EUROOPA
KOMISJON

LIIDU VÄLISASJADE
JA JULGEOLEKUPOLIITIKA
KÕRGE ESINDAJA

Brüssel, 16.12.2020
JOIN(2020) 18 final

ÜHISTEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

ELi küberturvalisuse strateegia digikümnendi jaoks

ÜHISTEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

ELi küberturvalisuse strateegia digikümnendi jaoks

I. SISSEJUHATUS: KÜBERTURVALINE DIGIÜLEMINEK KEERULISES OHUKESKKONNAS

Küberturvalisus on eurooplaste julgeoleku lahutamatu osa. Olgu ühendatud seadmete ja elektrivõrkude puhul või pankades, õhusõidukites, haldusasutustes või haiglates – inimestel peab olema kõikjal kindlustunne, et nad on küberohtude eest kaitstud. ELi majandus, demokraatia ja ühiskond sõltuvad rohkem kui kunagi varem turvalistest ja usaldusväärsetest digivahenditest ja ühendatusest. Seetõttu on küberturvalisus vastupidava, keskkonnahoidliku ja digitaalse Euroopa ülesehitamiseks väga oluline.

Transport, energeetika ja tervishoid, telekommunikatsioon, rahandus, julgeolek, demokraatlikud protsessid, kosmose- ja kaitsevaldkond sõltuvad suurel määral võrgu- ja infosüsteemidest, mis on üha enam omavahel seotud. Sektoritevaheline vastastikune sõltuvus on väga suur, sest võrgud ja infosüsteemid omakorda sõltuvad stabiilsest elektrivarustusest. Ühendatud seadmeid on juba praegu rohkem kui planeedil inimesi ja prognooside kohaselt suureneb nende arv 2025. aastaks 25 miljardini[1] – neljandik neist Euroopas. Töökorralduse digitaliseerimist on kiirendanud COVID-19 pandeemia, mille ajal 40 % ELi töötajatest on läinud üle kaugtööle, millel on tõenäoliselt alaline mõju igapäevaelule[2]. See suurendab küberrünnetele avatud nõrku kohti[3]. Tarbijale tarnitakse sageli ühendatud seadmeid, millel on teadaolev turvaauk, mis suurendab veelgi pahatahtliku kübertegevuse ründepinda[4]. ELi tööstusmaastik on üha enam digitaliseeritud ja ühendatud. See tähendab seda, et küberrünnetel võib olla valdkondlikele sidusrühmadele ja ökosüsteemidele palju suurem mõju kui kunagi varem.

Ohumaastiku teevad keerukamaks geopoliitilised pinged, mis tekivad seoses ülemaailmse ja avatud interneti ning tehnoloogia üle kontrolli saamisega tarneahelas[5]. Nende pingete tõttu rajab üha rohkem rahvusriike digitaalseid piire. Piirangud internetis ja interneti suhtes ohustavad ülemaailmset ja avatud küberruumi ning õigusriigi põhimõtet, põhiõigusi, vabadust ja demokraatiat, mis on ELi põhiväärtused. Küberruumi kasutatakse üha

[1]Telekommunikatsioonivaldkonna kutseliidu GSMA hinnang, https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). International Data Corporation prognoosib 42,6 miljardit ühendatud masinat, sensorit ja kaamerat, https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2]2020. aasta juunis korraldatud uuringus ütles 47 % ettevõtete juhtidest, et nad kavatsevad võimaldada töötajatel teha täistööajaga kaugtööd isegi siis, kui on võimalik naasta töökohta, 82 % kavatses võimaldada osalist kaugtööd, https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[4]Seni üks kõige kahjulikumatest pahavaradest Mirai lõi rohkem kui 600 000 seadmest koosnevad bottnetid, mis häirisid paljude oluliste veebisaitide tööd Euroopas ja Ameerika Ühendriikides.

[5]Sealhulgas elektroonilised komponendid, andmeanalüüs, pilvandmetöötlus, 5G- ja veelgi parema ühendusega kiiremad ja arukamad võrgud, krüpteerimine, tehisintellekt ning uued arvutus- ja usaldusväärse andmetöötluse paradigmad, nagu plokiahel, üleminek pilvandmetöötluselt servtöötlusele ja kvantarvutus.

enam poliitilistel ja ideoloogilistel eesmärkidel ning suurenev polariseerumine rahvusvahelisel tasandil takistab tõhusat mitmepoolsust. Hübriidohud hõlmavad desinformatsiooni levitamise kampaaniaid koos taristu, majandusprotsesside ja demokraatlike institutsioonide vastu suunatud küberrünnetega, mille tagajärjeks võib olla füüsiline kahju, ebaseaduslik juurdepääs isikuandmetele, tööstus- või riigisaladuste vargus, usaldamatuse teke ja sotsiaalse ühtekuuluvuse nõrgenemine. Need tegevused õõnestavad rahvusvahelist julgeolekut ja stabiilsust ning kasu, mida küberruum toob majanduslikule, sotsiaalsele ja poliitilisele arengule.

Elutähtsa taristu sihipärane pahatahtlik ründamine on suur ülemaailmne oht[6]**.** Internetil on detsentraliseeritud ülesehitus, milles ei ole keskset struktuuri, ja sidusrühma-ülene juhtimine. See on suutnud tulla toime internetiliikluse mahtude üha kasvava suurenemisega, olles samal ajal pidevalt pahatahtlike rünnete sihtmärk[7]. Samal ajal usaldatakse üha enam ülemaailmse ja avatud interneti põhifunktsioone, nagu domeeninimede süsteem (DNS), ning põhilisi side ja veebimajutuse, rakenduste ja andmete jaoks vajalikke internetiteenuseid. Need teenused on üha enam koondunud väheste eraettevõtete kätte[8]. See muudab Euroopa majanduse ja ühiskonna haavatavaks geopoliitiliste ja tehnoloogiliste vapustuste suhtes, mis mõjutavad interneti tuuma või ühte või mitut sellist ettevõtet. Interneti laialdasem kasutamine ja pandeemia tõttu muutuvad kasutusmustrid on veelgi rohkem paljastanud digitaristust sõltuvate tarneahelate hapruse.

Mure turvalisuse pärast takistab inimestel veebiteenuseid kasutamast kõige enam[9]**.** Umbes kaks viiendikku ELi kasutajatest on puutunud kokku turvalisusprobleemidega ja kolm viiendikku tunneb, et nad ei suuda end küberkuritegevuse eest kaitsta[10]. Kolmandik on viimase kolme aasta jooksul saanud eksitavaid e-kirju või telefonikõnesid, milles küsitakse isikuandmeid, kuid 83 % ei ole kunagi küberkuritegevusest teatanud. Küberründed on mõjutanud üht ettevõtjat kaheksast[11]. Samal aastal nakatatakse uuesti üle poole sellistest äri- ja tarbijaklassi personaalarvutitest, mida on juba ühe korra pahavaraga nakatatud[12]. Igal aastal lähevad andmerikete tõttu sajad miljonid andmed kaotsi, rikkest ühele ettevõttele tekkiv

[6]Maailma Majandusfoorumi 2020. aasta ülemaailmsete riskide aruanne.

[7]Majanduskoostöö ja Arengu Organisatsiooni andmetel suurendas pandeemia internetiliiklust 60 %, https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Elektroonilise Side Euroopa Reguleerivate Asutuste Amet ja komisjon avaldavad korrapäraselt aruandeid interneti andmesidevõimsuse kohta koroonaviiruse leviku tõkestamise piirangute ajal. ENISA aruande kohaselt suurenes hajusate teenusetõkestusrünnete koguarv 2019. aasta kolmandas kvartalis 2018. aasta kolmanda kvartaliga võrreldes 241 %. Need ründed muutuvad üha intensiivsemaks. Suurim rünne toimus 2020. aasta veebruaris ja tõi kaasa tippkoormuse 2,3 terabitti sekundis. 2020. aasta augustis põhjustas USA internetiteenuse osutaja CenturyLinki marsruutimisprobleem seisaku, mille tõttu vähenes ülemaailmne veebiliiklus 3,5 %, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

[8]„Ülemaailmse interneti olukord: konsolideerimine internetimajanduses“, Internet Society, https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/.

[9]https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

[10]Digitaalmajanduse ja -ühiskonna indeks 2020, https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

[11]„IKT-turvameetmed, mida võtavad enamik ELi ettevõtetest“, Eurostati pressiteade, 6/2020, 13. jaanuar 2020. „Küberründed elutähtsa taristus vastu on muutunud tavapäraseks sellistes valdkondades nagu energeetika, tervishoid ja transport“, Maailma Majandusfoorumi 2020. aasta ülemaailmsete riskide aruanne.

[12] Allikas: Comparitech.

keskmine kulu suurenes 2018. aastal rohkem kui 3,5 miljoni euroni[13]. Küberründe mõju ei saa sageli isoleerida ning see võib vallandada ahelreaktsiooni kogu majanduses ja ühiskonnas, mõjutades miljoneid inimesi[14].

Peaaegu igat liiki kuritegude uurimisel on digitaalne komponent. 2019. aastal teatati, et vahejuhtumite arv aastas on kolmekordistunud. Hinnanguliselt on liikvel 700 miljonit uut pahavara versiooni – see on kõige sagedasem küberründajate vahend[15]. Küberkuritegevuse aastakulu maailmamajandusele on 2020. aastal hinnanguliselt 5,5 triljonit eurot, mis on kaks korda rohkem kui 2015. aastal[16]. See on suurim majandusliku jõukuse ülekandmine ajaloos, suurem isegi ülemaailmsest uimastikaubandusest. Laiaulatuslik WannaCry lunavararünne 2017. aastal põhjustas maailma majandusele hinnanguliselt üle 6,5 miljardi eurose kulu[17].

Avaliku ja tootmissektori kõrval on üks küberrünnete sagedasemaid sihtmärke digiteenused ja finantssektor, kuid ettevõtjate ja üksikisikute kübervalmidus ja -teadlikkus on endiselt madal[18] ning töötajate küberturvalisusoskused on väga puudulikud[19]. 2019. aastal toimus peaaegu 450 küberturvalisuse intsidenti, mis hõlmasid Euroopa elutähtsaid taristuid, nagu rahandus ja energeetika[20]. Pandeemia ajal on eriti rängalt kannatada saanud tervishoiuorganisatsioonid ja -töötajad. Kuna tehnoloogia muutub füüsilisest maailmast lahutamatuks, ohustavad küberründed kõige ebasoodsamas olukorras inimeste elu ja heaolu[21]. Rohkem kui kahte kolmandikku ettevõtetest, eelkõige VKEd, peetakse küberturvalisuse valdkonnas algajateks ning Euroopa ettevõtteid peetakse vähem ettevalmistunuks kui Aasia ja Ameerika omasid[22]. Hinnanguliselt on Euroopas 291 000 küberturvalisuse spetsialisti ametikohta täitmata. Küberturvalisuse spetsialistide värbamine ja koolitamine on aeganõudev, mis toob organisatsioonidele kaasa suuremad küberturvalisuse riskid[23].

ELil puudub kollektiivne olukorrateadlikkus küberohtudest. Seda seetõttu, et riiklikud ametiasutused ei kogu ega jaga süstemaatiliselt teavet, näiteks erasektorist kättesaadavat teavet, mis võiks aidata hinnata küberturvalisuse olukorda ELis. Liikmesriigid teatavad vaid

---

[13] „Aruanne andmeriketest tulenevate aastakulude kohta“, Ponemon Institute, 2020 (põhineb 17 geograafilises piirkonnas ja 17 tööstusharus hiljuti toime pandud 524 rikkumise kvantitatiivsel analüüsil), https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[14] Teadusuuringute Ühiskeskuse aruanne „Küberturvalisus – meie digitaalne soomus“, https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor.

[15] Allikas: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] „Küberturvalisus – meie digitaalne soomus“, Teadusuuringute Ühiskeskuse aruanne.

[17] Allikas: Cyence.

[18] Ettevõtjate, eriti VKEde teadlikkus ärisaladuste kübervargusest on endiselt väike. „Tööstusspionaaži ja ärisaladuste kübervarguse ulatuse ja mõju uuring: levitamisaruanne ärisaladuste kübervarguse vastu võitlemise ja selle ennetamise meetmete kohta“, PwC, 2018.

[19] Vt ENISA 2020. aasta aruannet ohumaastiku kohta. Samuti „Andmerikete uurimise aruanne“, Verizon, 2020, https://enterprise.verizon.com/resources/reports/dbir/.

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

[21] Lunavara sihtmärgiks on olnud haiglad ja terviseandmed, nt Rumeenias (juuni 2020), Düsseldorfis (september 2020) ja Vastaamos (oktoober 2020).

[22] „Infoturbe olukord maailmas 2018“, PwC ja „Küberturvalisuse imperatiiv“, ESI Thoughtlab, 2019.

[23] „Küberturvalisuse alaste oskuste arendamine ELis: küberturvalisuse alase õppe kraadide sertifitseerimine ja ENISA küberturvalisuse alase kõrghariduse andmebaas“, Euroopa Liidu Küberturvalisuse Amet (ENISA), detsember 2019.

murdosa juhtumitest ning teabe jagamine ei ole süstemaatiline ega kõikehõlmav[24]; küberründed võivad olla vaid üks Euroopa ühiskondade vastu suunatud kooskõlastatud pahatahtlike rünnete tahkudest. Liikmesriikide vaheline operatiivabi on praegu piiratud ning liikmesriikide ja ELi institutsioonide, asutuste ja ametite vahel ei ole suuremahuliste piiriüleste küberintsidentide või -kriiside puhuks operatiivmehhanismi loodud[25].

Seetõttu on oluline suurendada küberturvalisust, et inimesed saaksid innovatsiooni, võrguühendust ja automatiseerimist usaldada, neid kasutada ja neist kasu saada ning et kaitsta põhiõigusi ja -vabadusi, sealhulgas õigust eraelu puutumatusele ja isikuandmete kaitsele, ning väljendus- ja teabevabadust. Küberturvalisus on hädavajalik võrguühenduse ning ülemaailmse ja avatud interneti jaoks, mis peab toetama majanduse ja ühiskonna arengut 2020. aastatel. See aitab luua rohkem ja paremaid töökohti, muuta tööpaigad paindlikkumaks, edendada , tõhusamat ja säästvamat transporti ja põllumajandust ning tagada lihtsam ja õiglasem juurdepääs tervishoiuteenustele. See on oluline ka selleks, et minna Euroopa rohelise kokkuleppe[26] raames üle puhtamale energiale, kasutades selleks piiriüleseid võrke ja arukaid arvesteid ning vältides andmete tarbetut dubleerimist. Lisaks on see oluline rahvusvahelise julgeoleku ja stabiilsuse ning majanduse, demokraatia ja ühiskonna arengu jaoks kogu maailmas. Valitsused, ettevõtjad ja üksikisikud peavad seetõttu kasutama digivahendeid vastutustundlikult ja turvateadlikult. Küberturvalisuse alane teadlikkus ja küberhügieen peavad toetama igapäevaste tegevuste digiüleminekut.

