EUROOPA
KOMISJON

Brüssel, 5.7.2016
COM(2016) 410 final

KOMISJONI TEATIS EUROOPA PARLAMENDILE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE

Euroopa kübervastupidavusvõime süsteemi tugevdamine

ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine

1. SISSEJUHATUS/TAUST

Iga päev esineb Euroopa ettevõtjatele ja majandusele tervikuna suuri majanduskahjusid põhjustavaid küberjulgeoleku intsidente. Sellised intsidendid õõnestavad kodanike ja ettevõtjate usaldust digitaalse ühiskonna vastu. Kaubanduslike ärisaladuste, äriteabe ja isikuandmete varguse, teenuste (sh põhiteenuste) ja taristu häirimise tõttu kantud majanduskahjud ulatuvad igal aastal sadadesse miljarditesse eurodesse[1]. See võib evida mõju ka kodanike põhiõigustele ja ühiskonnale tervikuna.

Küberjulgeoleku väljakutsetele reageerimisel moodustavad Euroopa Liidu poliitikameetmete tuumiku 2013. aasta Euroopa Liidu küberjulgeoleku strateegia[2] (edaspidi „ELi küberjulgeoleku strateegia“) ja selle peamiseks väljundiks olev peagi vastuvõetav küberjulgeoleku direktiiv[3] ning infosüsteemide vastu suunatud ründeid käsitlev direktiiv 2013/40/EL. Lisaks on ELi käsutuses eriüksused nagu Euroopa Liidu Võrgu- ja Infoturbeamet (edaspidi „ENISA“), Europoli juurde kuuluv küberkuritegevuse vastase võitluse Euroopa keskus (edaspidi „EC3“) ning infoturbeintsidentidega tegelev rühm (edaspidi „CERT-EU“). Hiljuti algatati erinevates elutähtsates sektoris (nt energia ja transport) küberjulgeoleku parandamiseks mitmed valdkondlikud algatused.

Nimetatud positiivsetest saavutustest hoolimata on EL küberintsidentide suhtes endiselt haavatav. See võib ohustada digitaalset ühtset turgu ning ühiskonna majanduslikku ja sotsiaalset toimimist. Intsidentide mõju ei pruugi piirduda üksnes majandusega. Hübriidohtude[4] korral võidakse kasutada küberrünnakuid, et kooskõlastatult ühes muude tegevustega riiki destabiliseerida või poliitilisi institutsioone kõigutada.

Seda silmas pidades võib samal ajal mitut liikmesriiki puudutava laiaulatusliku küberintsidendiga toimetulek olla ELi jaoks keerukas. Komisjon otsib sünergias hübriidohtudega võitlemise ja Euroopa julgeoleku tegevuskava rakendamise teatistega[5] viise, kuidas küberjulgeolekuolukorra muutumisega toime tulla ning hinnata, kas ELil oleks tarvis lisameetmeid, et küberjulgeolekus vastupidavusvõimet ning intsidentidele reageerimist parandada.

Lisaks käsitleb komisjon küberjulgeoleku tööstussuutlikkust ELis. Kuigi Euroopas ei ole digitehnoloogia kogu väärtusahela jaoks vajalikku vilumust, on sellegipoolest vaja säilitada ja arendada teatavaid olulisi võimeid. Kübejulgeolekus võimalikult kõrget taset pakkuvate toodete ja teenuste tarne aitab avada Euroopa küberjulgeolekutööstuse potentsiaali ning võib kujuneda märkimisväärseks konkurentsieeliseks. Kõigi eelduste kohaselt on üleilmne küberjulgeolekuturg üks IKT sektori kiiremalt arenevaid segmente[6]. Kui EL soovib selles valdkonnas liidrite sekka tõusta, ei saa seda teha ilma, et tagatud oleks andmeturbe (sh isikuandmete kaitse) põhimõtete austamine ning intsidentidele reageerimise tulemuslikkus.

