalisuse Amet küberkuritegevuse ohjeldamisel arvesse Euroopa Liidu Õiguskaitsekoolituse Ameti (CEPOL) ja Europoli tegevust küberrünnete tegevuskoolituse vajaduste analüüsi[57] koostamisel.

Euroopa küberturbeoskuste raamistikku täiendatakse korrapäraselt ja see vaadatakse akadeemia raames iga kahe aasta tagant läbi. Lisaks aitavad komisjon ja Euroopa välisteenistus ELi ametite ja organite, nagu Euroopa Julgeoleku- ja Kaitsekolledži,[58] Europoli ja CEPOLi[59] toel kindlaks määrata asjaomaste sektorite erivajadustele vastavaid ametikirjeldusi ja nendega seotud oskusi.

Samuti luuakse seosed Euroopa küberturbeoskuste raamistiku ja ELi tööhõivepoliitika asjakohaste vahendite vahel[60]. Muu hulgas on kavas lisada Euroopa küberturbeoskuste raamistiku ametikirjeldused ja nendega seotud oskused **oskuste, kompetentside, kvalifikatsioonide ja ametite Euroopa klassifikaatorisse**. See parandab küberturvalisuse valdkonnas ametikohtade ja oskuste klassifikatsiooni ja omavahelisi seoseid, lihtsustades

[52] Euroopa küberturbeoskuste raamistik (ECSF) – ENISA (europa.eu). Euroopa küberturbeoskuste raamistiku abil saab määrata kindlaks ja omavahel seostada Euroopa küberturvalisuse spetsialistide ametikirjeldustele vastavaid ülesandeid, pädevusi, oskusi ja teadmisi. Selles esitatakse kõik küberturvalisusega seotud tegevused koondatuna ühtseteks ametikirjeldusteks, millest igaühe puhul määratakse üksikasjalikult kindlaks kohustused, oskused, koostoimevajadus ja vastastikune sõltuvus teistest profiilidest.

[53] Euroopa e-pädevuste raamistik (e-CF) | Esco (europa.eu) Euroopa e-pädevuste raamistikuga on esitatud püsivad seosed IKT-pädevuste ja muude valdkonna jaoks oluliste raamistike, näiteks Euroopa kodanike digipädevuse raamistiku vahel.

[54] Vt selle kohta Euroopa küberturbeoskuste raamistiku (ECSF) kasutusjuhend, september 2022.

[55] Vt näiteks Euroopa Kutseõppe Arenduskeskuse (Cedefop) töövahend Skills-OVATE.

[56] ELi Küberturvalisuse Amet tugineb muude ELi rahastatud projektide (nt REWIRE, Euroopa ühtne oskuste andmeruum (DS4S), CyberSecPro, Concordia) tulemustele ja sarnastes algatustes (nt „Küberturbeoskustega töötajate väljaõpetamine viies riigis: Austraalia, Kanada, Uus-Meremaa, Ühendkuningriigi ja Ameerika Ühendriikide kogemused“, OECD aruanne, mis avaldati 21. märtsil 2023) kasutatud meetoditele, et arusaam vajadustest oleks nõudluse arenedes ka edaspidi ajakohane.

[57] CEPOLi tegevuskoolituse vajaduste analüüs (OTNA)

[58] Vt selle kohta ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“ (JOIN(2022) 49 final).

[59] Sellega seoses pööratakse tähelepanu küberkuritegevuse alase koolituse pädevusraamistikule, mida praegu välja töötatakse.

[60] Näiteks oskuste, kompetentside, kvalifikatsioonide ja ametite Euroopa klassifikaator (ESCO), Europass, Euroopa tööturuasutuste võrgustik (EURES).

üksikisikute oskuste täiendamist ja ümberõpet ning toetades oskustepõhist töövahendust ja piiriülest liikuvust.

4.2.Koostöö küberturvalisuse alase hariduse ja koolituse õppekavade väljatöötamisel

Kui Euroopa digitaristu konsortsium on loodud, peaks liikmesriigid akadeemiat toetama, et muuta see Euroopas **küberturbekoolituste kavandamise ja pakkumise keskuseks**, mis suudaks õpetada kõige nõutumaid oskusi ning pakkuda idufirmadele ja VKEdele ning haldusasutustele küberturvalisusega tegelevates uuenduslikes ettevõtetes ja küberturvalisuse pädevuskeskustes töökohapõhist õpet ja praktikavõimalusi. Et kujundada välja kõigi küberturvalisuse koolitusprogrammide parimad tavad, peaks Euroopa digitaristu konsortsium tegema koolituste kavandamisel koostööd kõigi asjaomaste sidusrühmadega, sealhulgas ettevõtetega, ja tuginema sellistele projektidele nagu **CyberSecPro**,[61] mida rahastatakse programmist „Digitaalne Euroopa“ ja mis ühendab 17 kõrgharidusasutust ja 13 turvaettevõtet 16 liikmesriigist.