ELi uus kübertuvalisuse strateegia digikümnendi jaoks on järgmiste algatuste põhikomponent: „Euroopa digituleviku kujundamine“[27], komisjoni koostatud Euroopa taastekava[28], ELi julgeolekuliidu strateegia aastateks 2020–2025[29], Euroopa Liidu üldine välis- ja julgeolekupoliitika strateegia[30], Euroopa Ülemkogu strateegiline tegevuskava aastateks 2019–2024[31]. Selles strateegias nähakse ette, kuidas EL hakkab kaitsma oma inimesi, ettevõtjaid ja institutsioone küberohtude eest ning kuidas ta edendab rahvusvahelist koostööd ning juhib avatud ja ülemaailmse interneti turvaliseks muutmist.

II. MÕTLEME ÜLEMAAILMSELT, TEGUTSEME EUROOPLASTENA

Selle strateegia eesmärk on tagada tugevate kaitsevahenditega ülemaailmne ja avatud internet, et reageerida Euroopa inimeste turvalisust ning põhiõigusi ja -vabadusi ähvardavatele ohtudele. Arvestades eelmiste strateegiate edusamme, sisaldab see konkreetseid ettepanekuid **kolme peamise vahendi – regulatiivne, investeerimis- ja poliitikavahend** – kasutuselevõtuks. Nendega **käsitletakse kolme tegevusvaldkonda: 1) vastupidavus, tehnoloogiline suveräänsus ja juhtpositsioon, 2) tegevussuutlikkuse suurendamine, et ennetada, heidutada ja reageerida, ning 3) ülemaailmse ja avatud küberruumi edendamine**. EL on pühendunud selle strateegia toetamisele, tehes **ELi digiüleminekusse** uue tehnoloogia- ja tööstuspoliitika ning taastekava raames **järgmise**

[24]Liikmesriigid peavad igal aastal esitama koostöörühmale kokkuvõtva aruande võrgu- ja infosüsteemide turvalisust käsitleva direktiivi (direktiiv (EL) 2016/1148) artikli 10 lõike 3 kohaselt saadud teadete kohta.
[25]CSIRTide võrgustiku liikmete hulgas toimuvaks vastastikuseks abistamiseks on kehtestatud standardne töökord.
[26]„Euroopa roheline kokkulepe“, COM(2019) 640 final.
[27]„Euroopa digituleviku kujundamine“, COM(2020) 67 final.
[28]„Euroopa võimalus: parandame vead ja teeme ettevalmistusi järgmise põlvkonna jaoks“, COM(2020) 98 final.
[29]ELi julgeolekuliidu strateegia aastateks 2020–2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en.
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#.

seitsme aasta jooksul enneolematult suuri investeeringuid, mis on varasemate määradega võrreldes kuni neljakordsed [32].

Küberturvalisus tuleb integreerida kõigisse nendesse digivaldkonna investeeringutesse, eelkõige selliste põhitehnoloogiate puhul nagu tehisintellekt, krüpteerimine ja kvantarvutus, kasutades stiimuleid, kohustusi ja võrdlusaluseid. See võib hoogustada Euroopa küberturvalisuse tööstuse kasvu ja tagada kindluse, mida on vaja varasemate süsteemide järkjärguliseks kaotamiseks. Euroopa Kaitsefondist toetatakse Euroopa küberkaitselahendusi Euroopa kaitsesektori tehnoloogilise ja tööstusliku baasi osana. Küberturvalisus on lisatud välisrahastamisvahenditesse, eelkõige naabruspoliitika, arengu- ja rahvusvahelise koostöö rahastamisvahendisse, et toetada meie partnereid. Tehnoloogiate väärkasutamise ennetamine, elutähtsa taristu kaitse ja tarneahelate terviklikkuse tagamine võimaldab ELil järgida ka ÜRO norme, eeskirju ja riigi vastutustundliku käitumise põhimõtteid[33].

1. VASTUPIDAVUS, TEHNOLOOGILINE SUVERÄÄNSUS JA JUHTPOSITSIOON

ELi elutähtis taristu ja põhiteenused on üha enam üksteisest sõltuvad ja digitaliseeritud. Kõik internetiga ühendatud asjad ELis, olgu need siis automatiseeritud autod, tööstuslikud juhtimissüsteemid või kodumasinad, ja tarneahelad, mis teevad need kättesaadavaks, peavad olema sisseprojekteeritud turbega, küberintsidentidele vastupidavad ja turvaaukude avastamise korral kiiresti parandatavad. See on väga oluline, et anda ELi era- ja avalikule sektorile võimalus valida kõige turvalisema taristu ja teenuste seast. Eelseisev aastakümme annab ELile võimaluse juhtida turvalise tehnoloogia arendamist kogu tarneahela ulatuses. Vastupidavuse ning tööstus- ja tehnoloogiasektoris suurema küberturvalisuse tagamiseks tuleks kaasata kõik vajalikud reguleerimis-, investeerimis- ja poliitikavahendid. Sisseprojekteeritud küberturbega tööstusprotsessid, -toimingud ja -seadmed võivad maandada riske, vähendada nii ettevõtjate kui ka laiema ühiskonna kulusid ning suurendada seeläbi vastupidavust.

1.1 Vastupidav taristu ja elutähtsad teenused

Küberturvalisuse toodete ühtne turg põhineb ELi **eeskirjadel võrgu- ja infosüsteemide turvalisuse kohta**. Komisjon teeb ettepaneku muuta neid eeskirju läbivaadatud võrgu- ja infoturbe direktiivi alusel, et **suurendada kõigi majanduse ja ühiskonna jaoks oluliste sektorite, sealhulgas nii avaliku kui ka erasektori kübervastupidavusvõimet**[34]. Läbivaatamine on vajalik, et vähendada vastuolusid siseturul, ühtlustades kohaldamisala, turva- ja intsidentidest teatamise nõudeid, riiklikku järelevalvet ja jõustamist ning pädevate asutuste suutlikkust.

[32] Kogu digitehnoloogia tarneahelasse tehtavad toetuste ja laenude vormis investeeringud, millega aidata kaasa digiüleminekule ja sellest tulenevate probleemide lahendamisele, peaksid moodustama vähemalt 20 % 672,5 miljardi euro suurusest taaste ja vastupidavuse rahastamisvahendist ehk kokku 134,5 miljardit eurot . ELi rahastus 2021.–2027. aasta mitmeaastases finantsraamistikus, mis on programmi „Digitaalne Euroopa“ raames ette nähtud küberturvalisusele ja programmi „Euroopa horisont“ raames küberturvalisuse teadusuuringutele (eelkõige VKEde toetamiseks), võib ulatuda kokku 2 miljardi euroni, millele lisanduvad liikmesriikide ja valdkondlike sidusrühmade investeeringud.

[33] https://undocs.org/A/70/174

[34] [*insert reference to NIS proposal*]

Uuendatud võrgu- ja infoturbe direktiiv loob aluse konkreetsematele eeskirjadele, mis on vajalikud ka strateegiliselt oluliste sektorite jaoks, sealhulgas energeetika, transport ja tervishoid. Selleks et tagada ühtne lähenemisviis, nagu on välja kuulutatud julgeolekuliidu strateegias (2020–2025), tehakse ettepanek uuendatud direktiivi kohta koos ettepanekuga elutähtsa taristu vastupidavust käsitlevate õigusaktide läbivaatamise kohta[35]. Digikomponente sisaldavenergiatehnoloogia ja sellega seotud tarneahelate turvalisus on oluline selleks, et põhiteenused ei katkeks ja elutähtsa energiataristu üle säiliks strateegiline kontroll. Seepärast teeb komisjon ettepaneku võtta 2022. aasta lõpuks vastu meetmed, sealhulgas võrgueeskiri, millega kehtestatakse piiriüleste elektrivoogude puhul küberturvalisuse eeskirjad. Finantssektor peab tugevdama ka digitaalset operatiivvastupidavust ning tagama suutlikkuse tulla toime igat liiki IKT-häirete ja -ohtudega, nagu komisjon on ette näinud[36]. Transpordi valdkonnas lisas komisjon küberturvalisuse sätted[37] lennundusjulgestust käsitlevatesse ELi õigusaktidesse ning jätkab jõupingutusi kõigi transpordiliikide kübervastupidavusvõime suurendamiseks. **Demokraatlike protsesside ja institutsioonide** kübervastupidavusvõime tugevdamine on keskne komponent ka Euroopa demokraatia tegevuskavas, mille eesmärk on kaitsta ja edendada vabasid valimisi ning demokraatlikku arutelu ja meedia pluralismi[38]. Taristu ja teenuste turvalisuse tagamiseks tulevase kosmoseprogrammi raames jätkab komisjon Galileo küberturvalisuse strateegia süvendamist, pidades silmas järgmise põlvkonna globaalse satelliitnavigatsioonisüsteemi teenuseid ja muid uusi kosmoseprogrammi komponente[39].

1.2 Euroopa küberturvalisuse kaitsekilbi loomine

Olukorras, kus ühendatus laieneb ja küberründed muutuvad üha keerukamaks, täidavad teabe jagamise ja analüüsimise keskused (ISACid) väärtuslikku ülesannet, sealhulgas valdkondlikul tasandil, võimaldades eri sidusrühmade vahel küberohtude kohta teavet vahetada[40]. Lisaks on võrke ja arvutisüsteeme vaja pidevalt jälgida ja analüüsida, et avastada sissetunge ja kõrvalekaldeid reaalajas. Paljud eraettevõtjad, avalik-õiguslikud organisatsioonid ja riigiasutused on seetõttu loonud küberturbe intsidentide lahendamise üksused (CSIRTd) ja turbekeskused (SOCid).

Turbekeskused on väga olulised logide kogumiseks[41] ja jälgitavates sidevõrkudes toimuvate kahtlaste intsidentide isoleerimiseks. Nende tegevus põhineb signaalide ja mustrite avastamisel ning hinnatavatest andmehulkadest ohtude kohta teadmiste ammutamisel. Turbekeskused on kaasa aidanud pahatahtlike täitmiskoodide avastamisele ja see on omakorda aidanud küberründe kontrolli alla saada. Nendes keskustes tehtav töö on väga

[35] [insert reference to *proposal* for a directive on resilience of critical entities]
[36] Ettepanek: määrus, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014, COM(2020)595 final.
[37] Komisjoni rakendusmäärus (EL) 2019/1583.
[38] Teatis Euroopa demokraatia tegevuskava kohta, COM(2020) 790. Kava kohaselt toetab Euroopa valimiskoostöö võrgustik ja liikmesriikide valimisvõrgustikud ühiste eksperdirühmade lähetamist, et võidelda valimisprotsessi ähvardavate ohtude, sealhulgas küberohtude vastu, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.
[39] See hõlmab uut riikliku satelliitside algatust (GOVSATCOM) ja kosmoseprügi algatust (SST)
[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.
[41] Sellisel viisil, et õiguskaitseasutused ja kohtud saavad kasutada neid tõenditena.

nõudlik ja kiireloomuline, mistõttu võib sealjuures palju kasu olla tehisintellektist ja eelkõige masinõppemeetoditest[42].

Komisjon teeb ettepaneku luua **kogu ELi hõlmava turbekeskuste võrgustiku**[43] ja toetada olemasolevate keskuste täiustamist ja uute loomist. Samuti hakkab ta toetama neid keskusi haldavate töötajate koolitamist ja oskuste täiustamist. Komisjon võiks vastavalt vajaduste analüüsile, mis tehakse koos asjaomaste sidusrühmadega ja mida toetab Euroopa Liidu Küberturvalisuse Amet (ENISA), eraldada üle 300 miljoni euro avaliku ja erasektori ning piiriülese koostöö toetamiseks riiklike ja valdkondlike võrgustike loomisel, kaasates ka VKEsid ja tuginedes asjakohasele juhtimissüsteemile, andmete jagamisele ja turvalisussätetele.

Liikmesriike julgustatakse sellesse projekti kaasinvesteerima. Sel juhul saaksid keskused avastatud signaale tõhusamalt jagada ja seostada ning koguda ohtude kohta kvaliteetset luureteavet, mida jagatakse ISACide ja riikide ametiasutustega, võimaldades seega saada täielikum olukorrateadlikkus. Võrgustiku eesmärk oleks ühendada järk-järgult võimalikult palju keskusi kogu ELis, et luua ühine teadmiste baas ja jagada parimaid tavasid. Nendele keskustele antakse toetust, et parandada tipptasemel tehisintellekti ja masinõppe abil intsidentide avastamise, analüüsimise ning neile reageerimise kiirust . Seda täiendatakse veel superarvutitaristuga, mille on ELis välja töötanud Euroopa kõrgjõudlusega andmetöötluse ühisettevõte[44].

Pidevat koostööd tehes annab võrgustik ametiasutustele ja kõigile huvitatud sidusrühmadele, sealhulgas ühisele küberüksusele (vt punkt 2.1), küberintsidentide kohta õigeaegseid hoiatusi. **See toimib ELi jaoks küberturvalisuse kaitsekilbina**, mis tagab kindla jälgimisseadmete võrgu, mis suudab avastada võimalikud ohud enne, kui need jõuavad põhjustada ulatuslikku kahju.

1.3 Üliturvaline sidetaristu

Euroopa Liidus toimiv riiklik satelliitside,[45] pakub turvalist ja kulutõhusat kosmosepõhist sidevõimet, et tagada ELi ja selle liikmesriikide, sealhulgas riiklike julgeolekuvaldkonna osalejate ning ELi institutsioonide ametite ja asutuste juhitavad julgeoleku ja turvalisuse seisukohast olulised missioonid ja operatsioonid.