[1] *Puhaskahjumid: Küberkuritegevuse kogukulude hinnang – küberkuritegevuse majandusmõju II; Strateegiliste ja rahvusvaheliste uuringute keskus; juuni 2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.
[6] Vt SWD(2016) 216.

See oleks tugev argument ELi investeerimisel, aidates seega saavutada digitaalse ühtse turu kaugeleulatuvaid majanduskasvu ja töökohtade loomise eesmärke.

Eespool loetletu saavutamine eeldab kindlat tahet ja seda eeskätt allpool loetletud tegevuse elluviimisel.

i) Intensiivsem koostöö valmisoleku parandamiseks ja küberintsidentide lahendamiseks

Olemasolevaid ja kokkulepitud koostöömehhanisme tuleb tugevdada, et suurendada ELi vastupidavust ja valmisolekut, sh võimalikku üleeuroopalist kübejulgeolekukriisi silmas pidades. Need koostöömehhanismid peaksid olema terviklikud, hõlmates intsidendi elutsüklit alates ennetamisest kuni lõpuks süüdistuse esitamiseni. Liikmesriikide tulemuslik koostöö ja elutähtsate ettevõtjate turvanõuete tegelikkuses rakendamine eeldab, et küberjulgeolekutööstus suudab pakkuda töökindlaid tehnilisi lahendusi.

Samal ajal on kõikjal ELis vaja elutähtsa kübervara vastupidavuse tagamiseks pidevalt pingutada, et leida võimalusi sektoriüleseks sünergiaks ja kübernõuded asjakohasesse ELi poliitikasse üle võtta. Komisjon kaalub, kas 2013. aasta ELi küberjulgeoleku strateegiat on vaja lähitulevikus ajakohastada.

ii) Euroopa küberjulgeoleku ühtse turu väljakutsetega toimetulemine

Digitaalse ühtse turu strateegias[7] tunnistati, et kiirelt muutuva tehnoloogia valdkonnas ja võrguturvalisuse veebilahenduste suhtes on endiselt teatavaid puudujääke. Samal ajal nähtub turu-uuringutest, et ELi siseturg on küberjulgeoleku toodete ja teenuste pakkumisel endiselt geograafiliselt killustatud[8]. Käesolevas teatises loetletakse mitmeid turupõhiseid poliitikameetmeid, mille abil ühtse turu kõnealuste puudujääkide ja väljakutsetega toime tulla.

iii) Küberjulgeoleku valdkonnas tööstussuutlikkuse kasvatamine

Komisjon on ELi küberjulgeoleku strateegia ja digitaalse ühtse turu strateegiaga seadnud eesmärgiks edendada ELi küberjulgeolekutööstuse poolt suuremal arvul toodete ja teenuste pakkumist. Sellest tulenevalt võtab komisjon ka vastu küberjulgeoleku lepingulist avaliku ja erasektori partnerlust ettevalmistava otsuse, et Euroopas küberjulgeoleku vallas tipptasemel teadusuuringutele ja uuenduslikkusele kaasa aitamisega panustada konkurentsivõime suurendamisse.

2. KOOSTÖÖ, TEADMISTE JA SUUTLIKKUSE UUELE TASEMELE VIIMINE

ELi küberjulgeoleku strateegia ja eelkõige tulevane küberjulgeoleku direktiiv[9] aitavad luua keskkonda, mis soodustab kõikides liikmesriikides ELi tasandil koostöö tegemist. Direktiivi kiire ja tulemuslik rakendamine on otsustava tähtsusega, et majanduslikus ja ühiskondlikus elus digitehnoloogia kasutamist suurendada (arvestades sh pilveteenuseid, asjade internetti ja masinatevahelist andmevahetust), tagada järjest ulatuslikum piiriülene omavaheline

[7] COM(2015) 192.
[8] Vt SWD(2016) 216.
[9] Küberjulgeoleku direktiivis nõutakse liikmesriikidelt valdkondades nagu energia, transport, majandus ja tervis erinevate elutähtsate teenuste osutajate tuvastamist, küberjulgeoleku riskide hindamist ning ka tagamist, et teatavad digiteenuste osutajad rakendaksid selliste riskide maandamiseks sobivaid meetmeid.