Akadeemia teeb koostööd kõigi asjaomaste sidusrühmadega, et **meelitada noori** valima küberturvalisuse eriala. Kooskõlas nõukogu soovituse ettepanekuga hariduses ja koolituses digioskuste õpetamise täiustamise kohta peaksid liikmesriigid kehtestama ja tugevdama meetmeid spetsialiseerunud õpetajate ja koolitajate värbamiseks ja koolitamiseks ning küberturbeoskuste omandamise hõlbustamiseks, sealhulgas praktikakohtade kaudu. Soodustada tuleks küberturvalisuse küsimuste integreerimist haridus- ja koolitusprogrammidesse ja tagada samal ajal nende kättesaadavus. Selleks tuleks arendada **õpipoisiõppe**- ja praktikavõimalusi, edendada uuenduslikke lähenemisviise, sealhulgas näiteks tõsimänge ja jagatud simulatsiooniplatvorme, korraldada küberturvalisusega seotud ametikohtadel kümblusõppenädalaid ning täpsustada mittetehniliste ametikohtade kirjeldusi. Samuti tuleks luua küberturvalisuse alases õppes osalemise võimalusi raskesti ligipääsetavate rühmade, nagu kõrvalistes piirkondades elavate, puuetega noorte ja muude vähemusrühmade jaoks.

Komisjon toetab jätkuvalt mikrokvalifikatsioonitunnistusega päädivate kursuste ja kutseõppekavade väljatöötamist. Programmi „Erasmus+“ raames rahastatakse jätkuvalt **ühiseid bakalaureuse- ja magistriõppekavu**, **mikrokvalifikatsioonitunnistusega päädivaid ühiseid kursusi ja mooduleid** ning **kombineeritud intensiivõppekavu**[62] kõigil teemadel, sealhulgas **küberturvalisuse valdkonnas**. Samuti tuleb toetada **Euroopa ülikoolide algatuse**[63] ja **kutsehariduse tipptaseme keskuste**[64] käivitumist, et kehutada kõrgharidus- ja asjaomaseid kutseharidusasutusi kogu Euroopas suuremale koostööle. Sellist tihedamat koostööd toetataks ELi rahastamisprogrammidega, sealhulgas programmiga „Erasmus+“ ja programmiga „Digitaalne Euroopa“, samuti **isiklike õppekontode**[65] arendamiseks ette nähtud ELi rahaliste vahenditega.

Et hõlbustada liikmesriikides koostööd ühelt poolt akadeemiliste ringkondade ja küberturbeoskuste koolitajate ning teiselt poolt era- ja avaliku sektori tööandjate vahel ning

[61] CyberSecPro . See hakkab näiteks tegema ülikoolides pakutavate küberturvalisuse programmide, kursuste ja suvekoolide ning Euroopa ainepunktisüsteemi (ECTS) kasutatavate hindamistabelite analüüsi, kaasab kolme aasta jooksul rohkem kui 530 praktikanti ja koolitab väliseid isikuid eri tööstusharudest ja sektoritest.

[62] Kombineeritud intensiivõppekavades kaasnevad veebiõppega lühiajalised kohalõppeperioodid.

[63] Euroopa ülikoolide algatus |Euroopa haridusruum (europa.eu).

[64] Kutsehariduse tipptaseme keskused | Erasmus+ (europa.eu)

[65] Kooskõlas nõukogu 16. juuni 2022. aasta soovitusega, mis käsitleb isiklikke õppekontosid.

luua avaliku ja erasektori vahel koostoimet, kutsutakse riiklikke koordineerimiskeskusi üles uurima võimalusi luua liikmesriikidesse **küberlinnakuid**. Küberlinnakud peaksid hakkama toimima küberturvalisuse kogukonna riikliku tasandi tippkeskustena. Akadeemia aitaks neil luua suhteid teiste liikmesriikide küberlinnakutega ja oma tegevust koordineerida.

Et suurendada liikmesriikide koolituspakkumisi, tõhustab Euroopa Liidu Küberturvalisuse Amet küberturbekoolitust, viies oma **kursusekataloogi**[66] kooskõlla Euroopa küberturbeoskuste raamistiku ametikirjeldustega ja töötades välja igale ametikirjeldusele vastava koolitusmooduli. Euroopa Liidu Küberturvalisuse Amet laiendab ka oma **koolitajate koolitamise programmi**,[67] võttes arvesse ELi institutsioonide, organite ja asutuste ning liikmesriikide ametiasutuste ning küberturvalisuse 2. direktiivi kohaste **avaliku ja erasektori elutähtsate teenuste operaatorite** vajadusi.