Liikmesriigid on võtnud kohustuse teha komisjoniga koostööd, et võtta Euroopa jaoks kasutusele turvaline kvantsidetaristu[46]. Kvantsidetaristu pakub avaliku sektori asutustele konfidentsiaalse teabe edastamiseks täiesti uut Euroopa tehnoloogia abil loodud ja üliturvalisel krüpteerimisel põhinevat viisi, et kaitsta neid küberrünnete eest. Sellel on kaks põhikomponenti: olemasolevad kiudoptilised maasidevõrgud, mis ühendavad strateegilisi

[42] „SOCde tõhususe suurendamine, 2019“, Ponemon Institute Researchi uuring; tehisintellekti kasutamise kohta turbekeskustes vt nt: Khraisat, A., Gondal, I., Vamplew, P. *et al.* „Sissetungi avastamise süsteemide uuring: tehnikad, andmekogud ja probleemid“, Cybersecur 2, 20 (2019).

[43] Töötatakse välja üksikasjalikum kord nende keskuste juhtimiseks, toimimiseks ja rahastamiseks ning viisid, kuidas need saavad täiendada olemasolevaid struktuure, nagu digitaalse innovatsiooni keskuseid.

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking.

[45] Riiklik satelliitside on liidu kosmoseprogrammi osa.

[46] Enamik liikmesriike on allkirjastanud EuroQCI deklaratsiooni ning arendustegevus ja taristu kasutuselevõtt toimuvad 2021.–2027. aastal programmidest „Euroopa horisont“ ja „Digitaalne Euroopa“ ning Euroopa Kosmoseagentuuri pakutava rahastuse abil vastavalt asjakohasele juhtimiskorrale, https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

punkte riiklikul ja piiriülesel tasandil; ning nendega seotud kosmosesatelliidid, mis katavad kogu ELi, sealhulgas selle ülemereterritooriume[47]. See algatus, mille eesmärk on töötada välja ja võtta kasutusele uusi ja turvalisemaid krüpteerimise vorme ning töötada välja uusi viise elutähtsate side- ja andmeressursside kaitsmiseks, võib aidata kaitsta tundlikku teavet ja hoida seeläbi elutähtsat taristut turvalisena.

Seda silmas pidades ja veelgi kaugemale minnes uurib komisjon võimalust võtta kasutusele mitmeorbitaalne turvaline ühendussüsteem. Riiklikule satelliitsidesüsteemile ja kvantsidetaristule tuginedes integreeritaks sellesse tipptasemel tehnoloogiad (kvanttehnoloogia, 5G, tehisintellekt, servandmetöötlus), mis järgivad kõige rangemat küberturvalisuse raamistikku, et toetada sisseprojekteeritud turbega teenuseid, nagu usaldusväärne, turvaline ja kulutõhus ühendatus ning krüptitud side valitsuste kriitilise tähtsusega tegevuse jaoks.

1.4 Järgmise põlvkonna lairibamobiilsidevõrkude turvalisuse tagamine

ELi kodanikud ja ettevõtted, kes kasutavad **5G- ja järgmiste põlvkondade võrkude** pakutavaid tipptasemel uuenduslikke rakendusi, peaksid saama olla kindlad sellele, et rakendatakse rangeimaid turvastandardeid. Liikmesriigid on koos komisjoniga ja ENISA toel kehtestanud ELi 2020. aasta jaanuari 5G küberturvalisuse meetmepaketti[48] kasutades 5G küberturvalisuse suhtes laiaulatusliku ja objektiivse riskipõhise lähenemisviisi, mis põhineb võimalike riskimaanduskavade hindamisel ja kõige tulemuslikumate meetmete kindlaksmääramisel. Lisaks tugevdab EL oma suutlikkust 5G ja kõrgemal tasemel, et vältida sõltuvust ning edendada jätkusuutlikku ja mitmekesist tarneahelat.

2020. aasta detsembris avaldas komisjon aruande 5G-võrkude küberturvalisust käsitleva 26. märtsi 2019. aasta soovituse mõju kohta[49]. See näitas, et pärast meetmepaketis kokkuleppimist on tehtud märkimisväärseid edusamme ning et enamik liikmesriike on graafikus, et viia lähitulevikus lõpule märkimisväärne osa meetmepaketi rakendamisest, kuigi mõningate erinevuste ja kõrvaldamata lünkadega, mis on kindlaks tehtud juba 2020. aasta juulis avaldatud eduaruandes[50].

2020. aasta oktoobris kutsus Euroopa Ülemkogu ELi ja liikmesriike üles „kasutama täielikult ära 5G küberturvalisuse meetmepaketti“ ja kohaldama asjakohaseid piiranguid kõrge riskitasemega tarnijate suhtes põhivarade puhul, mis on ELi koordineeritud riskihindamises määratletud kriitilise tähtsusega ja tundlikuna, tuginedes ühistele objektiivsetele kriteeriumidele[51].

[47]Kosmosekomponendi arendamine on vajalik selleks, et saavutada pikad kakspunktühendused (>1000 km), mida maapealne taristu ei suuda toetada. Kvantmehaanika omadusi kasutades annab kvantsidetaristu osalistele kõigepealt võimaluse jagada turvaliselt juhuslikke salajasi võtmeid, mida kasutatakse sõnumite krüpteerimiseks ja dekrüpteerimiseks. Kasutusele võetakse ka testimis- ja vastavustaristu, mis aitab hinnata Euroopa kvantsideseadmete ja -süsteemide vastavust kvantsidetaristule ning sertifitseerida ja valideerida need enne kvantsidetaristusse integreerimist. Sellesse saab lisada täiendavaid rakendusi, kui need saavutavad vajaliku tehnoloogilise küpsuse taseme. Praegune OpenQKD katseprojekt (https://openqkd.eu/) on selle testimis- ja vastavustaristu eelkäija.
[48]Teatis „5G turvaline kasutuselevõtt ELis: ELi meetmepaketi rakendamine“, (COM(2020) 50).
[49]Komisjoni aruanne 5G-võrkude küberturvalisust käsitleva 26. märtsi 2019. aasta soovituse mõju kohta.
[50]Võrgu- ja infoturbe koostöörühma 24. juuli 2020. aasta aruanne meetmepaketi rakendamise kohta.
[51]Euroopa Ülemkogu erakorraline kohtumine (1.–2. oktoober 2020) – järeldused, EUCO 13/20.

Tulevikku vaadates peaksid EL ja selle liikmesriigid tagama, et kindlakstehtud riske maandatakse piisavalt ja koordineeritult, eelkõige seoses eesmärgiga minimeerida kokkupuudet kõrge riskitasemega tarnijatega ja vältida nendest tarnijatest riiklikul ja liidu tasandil sõltuvusse sattumist, ning et võetakse arvesse kõiki uusi olulisi arenguid ja riske. Liikmesriike kutsutakse üles digitaalsesse võimekusse ja ühendatusse investeerimisel meetmepaketti täiel määral ära kasutama.

2019. aasta soovituse mõju käsitleva aruande põhjal julgustab komisjon liikmesriike kiirendama tööd, et viia peamiste meetmepaketi meetmete rakendamine lõpule 2021. aasta teiseks kvartaliks. Samuti kutsub komisjon liikmesriike üles jätkama ühiselt tehtud edusammude jälgimist ja tagama lähenemisviiside edasine ühtlustamine. ELi tasandil püütakse selle protsessi toetamiseks saavutada kolm peamist eesmärki: tagada riskimaandamise käsituste edasine lähendamine kogu ELis, toetada pidevat teadmiste vahetamist ja suutlikkuse suurendamist ning edendada tarneahela vastupidavust ja muid ELi strateegilisi turvalisuseesmärke. Nende põhieesmärkidega seotud konkreetsed meetmed on esitatud käesoleva teatise temaatilises liites.

Komisjon jätkab tihedat koostööd liikmesriikidega, et need eesmärgid ja meetmed ENISA toetuse abiga täita (vt lisa).

Lisaks on ELi 5G meetmepakett suurendanud huvi ELi-välistes riikides, kes töötavad praegu välja oma lähenemisviise sidevõrkude turvalisuse tagamiseks. Komisjoni talitused koos Euroopa välisteenistuse ja ELi delegatsioonide võrgustikuga on valmis andma ametiasutustele kogu maailmas nende soovi korral oma tervikliku, objektiivse ja riskipõhise lähenemisviisi kohta täiendavat teavet.

1.5 Turvaliste asjade internett

Iga ühendatud ese sisaldab turvaauke, mida saab ära kasutada ulatuslike tagajärgedega. Siseturu eeskirjad sisaldavad kaitsemeetmeid mitteturvaliste toodete ja teenuste vastu. Komisjon juba töötab selle nimel, et tagada **küberturvalisuse määruse alusel läbipaistvad turvalahendused ja sertifitseerimine** ning luua stiimulid ohutute toodete ja teenuste arendamiseks, kahjustamata nende toimivust[52]. Komisjon võtab 2021. aasta esimeses kvartalis vastu oma esimese liidu jooksva tööprogrammi (mida ajakohastatakse vähemalt kord kolme aasta tagant), et võimaldada valdkondlikel sidusrühmadel, riikide ametiasutustel ja standardiametitel valmistuda tulevasteks Euroopa küberturvalisuse sertifitseerimise kavadeks[53]. Kuna asjade internet laieneb, tuleb jõustatavaid eeskirju tugevdada, et tagada nii üldine vastupidavus kui ka suurendada küberturvalisust.

Komisjon kaalub võimalust kehtestada terviklik lähenemisviis, sealhulgas võimalikud **uued horisontaalsed eeskirjad, et suurendada kõigi siseturule lastavate ühendatud toodete ja**

[52]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) . Küberturvalisuse määrusega edendatakse IKT sertifitseerimist ELi tasandil, nähes ette Euroopa küberturvalisuse sertifitseerimise raamistiku, millega luua vabatahtlikke Euroopa küberturvalisuse sertifitseerimise kavasid, et tagada IKT-toodete, -teenuste ja -protsesside piisav küberturvalisus liidus ning vähendada siseturul kehtivate küberturvalisuse sertifitseerimise kavade killustatust. Küberturvalisuse reitingutega tegelevad ettevõtjad asuvad tihti väljaspool ELi ning nende läbipaistvus ja järelevalve nende üle piiratud, https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

[53]Nagu nõutakse küberturvalisuse määruse artikli 47 lõikega 5.

nendega seotud teenuste küberturvalisust[54]. Sellised eeskirjad võiksid sisaldada **ühendatud seadmete tootjate uut hoolsuskohustust** tegeleda tarkvara turvaaukudega, sealhulgas teha tarkvara ja turvauuendusi, ning tagada, et kasutusaja lõpus kustutatakse isikuandmed ja muud tundlikud andmed. Need eeskirjad toetaksid ringmajanduse tegevuskavas esitatud vananenud tarkvara ajakohastamise õiguse rakendamist ning täiendaksid konkreetsete tooteliikide suhtes võetavaid meetmeid, nagu kavandatavad nõuded teatavate traadita toodete turule pääsu suhtes (raadioseadmete direktiivi[55] alusel vastuvõetavas delegeeritud õigusaktis), ja eesmärki kohaldada alates 2022. aasta juulist mootorsõidukite küberturvalisuse eeskirju kõikide uut tüüpi sõidukite suhtes[56]. Lisaks tugineksid need selliste üldiste tooteohutuseeskirjade kavandatud läbivaatamisele, mis ei käsitle otseselt küberturvalisusega seotud aspekte[57].

1.6 Turvalisem ülemaailmne internet

Tuumprotokollide kogum ja tugitaristu tagab interneti toimimise ja tervikluse kogu maailmas[58]. See kogum hõlmab domeeninimede süsteemi ning selle hierarhilist ja delegeeritud tsoonisüsteemi, alustades hierarhia tipust juurtsooni ja 13 domeeninimede süsteemi juurserveriga, millest ülemaailmne internet sõltub[59]. Komisjon kavatseb töötada välja **ELi toetatava hädaolukorra lahendamise plaani, et reageerida äärmuslikele sündmustele, mis mõjutavad ülemaailmse domeeninimede süsteemi juursüsteemi terviklikkust ja kättesaadavust**. Komisjon teeb koostööd ENISA, liikmesriikide, kahe ELi domeeninimede süsteemi juurserveri operaatori[60] ja sidusrühmaülese kogukonnaga, et hinnata milline roll on nendel operaatoritel selles, et internet jääb igal juhul ülemaailmselt kättesaadavaks.

Selleks et kliendil oleks internetis juurdepääs teatava domeeninime all olevale ressursile, tuleb tema (tavaliselt ühtse ressursilokaatori ehk URLi) taotlus tõlkida või teisendada (resolvida) IP-aadressiks, viidates domeeninimede süsteemi nimeserveritele. Inimesed ja organisatsioonid ELis sõltuvad aga üha enam mõnest üksikust avalikust DNS-resolverist, mida käitavad ELi-välised üksused. Selline DNS-resolvimise koondumine väheste ettevõtjate[61] kätte muudab resolvimise haavatavaks suurintsidentide korral, mis mõjutavad

[54]Nõukogu järeldustes kutsutakse üles võtma ühendatud seadmete küberturvalisuse suhtes horisontaalseid meetmeid, 13629/20, 2. detsember 2020.
[55]Direktiiv 2014/53/EL
[56] Vastavalt 2020. aasta juunis vastu võetud ÜRO määrusele, http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.
[57]Kehtivate üldiste tooteohutuseeskirjade (direktiiv 2001/95/EÜ) läbivaatamine, kohandatud eeskirju on kavas kehtestada ka digikontekstis kehtiva tootjavastutuse suhtes vastavalt vastutust käsitlevale ELi õigusraamistikule.
[58]„Avatud interneti avalik tuum, nimelt selle põhilised protokollid ja taristu, mis on ülemaailmne avalik hüve, tagab interneti kui terviku põhifunktsionaalsuse ja toetab selle tavapärast toimimist. ENISA peaks toetama avatud interneti avaliku tuuma toimimise, sealhulgas põhiliste protokollide (eelkõige domeeninimede süsteem, BGP ja IPv6) turvalisust ja stabiilsust, domeeninimede süsteemi (kaasa arvatud kõigi tippdomeenide) ja juurserverite toimimist“, küberturvalisuse määruse põhjendus 23.
[59]https://www.iana.org/domains/root/servers
[60]Netnodi käitatavad i.root-serverid Rootsis ja RIPE NCC käitatavad k.root-serverid Madalmaades.
[61]„Konsolideerimine DNS-resolverite turul – kui palju, kui kiiresti, kui ohtlik?“ „Tõendid interneti entroopia vähenemise kohta – liiasuse puudumine DNS-resolvimises suurte veebisaitide ja teenuste puhul“

üht olulist teenuseosutajat, ning raskendab ELi asutustel võimalikele pahatahtlikele küberrünnetele ning geopoliitilistele ja tehnilistele suurintsidentidele reageerimist[62].