ühendamine ja pidades silmas kiiresti muutuvaid küberohte[10]. Selles kontekstis peab EL valmistuma laiaulatusliku küberkriisi võimaluseks[11], sh näiteks olukorraks, et mitme liikmesriigi elutähtsate teabesüsteemide vastu korraldatakse rünnakud samal ajal[12].

ELi tasandi koostöö on seega möödapääsmatu, et lahendada nii piiratud ulatusega, kuid levipotentsiaaliga küberintsidente, kui ka võimalike laiaulatuslike küberrünnakuid mitmes liikmesriigis. ELil tuleb olemasolevatesse kriisiohjamise mehhanismidesse integreerida küberelemendid. Samuti tuleb tagada tulemusliku koostöö ja kiire teabevahetuse mehhanismid, millega nii sektorite kui ka liikmesriikide üleselt sellistele intsidentidele reageerida ja nende levimist ära hoida. Lisaks peavad need mehhanismid toimima sidusalt, aidates nii kaasa terrorismi, organiseeritud kuritegevuse ja küberkuritegevuse vastasele võitlusele. See parandaks ka ELi võimet üleilmsetele ohtudele ja intsidentidele reageerimist rahvusvaheliste partneritega kooskõlastada.

2.1. Küberjulgeoleku koostöömehhanismide täiel määral ärakasutamine ning liikumine ENISA 2.0 suunas

Küberjulgeoleku direktiivis nõutud riiklikus suutlikkuses on oluline roll küberohtudele ja -intsidentidele kiirelt reageerimise eest vastutavatel küberturbe intsidentide lahendamise üksustel (CSIRTid). Liikmesriigid moodustavad konkreetseid küberjulgeoleku intsidente ja riske käsitleva teabevahetuse vallas tulemusliku koostöö edendamiseks CSIRTide võrgu. Lisaks luuakse direktiiviga koostöörühm, et toetada ja hõlbustada liikmesriikide vahelist strateegilist koostööd ning suurendada nende vastastikust usaldust.

Arvestades küberohtude olemust ja mitmekesisust, julgustab komisjon liikmesriike küberjulgeoleku koostöömehhanisme täiel määral ära kasutama ning laiaulatuslikuks küberintsidendiks valmisolekuga seonduvat piiriülest koostööd parandama. Ulatusliku küberintsidendi puhul oleks sellises täiendavas koostöös abi sellest, kui küberintsidentide ökosüsteemi erinevate elementide piires kasutataks kriisiaegse koostöö kooskõlastatud lähenemisviisi. Sellise lähenemisviisi saab sätestada näidiskavas, mis peaks ühtlasi tagama sünergia ja sidususe olemasolevate kriisiohjamise mehhanismidega[13]. Seda tuleks seejärel regulaarselt katsetada nii küberkriiside kui ka muude kriiside ohjamise õppustel. See peaks sisaldama ELi tasandi asutuste nagu ENISA, CERT-EU ja Europoli juurde kuuluva EC3 tegevust ning CSIRTde võrgu arendatud vahendite kasutamist. 2017. aasta esimeses pooles esitab komisjon sellise koostöö näidiskava tutvumiseks koostöörühmale, CSIRTde võrgule ja muudele asjaomasele sidusrühmadele.

Praegu on küberjulgeolekuga seonduvad teadmised ja eksperdioskused küll ELi tasandil olemas, kuid mitte ühes kohas ja struktureerituna. Küberjulgeoleku koostöömehhanismide toetamiseks tuleks teave koondada ühte „infosõlme“, et see kõikidele liikmesriikidele nõudmise korral hõlpsalt kättesaadavaks teha. See „sõlm“ oleks keskne ressurss, mille kaudu ELi institutsioonid ja liikmesriigid saaksid vajaduse korral teavet vahetada. Lihtsam