Lisaks parandavad muud ELi ametid ja organid oma küberturbekoolituste pakkumist. ELi küberkaitsepoliitika rakendamisel töötab **Euroopa Julgeoleku- ja Kaitsekolledž** välja uued küberturvalisuse valdkonna kursused ja viib mõned oma praegused kursused Euroopa küberturbeoskuste raamistikuga kooskõlla. Nende uute kursuste loomisel saab õpiväljundid sertifitseerida[68]. Euroopa Julgeoleku- ja Kaitsekolledž uurib koostöös komisjoniga võimalust integreerida sertifikaadid Euroopa digiidentiteedikukrusse. Euroopa Julgeoleku- ja Kaitsekolledž uurib täiendavalt, milliseid mehhanisme võiks kasutada sertifikaatide väljastamise aluseks olevate oskuste hindamisel. Samuti püütakse küberkuritegevuse vastase võitluse vallas luua tihedad sidemed **CEPOLi küberkuritegevuse akadeemiaga**,[69] et otsida koolituskavade koostamisel ja rakendamisel koostoimet ja täiendavust.

4.3.Küberturbekoolituste ja sertifitseerimise koostoime ja nähtavus kõigis liikmesriikides

Akadeemia peaks pöörama tähelepanu koolituste ja sertifikaatide nähtavusele ja koostoimele. Sellest oleks kasu nii tsiviil-, kaitse-, õiguskaitse- kui ka diplomaatiaalasele küberkogukonnale, kuna kõik sektorid vajavad paljudel juhtudel samu teadmisi, mis põhinevad sarnastel õppekavadel ja õpitulemustel.

Akadeemia toimiks **ühtse kontaktpunktina** nende jaoks, kes on huvitatud küberturvalisuse alasest karjäärist. Lühiajalises perspektiivis tõhustatakse selleks Euroopa küberturvalisuse kogukonna toetusprojektis osalejate toel komisjoni **digioskuste ja töökohtade platvormi**. Teatav osa küberturvalisuse valdkonna karjäärimudelitest seotakse olemasolevate vahenditega. See puudutab nii kõrghariduskavasid kui ka koolitusvõimalusi, sealhulgas mikrokvalifikatsioonitunnistusega päädivaid kursusi ja kutseõppekavasid, ja tööpakkumisi. Selleks toetutakse juba tehtud jõupingutustele ja käivitatud algatustele, neid platvormiga integreerides. Näiteks Euroopa Liidu Küberturvalisuse Amet on koostöös akadeemiliste ringkondadega **kaardistanud haridusasutused**, mis pakuvad küberturvalisuse programme. Seda tegevust peaksid aitama tõhustada riiklikud koordineerimiskeskused. Lisaks töötab Euroopa Liidu Küberturvalisuse Amet riiklike koordinatsioonikeskuste, komisjoni ja Euroopa küberturvalisuse kogukonna toetusprojektis osalejate toel ning koostöös

[66] Koolituskursused — ENISA (europa.eu)

[67] Koolitajate koolitamise programm — ENISA (europa.eu)

[68] Kooskõlas nõukogu 19. oktoobri 2020. aasta otsuse (ÜVJP) 2020/1515 (millega luuakse Euroopa Julgeoleku- ja Kaitsekolledž ning tunnistatakse kehtetuks otsus (ÜVJP) 2016/2382) artikli 20 lõikega 4.

[69] 2019. aastal loodi CEPOLi küberkuritegevuse akadeemia näol tipptasemel platvorm, millega parandada Euroopas küberkuritegevuse alaseid teadmisi ja kübersuutlikkust.

sertifitseerimisasutustega ja muudele asjakohastele algatustele[70] tuginedes välja kaks **avaliku ja erasektori koolituste ja küberturvalisuse sertifikaatide hoidlat**. Need integreeritakse ka digioskuste ja töökohtade platvormi ühtsesse kontaktpunkti. Hoidlaid saavad oma töös kasutada ka riiklikud koordineerimiskeskused, kelle ülesandeks ongi just küberturvalisuse haridusprogramme[71] edendada ja levitada.

Samuti on vaja anda kutsetöötajatele kinnitus selle kohta, et koolitus, millel nad osalevad, on nõutava tasemega. Sellega seoses töötab Euroopa Küberturvalisuse Amet välja Euroopa küberturvalisuse atesteerimiskava koostamise uurimiseks **katseprojekti**.