Turu kontsentreerumisega seotud turvaintsidentide vähendamiseks julgustab komisjon asjaomaseid sidusrühmi, sealhulgas ELi äriühinguid, internetiteenuse osutajaid ja veebilehitseja müüjaid, võtma vastu DNS-resolvimise mitmekesistamise strateegia. Samuti kavatseb komisjon anda panuse internetiühenduse turvaliseks muutmisesse, toetades **Euroopa avaliku DNS-resolveriteenuse** arendamist. Algatus DNS4EU hakkab ülemaailmsele internetile juurdepääsemiseks pakkuma alternatiivset Euroopa teenust. See on läbipaistev, vastab viimastele turvanõuetele, sellesse on sisse projekteeritud andmekaitse ja eraelu puutumatuse vaikestandardid ja -eeskirjad ning see kuulub Euroopa andme- ja pilvandmetöötluse tööstusliitu[63].

Samuti **kiirendab komisjon koostöös liikmesriikide ja valdkondlike sidusrühmadega peamiste internetistandardite, sealhulgas IPv6**[64] **ning hästi toimivate internetiturvalisuse standardite ning domeeninimede süsteemi,**[65] **marsruutimise ja e-posti turvalisuse valdkonnas heade tavade kasutuselevõttu**, välistamata reguleerivaid turukorraldusmeetmeid, nagu Euroopa aegumisklausel IPv4-aadresside puhul, kui nende eesmärkide saavutamiseks ei ole tehtud piisavalt edusamme. EL peaks (nt ELi-Aafrika strateegia[66] raames) edendama nende standardite rakendamist partnerriikides, et toetada ülemaailmse ja avatud interneti edendamist ning tõrjuda suletud ja kontrollipõhiseid internetimudeleid. Lõpuks kaalub komisjon vajadust mehhanismi järele, mis võimaldaks internetiliikluse koondandmeid süstemaatilisemalt jälgida ja koguda ning anda nõu võimalike häirete kohta[67].

1.7 Jõulisem tegevus tehnoloogia tarneahelas

Tänu 2021.–2027. aasta mitmeaastases finantsraamistikus küberturvalisele digiüleminekule kavandatud rahalisele toetusele on ELil ainulaadne võimalus koondada oma varad, et tugevdada kooskõlas oma väärtuste ja prioriteetidega oma tööstusstrateegiat[68] ning juhtpositsiooni digitehnoloogia ja küberturvalisuse valdkonnas kogu digitarneahelas (sealhulgas andmed ja pilvandmetöötlus, järgmise põlvkonna protsessortehnoloogiad, üliturvaline ühendatus ja 6G-võrgud). Avaliku sektori meetmed peaks tuginema ELi riigihangete õigusraamistiku ja üleeuroopalist huvi pakkuvate tähtsate projektide pakutavatele vahenditele. Lisaks saab nendega kaasata avaliku ja erasektori partnerluste kaudu erainvesteeringuid (tuginedes sealhulgas küberturvalisuse alasele avaliku ja erasektori lepingulisele partnerlusele ja selle rakendamisele Euroopa küberturvalisuse organisatsiooni

[62]Samuti on tõendeid selle kohta, et domeeninimede süsteemi andmeid saab kasutada profileerimiseks, mis mõjutab eraelu puutumatust ja andmekaitseõigusi.
[63]Ühisdeklaratsioon ettevõtetele ja avalikule sektorile järgmise põlvkonna pilveteenuste loomise kohta, https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe
[64]IPv6 kasutuselevõtt on nüüd edenenud, kuna IPv4-aadresside pakkumine on oluliselt vähenenud ja nende hind on tõusnud. IPv6 kasutuselevõtt ELis on aga ebaühtlane.
[65]Kõnealused standardid on muu hulgas DNSSEC, HTTPS, DNS üle HTTPSi (DoH), DNS üle TLSi (DoT), SPF, DKIM, DMARC, STARTTLS, DANE ning marsruutimisnormid ja head tavad, nt vastastikku kokkulepitud marsruutimisturvalisuse normid (MANRS).
[66]Ühisteatis „Tervikliku Aafrika strateegia suunas“, 9.3.2020, JOIN(2020) 4 final.
[67]Selline interneti vaatluskeskus võiks kuuluda Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse tegevusvaldkonda; ettepanek: määrus, millega luuakse Euroopa küberturvalisuse uurimis- ja pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik, COM(2018) 630 final.
[68]Teatis „Euroopa uus tööstusstrateegia“, COM/2020/102 final.

kaudu) ja riskikapitali VKEde või tööstusliitude ning tehnoloogiasuutlikkuse strateegiate toetamiseks.

Erilist tähelepanu pööratakse ka tehnilise toetuse vahendile[69] ja sellele, et VKEd, eelkõige need, kes ei kuulu läbivaadatud võrgu- ja infoturbe direktiivi kohaldamisalasse, saaksid uusimaid küberturvalisuse vahendeid võimalikult hästi kasutada, sealhulgas programmi „Digitaalne Euroopa“ kuuluvate digitaalse innovatsiooni keskuste spetsiaalsete meetmete abil. Kavandatava **küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse ning riiklike koordineerimiskeskuste võrgustiku** (CCCN) raames peaksid liikmesriigid ja tööstusringkonnad tegema ühiselt hallatava partnerluse alusel võrdses mahus investeeringuid. CCCN, mille puhul on olulisel kohal valdkondlike sidusrühmade ja akadeemiliste ringkondade panus, peaks olema kesksel kohal ELi tehnoloogilise suveräänsuse arendamisel küberturvalisuse valdkonnas ning suutlikkuse suurendamisel, et muuta 5G ja muud tundlikud taristud turvalisemaks ja vähendada otsustava tähtsusega tehnoloogia puhul sõltuvust muust maailmast.

Komisjon kavatseb toetada (võimalik, et koostöös CCCNga) spetsiaalse küberturvalisuse magistriprogrammi väljatöötamist ning anda oma panuse pärast 2020. aastat kehtivasse Euroopa ühisesse küberturvalisuse alaste teadusuuringute ja innovatsiooni tegevuskavasse. CCCNi kaudu tehtavad investeeringud peaksid põhinema ka küberturvalisuse tippkeskuste võrgustike teadus- ja arenduskoostööl, tuues kokku Euroopa parimad uurimisrühmad ja tööstusringkonnad, et töötada välja ja rakendada ühiseid teadusuuringute kavasid kooskõlas Euroopa Küberturvalisuse Organisatsiooni tegevuskavaga[70]. Komisjon tugineb jätkuvalt ENISA ja Europoli uurimistööle ning toetab endiselt programmi „Euroopa horisont“ raames ka üksikisikutest veebiinnovaatoreid, kes arendavad eraelu puutumatust kaitsvaid ja turvalisi sidetehnoloogiaid, mis põhinevad avatud lähtekoodiga tarkvaral ja riistvaral, nagu praegu järgmise põlvkonna interneti algatuse raames.

1.8 Küberoskustega tööjõud ELis

ELi jõupingutused täiendada töötajate oskusi, meelitada ligi ja hoida parimaid küberturvalisuse spetsialiste ning investeerida maailmatasemel teadusuuringutesse ja innovatsiooni moodustavad olulise osa üldisest kaitsest küberohtude eest. Sellel valdkonnal on suur potentsiaal. Seepärast tuleb mitmekülgsema talendipagasi arendamisele, ligimeelitamisele ja hoidmisele rohkem tähelepanu pöörata. Uuendatud digiõppe tegevuskavaga suurendatakse üksikisikute, eelkõige laste ja noorte ning organisatsioonide, eelkõige VKEde teadlikkust küberturvalisusest[71]. See julgustab ka naisi omandama teadus-, tehnoloogia-, inseneri- ja matemaatikaharidust ning innustab korraldama IKT-spetsialistidele digioskustealast ümber- ja täiendõpet. Lisaks töötab komisjon koos Europoli juures tegutseva Euroopa Liidu Intellektuaalomandi Ameti, ENISA, liikmesriikide ja erasektoriga välja teadlikkuse suurendamise vahendid ja suunised, et ELi ettevõtjad oleksid vastupidavamad **küberruumi kasutades toime pandud intellektuaalomandi varguste suhtes**[72].

Haridus, sealhulgas kutseharidus ja -koolitus, teadlikkus ja õppused peaksid samuti suurendama küberturvalisuse ja -kaitse pädevust ELi tasandil. Selleks peaksid asjaomased

[69] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0409:FIN .
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en.
[72] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2187

ELi osalejad, nagu ENISA, Euroopa Kaitseagentuur (EDA) ning Euroopa Julgeoleku- ja Kaitsekolledž (ESDC),[73] arendama oma tegevuste koostoimet.

Strateegilised algatused

Euroopa Liidu eesmärgid:

- võtta vastu läbivaadatud võrgu- ja infoturbe direktiiv;
- kehtestada turvaliste asjade internetti käsitlevad reguleerivad meetmed;
- kaasata aastatel 2021–2027 CCCNi küberturvalisusinvesteeringute abil (eelkõige programmide „Digitaalne Euroopa“ ja „Euroopa horisont“ ning taasterahastu kaudu) kuni 4,5 miljardit eurot avaliku ja erasektori investeeringuid;
- luua tehisintellektil põhinevate turbekeskuste ELi võrgustik ja üliturvaline sidetaristu, mis kasutab kvanttehnoloogiaid;
- võtta laialdaselt kasutusele küberturvalisuse tehnoloogia digitaalse innovatsiooni keskuste raames VKEdele suunatud toetuse kaudu;
- töötada välja ELi DNS-resolver kui ELi kodanikele, ettevõtjatele ja avalikele asutustele mõeldud turvaline ja avatud alternatiiv internetile juurdepääsu saamiseks ning
- viia 5G meetmepaketi rakendamine lõpule 2021. aasta teiseks kvartaliks (vt liide).

2. SUUREM TEGEVUSSUUTLIKKUS KÜBERRÜNNETE ENNETAMISEKS, RÜNDAMAST HEIDUTAMISEKS JA RÜNNETELE REAGEERIMISEKS

Küberintsidendid, olgu need juhuslikud või lähtugu kurjategijate, riiklike või valitsusväliste osalejate tahtlikust tegevusest, võivad põhjustada tohutut kahju. Need võivad olla väga ulatuslikud ja keerukad – näiteks sageli kasutatakse lõppsihtmärgi kahjustamiseks kolmandate osapoolte teenuseid, riist- ja tarkvara. See nõuab ELilt ühiste ohtudega võitlemiseks süstemaatilist ja põhjalikku koostööd ja teabevahetust. **Kõigi regulatiivsete vahendite rakendamise, osapoolte mobiliseerimise ja tiheda koostöö kaudu** toetab EL liikmesriike nende kodanike ning majanduslike ja riiklike julgeolekuhuvide kaitsmisel, pidades sealjuures täielikult kinni põhiõigustest ja -vabadustest ning järgides õigusriikluse põhimõtet. Küberohtude ennetamisel, tõkestamisel, ohustamast heidutamisel ja ohtudele reageerimisel on oma valdkonnas kasutada olevate töövahendite ja algatuste toel[74] tegevad eri kogukonnad, mille ridades on esindatud võrgustikud, ELi institutsioonid, organid ja asutused, samuti liikmesriikide ametiasutused. Need kogukonnad on järgmised: i) võrgu- ja infoturbeasutuste, näiteks küberturbe intsidentide lahendamise üksuste kogukond ja

[73]Küberkaitsehariduse, -koolituse ja -õppuste ning hindamisplatvormi (ETEE) kaudu.

[74]Sealhulgas Euroopa Liidu Küberturvalisuse Ameti (ENISA) toetus operatiivkoostööle ja kriisiohjamisele; küberturbe intsidentide lahendamise üksuste võrgustik; küberkriiside kontaktasutuste võrgustik (CyCLONe, millest läbivaadatud võrgu- ja infoturbe direktiivis saab EU-CyCLONe); võrgu- ja infoturbe koostöörühm; rescEU; Europoli juures tegutsevad küberkuritegevuse vastase võitluse Euroopa keskus ja küberkuritegevusega tegelev ühine töökond ning hädaolukordades õiguskaitsealase reageerimise protokoll; ELi luure- ja situatsioonikeskus (EU INTCEN) ja küberdiplomaatia meetmete kogum; ühtne luureandmete analüüsivõime üksus (SIAC); alalise struktureeritud koostöö (PESCO) raames käsitletavad küberprojektid, eelkõige küberturbe kiirreageerimisrühmad ja vastastikune abi küberturvalisuse valdkonnas (CRRT).

katastroofidele reageerijate kogukond; ii) õiguskaitse- ja õigusasutuste kogukond; iii) küberdiplomaatia kogukond; iv) küberkaitse kogukond.

2.1 Ühine küberüksus

Ühine küberüksus võiks olla ELi erinevate küberturvalisuse kogukondade jaoks tegutsev virtuaalne ja füüsiline koostööplatvorm, milles keskendutakse operatiivsele ja tehnilisele koordineerimisele, pidades silmas just olulisemaid piiriüleseid küberintsidente ja -ohte.

Ühine küberüksus on Euroopa tulevase **küberturvalisuse kriisireguleerimise raamistiku** oluline komponent. Nagu on märgitud komisjoni presidendi poliitilistes suunistes,[75] peaks üksus võimaldama liikmesriikidel ning ELi institutsioonidel, organitel ja asutustel kasutada täiel määral ära olemasolevaid struktuure, ressursse ja võimeid, lähtudes sealjuures eelkõige **jagamisvajaduse** põhimõttest. Üksus annaks võimaluse kindlustada edusamme, mida on seni tehtud 2017. aasta ulatuslike küberintsidentide ja kriiside koordineeritud reageerimise soovituse rakendamisel[76]. Samuti annaks see võimaluse veelgi tugevdada soovituses visandatud koostööraamistikku ning rakendada ellu muu hulgas võrgu- ja infoturbe koostöörühmas ja CyCLONe võrgustikus saavutatud tulemusi.