[10] Vt SWD(2016) 216.
[11] Vt nt ENISA aruanne: ELi tasandi kriisiohjamise üldlevinud tavad ja nende kohaldatavus küberkriiside esinemisel (aprill 2016).
[12] Vt SWD(2016) 216.
[13] Eelkõige ELi integreeritud kord poliitiliseks reageerimiseks kriisidele, sh otsus solidaarsusklausli liidupoolse rakendamise korra kohta (24. juuli 2014) ning ühise julgeoleku- ja kaitsepoliitika otsustusprotsessid.

juurdepääs küberjulgeolekuriskide ja võimalike vastumeetmete alasele paremini struktureeritud teabele peaks aitama liikmesriikidel suutlikkust parandada ja tavasid ühtlustada, suurendades seega üldist vastupidavusvõimet rünnakute suhtes. Komisjon aitab koos ENISA, CERT-EU ja oma Teadusuuringute Ühiskeskuse eksperditeadmiste toel kaasa sõlme loomisele ja selle jätkusuutlikkuse tagamisele.

Lisaks tuleks ELi tasandil luua regulaarselt kohtuv küberjulgeoleku valdkonna kõrgetasemeline nõuanderühm[14], kuhu kuuluvad eksperdid ja otsusetegijad tööstus- ja teadusringkondadest ning kodanikuühiskonna ja muude asjaomaste organisatsioonide ridadest. See rühm võimaldaks komisjonil avatud ja läbipaistval viisil hankida küberjulgeoleku strateegia poliitika ning võimalike regulatiivsete ja muude poliitiliste meetmete kohta välisekspertide arvamust ja nõu. See täiendaks muid küberjulgeoleku struktuure ja ühenduks nendega[15] .

Lisaks peab komisjon 20. juuniks 2018 andma hinnangu ENISA tööle ning ENISA volituste võimalik muutmine või uuendamine tuleb vastu võtta 19. juuniks 2020[16]. Küberjulgeoleku praegust olukorda silmas pidades soovib komisjon hindamise kiiremini ette võtta ja olenevalt selle tulemusest esitada nii pea kui võimalik ka oma ettepaneku.

ENISA volituste muutmise võimaliku vajaduse hindamisel võtab komisjon arvesse eespool kirjeldatud väljakutseid küberjulgeoleku tagamisel ning üldiseid pingutusi intensiivsema koostöö ning teadmiste jagamise nimel. Ühtlasi annab see protsess võimaluse hinnata, kas oleks võimalik parandada ameti võimekust ja suutlikkust jätkusuutlikul viisil toetada liikmesriike küberjulgeoleku vastupidavusvõime saavutamisel. ENISA volituste kaalumisel tuleks lisaks arvestada ametile küberjulgeoleku direktiiviga pandud uusi ülesandeid, küberjulgeolekutööstust toetavaid uusi poliitikaeesmärke (digitaalse ühtse turu strateegia ja eriti lepinguline avaliku ja erasektori partnerlus), elutähtsate sektorite turvamise muutlikke vajadusi ja uusi väljakutseid piiriüleste intsidentide lahendamisel, sh küberkriisidele kooskõlastatult reageerimist.

Komisjon teeb järgmist:

- esitab 2017. aasta esimeses pooles kaalumiseks ELi tasandil laiaulatuslike küberintsidentidega toimetuleku koostöö näidiskava;
- hõlbustab „infosõlme“ loomist, et toetada ELi ametite ja liikmesriikide vahelist teabevahetust;
- loob küberjulgeoleku valdkonna kõrgetasemelise nõuanderühma ning
- viib 2017. aasta lõpuks lõpule ENISA hindamise. Sellises hindamises analüüsitakse, kas ENISA volitusi on vaja muuta või pikendada, ning kui on vaja, seatakse eesmärgiks esitada vastav ettepanek võimalikult ruttu.