Ehkki oskuste ja koolituste kindlaksmääramine ning nende sidumine ametikirjeldustega on oluline, on ühtlasi tarvis tagada see, et küberturbeteenuste osutajad oleksid vajaliku pädevuse, oskuste ja kogemustega. See kehtib eelkõige turbetarnijate kohta sellistes valdkondades nagu intsidentidele reageerimine, läbistustestimine, turvaauditid ja konsultatsioonid. Küberturvalisuse 2. direktiivis ja kübersolidaarsuse määruse ettepanekus on sätestatud turbetarnijate konkreetsed ülesanded. Seepärast teeb komisjon ettepaneku **küberturvalisuse määrust**[72] **sihipäraselt muuta**, et näha ELi tasandil ette turbetarnijate sertifitseerimise kavad. Sertifitseerimiskavadega tuleks muu hulgas tagada see, et teenuseid osutavad töötajad, kellel on asjaomastes valdkondades väga rikkalikud tehnilised teadmised ja pädevus.

Mikrokvalifikatsioonide kvaliteedi tagamise ja tunnustamise mehhanismid[73] aitavad parandada õpitulemuste läbipaistvust, võrreldavust ning ülekantavust. Kooskõlas nõukogu soovitusega, milles käsitletakse Euroopa lähenemisviisi mikrokvalifikatsioonitunnistustele,[74] julgustatakse liikmesriike lisama küberturvalisuse mikrokvalifikatsioonitunnistused oma riiklikesse kvalifikatsiooniraamistikesse. See võimaldaks neil siduda küberturvalisuse mikrokvalifikatsioonitunnistused Euroopa kvalifikatsiooniraamistikuga[75]. Euroopa digitaalsete kvalifikatsioonitunnistuste taristu võimaldab välja anda digitaalselt allkirjastatud üksikisikute küberturvalisuse valdkonna kvalifikatsiooni- ja mikrokvalifikatsioonitunnistusi. Need sisaldavad rikkalikke andmeid, sealhulgas küberturvalisuse valdkonna õpiväljundite kohta, ja neid saab säilitada tulevases **Euroopa digiidentiteedikukrus**[76].

Akadeemiaga seotud meetmed

Liikmesriigid ja erasektor

[70] Näiteks W4C Academy – Women4Cyber või õiguskaitse- ja kohtuasutuste ülemaailmse küberkuritegevuse sertifitseerimise projekt.

[71] "1. Riiklikel koordineerimiskeskustel on järgmised ülesanded: (...) g) ilma et see piiraks liikmesriikide pädevust hariduse valdkonnas ja võttes arvesse ENISA asjakohaseid ülesandeid, suhelda riiklike asutustega seoses nende võimaliku panusega küberturvalisuse alaste haridusprogrammide edendamisse ja levitamisse" (küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse määruse artikli 7 lõike 1 punkt g). Vt ka seonduv põhjendus 28.

[72] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta 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).

[73] Näiteks väiksemahuliste koolituste õpiväljundite registreerimine ja tõendamine.

[74] Nõukogu soovitus, milles käsitletakse Euroopa lähenemisviisi elukestvat õpet ja tööalast konkurentsivõimet toetavatele mikrokvalifikatsioonitunnistustele.

[75] Nõukogu 22. mai 2017. aasta soovitus, milles käsitletakse elukestva õppe Euroopa kvalifikatsiooniraamistikku ning millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu 23. aprilli 2008. aasta soovitus Euroopa kvalifikatsiooniraamistiku loomise kohta elukestva õppe valdkonnas

[76] Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega.

- Tagada toetus küberturvalisuse alase õppe **mikrokvalifikatsioonitunnistuste** väljatöötamisele ja tunnustamisele kooskõlas nõukogu soovitusega, mis käsitleb Euroopa lähenemisviisi mikrokvalifikatsioonitunnistustele.
- Lisada küberturvalisuse valdkonna kvalifikatsioonid, sealhulgas mikrokvalifikatsioonid **riiklikesse kvalifikatsiooniraamistikesse**.
- Pakkuda küberturbeoskuste arendamise algatustes osalevatele inimestele õpipoisiõppe näol **töökohapõhise õppe võimalust**.

Komisjon

- Luua **digioskuste ja töökohtade platvormi** kaudu 2023. aasta lõpuks küberturvalisuse programmide, olemasolevate koolituste ja küberturvalisuse sertifitseerimise jaoks **ühtne kontaktpunkt** (lühiajaline perspektiiv).
- Teha 18. aprillil 2023 ettepanek muuta **küberturvalisuse määrust**, et võimaldada turbetarnijate sertifitseerimist.

ELi organid ja asutused

- Luua 2023. aasta lõpuks **Euroopa küberturbeoskuste raamistik**, mille abil ühtlustada küberturvalisuse valdkonna ametikirjeldusi ja nendega seonduvaid oskusi.
- Euroopa Liidu Küberturvalisuse Amet: algatada 2023. aasta teises kvartalis katseprojekt, millega luua **Euroopa küberturbeoskuste atesteerimise kava**.
- Euroopa Liidu Küberturvalisuse Amet: vaadata läbi oma **kursusekataloog** ja käivitada avaliku ja erasektori elutähtsate teenuste operaatorite jaoks 2023. aasta lõpuks **koolitajate koolitamise programm**.
- Viia 2023. aasta keskpaigaks lõpule **Euroopa Julgeoleku- ja Kaitsekolledži õppekavade vastavusse viimine Euroopa küberturbeoskuste raamistikuga**.