Üksuse loomine võimaldaks kõrvaldada **kaks peamist vajakut**, mis praegu pärisvad liidu reaktsiooni teda mõjutavatele piiriülestele küberohtudele ja -intsidentidele ning suurendavad liidu haavatavust. Esiteks ei ole küberturvalisusega tegelevatel tsiviilsfääri, diplomaatilistel, õiguskaitse ja kaitsevaldkonna **kogukondadel** veel olemas piisavat kokkupuuteala, mille abil edendada struktureeritud koostööd ning hõlbustada operatiiv- ja tehnilist koostööd. Teiseks ei ole küberturvalisuse sidusrühmad suutnud operatiivkoostöö ja vastastikuse abi vallas rakendada olemasolevate võrgustike ja kogukondade **täit potentsiaali**. Muu hulgas on puudu platvorm, mis võimaldaks operatiivkoostööd erasektoriga. Üksus peaks parandama ja kiirendama koordineerimist ning võimaldama ELil tulla toime ulatuslike küberintsidentide ja -kriisidega ning neile adekvaatselt reageerida.

Ühisest küberüksusest ei tohiks saada eraldiseisev organ ning see ei tohiks mõjutada riiklike küberturvalisuse asutuste ega ELi institutsioonide, organite ja asutuste pädevust ja volitusi. Pigem peaks üksus tegutsema ühtse tagalastruktuurina, kus osalejad saavad üksteist toetada ja vastastikku kogemusi vahetada, eriti olukorras, kus eri küberkogukonnad peavad tegema tihedat koostööd. Viimasel ajal aset leidnud intsidendid annavad tunnistust sellest, et EL peab küberohtude arenguga sammu pidamiseks suurendama oma söakust ja valmisolekut. Seetõttu on ühise küberüksuse ELi-poolsed osalejad (komisjon ning ELi asutused ja organid) valmis parema valmisoleku ja vastupidavuse tagamiseks märkimisväärselt suurendama panustatavaid ressursse ja oma suutlikkust.

Ühine küberüksus täidaks kolme peamist eesmärki. Esiteks tagaks see **valmisoleku** kõigis küberturvalisuse kogukondades; teiseks tagaks see teabe jagamise kaudu pideva ühise **olukorrateadlikkuse**; kolmandaks tagaks see **intsidentidele reageerimise** ja intsidentidest taastumise suurema koordineerituse. Nende eesmärkide saavutamiseks peab liit võtma aluseks vanad head **põhimõtted**, nagu **turvaline ja kiire teabevahetus**, parem **koostöö** osalejate vahel, sealhulgas liikmesriikide ja asjaomaste ELi institutsioonide ja asutuste vahel,

[75] Poliitilised suunised järgmisele Euroopa Komisjonile (2019–2024) – „Liit, mis seab kõrgemad sihid: minu tegevuskava Euroopa jaoks“, Ursula von der Leyen.

[76] 13. septembri 2017. aasta soovitus koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (C(2017) 6100 final).

struktuurne **partnerlus usaldusväärsete valdkondlike sidusrühmadega** ja hõlpsam koordineeritud **koostöö välispartneritega**. Üksus peaks selleks kindlaks tegema liikmesriikide ja ELi tasandi võimed ning hõlbustama koostööraamistiku väljatöötamist.

Et ühisest küberüksusest saaks ELi küberturvalisuse operatiivkoostöö kese, püüab komisjon koostöös liikmesriikide ja ELi asjaomaste institutsioonide, organite ja asutustega, sealhulgas Euroopa Liidu Küberturvalisuse Ameti, ELi institutsioonide ja ametite infoturbeintsidentidega tegeleva rühma ja Europoliga, edendada **järkjärgulist ja kaasavat lähenemisviisi,** austades samas kõigi osapoolte pädevust ja volitusi. Kooskõlas selle lähenemisviisiga saab üksus panustada ka sellesse, et asjaomase küberkogukonna liikmed tugevdaksid vastavalt vajadustele oma koostööd.

Ühise küberüksuse loomisel on ette nähtud neli peamist sammu:

- *tuvastada* liikmesriikide ja ELi tasandi asjaomased võimed;
- *valmistada ette* struktureeritud koostöö ja abi raamistik;
- *võtta* raamistik *kasutusele*, toetudes osalejate poolt panustatud vahenditele, ja käivitada üksuse töö;
- *laiendada* raamistikku, lisades koordineeritud reageerimisvõime suurendamiseks valdkondlike sidusrühmade ja väliste partnerite panuse.

Liikmesriikide ning ELi institutsioonide, organite ja asutustega[77] peetavate konsultatsioonide põhjal paneb komisjon oma pädevuse piires tegutseva kõrge esindaja osalusel 2021. aasta veebruaris ette protsessi, vahe-eesmärgid ja ajakava **ühise küberüksuse rajamise etappide jaoks (võimete tuvastamine, raamistiku ette valmistamine ja kasutuselevõtt ning tegevuse laiendamine)**.

2.2 Võitlus küberkuritegevusega

Inimeste sõltuvus internetist on hüppeliselt suurendanud küberkuritegude ründepinda ja viinud olukorrani, kus peaaegu igat liiki kuritegude uurimine sisaldab digitaalset mõõdet. Küberkurjategijad ja kõik need, kes kasutavad oma ebaseadusliku tegevuse kavandamiseks ja elluviimiseks kübervahendeid, võivad ohustada ühiskonna alustalasid. Seetõttu on küberturvalisus tihedalt seotud ELi üldise julgeolekupoliitikaga, millest annavad tunnistust ELi 2020. aasta julgeolekuliidu strateegia ja ELi terrorismivastase võitluse tegevuskava küberohte käsitlevad osad[78].

Tõhus võitlus küberkuritegevuse vastu on küberturvalisuse tagamise alus: heidutust ei ole võimalik saavutada üksnes vastupidavuse abil, vaid see nõuab ka õigusrikkujate tuvastamist ja vastutusele võtmist. Seetõttu on oluline edendada koostööd ja teabevahetust küberturvalisuse valdkonna sidusrühmade ja õiguskaitseasutuste vahel. ELi tasandil on tõhusa koostöö loonud Europol ja ENISA, kes peavad ühiseid konverentse ja seminare ning on esitanud komisjonile, liikmesriikidele ja teistele sidusrühmadele ühisaruandeid

[77]Konsultatsioonid liikmesriikidega (sealhulgas õppuse Blue OLEx20 käigus, millel osalesid riiklike küberturvalisuse asutuste juhid) ning ELi institutsioonide, organite ja asutustega toimusid 2020. aasta juulist novembrini.

[78]Teatis, mis käsitleb ELi 9. detsembri 2020. aasta terrorismivastase võitluse tegevuskava: enneta, hoia ära, kaitse ja reageeri, COM(2020) 795 final.

küberturvalisuse ohtude ja tehnoloogiliste probleemide kohta. Komisjon jätkab integreeritud lähenemisviisi toetamist, et reaktsioon intsidentidele oleks ühtne ja tõhus ning põhineks terviklikul teabepildil.

Selle ühe osana peavad EL ja liikmesriigid laiendama ja parandama õiguskaitseasutuste suutlikkust uurida küberkuritegevust, austades sealjuures täielikult põhiõigusi ning püüdes saavutada vajalikku tasakaalu erinevate õiguste ja huvide vahel. ELi reaktsioon küberkuritegevusele peab tuginema täielikult rakendatud ja eesmärgipärastele õigusaktidele ning erilist tähelepanu tuleb pöörata võitlusele laste seksuaalse ärakasutamisega internetis ja digiuurimisele, sealhulgas seoses kuritegevusega nn tumevõrgus. Õiguskaitseasutustel peab digiuurimise vajadusi silmas pidades olema kogu vajalik varustus. Seepärast esitab komisjon tegevuskava õiguskaitseasutuste digisuutlikkuse parandamiseks, tagades neile vajalikud oskused ja vahendid. Europol arendab edasi oma rolli eksperdikeskusena, et toetada riiklike õiguskaitseasutuste võitlust küberruumi kasutades toime pandud ja küberneetiliste vahendite olemasolust sõltuva kuritegevuse vastu ning aidata kaasa ühiste kohtuekspertiisi standardite kindlaks määramisele (Europoli innovatsioonilabori ja -keskuse kaudu). Kõik need tegevused nõuavad asjakohast kaastööd liikmesriikidelt, keda julgustatakse kasutama ära Sisejulgeolekufondi riiklikke programme ja esitama projektikonkurssidele projekte temaatilise rahastu kaudu toetuse saamiseks.

Komisjon kasutab kõiki asjakohaseid vahendeid, sealhulgas rikkumismenetlust, et tagada 2013. aasta infosüsteemide vastu suunatud ründeid käsitleva direktiivi[79] täielik ülevõtmine ja rakendamine, sealhulgas statistika esitamine liikmesriikide poolt. Komisjonil on kavas parandada domeeninimede kuritarvitamise ennetamist, sealhulgas seoses ebaseadusliku sisu levitamise juhtumitega, ning taotleda täpsete registreerimisandmete kättesaadavust, jätkates koostööd interneti nimede ja numbrite määramise korporatsiooniga (ICANN) ja muude interneti halduse sidusrühmadega, eelkõige ICANNi valitsuste nõuandekomitee avaliku ohutuse töörühma kaudu. Ka läbivaadatud võrgu- ja infoturbe direktiivis nähakse ette domeeninimede ja registreerimisandmete täpsete ja täielike andmebaaside ehk WHOIS-andmete säilitamine ning sellistele andmebaasidele seadusliku juurdepääsu võimaldamine, mis on oluline domeeninimede süsteemi turvalisuse, stabiilsuse ja vastupidavuse tagamiseks.

Samuti jätkab komisjon tööd selle nimel, et saavutada piiriülene juurdepääs elektroonilistele tõenditele kriminaaluurimiste jaoks (mida on vaja 85 % uurimiste puhul, kusjuures 65 % kõigist taotlustest tuleb esitada muus jurisdiktsioonis asuvatele asutustele), pakkudes selleks asjakohaseid kanaleid ja täpsustades norme. Selleks hoogustab komisjon elektrooniliste tõendite paketi ja praktiliste meetmete[80] vastuvõtmist ja rakendamist. Elektroonilisi tõendeid käsitlevate ettepanekute kiire vastuvõtmine Euroopa Parlamendis ja nõukogus ongi oluline eelkõige selleks, et anda ekspertide käsutusse tõhus töövahend. Elektrooniliste tõendite puhul on oluline nende loetavus, mistõttu jätkab komisjon õiguskaitsealase suutlikkuse toetamist digiuurimise valdkonnas, sealhulgas krüpteerimise puhul niivõrd, kuivõrd seda

[79]Direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid.

[80]COM(2018) 225 ja 226; C(2020) 2779 lõplik. Muu hulgas sai projekt SIRIUS hiljuti partnerluse rahastamisvahendist täiendava rahastuse, et parandada kanaleid, mille abil saada seaduslik piiriülene juurdepääs elektroonilistele tõenditele kriminaaluurimise jaoks (mida on vaja 85 % uurimiste puhul, kusjuures 65 % kõigist taotlustest tuleb esitada muus jurisdiktsioonis asuvatele asutustele), ning kehtestada rahvusvahelisel tasandil ühilduvad normid.

kriminaaluurimises vaja läheb, tagades samal ajal täielikult põhiõiguste kaitse ja küberturvalisuse.

2.3 ELi küberdiplomaatia meetmete kogum

Et ennetada ja tõkestada pahatahtlikku kübertegevust, heidutada seda toime panemast ja sellele reageerida, on ELil kasutada **küberdiplomaatia meetmete kogum**[81]. Pärast seda, kui 2019. aasta mais kehtestati küberrünnete vastaste sihipäraste piiravate meetmete õigusraamistik,[82] lisas EL 2020. aasta juulis õigusraamistikuga ette nähtud sanktsioonide korra alusel loetellu kuus isikut ja kolm üksust, kes on vastutavad ELi ja selle liikmesriike mõjutavate küberrünnete eest või on nendega seotud[83]. Oktoobris 2020 kanti loetellu veel kaks isikut ja üks asutus[84]. Pahatahtliku kübertegevuse, sealhulgas pikaldase toimega kübertegevuse vastu tuleks võidelda tõhusa ja tervikliku diplomaatilise ühistegevusega, kasutades kõiki ELi tasandil kättesaadavaid meetmeid.

Et ELi ühine diplomaatiline tegevus oleks kiire ja tõhus, on vaja usaldusväärset ühist olukorrateadlikkust ja võimet valmistada kiiresti ette ELi ühine seisukoht. Liidu välisasjade ja julgeolekupoliitika kõrge esindaja innustab looma ELi luure- ja situatsioonikeskuses (INTCEN) tegutseva **liikmesriikide ELi küberluure töörühma** ja aitab sellele kaasa, et edendada strateegilist luurekoostööd küberohtude ja -tegevuse vallas. See töö aitab parandada olukorrateadlikkust ELis ja hõlbustab otsustusprotsessi ühise diplomaatilise vastuse kujundamiseks. Töörühma ülesandeks on koguda ja hinnata olukorrateadlikkuse parandamiseks asjakohast teavet, tehes koostööd olemasolevate struktuuridega,[85] sealhulgas vajaduse korral nendega, mis tegelevad hübriid- ja välissekkumise ohuga laiemalt.

Et tugevdada ELi suutlikkust ennetada ja tõkestada pahatahtlikku käitumist küberruumis, pahatahtlikult käitumast heidutada ning sellele reageerida, esitab kõrge esindaja komisjoni osalusel ja kooskõlas oma pädevustega ettepaneku, et EL määraks senisest täpsemini kindlaks oma **küberheidutuse alused**. Tuginedes senisele küberdiplomaatia meetmete kogumi raames tehtud tööle, peaks ELi küberheidutus aitama kaasa riikide vastutustundlikule käitumisele ja koostööle küberruumis ning koondama jõupingutused võitluseks kõige suurema mõjuga küberrünnete vastu, eelkõige puudutab see ründeid elutähtsa taristu ning demokraatlike institutsioonide ja protsesside[86] vastu, aga samuti ründeid tarneahelate vastu ja küberruumi

[81] https://www.consilium.europa.eu/et/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82] Nõukogu 17. mai 2019. aasta otsus (ÜVJP) 2019/797 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberründeid (ELT L 129 I, 17.5.2019, lk 13). Nõukogu 17. mai 2019. aasta määrus (EL) 2019/796
piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberründeid (ELT L 129 I, 17.5.2019, lk 1).