[14] Komisjoni eksperdirühmade suhtes kohaldatakse horisontaalseid eeskirju, mis on kehtestatud komisjoni otsusega C(2016) 3301.
[15] Nt küberjulgeoleku platvorm, küberjulgeoleku lepinguline avaliku ja erasektori partnerlus ning valdkondlikud platvormid nagu energiaekspertide küberjulgeoleku platvorm (EECSP). See peaks ühenduma ka Euroopa tööstuse digitaliseerimise teatises väljakuulutatud kõrgetasemelise ümarlaua tööga: COM(2016) 180.
[16] Määrus (EL) nr 526/2013, millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004.

2.2. Suurem rõhk küberjulgeoleku valdkonnas haridusele, koolitusele ja õppustele

Küberjulgeoleku vastupidavusvõime saavutamiseks on ülimalt oluline tagada vajalikul tasemel oskused ja koolitus nii kübejulgeoleku intsidentide ärahoidmise kui ka selliste intsidentide lahendamise ja nende mõju leevendamise vallas.

Praegu on suutlikkuse suurendamise toetamisel (sh küberkriminalistikas) oluline roll ENISA-l, Euroopa küberkuritegevuse alase koolituse ja hariduse rühmal koostöös küberkuritegevuse vastase võitluse Euroopa keskusega (Europoli juures) ja Euroopa Politseikolledžil, kes kõik töötavad välja käsiraamatuid ning korraldavad koolitusi ja küberjulgeoleku õppuseid.

Samas on küberruum kiirelt arenev valdkond, kus on olulisel kohal kahese kasutuse võime. Seega on koolituste ja õppuste puhul vaja ELi vastupidavusvõime ja kiirreageerimisvõime suurendamiseks arendada tsiviil- ja sõjandusvaldkonna koostööd ja sünergiat.

Seda vajadust silmas pidades ning küberjulgeoleku direktiivi ja ELi küberkaitsepoliitika raamistiku[17] vastuvõtmise jätkuna teevad komisjoni talitused koostööd liikmesriikidega, Euroopa välisteenistusega, ENISAga ja muude asjaomaste ELi asutustega,[18] et luua küberjulgeoleku õppuste, haridus- ja koolitusplatvorm, mis edendaks tsiviil- ja kaitsevaldkonna koolituste sünergiat.

Komisjon teeb järgmist:

- teeb küberjulgeoleku koolitusplatvormi loomiseks tihedat koostööd liikmesriikidega, ENISA, EEASi ja muude asjakohaste ELi asutustega.

2.3. Sektoritevahelise seotuse ja olulise avaliku võrgutaristu vastupidavusvõime käsitlemine

Laiaulatusliku küberintsidendi riski ja mõju hindamisel on oluline tegur piiriülesuse ja sektorite omavahelise seotuse määr. Tõsine küberintsident ühes sektoris või ühes liikmesriigis võib muid liikmesriike või muid sektoreid otseselt või kaudselt mõjutada või muudesse liikmesriikidesse või sektoritesse levida.

Piiriülene ja sektoriülene koostöö hõlbustab teabe ja eksperditeadmiste vahetamist ning aitab seega kaasa valmisolekule ja vastupidavusvõimele. Komisjon on elutähtsate infrastruktuuride kaitse programmi[19] rakendamise kaudu mitmesugustes sektorites toetanud tööd, mille eesmärk on olnud vastastikuse sõltuvuse parem mõistmine.

Samal ajal on sektoriüleste riskidega toimetulemisel tingimata vaja, et iga sektor eraldivõetuna suudaks küberintsidente tuvastada, nendeks valmistuda ja neile reageerida. Komisjon hindab küberintsidentidest tulenevaid riske omavahel tihedalt seotud sektorites nii riigi piires kui ka piiriüleselt ning seda eelkõige küberjulgeoleku direktiiviga hõlmatud sektorites ja võttes arvesse ka rahvusvahelise tasandi arengusuundumusi[20]. Nimetatud

[17] Euroopa Liidu välisasjade nõukogu võttis vastu 18. novembril 2014, dokument 15585/14.
[18] Näiteks Euroopa Julgeoleku- ja Kaitsekolledž, EC3, Euroopa Politseikolledž ja Euroopa Kaitseagentuur.
[19] SWD(2013) 318.
[20] Nt Euroopa Lennundusohutusameti vastu võetud küberjulgeoleku tegevuskava, küberjulgeoleku tegevuskava, Rahvusvahelise Tsiviillennunduse Organisatsiooni ja Rahvusvahelise Mereorganisatsiooni töö.

hindamise järel kaalub komisjon, kas sellistes elutähtsates sektorites on küberriskideks valmisolekuks vaja veel erieeskirju ja/või erisuuniseid.