5. Sidusrühmade lubadused panustada küberturbeoskustega töötajate nappuse ületamisse

Et võtta käsile küberturbeoskustega töötajate nappus, töötatakse akadeemia raames välja sidusrühmade kaasamise koordineeritud lähenemisviis. Sellega püütakse muuta sammud, mida sidusrühmad küberturbeoskustega töötajate nappuse vähendamiseks teevad, võimalikult nähtavaks ja mõjukaks.

Komisjon kutsub sidusrühmi üles andma töötajate ümberõppesse ja nende oskuste täiendamisse panustamisel selgeid lubadusi, tuginedes sealjuures võimalikult palju küberturbeoskuste vallas kindlaks tehtud lünkadele. **Sidusrühmade küberturvalisuse alastest lubadustest** tuleks teada anda **digioskuste ja töökohtade platvormi** kaudu, nagu on tehtud muude digivaldkonna lubadustega, mis on praeguseks platvormil nähtavad. Komisjon julgustab sidusrühmi, kes on andnud platvormi kaudu küberturvalisuse alase lubaduse, liituma ka **oskuste pakti digitaalse ökosüsteemi alase ulatusliku partnerlusega**[77]. Digioskuste ja töökohtade platvormi kaudu tuleks esitada ka digitaalse ökosüsteemi alase ulatusliku partnerluse raames antud küberturvalisuse alaseid lubadusi. Teisipidi tuleks ka digioskuste ja töökohtade platvormi raames antud lubadustest teada anda oskuste pakti digitaalse ökosüsteemi alase ulatusliku partnerluse raames.

[77] Uued Euroopa partnerlused, mille abil muuta digikümnendi eesmärgid tegelikkuseks | Euroopa digituleviku kujundamine (europa.eu). Partnerlused on loodud oskuste pakti alusel IKT-valdkonna puuduste kõrvaldamiseks.

Lisaks kutsub komisjon liikmesriike üles **jätkama jõupingutusi deklaratsiooni „Naised digivaldkonnas“**[78] rakendamiseks, et julgustada naisi etendama digitaaltehnoloogia sektoris aktiivset ja olulist osa ning saavutama küberturvalisusega seotud ametikohtadel parema soolise tasakaalu. Samuti julgustab komisjon liikmesriike arendama koostoimet **Euroopa Sotsiaalfond+** (ESF+) programmidega, et toetada täiendavalt tööhõive soolise võrdsuse eesmärki, [79] näiteks **naiste ja tütarlaste jaoks loodud asjakohaste mentorlusprogrammide** abil. Selliste programmide abil saab luua tütarlaste jaoks rollimudeleid, et meelitada neid küberturvalisuse kutsealadele, ja võidelda samal ajal sooliste stereotüüpide vastu. Samuti soodustaks see naiste oskuste täiendamist ja ümberõpet ning aitaks luua sellist kogukonda, mis toetab naisi küberturvalisuse valdkonna tööturule sisenemisel ja seal karjääri tegemisel.

Liikmesriigid peaksid võtma oma **riiklikus küberturvalisuse strateegias vastu meetmed, millega küberturbeoskustega töötajate nappust leevendada,**[80] määrates kindlaks sammud, mida astuda oskuste nappuse korvamiseks, ja kujundades neid sihipärasemaks, et tagada kokkuvõttes küberturvalisuse 2. direktiivi kohaste kohustuste nõuetekohane täitmine.

Mõned liikmesriigid on püüdnud luua **koostoimet tsiviil-, kaitse- ja õiguskaitsealgatuste vahel**. Näiteks saab tööjõudu kasvatada riikliku kohustusliku kaitseväeteenistuse arvelt ja rakendada küberreserviste ehk sõjaväelise väljaõppe saanud kodanikke, kes täidavad relvajõududes küberturvalisusega seotud ametikohti.[81] Selline koostoime võimaldaks elanikel ja eelkõige noortel täiskasvanutel oma küberturbe- ja küberkaitseoskusi arendada. Sama kehtib ka **küberkuritegevuse** ohjeldamise seisukohast, kuna üldiste küberturvalisuse valdkonna jõupingutuste ja küberintsidentidega seotud õiguskaitsetegevuse vahel on palju sarnasusi. Komisjon julgustab liikmesriike selliseid algatusi arutama ja kutsub üles hindama, kuidas vajalike oskustega tööjõud saaks kõige paremini teenindada nii küberturvalisuse valdkonna kaitse- kui ka tsiviilkogukondi.