[83] Nõukogu 30. juuli 2020. aasta otsus (ÜVJP) 2020/1127, millega muudetakse otsust (ÜVJP) 2019/797 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberründeid (ST/9564/2020/INIT) (ELT L 246, 30.7.2020, lk 12–17). Nõukogu 30. juuli 2020. aasta rakendusmäärus (EL) 2020/1125, millega rakendatakse määrust (EL) 2019/796 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberründeid (ST/9568/2020/INIT)(ELT L 246, 30.7.2020, lk 4–9).

[84] Nõukogu 22. oktoobri 2020. aasta otsus (ÜVJP) 2020/1537, millega muudetakse otsust (ÜVJP) 2019/797 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberründeid (ELT L 351 I, 22.10.2020, lk 5–7). Nõukogu 22. oktoobri 2020. aasta rakendusmäärus (EL) 2020/1536, millega rakendatakse määrust (EL) 2019/796 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberründeid (ELT L 351I, 22.10.2020, lk 1–4).

[85] Näiteks ELi ühtne luureandmete analüüsivõime üksus (SIAC) ja vajadust mööda alalise struktureeritud koostöö (PESCO) raames loodud asjaomased projektid ning 2018. aasta kiirhoiatussüsteem, mis rajati selleks, et toetada võitlust desinformatsiooniga ELis.

[86] Sealjuures püütakse saavutada koostoimet Euroopa demokraatia tegevuskava algatustega.

kasutades toime pandud intellektuaalomandi vargust. Küberheidutuse alustes tuleb välja tuua, kuidas EL ja liikmesriigid saaksid kasutada oma poliitilisi, majanduslikke, diplomaatilisi, õiguslikke ja strateegilise kommunikatsiooni vahendeid pahatahtliku kübertegevuse vastu võitlemiseks, ning samuti tuleks käsitleda seda, kuidas saaksid EL ja liikmesriigid suurendada oma suutlikkust tuvastada pahatahtliku kübertegevuse toimepanijad. Peale selle kavatseb kõrge esindaja üheskoos nõukogu ja komisjoniga kaaluda **küberdiplomaatia meetmete kogumi raames täiendavate meetmete** võtmist, vaadeldes sealhulgas võimalust võtta täiendavaid piiravaid meetmeid ning kasutada **horisontaalse sanktsioonide korra alusel küberrünnete toimepanijate loetellu kandmise üle hääletades kvalifitseeritud häälteenamust**. Samuti peaks EL jätkama jõupingutusi, et **tugevdada koostööd rahvusvaheliste partneritega**, sealhulgas NATOga, ning edendada nendega ühist arusaama ohuolukorrast, arendada koostöömehhanisme ja määrata kindlaks ühised diplomaatilised meetmed.

Ühtlasi teeb kõrge esindaja komisjoni osalusel ettepaneku ajakohastada **küberdiplomaatia meetmete kogumi rakendussuuniseid**,[87] muu hulgas otsustusprotsessi tõhustamiseks, ning jätkab korrapäraselt küberdiplomaatia meetmete kogumiga seotud õppuste ja hindamiste korraldamist. EL peaks paremini **integreerima küberdiplomaatia meetmed ELi kriisimehhanismidesse** ning püüdma saavutada selle koostoimet hübriidohtudega võitlemise ühises raamistikus[88] hübriidohtude, desinformatsiooni ja välise sekkumise vastu võitlemiseks tehtavate jõupingutuste ja Euroopa demokraatia tegevuskavaga. Sellega seoses peaks EL kaaluma võimalust kasutada küberdiplomaatia meetmete kogumit koostoimes ELi lepingu artikli 42 lõikega 7 ja ELi toimimise lepingu artikliga 222[89].

2.4 Küberkaitsevõime suurendamine

Vastavalt ELi 2016. aasta üldisest strateegiast[90] tulenevale ELi ambitsioonitasemele peavad EL ja liikmesriigid suurendama oma suutlikkust küberohte ennetada ja neile reageerida. Sel eesmärgil esitab kõrge esindaja koostöös komisjoniga **ülevaate ELi küberkaitsepoliitika raamistikust**, millega tõhustatakse koordineerimist ja koostööd ELi-poolsete osalejate[91] vahel, samuti koordineerimist ja koostööd liikmesriikidega ning liikmesriikide vahel, sealhulgas seoses ühise julgeoleku- ja kaitsepoliitika (ÜJKP) missioonide ja operatsioonidega. Küberkaitsepoliitika raamistik peaks andma teavet tulevaste strateegiliste suuniste[92] jaoks, millega tagada küberturvalisuse ja küberkaitse edasine integreerimine laiemasse julgeoleku- ja kaitsetegevusse.

2018. aastal määratles EL küberruumi julgeolekupoliitika tegevusvaldkonnana[93]. ELi sõjaline komitee peaks peatselt koostatavas dokumendis **„Sõjaline visioon ja strateegia küberruumi kui tegevusvaldkonna jaoks“** kindlaks määrama, mil määral võimaldab küberruum ELi ÜJKP sõjalisi missioone ja operatsioone. Euroopa Kaitseagentuuri (EDA) loodud **sõjaline**

[87] 13007/17
[88] https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52016JC0018&from=ET
[89] Vastavalt vastastikuse kaitse klausel ja solidaarsusklausel.
[90] Nõukogu järeldused (14149/16) ELi üldise strateegia rakendamise kohta julgeoleku- ja kaitsevaldkonnas.
[91] Eelkõige Euroopa välisteenistus, sealhulgas ELi sõjaline staap (EUMS), Euroopa Julgeoleku- ja Kaitsekolledž (ESDC), komisjon ja ELi ametid, eelkõige Euroopa Kaitseagentuur (EDA).
[92] Nõukogu 17. juuni 2020. aasta järeldused julgeoleku ja kaitse kohta (8910/20)
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/et/pdf

CERT-võrgustik[94] aitab märkimisväärselt kaasa liikmesriikidevahelise koostöö suurendamisele. Lisaks tugevdatakse kosmoseprogrammi raames käitatava elutähtsa kosmosetaristu küberturvalisuse tagamiseks Euroopa Kosmoseprogrammiametit, eelkõige Galileo turvaseirekeskust, ning laiendatakse selle volitusi kosmoseprogrammi muudele elutähtsatele komponentidele.

EL ja liikmesriigid peaksid veelgi hoogustama ELi küberkaitsepoliitika raamistiku ja muude poliitikavahendite kaudu **tipptasemel küberkaitsevõime arendamist**, tuginedes vajaduse korral Euroopa Kaitseagentuuri tööle. Selleks tuleb rõhku panna uue, kekse tähtsusega tehnoloogia, nagu tehisintellekti, krüpteerimise ja kvantarvutuse arendamisele ja kasutamisele. Kooskõlas ELi 2018. aasta võimete arendamise prioriteetidega[95] ja lähtudes esimese täieliku kaitseküsimuste iga-aastase kooskõlastatud läbivaatamise aruande tulemustest,[96] peaks EL jätkuvalt edendama koostööd liikmesriikide vahel **küberkaitsealaste uuringute, innovatsiooni ja võimearenduse vallas**, ergutades liikmesriike kasutama täiel määral ära **alalise struktureeritud koostöö (PESCO)**[97] ja **Euroopa Kaitsefondi**[98] pakutavaid võimalusi.

Komisjoni tulevases tegevuskavas tsiviil-, kaitse- ja kosmosetööstuse koostoime kohta, mis esitatakse 2021. aasta esimeses kvartalis, sisalduvad meetmed, millega edendada koostoimet programmide, tehnoloogia, innovatsiooni ja iduettevõtete tasandil, pidades silmas asjaomaste programmide[99] juhtimisstruktuuri.

Lisaks tuleks teabevahetuse ja vastastikuse abi edendamiseks arendada koostoimet ja puutepunkte muudes raamistikes tehtavate küberkaitsealgatuste vahel, sealhulgas liikmesriikide vahel alalise struktureeritud koostöö raames toimuvate kübervaldkonna koostööprojektide vahel, [100] samuti ELi küberturvalisuse struktuuridega.

Strateegilised algatused

Euroopa Liidu eesmärgid:

- viia lõpule Euroopa küberturvalisuse kriisireguleerimise raamistiku väljatöötamine ning määrata kindlaks ühise küberüksuse loomise protsess, vahe-eesmärgid ja ajakava;
- jätkata julgeolekuliidu strateegia raames küberkuritegevuse teemade käsitlemist;
- julgustada looma ELi luure- ja situatsioonikeskuses tegutseva liikmesriikide

[94] ELi sõjalise CERT-võrgustiku loomine vastab 2018. aasta küberkaitsepoliitika raamistikus kindlaks määratud eesmärgile ning sellega püütakse edendada aktiivset suhtlust ja teabevahetust ELi liikmesriikide sõjaliste CERTide vahel.

[95] 2018. aasta juunis leppisid liikmesriigid Euroopa Kaitseagentuuri juhtnõukogus kokku kaitsealase koostöö suunamises ELi tasandil.

[96] Heaks kiidetud kaitseministrite poolt Euroopa Kaitseagentuuri juhtnõukogus novembris 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

[97] Praegu on käimas mitu kübervaldkonnaga seotud PESCO projekti, eelkõige küberohtudele ja -intsidentidele reageerimise teabevahetuse platvorm, küberturbe kiirreageerimisrühmad ja vastastikune abi küberturvalisuse valdkonnas, ELi küberakadeemia ja innovatsioonikeskus ning küber- ja teabevaldkonna koordinatsioonikeskus (CIDCC).

[98] Euroopa Kaitsefondi raames on komisjon juba leidnud võimalusi küberkaitsealaseks teadus- ja arendustegevuseks, millega tugevdada kaitsetööstuse koostööd ning innovatsiooni- ja konkurentsivõimet.

[99] Näiteks „Euroopa horisont“, „Digitaalne Euroopa“ ja Euroopa Kaitsefond.

[100] https://pesco.europa.eu/

küberluure töörühma ja sellele kaasa aidata;

- arendada oma **küberheidutusvõimet**, et ennetada ja tõkestada pahatahtlikku kübertegevust, heidutada seda toime panemast ja sellele reageerida;
- vaadata läbi küberkaitsepoliitika raamistik;
- arendada ÜJKP sõjaliste missioonide ja operatsioonide jaoks välja ELi sõjaline visioon ja strateegia küberruumi kui tegevusvaldkonna jaoks;
- toetada tsiviil-, kaitse- ja kosmosetööstuse koostoimet;
- suurendada kosmoseprogrammi elutähtsa kosmosetaristu küberturvalisust.

3. ÜLEMAAILMSE JA AVATUD KÜBERRUUMI EDENDAMINE

EL peaks jätkama koostööd rahvusvaheliste partneritega, et edendada oma poliitilist mudelit ja sellist käsitust küberruumist, mis rajaneb õigusriigi põhimõttele, inimõigustele, põhivabadustele ja demokraatlikele väärtustele, panustades sotsiaalsesse, majanduslikku ja poliitilisse arengusse kogu maailmas. Sellega seoses peaks EL jätkama panustamist ka julgeolekuliidu algatusse. Küberruumi hoidmiseks ülemaailmse, avatud, stabiilse ja turvalisena on tarvilik rahvusvaheline koostöö. EL peaks seetõttu jätkama koostööd kolmandate riikide, rahvusvaheliste organisatsioonide ja sidusrühmaüleste kogukondadega ning töötama välja sidusa ja tervikliku rahvusvahelise küberpoliitika ja viima seda ellu, võttes arvesse uue tehnoloogia majanduslike aspektide, sisejulgeoleku ning välis-, julgeoleku- ja kaitsepoliitika üha suuremat omavahelist seotust. ELil kui tugeval majandus- ja kaubandusblokil, mis põhineb demokraatlikel põhiväärtustel ning õigusriikluse ja põhiõiguste austamisel, on väga hea võimalus juhtida rahvusvaheliste normide ja standardite kujundamist ja levitamist.

3.1. ELi juhtroll küberruumi standardite, normide ja raamistike kujundamisel

Rahvusvahelise standardimise hoogustamine

Et edendada ja kaitsta rahvusvahelisel tasandil oma käsitust küberruumist, peab EL **suurendama oma osalust ja juhtpositsiooni rahvusvaheliste standardite kujundamisel ning esindatust rahvusvahelistes ja Euroopa standardiorganisatsioonides ja muudes standardite arendamisega tegelevates organisatsioonides**[101]. Kuna digitehnoloogia areneb kiiresti, on sellistes valdkondades nagu tehisintellekt, pilvandmetöötlus, kvantarvutus ja kvantside rahvusvahelistel standarditel traditsiooniliste regulatiivsete meetmete kõrval üha suurem tähtsus. Kolmandad riigid kasutavad rahvusvahelist standardimist üha enam selleks, et edendada oma poliitilisi ja ideoloogilisi põhimõtteid, mis sageli ei vasta ELi väärtustele. Lisaks suureneb oht, et kasutusele võetakse konkureerivaid rahvusvahelisi standardimise raamistikke, mis võib viia killustumiseni.

Kujunemisjärgus tehnoloogiat ja interneti põhiarhitektuuri reguleerivate rahvusvaheliste standardite kujundamine kooskõlaliseks ELi väärtustega aitab saavutada seda, et internet jääb

[101] Näiteks Rahvusvaheline Standardiorganisatsioon (ISO), Rahvusvaheline Elektrotehnikakomisjon (IEC), Rahvusvaheline Telekommunikatsiooni Liit (ITU), Euroopa Standardikomitee (CEN), Euroopa Elektrotehnika Standardikomitee (CENELEC), Euroopa Telekommunikatsioonistandardite Instituut (ETSI), Interneti tehniline operatiivkogu, 3. põlvkonna partnerlusprojekti (3GPP) and tElektri- ja Elektroonikainseneride Instituut (IEEE).

ülemaailmseks ja avatuks, et tehnoloogia on inimkeskne ega riiva eraelu puutumatust ning selle kasutus on seaduslik, ohutu ja eetiline. Tulevase standardimisstrateegia raames peaks EL määrama kindlaks oma **rahvusvahelise standardimise eesmärgid** ning viima läbi tarmuka ja koordineeritud teavituskampaania, millega neid rahvusvahelisel tasandil edendada. Samuti tuleks püüelda tihedama koostöö ja koormuse jagamise poole sarnaselt meelestatud partnerite ja Euroopa sidusrühmadega.