Euroopa tasandil saavad küberintsidentideks valmistumisel ja neile reageerimisel olulise rolli võtta valdkondlikud teabe jagamise ja analüüsimise keskused[21] (ISACid) ja vastavad CSIRTid. Muutlike ohtude kohta tulemusliku teabevoo tagamiseks ja küberintsidentidele reageerimise hõlbustamiseks tuleks ISACe julgustada koostööle CSIRTide võrguga küberjulgeoleku direktiivi raames ja küberkuritegevuse vastase võitluse Euroopa keskusega (Europoli juures), CERT-EUga, samuti asjaomaste õiguskaitseasutustega.

Sidusrühmade ja ametiasutuste vahelise teabevahetuse puhul peab osalistel olema küberriskide kogu elutsükli kestel kindlus, et sellele ei järgne vastutusele võtmist. Komisjon on täheldanud, et sarnased mured on üsna levinud ja pidurdavad ettevõtjate seas ohu kohta väärtusliku teabe jagamist nii oma kolleegidega kui ka sektoriüleselt või ametiasutustega ja eriti piiriüleselt. Komisjon soovib küberohte käsitleva teabevahetuse parandamise huvides selliseid probleeme uurida ja neid leevendada.

Seega on selleks, et julgustada ettevõtteid ärisaladuste kübervargustest teatama, ülimalt oluline, et olemas oleks konfidentsiaalsust tagavad usaldusväärsed aruandluskanalid. See võimaldaks seirata ja hinnata nii Euroopa tööstuse kantud kahju (mille tulemusel väheneb ka müük ja töökohtade arv) kui ka teadusasutuste kantud kahju. Ühtlasi aitaks see paremini kujundada vajalikke poliitikameetmeid. Komisjon loob ENISA, Euroopa Liidu Intellektuaalomandi Ameti (EUIPO), Europoli juurde kuuluva EC3 abiga ja erasektori sidusrühmadega läbi rääkides usaldusväärsed kanalid, mille kaudu vabatahtlikult teatada ärisaladuste kübervargusest. See peaks võimaldama ELi tasandil koguda anonüümseid koondandmeid. Neid andmeid saab jagada liikmesriikidega, et neid kasutada diplomaatilistes pingutustes ja teadlikkuse suurendamise meetmetes, mis aitaksid ELi immateriaalset vara küberrünnakute eest kaitsta.

Valdkondliku küberturvalisuse toetamiseks edendab komisjon ka küberturvalisuse elemendiga arvestamist küberturvalisuse jaoks olulise ELi valdkondliku poliitika väljatöötamisel.

Oluline roll on ka ametiasutustel, kes peavad probleemide väljaselgitamiseks kontrollima interneti põhitaristu terviklikkust, teavitama vastavate võrkude eest vastutavaid pooli ning vajaduse korral abistama teadaoleva haavatavuse kõrvaldamisel. Riigi reguleerivad asutused võiks avaliku võrgutaristu regulaarseks kontrollimiseks rakendada CSIRTide suutlikkust. Sellest lähtuvalt võiksid nad ettevõtjaid julgustada kõnealuse kontrollimise käigus tuvastatud võimalikke puudujääke või haavatavusi kõrvaldama.