Komisjon kaalub ettepanekuid selle kohta, kuidas täita praegused ja edaspidi tekkivad lüngad, mis on ELi institutsioonide, organite ja asutuste vajaduste läbivaatamisel avastatud. Muu hulgas julgustab komisjon töötajaid kasutama ELi ja USA vahelise dialoogi raames edaspidi loodavat **ELi ja Ameerika Ühendriikide (USA) küberturvalisuse grandiprogrammi**.

Akadeemiaga seotud meetmed

Erasektor

- Anda 18. aprillil 2023 digioskuste ja töökohtade platvormi kaudu konkreetsed **küberturvalisuse alased lubadused**.

Liikmesriigid

- Lisada **oma riigi küberturvalisuse strateegiasse** meetmed küberturbeoskuste nappuse kõrvaldamiseks.

Liikmesriigid ja erasektor

[78] ELi riigid lubavad edendada naiste osalust digisektoris | Euroopa digituleviku kujundamine (europa.eu).

[79] Euroopa Parlamendi ja nõukogu 24. juuni 2021. aasta määruse (EL) 2021/1057 (millega luuakse Euroopa Sotsiaalfond+ (ESF+) ja tunnistatakse kehtetuks määrus (EL) nr 1296/2013) artikli 4 lõike 1 punkt c.

[80] Küberturvalisuse 2. direktiivi artikli 7 lõike 2 punkt f

[81] Aruanne – „Küberajateenistus: kogemused ja parimad tavad valitud riikidest“, Martin Hurt ja Tiia Sõmer, Rahvusvaheline Kaitseuuringute Keskus, veebruar 2021

- Rakendada deklaratsiooni „Naised digivaldkonnas“, et saavutada 2030. aastaks küberturvalisusega seotud ametikohtadel parem sooline tasakaal.

6. Rahastus: maksimeerida parema koostoime abil küberturbeoskuste arendamiseks tehtavate kulutuste mõju

Akadeemia kaudu maksimeeritakse küberturbeoskustesse tehtavate investeeringute mõju, luues ühtse kontaktpunkti, mille abil suunata rahalisi vahendeid paremini vastavalt turu vajadustele ja võtta rahalised vahendid laiemalt kasutusele ning tekitada koostoimet instrumentide vahel, vältides sealjuures jõupingutuste dubleerimist[82].

6.1. Rahastuse vastavus vajadustele

Akadeemia raames kogub küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus komisjoni, Euroopa küberturvalisuse kogukonna toetusprojektis osalejate ja riiklike koordineerimiskeskuste toel **teavet selle kohta, kuidas ELi vahendeid küberturbeoskuste rahastamiseks kasutatakse**, ning hindab, kuidas toetatakse ELi rahaliste vahenditega küberturbeoskustega töötajate nappuse vähendamist. Koondatud teabe põhjal püüab küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus parandada ELi rahaliste vahendite suunamist, lähtudes kindlakstehtud vajadustest. Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus rahastab meetmeid, millega kõrvaldada küberturvalisuse valdkonna töötajate kõige pakilisemad puudujäägid, sealhulgas need, mis on seotud küberturvalisuse poliitika rakendamisega.

6.2. Küberturbeoskuste rahastusvõimaluste ja partnerlusalgatuste nähtavus

Lühikeses perspektiivis hakkab sidusrühmade jaoks ühtse kontaktpunktina toimima **digioskuste ja töökohtade platvorm**, kus tehakse kättesaadavaks kogu teave küberturbeoskuste rahastamisvõimaluste kohta.

EL investeerib inimestesse ja nende oskustesse, sõlmides partnerlusi ettevõtlusringkondadega ning hoogustades **Euroopa oskuste tegevuskavas**[83] ette nähtud vahendite abil, sh **oskuste pakti**[84] ja **digiõppe tegevuskava**[85] abil, ümberõppe ja oskuste täiendamise meetmeid. **Programmist „Digitaalne Euroopa“** rahastatakse küberturbeoskustega seotud õppimisvõimalusi, sealhulgas mitut riiki hõlmavaid projektialgatusi, täiendades programmiga „Euroopa horisont“ küberturvalisuse alastele teadusuuringutele ja uuenduslikele tehnoloogilistele lahendustele pakutavat toetust. **Euroopa Kaitsefondist**[86] rahastatakse teadusuuringuid ja tehnoloogiaarendust, et viia läbi tulemuslikke küberoperatsioone,

[82] Rahastamisvõimalused (europa.eu) Oskuste pakti tugiteenistus loob oskuste rahastamisega seotud teabe jagamiseks ühtse kontaktpunkti, sealhulgas digitaalse ökosüsteemi jaoks. Oskuste pakti tugiteenistus annab rahastamisvahendite kohta üldist teavet, mis ei puuduta kitsalt küberturbeoskusi, kuid sellele vaatamata tuleks akadeemial selle tegevust dubleerimise vältimiseks arvesse võtta.