Riikide vastutustundliku käitumise edendamine

EL jätkab koostööd rahvusvaheliste partneritega, et edendada ülemaailmset, avatud, stabiilset ja turvalist küberruumi, kus **peetakse kinni rahvusvahelisest õigusest, eelkõige ÜRO põhikirjast**,[102] ning **järgitakse vabatahtlikke mittesiduvaid norme ja reegleid ning riikide vastutustundliku käitumise põhimõtteid**[103]. Olukorras, kus tulemuslik mitmepoolne arutelu rahvusvahelise julgeoleku üle küberruumis on soikunud, peavad EL ja liikmesriigid olema ÜROs ja muudel asjakohastel rahvusvahelistel foorumitel toimuvates aruteludes kindlasti senisest tegusamad. ELil on kõik võimalused **liikmesriikide seisukohti rahvusvahelistel foorumitel edendada, koordineerida ja konsolideerida**. Selleks **tuleks välja töötada ühtne liidu seisukoht rahvusvahelise õiguse kohaldamise kohta küberruumis**. Kõrge esindaja kavatseb koos liikmesriikidega teha kaasava ja konsensuspõhise ettepaneku leppida ÜRO tasandil kokku **riikide vastutustundlikku küberkäitumist** edendavas poliitiliselt siduvas **tegevuskavas**[104]**.** Tegevuskava tugineks ÜRO Peaassambleel heaks kiidetud dokumentidele[105] ning sellega nähtaks ette ÜRO raames tegutsev koostöö- ja parimate tavade vahetamise platvorm ning riikide vastutustundliku käitumise normide rakendamise ja suutlikkuse suurendamise mehhanism. Lisaks on kõrgel esindajal kavas täiustada riikide vahel **usaldust suurendavate meetmete** rakendamist, sealhulgas parimate tavade vahetamist piirkondlikul ja mitmepoolsel tasandil ning piirkondadevahelist koostööd.

Suurenenud üleilmne ühenduvus ei tohi viia tsensuuri, massilise jälgimise, andmekaitse rikkumiste ega kodanikuühiskonna, akadeemiliste ringkondade ja kodanike vastu suunatud repressioonideni. **Inimõiguste ja põhivabaduste kaitsmisel** internetis peaks EL püsima jätkuvalt juhtrollis. Selleks peaks EL veelgi edendama rahvusvahelise inimõigustealase õiguse ja standardite[106] järgimist, käivitama oma inimõiguste ja demokraatia tegevuskava (2020–2024)[107] ning propageerima oma inimõigustealaseid suuniseid sõnavabaduse kohta internetis ja mujal,[108] **tugevdades ELi poliitikavahendite praktilist kohaldamist**. EL peaks tegema pidevaid jõupingutusi, et **kaitsta inimõiguste kaitsjaid, kodanikuühiskonda ja akadeemilisi ringkondi küberturvalisuse, andmekaitse, jälgimise ja veebitsensuuri küsimustes**. Selleks peaks EL andma täiendavaid praktilisi suuniseid, edendama parimaid

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] Vastavalt rahvusvahelise julgeoleku kontekstis info- ja telekommunikatsioonivaldkonna arenguga tegelevate valitsuseekspertide rühmade (UNGGE) asjaomastele aruannetele, mille ÜRO Peaassamblee on heaks kiitnud (eelkõige 2015., 2013. ja 2010. aasta aruanne).

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Vastavalt rahvusvahelise julgeoleku kontekstis info- ja telekommunikatsioonivaldkonna arenguga tegelevate valitsuseekspertide rühmade (UNGGE) asjaomastele aruannetele, mille ÜRO Peaassamblee on heaks kiitnud (eelkõige 2015., 2013. ja 2010. aasta aruanne).

[106] Eelkõige ÜRO harta ja inimõiguste ülddeklaratsioon.

[107] https://www.consilium.europa.eu/et/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

tavasid ja suurendama jõupingutusi, et ennetada kujunemisjärgus tehnoloogia väärkasutamist, kasutades selleks vajaduse korral diplomaatilisi meetmeid ja ekspordikontrolli sellise tehnoloogia suhtes. EL peaks samuti jätkama võitlust kõige haavatavamate ühiskonnaliikmete kaitsmise nimel internetis, kehtestades õigusnormid laste paremaks kaitsmiseks seksuaalse väärkohtlemise ja ärakasutamise eest ning lapse õiguste strateegia.

Budapesti küberkuritegevuse konventsioon

EL toetab jätkuvalt kolmandaid riike, kes soovivad liituda **Euroopa Nõukogu Budapesti küberkuritegevuse konventsiooniga**, ning jätkab tööd, et viia lõpule **Budapesti konventsiooni teine lisaprotokoll**, mis sisaldab meetmeid õiguskaitse- ja õigusasutuste rahvusvahelise koostöö parandamiseks, samuti teiste riikide ametiasutuste ja teenuseosutajate vahelise koostöö parandamiseks. Teise lisaprotokolli üle käivatel läbirääkimistel osaleb ELi nimel komisjon[109]. Praegune algatus leppida kokku uues küberkuritegevust käsitlevas rahvusvahelises õigusaktis ÜRO tasandil võib suurendada lõhesid ja aeglustada vajalikke riiklikke reforme, samuti riikide jõupingutusi oma suutlikkuse suurendamiseks, mis võib lõpuks takistada tulemuslikku rahvusvahelist koostööd küberkuritegevuse vastu võitlemisel: EL ei näe vajadust ühegi uue küberkuritegevust käsitleva õigusakti järele ÜRO tasandil. EL osaleb jätkuvalt **küberkuritegevust käsitlevas mitmepoolses teabevahetuses**, et tagada kaasatuse ja läbipaistvuse kaudu inimõiguste ja põhivabaduste austamine ning võtta kõigi osapoolte hüvanguks arvesse olemasolevaid eksperditeadmisi.

3.2 Koostöö partnerite ja sidusrühmaülese kogukonnaga

EL peaks **tugevdama ja laiendama oma küberdialoogi kolmandate riikidega**, et edendada oma väärtusi ja käsitust küberruumist, jagada parimaid tavasid ja teha tõhusamat koostööd. EL peaks samuti looma **struktureeritud teabevahetuse piirkondlike organisatsioonidega**, nagu Aafrika Liit, ASEANi piirkondlik foorum, Ameerika Riikide Organisatsioon ja Euroopa Julgeolekukoostöö Organisatsioon. Ühtlasi peaks EL püüdma teistegi partneritega leppida ühist huvi pakkuvates küsimustes võimalust mööda kokku ühistes lähtepunktides. Tehes koostööd ELi delegatsioonidega ja vajaduse korral liikmesriikide saatkondadega kogu maailmas, peaks EL moodustama mitteametliku **ELi küberdiplomaatia võrgustiku**, et edendada ELi käsitust küberruumist, vahetada teavet ja kooskõlastada korrapäraselt küberruumi arengust lähtuvaid tegevusi [110].

Tuginedes 8. juuli 2016. aasta[111] ja 10. juuli 2018. aasta ühisdeklaratsioonidele, peaks EL jätkama [112]**ELi ja NATO koostöö** edendamist, eelkõige küberkaitse koostalitlusnõuete asjus. Sellega seoses peaks EL jätkama asjaomaste ÜJKP struktuuride integreerimist NATO liitlasvägede missioonide võrgustikku, võimaldades vajadust mööda võrgustike koostalitlust NATO ja selle partnerriikidega. Lisaks tuleks täiendavalt uurida ELi ja NATO koostööd hariduse, koolituse ja õppuste valdkonnas, otsides muu hulgas koostöövõimalusi Euroopa Julgeoleku- ja Kaitsekolledži ning NATO Küberkaitsekoostöö Keskuse vahel.

Kooskõlas oma väärtustega toetab EL kindlalt **sidusrühmaülest interneti haldamise mudelit**. Internett ei tohiks langeda ühegi üksiku valitsuse ega rahvusvahelise organisatsiooni

[109] Nõukogu 2019. aasta juuni otsus (viitenumber 9116/19)
[110]Vajaduse korral saaks selle abil täiendada liikmesriikide välisministeeriume hõlmava ELi mitteametliku digitaalse diplomaatia võrgustiku tegevust.
[111] http://www.consilium.europa.eu/et/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[112] https://www.consilium.europa.eu/et/press/press-releases/2018/07/10/eu-nato-joint-declaration/

kontrolli alla. EL peaks jätkama osalemist rahvusvahelistel foorumitel,[113] et tõhustada koostööd ning tagada põhiõiguste ja -vabaduste kaitse, sealhulgas eelkõige inimväärikuse, eraelu puutumatuse ning sõna- ja teabevabaduse kaitse. Et edendada küberturvalisuse küsimuses sidusrühmaülest koostööd, püüavad komisjon ja kõrge esindaja kooskõlas oma vastavate pädevustega tugevdada **korrapärast ja struktureeritud teabevahetust sidusrühmadega**, sealhulgas erasektori, akadeemiliste ringkondade ja kodanikuühiskonnaga, rõhutades, et küberruum põhineb osalejate vastastikusel seotusel ning selleks, et see püsiks ülemaailmne, avatud, stabiilne ja turvaline, peavad kõik sidusrühmad teabevahetuses osalema ja võtma vastutuse. Koostöö sidusrühmadega annab olulise lähtekoha ELi edasisteks sammudeks.

3.3. Ülemaailmse kübersuutlikkuse ja -vastupidavuse suurendamine

Selleks et kõik riigid saaksid osa sotsiaalsest, majanduslikust ja poliitilisest kasust, mida internett ja tehnoloogia toovad, toetab EL jätkuvalt oma partnereid, et suurendada nende kübervastupidavust ning suutlikkust uurida küberkuritegevust, viia süüdlased kohtu ette ja tegeleda küberohtudega. Üldise sidususe tagamiseks peaks EL töötama välja **ELi välise kübersuutlikkuse suurendamise tegevuskava**, et juhtida neid jõupingutusi kooskõlas oma välise kübersuutlikkuse suurendamise suuniste[114] ja kestliku arengu tegevuskavaga aastani 2030[115]. Nimetatud tegevuskavaga tuleks koondada liikmesriikide ning oma volituste piires tegutsevate asjaomaste ELi institutsioonide, organite ja asutuste ning algatuste, sealhulgas ELi kübersuutlikkuse suurendamise võrgustiku[116] raames loodud eksperditeadmised. ELi asjaomaste institutsiooniliste sidusrühmade koondamiseks luuakse **ELi kübersuutlikkuse suurendamise nõukogu**, mis jälgib tehtud edusamme ning teeb kindlaks edasised koostöövõimalused ja võimalikud lüngad. Lisaks võib see toetada tõhustatud koostööd liikmesriikidega, samuti avaliku ja erasektori partneritega ning muude asjaomaste rahvusvaheliste organitega, et tagada jõupingutuste koordineerimine ja vältida dubleerimist.

ELi tegevus **kübersuutlikkuse suurendamisel** peaks jätkuvalt keskenduma Lääne-Balkani piirkonnale ja ELi naaberriikidele, samuti partnerriikidele, kus toimub kiire digitaalne areng. EL peaks oma jõupingutustes toetama partnerriikides ELi küberdiplomaatia põhimõtetest ja standarditest lähtuvate õigusaktide ja poliitika väljatöötamist. Sellega seoses peaksid ELi jõupingutused suutlikkuse suurendamiseks digiülemineku valdkonnas hõlmama standardelemendina ka küberturvalisust. Selleks peaks EL töötama nende töötajate jaoks, kes tegelevad välise digi- ja kübersuutlikkuse suurendamisega, välja eraldi koolitusprogrammi. Samuti peaks EL kooskõlas Euroopa demokraatia tegevuskava raames tehtavate jõupingutustega abistama asjassepuutuvaid riike võitluses kasvava pahatahtliku kübertegevusega, mis kahjustab nende ühiskondade arengut ning **demokraatlike süsteemide terviklikkust ja turvalisust**. Sellega seoses võiks olla kasu üksteise kogemusest õppimisest, seda nii ELi liikmesriikide seas kui ka ELi asjaomaste ametite ja kolmandate riikide vahel.

[113] Näiteks interneti nimede ja numbrite määramise korporatsioon (ICANN) ja Interneti Haldamise Foorum (IGF).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

2018. aasta ÜJKP tsiviiltegevuse kokkuleppe[117] kontekstis võivad ÜJKP tsiviilmissioonid aidata kaasa ELi üldistele jõupingutustele küberturvalisuse probleemide lahendamisel, eelkõige tugevdades partnerriikides õigusriiklust ning õiguskaitse ja tsiviilhalduse võimekust.

Strateegilised algatused

Euroopa Liidu eesmärgid:

- määrata kindlaks eesmärgid rahvusvahelistes standardimisprotsessides ja edendada neid rahvusvahelisel tasandil;
- edendada küberruumis rahvusvahelist julgeolekut ja stabiilsust, esitades ELi ja liikmesriikide nimel ettepaneku leppida ÜRO tasandil kokku riikide vastutustundlikku küberkäitumist edendavas tegevuskavas;
- pakkuda praktilisi suuniseid inimõiguste ja põhivabaduste kohaldamise kohta küberruumis;
- kaitsta lapsi veelgi innukamalt seksuaalse väärkohtlemise ja ärakasutamise eest ning koostada lapse õiguste strateegia;
- edendada Budapesti küberkuritegevuse konventsiooni, sealhulgas Budapesti konventsiooni teise lisaprotokolli lõpuleviimist;
- laiendada ELi küberdialoogi kolmandatele riikidele ning piirkondlikele ja rahvusvahelistele organisatsioonidele, sealhulgas ELi mitteametliku küberdiplomaatia võrgustiku kaudu;
- tugevdada teabevahetust sidusrühmaülese kogukonnaga, eelkõige korrapärase ja struktureeritud teabevahetuse kaudu, kuhu on kaasatud erasektor, akadeemilised ringkonnad ja kodanikuühiskond;
- teha ettepanek ELi välise kübersuutlikkuse suurendamise tegevuskava koostamise ja ELi kübersuutlikkuse suurendamise nõukogu loomise kohta.

III. KÜBERTURVALISUS ELi INSTITUTSIOONIDES, ORGANITES JA ASUTUSTES

Arvestades **ELi institutsioonide, organite ja asutuste** suurt poliitilist tähtsust, nende suurt rolli väga tundlike küsimuste koordineerimisel ning suurte avaliku sektori rahasummade haldamisel, on nad **küberrünnete ja eelkõige küberspionaaži regulaarne sihtmärk**. Kuid kübervastupidavus ning pahatahtliku kübertegevuse avastamise ja sellele reageerimise võime on nendes üksustes väga erineva tasemega. Seetõttu on vaja küberturvalisuse üldist taset sidusate ja ühtsete normide abil parandada.