Komisjon uurib seega, millised õiguslikud ja korralduslikud tingimused peavad olema täidetud, et riigi reguleerivatel asutustel oleks koostöös riigi küberjulgeoleku asutustega võimalik rakendada CSIRTe, et regulaarselt kontrollida avaliku võrgutaristu haavatavust. Riiklikke CSIRTe tuleks julgustada tegema CSIRTde võrgu raames koostööd seoses võrkude seire parimate tavadega, hõlbustades nii laiaulatuslike intsidentide ärahoidmist.

[21] Vt nt Euroopa Energia ISAC (http://www.ee-isac.eu).

Komisjon teeb järgmist:

- soodustab Euroopa valdkondlike teabe jagamise ja analüüsimise koostöökeskuste loomist, toetab nende koostööd CSIRTidega ja püüab kõrvaldada turuosaliste poolset teabe jagamist takistavad tõkked;
- uurib strateegilist/süsteemset riski, mida põhjustaksid küberintsidendid omavahel väga tihedalt seotud sektorites nii riigi piires kui ka piiriüleselt;
- hindab elutähtsates sektorites küberriskideks valmisoleku vajadust ning vajaduse korral kaalub lisaeeskirju ja/või -suuniseid;
- asutab koos ENISA, EUIPO ja EC3ga usaldusväärsed kanalid, mille kaudu vabatahtlikult teatada ärisaladuste kübervargusest;
- edendab küberturvalisuse meetmete integreerimist Euroopa valdkonnapoliitikasse ning
- uurib, millised tingimused peavad olema täidetud, et liikmesriikide ametiasutused saaksid olulise võrgutaristu haavatavuse regulaarseks kontrollimiseks rakendada CSIRTe.

3. EUROOPA KÜBERJULGEOLEKU ÜHTSE TURU VÄLJAKUTSETELE VASTAMINE

Euroopa vajab väga kvaliteetseid, taskukohaseid ja koostalitlusvõimelisi küberjulgeolekutooteid ja -lahendusi. Paraku on IKT-turbetoodete ja -teenuste tarne ühtsel turul endiselt geograafiliselt väga killustatud. Esiteks teeb see Euroopa ettevõtjate jaoks riiklikul, Euroopa ja üleilmsel tasandil konkureerimise keerukaks; teiseks tähendab see kodanike ja ettevõtjate jaoks võimaliku ja kasutatava küberjulgeolekutehnoloogia kättesaadavust väiksemas valikus [22].

Tõepoolest on küberjulgeolekutööstus Euroopas peamiselt arenenud riikliku, täpsemalt valitsuse (sh kaitsesektori) nõudluse najal. Suurem osa Euroopa kaitsetööstusettevõtjatest on loonud küberjulgeoleku osakonnad[23]. Sellega paralleelselt on esile kerkinud paljud uuenduslikud VKEd nii eri-/nišitoodete (nt krüpteerimissüsteemide) turgudel kui ka küll traditsioonilistel (nt viirusetõrje tarkvara) turgudel, kuid uute ärimudelitega.

Ent ettevõtjatel on kodusest siseturust suuremaks kasvamisel raskusi. See, et piiriüleselt pakutavate toodete puhul jääb vajaka usaldusest, tuli otsustava tegurina välja kõikides komisjoni korraldatud konsultatsioonides[24]. Seetõttu toimuvad hanked suuresti endiselt vastava liikmesriigi piires ning paljud ettevõtjad näevad ränka vaeva mastaabisäästu saavutamiseks, et seeläbi saada konkurentsivõimelisemaks nii siseturul kui ka üleilmselt.

Kübejulgeoleku ühtse turu kitsaskohtade hulka kuulub koostalitusvõimeliste lahenduste (tehniliste standardite), tavade (protsessistandardite) ja ELi üleste

[22] Vt SWD(2016) 216.
[23] Vt SWD(2016) 216.
[24] Vt SWD(2016) 215.

sertifitseerimismehhanismide puudumine. Selles kontekstis nimetati küberjulgeolekut digitaalsel ühtsel turul üheks IKT standardimise prioriteediks[25].