[83] Euroopa oskuste tegevuskava – Tööhõive, sotsiaalküsimused ja sotsiaalne kaasatus – Euroopa Komisjon (europa.eu)

[84] ELi rahastamisvahendid oskuste täiendamiseks ja ümberõppeks – Tööhõive, sotsiaalküsimused ja sotsiaalne kaasatus – Euroopa Komisjon (europa.eu)

[85] Digiõppe tegevuskava 2021–2027.

[86] Euroopa Parlamendi ja nõukogu 29. aprilli 2021. aasta määrus (EL) 2021/697, millega luuakse Euroopa kaitsefond ja tunnistatakse kehtetuks määrus (EL) 2018/1092

sealhulgas koolitusi ja õppusi[87]. Programmiga **„Erasmus+“** jätkatakse selliste algatuste toetamist, sealhulgas kombineeritud intensiivõppekavade ja koostööprojektide kaudu.

Liikmesriike julgustatakse kasutama ELi vahendeid, mida nad otseselt haldavad, küberturbeoskuste ja nendega seotud töökohtade toetamiseks. Ühtekuuluvuspoliitika vahendite, nagu **Euroopa Regionaalarengu Fondi** ja **ESF+** abil saaks oluliselt suurendada koostoimet selles valdkonnas[88].Ka **taaste- ja vastupidavusrahastu**[89] ja programm **„InvestEU“**[90] meetmete kohaldamisala võimaldab vastastikust täiendavust akadeemia eesmärkidega.

Akadeemiaga seotud meetmed

Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ja Euroopa Liidu Küberturvalisuse Amet

- **Kaardistada** 2024. aasta lõpuks ELi praegune küberturbeoskuste alane rahastus võrdluses turu vajadustega, hinnata selle **tulemuslikkust** ja määrata kindlaks **rahastusprioriteedid**.

Komisjon

- Luua 2023. aasta lõpuks digioskuste ja töökohtade platvormil küberturbeoskuste rahastamisvõimaluste jaoks **ühtne kontaktpunkt**.

7. Edusammude mõõtmine: integreeritud aruandlus

Akadeemia jaoks töötatakse välja **metoodika**, mis võimaldab **mõõta küberturbeoskuste nappuse kaotamisel tehtud edusamme**.

7.1. Küberturvalisuse näitajad, mille abil jälgida küberturvalisuse valdkonna tööturu arengut

Euroopa digitaalse tulemuslikkuse näitajad võetakse kokku **digitaalmajanduse ja -ühiskonna indeksi (DESI)** abil, mis võimaldab jälgida ELi liikmesriikide arengut. Küberturbeoskuste akadeemia kaudu töötab Euroopa Liidu Küberturvalisuse Amet koostöös komisjoni ja võrgu- ja infoturbe koostöörühmaga[91] välja **näitajad**, sealhulgas sooga seotud näitajad, et jälgida ELi liikmesriikides küberturvalisuse spetsialistide arvu suurendamisel tehtud edusamme, konsulteerides ka asjaomaste turuosaliste ja riiklike koordineerimiskeskustega. Euroopa Liidu Küberturvalisuse Amet tugineb digitaalmajanduse

[87] Liikmesriigid on lubanud viia läbi ühiseid koolitusi ja õppusi ning osaleda neil, mh alalise struktureeritud koostöö küberkoolituse ja -õppuste algatuste raames, nagu ELi küberakadeemia ja innovatsioonikeskus (EU CAIH) ja küberharjutusväljade liidud.

[88] Määruse (EL) 2021/1058 artikli 3 lõige 1 ja määruse (EL) 2021/1057 artikli 4 lõike 1 punkt g.

[89] Näiteks Eesti taaste- ja vastupidavuskavaga nähakse ette investeeringud digioskustesse (10 miljonit eurot), et muu hulgas vaadata läbi IKT-ekspertidele pakutavad koolitused, rahastada küberturvalisuse valdkonna IKT-spetsialistide oskuste täiendamist ja ümberõpet ning panustada IKT-spetsialistide kvalifikatsiooniraamistiku ümberkujundamise katseprojekti väljatöötamisse.

[90] Sidusrühmad (nt koolitajad ja ettevõtjad, kes soovivad kavandada küberturbekoolitusi või neid ümber kujundada) võivad pöörduda InvestEU nõustamiskeskuse poole, mis pakub projektide arendajatele ja ettevõtetele tehnilist tuge ja suutlikkuse suurendamist, ning tutvuda InvestEU portaaliga.