Infoturbe valdkonnas on tehtud edusamme **ELi salastatud teabe ja salastamata tundliku teabe kaitse normide** suurema ühtluse suunas. Salastatud teabe süsteemide koostalitlusvõime on siiski endiselt piiratud, mis takistab teabe sujuvat edastamist eri üksuste vahel. ELi salastatud teabe ja tundliku salastamata teabe käitlemist eri institutsioonides tuleks veelgi ühtlustada, andes sel viisil eeskuju koostalitlusvõime parandamiseks liikmesriikide

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/et/pdf.

vahel. Samuti tuleks menetluste lihtsustamiseks kehtestada liikmesriikide jaoks ühtsed alamstandardid. EL peaks arendama edasi oma võimet suhelda partneritega turvalisel viisil, tuginedes võimaluste piires kehtivatele korraldustele ja menetlustele.

Vastavalt julgeolekuliidu strateegia sätetele esitab komisjon 2021. aastal käimasolevale institutsioonidevahelisele küberturvalisusealasele arutelule[118] tuginedes **kõigile ELi institutsioonidele, organitele ja asutustele ettepaneku infoturvet käsitlevate ühiste siduvate eeskirjade ja küberturvalisust käsitlevate ühiste siduvate eeskirjade vastuvõtmiseks**.

Ka kaugtöö praegused ja tulevased suundumused nõuavad täiendavaid investeeringuid turvalisse varustusse, taristusse ja töövahenditesse, mis võimaldaksid kaugtööd tundlike ja salastatud dokumentidega.

Lisaks muutuvad küberohud üha laastavamaks ning ELi institutsioone, organeid ja asutusi tabavad üha sagedamini keerukad küberründed, mis kokku tekitab vajaduse suuremate investeeringute järele, et saavutada küberküpsuse kõrge tase. Kõigi ELi institutsioonide, organite ja asutuste jaoks on koostamisel küberteadlikkuse programm, mille abil suurendada töötajate teadlikkust ja küberhügieeni ning arendada ühiseid küberturvalisuse tavasid.

Vaja on **tugevdada CERT-EUd täiustatud rahastamismehhanismiga**, et suurendada selle suutlikkust aidata ELi institutsioonidel, organitel ja asutustel kohaldada uusi küberturvalisuse norme ja parandada oma kübervastupidavust. Samuti tuleb suurendada CERT-EU volitusi, et tagada sellele stabiilsed töövahendid nende eesmärkide saavutamiseks.

Strateegilised algatused

1. Määrus infoturbe kohta ELi institutsioonides, organites ja asutustes.
2. Määrus ELi institutsioonide, organite ja asutuste ühiste küberturvalisuse normide kohta.
3. Uus õiguslik alus CERT-EU volituste ja rahastamise suurendamiseks.

IV. JÄRELDUSED

Selle strateegia kooskõlastatud rakendamine aitab kaasa ELi küberturvalise digikümnendi eesmärkide ja julgeolekuliidu eesmärkide saavutamisele ning ELi positsiooni tugevdamisele kogu maailmas.

Oluliste teenuste ja elutähtsa taristu küberturvalisuse normide ja standardite kujundamisel peaks EL olema maailmatasemel esirinnas, samuti puudutab see uue tehnoloogia väljatöötamist ja rakendamist. Küberturvalise digiülemineku tagamisel on oma osa igal internetti kasutaval organisatsioonil ja üksikisikul.

Komisjon ja kõrge esindaja jälgivad kooskõlas oma vastavate pädevustega selle strateegia raames tehtavaid edusamme ja töötavad välja hindamiskriteeriumid. Järelevalve puhul tuleb arvesse võtta ka Euroopa Liidu Küberturvalisuse Ameti aruandeid ja komisjoni korrapäraseid julgeolekuliidu aruandeid. Strateegia tulemused aitavad kaasa eeloleva digikümnendi

[118]ELi korrapärased institutsioonidevahelised arutelud küberturvalisuse teemal moodustavad osa laiemast mõttevahetusest ELi institutsioonide digiülemineku võimaluste ja väljakutsete üle.

eesmärkide saavutamisele[119]. Kooskõlas oma vastavate pädevustega jätkavad komisjon ja kõrge esindaja koostööd liikmesriikidega, et teha kindlaks praktilised meetmed, mille abil tuua vajadust mööda kokku ELi neli küberturvalisuse kogukonda ehk elutähtsa taristu ja siseturu vastupidavuse kogukond, õiguse ja õiguskaitse kogukond, küberdiplomaatia kogukond ning küberkaitse kogukond. Lisaks jätkavad komisjon ja kõrge esindaja panustamist sidusrühmaülesesse kogukonda, rõhutades, et kõik internetikasutajad peavad aitama kaasa sellele, et säiliks ülemaailmne, avatud, stabiilne ja turvaline küberruum, kus igaüks saab elada ohutult oma digitaalset elu.

[119]Vastavalt komisjoni 2021. aasta tööprogrammile.

Liide: Edasised sammud 5G-võrkude küberturvalisuse suunas

5G-võrkude küberturvalisust käsitleva komisjoni soovituse läbivaatamise tulemuste[120] põhjal peaksid ELi tasandil tehtava koordineeritud töö järgmised sammud keskenduma kolmele peamisele eesmärgile ning lühiajalise ja keskpika perioodi peamistele meetmetele, mis on alltoodud tabelis liikmesriikide ametiasutuste, komisjoni ja ENISA jaoks ette nähtud.

Järgmise etapi esimeseks prioriteediks on **viia lõpule 5G küberturvalisuse meetmepaketi rakendamine riiklikul tasandil ja asuda käsitlema 2020. aasta juuli eduaruandes tõstatatud küsimusi**. Nagu juba eduaruandes märgitud, tuleks mõne meetmepaketis sisalduva strateegilise meetme puhul kasuks võrgu- ja infoturbe koostöörühma tööjaotuskava raames **tõhusam koordineerimine või teabevahetus**. Selle põhjal oleks võimalik hiljem välja töötada **parimad tavad või suunised**. Tehniliste meetmete suhtes võiks ENISA pakkuda täiendavat tuge. Selleks võiks ta oma senise töö põhjal ja teatavaid teemasid süvendatult uurides **töötada välja põhjaliku ülevaate kõigist mobiilsideoperaatoritele esitatavatest 5G küberturvalisuse nõudeid käsitlevatest suunistest**.

Teiseks on liikmesriigid rõhutanud, et arenguga kaasas käimiseks tuleb **pidevalt jälgida edasiminekut tehnoloogia, 5G arhitektuuri, ohtude ning 5G kasutuse ja -rakenduste vallas**. Samuti tuleb silmas pidada **muutuvaid väliseid tegureid, et edukalt tuvastada ja maandada uusi ja tekkivaid riske**. Lisaks tuleks esialgse riskianalüüsi mitut aspekti põhjalikumalt uurida, eelkõige selleks, et hõlmata kogu 5G ökosüsteemi, sealhulgas võrgutaristu ja 5G tarneahela kõiki asjakohaseid osi. Meetmepakett on kavandatud paindliku ja kohandatavana ning vajaduse korral võib seda keskpikas perspektiivis täiendada või muuta, et tagada selle terviklikkus ja ajakohasus.

Kolmandaks tuleks jätkata **ELi tasandi meetmete** võtmist, et toetada ja täiendada meetmepaketi eesmärke ning integreerida need täielikult asjaomastesse liidu ja komisjoni poliitikavaldkondadesse, eelkõige jätkates meetmeid, millest komisjon teatas oma 29. jaanuari 2020. aasta teatises meetmepaketi kohta[121]. Nimetatud meetmed hõlmasid paljusid valdkondi, nagu ELi rahastus turvaliste 5G võrkude jaoks, investeeringud 5G ja sellele järgnevasse tehnoloogiasse, kaubanduse kaitsemeetmed ja konkurents, et vältida moonutusi 5G tarneturul jne.

Juhtivad osalised peaksid 2021. aasta alguses leppima vajadust mööda kokku allpool esitatud meetmete rakendamise üksikasjalikus korras ja vahe-eesmärkides.

Eesmärk 1: tagada riskide tõhusaks maadamiseks ühtne lähenemisviis liikmesriikide lõikes		
Valdkonnad	**Peamised lühiajalised ja keskpika perioodi meetmed**	**Juhtivad osalejad**
Meetmepaketi rakendamine liikmesriikides	Viia meetmepaketi järeldustes soovitatud meetmed täielikult ellu 2021. aasta teiseks kvartaliks, tehes võrgu- ja infoturbe koostöörühma tööjaotuskava raames korrapäraselt kokkuvõtteid.	Liikmesriikide ametiasutused

[120] Komisjoni aruanne 5G-võrkude küberturvalisust käsitleva komisjoni 26. märtsi 2019. aasta soovituse 2019/534 mõju kohta.

[121] 29. jaanuari 2020. aasta teatis „5G turvaline kasutuselevõtt ELis: ELi meetmepaketi rakendamine“ (COM(2020) 50).

Teabe ja parimate tavade vahetamine tarnijatega seotud strateegiliste meetmete kohta	Tõhustada teabevahetust ja kaaluda parimate tavade loendi koostamist eelkõige järgmistes punktides: - piirangud kõrge riskitasemega tarnijatele (SM03) ja meetmed, mis on seotud hallatud teenuste osutamisega (SM04); - tarneahela turvalisus ja vastupidavus, sealhulgas järelmeetmed BERECi uuringule SM05-SM06 kohta.	Liikmesriikide ametiasutused, komisjon
Suutlikkuse suurendamine ja tehnilisi meetmeid käsitlevad suunised	Teha tehnilist süvakontrolli ning töötada välja ühised suunised ja vahendid, sealhulgas: - 5G küberturvalisuse kontrolli ja parimate tavade põhjalik ja dünaamiline maatriks; suunised teatavate tehniliste meetmepaketis sisalduvate meetmete rakendamiseks.	ENISA, liikmesriikide ametiasutused
Eesmärk 2: toetada pidevat teadmiste vahetust ja suutlikkuse suurendamist		
Valdkonnad	**Peamised lühiajalised ja keskpika perioodi meetmed**	**Juhtivad osalejad**
Pidev teadmiste kogumine	Korraldada teadmiste kogumist tehnoloogia arengu ja sellega seotud probleemide (avatud arhitektuur, 5G funktsioonid – nt virtualiseerimine, konteineriseerimine, viilutamine jne), ohtude arengu, toimunud intsidentide jms kohta.	ENISA, liikmesriikide ametiasutused, muud sidusrühmad
Riskihindamine	Liikmesriikide riskihinnanguid käsitleva teabe ajakohastamine ja vahetamine	Liikmesriikide ametiasutused, komisjon, ENISA
ELi rahastatavad ühisprojektid meetmepaketi rakendamiseks	Anda rahalist toetust projektidele, millega toetatakse meetmepaketi rakendamist, sh ELi rahastamisvahendite kaudu ja eelkõige programmi „Digitaalne Euroopa“ raames (nt liikmesriikide ametiasutuste suutlikkuse suurendamine, katsestendid ja muud edasiarendatud katsetamisvahendid jne).	Liikmesriikide ametiasutused, komisjon
Koostöö sidusrühmade seas	Edendada koostööd 5G küberturvalisusega tegelevate riiklike ametiasutuste (nt võrgu- ja infoturbe koostöörühm, küberturvalisuse asutused, telekommunikatsioonivaldkonda reguleerivad asutused) ja erasektori sidusrühmadega.	Liikmesriikide ametiasutused, komisjon, ENISA
Eesmärk 3: tarneahela vastupidavuse ja muude ELi strateegiliste julgeolekueesmärkide edendamine		
Valdkonnad	**Peamised lühiajalised ja keskpika perioodi meetmed**	**Juhtivad osalejad**
Standardimine	Koostada ja rakendada võrgu- ja infoturbe standardimise allrühma töö järgmise etapina tegevuskava ELi esindatuse suurendamiseks standardiasutustes, et saavutada konkreetsed turvalisuseesmärgid, sealhulgas edendada koostalitlusvõimelisi liideseid, et hõlbustada tarnijate mitmekesistamist.	Liikmesriikide ametiasutused
Tarneahela vastupidavus	- Viia läbi 5G ökosüsteemi ja tarneahela põhjalik analüüs, et saada parem ülevaade selle peamistest lülidest ja võimalikest kriitilise tähtsusega sõltuvustest ning jälgida neid. - Tagada, et 5G turg ja tarneahel oleks kooskõlas ELi	Liikmesriikide ametiasutused, komisjon

	kaubandus- ja konkurentsieeskirjade ja eesmärkidega, nagu on märgitud komisjoni 29. jaanuari teatises, ning et 5G väärtusahelat mõjutada võivate investeeringute suhtes kohaldataks meetmepaketi eesmärke arvestades välismaiste otseinvesteeringute taustauuringut. - Jälgida praegusi ja oodatavaid turusuundumusi ning hinnata avatud raadio juurdepääsuvõrkudega seotud riske ja võimalusi, korraldades selleks sõltumatu uuringu.	
Sertifitseerimine	Alustada tööd peamiste 5G komponentide ja tarnijate protsesside sertifitseerimise ettevalmistava kavaga, et maandada tehnilise haavatavusega seotud riske, nagu on kehtestatud meetmepaketi riskimaanduskavades.	Komisjon, ENISA, riiklikud ametiasutused, muud sidusrühmad
ELi suutlikkus ja võrkude turvaline kasutuselevõtt	- Investeerida teadus- ja arendustegevusse ja suutlikkuse suurendamisse, viies eelkõige ellu arukate võrkude ja teenuste partnerluse. - Rakendada ELi rahastamisprogrammide ja -vahendite (sise- ja välisrahastamise vahendite) suhtes asjakohaseid turvalisustingimusi, nagu on teatatud komisjoni 29. jaanuari teatises.	Liikmesriigid, komisjon 5G valdkonna sidusrühmad
Välisaspektid	Vastata positiivselt kolmandate riikidele, kes sooviksid mõista või ise rakendada ELi väljatöötatud meetmepaketi aluseks olevat lähenemisviisi.	Liikmesriigid, komisjon Euroopa välisteenistus, ELi delegatsioonid