[91] Tuginedes küberturvalisuse 2. direktiivi artikli 18 lõike 3 kohasele metoodikale, mille Euroopa Liidu Küberturvalisuse Amet töötab välja, et koostada iga kahe aasta tagant aruanne küberturvalisuse olukorra kohta liidus, ja seda metoodikat täiendada.

ja -ühiskonna indeksi puhul kasutatud metoodikale[92] ja tagab, et näitajad oleks kooskõlas Euroopa digieesmärgiga suurendada IKT-spetsialistide arvu ning saavutada IKT valdkonnas parem sooline tasakaal. Seejärel võtab komisjon eesmärgiks integreerida sellised näitajad digitaalmajanduse ja -ühiskonna indeksisse, et oleks võimalik jälgida küberturbeoskuste ja selle valdkonna tööturu arengut aastate kaupa.

7.2.Andmete kogumine ja aruandlus

Euroopa Liidu Küberturvalisuse Amet kogub näitajate koostamiseks andmeid Euroopa küberturvalisuse kogukonna toetusprojektis osalejate ja riiklike koordineerimiskeskuste toel. Kogutud andmete põhjal koostab Euroopa Liidu Küberturvalisuse Amet **iga-aastase aruande**, mida kasutatakse mh selleks, et koostada digikümnendi olukorda käsitlev aruanne,[93] mida võetakse omakorda koos digitaalmajanduse ja -ühiskonna indeksiga arvesse **Euroopa poolaasta** riigipõhiste analüüside ja soovituste koostamisel[94]. Lisaks kasutatakse küberturbeoskusi kajastavaid näitajaid Euroopa Liidu Küberturvalisuse Ameti poolt **iga kahe aasta tagant koostatavas ELi küberturvalisuse olukorda käsitlevas aruandes**, mis on ette nähtud küberturvalisuse 2. direktiiviga ja mis kajastab küberturvalisuse alast võimekust ja teadlikkust ning küberhügieeni ELis.

7.3.Küberturvalisuse valdkonna põhilised tulemusnäitajad

Euroopa küberturvalisuse valdkonna talendinappuse korvamiseks esitab Euroopa Liidu Küberturvalisuse Amet tihedas koostöös komisjoni ja riiklike koordineerimiskeskustega komisjonile põhilised tulemusnäitajad, mis põhinevad digikümnendi poliitikaprogrammis 2030 esitatud metoodikal ja asjaomases valdkonnas saadud kogemustel. ELi Küberturvalisuse Amet võtab liikmesriikide kasutatavaid peamisi tulemusnäitajaid, mida riiklike küberturvalisuse strateegiate hindamiseks kasutatakse, nõuetekohaselt arvesse[95].

Akadeemiaga seotud meetmed

ELi Küberturvalisuse Amet (ENISA)

- Valmistada 2023. aasta lõpuks ette küberturbeoskusi kajastavad **näitajad, sh põhilised tulemusnäitajad**.
- Koguda näitajate koostamiseks **andmeid** ja anda nende kohta aru, kusjuures esimene kogumine peab toimuma 2025. aastaks.

Komisjon

- Töötada selle nimel, et integreerida küberturvalisuse näitajad **digitaalmajanduse ja -ühiskonna indeksisse** ja **digikümnendi olukorda käsitlevasse aruandesse**.

8. Kokkuvõte

Käesoleva teatisega pannakse paika ELi spetsialistide küberturbeoskuste edendamise uus lähenemisviis. Selle algatusega püütakse vähendada küberturbeoskuste nappust ja varustada EL pidevalt muutuvatele ohtudele reageerimiseks vajaliku tööjõuga, aidata kaasa ELi

[92] Vt Digitaalmajanduse ja -ühiskonna indeksi 2022. aasta väljaande metodoloogiline teade, mis on kättesaadav võrgulehel Digitaalmajanduse ja -ühiskonna indeks (DESI) | Euroopa digituleviku kujundamine (europa.eu).

[93] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta otsus (EL) 2022/2481, millega luuakse digikümnendi poliitikaprogramm 2030

[94] Samas, põhjendus 25.

[95] Küberturvalisuse 2. direktiivi artikli 7 lõige 4.

küberrünnete eest kaitsmise meetmete väljatöötamisele ning luua uusi ärivõimalusi ja suurendada ELi konkurentsivõimet. Vajalike oskustega küberturvalisuse valdkonna töötajatest oleks kasu **tsiviil-, kaitse-, diplomaatilisel ja õiguskaitsekogukonnal** ja paraneks koostoime nende kogukondade vahel.

Komisjon kutsub liikmesriike ja kõiki sidusrühmi üles küberturbeoskuste akadeemia loomisele kaasa aitama.