Küberjulgeolekuettevõtjate kasvuvõimaluste piiratus ühtsel turul tähendab mitteeurooplastest investorite algatatud arvukaid ühinemisi ja omandamisi[26]. Selline arengusuundumus näitab küll küberjulgeoleku vallas Euroopa ettevõtjate uuenduslikkust, kuid ka ohtu, et Euroopa kaotab oskusteavet ja eksperditeadmisi ning toimub nn „ajude äravool".

Praktilisemate ja taskukohasemate lahenduste kasutuselevõtmisele kaasa aitava kübejulgeolekutoodete ja -teenuste integreerituma ühtse turu soodustamiseks on vaja kiirelt tegutseda.

Euroopa tööstusettevõtjate ja institutsioonide vahelist usaldust takistavad tegurid on ületatavad, kui koostööd soodustatakse juba uuenduslikkuse varases elutsüklis: nii küberjulgeolekutööstuses, samuti tarnijate ja ostjate vahel; ja sektoriüleses mõõtmes seeläbi, et kaasatakse praegu või tõenäoliselt tulevikus kübejulgeolekulahendusi tarbivad tööstused.

Samal ajal on Euroopas järjest tähtsamaks muutumas kahese kasutusega toodete, teenuste ja tehnoloogia arendamine. Järjest suuremal arvul lahendusi jõuab kaitseturule tsiviilturult[27]. Komisjon kavatseb tulevases Euroopa kaitsealases tegevuskavas kindlaks määrata meetmed, millega Euroopa tasandil tsiviil- ja sõjandusvaldkonna sünergiat veelgi süvendada.

3.1. Sertifitseerimine ja märgistamine

Sertifitseerimine on toodete ja teenuste suhtes suurema usalduse ja turvalisuse loomisel oluline. See kehtib ka suurel määral digitehnoloogiat kasutavate ja väga heal tasemel turvalisust eeldavate uute süsteemide suhtes, nt internetiühendusega ja automatiseeritud autod, e-tervis, tööstuslikud automatiseeritud juhtimissüsteemid või arukad võrgud.

Järjest tullakse välja riiklike algatustega, mille eesmärk on kehtestada traditsioonilise taristu IKT-komponentidele väga kõrged küberjulgeolekunõuded, sh sertifitseerimisnõuded. Kuigi need on olulised, kaasneb nendega ka risk, et ühtne turg killustub ja tekivad probleemid koostalitusvõimega. IKT-toodete turvalisuse sertifitseerimiseks on tulemuslikud süsteemid kehtestatud vaid mõnes üksikus liikmesriigis[28]. Seega võib juhtuda, et IKT müüja on mitmes liikmesriigis müümiseks sunnitud läbima mitu sertifitseerimismenetlust. Kõige halvemal juhul ei saa ühe liikmesriigi küberjulgeolekunõudeid täitvana projekteeritud toodet teises liikmesriigis turule lasta.

Küberjulgeoleku toimiva ühtse turu saavutamiseks tuleks võimaliku IKT-toodete ja -teenuste sertifitseerimise raamistikuga eesmärgiks seada, et i) hõlmatud oleks mitmesugused erinevad IKT-süsteemid, -tooted ja -teenused; ii) kohaldamine oleks tagatud 28 liikmesriigis ning iii) esindatud oleksid küberjulgeoleku kõik tasandid; võttes samas arvesse rahvusvahelisel tasandil toimuvat arengut.

[25] COM(2016) 176/2.
[26] Vt SWD(2016) 216.
[27] 2013. aastal oli kahese kasutuse valdkonnas eksport juba ligikaudu 20 % ELi kogueksportdist (maksumuse järgi). See hõlmab ELi-sisest kaubandust.
[28] Vt SWD(2016) 216 – infosüsteemide lepingu kohane kõrgemate ametnike rühm (nõukogu 31. märtsi 1992. aasta otsus (92/242/EMÜ)) ja muud kehtivad süsteemid, nt Commercial Product Assurance Ühendkuningriigis ja Certification Sécuritaire de Premier Niveau Prantsusmaal.

Selleks otstarbeks asutab komisjon spetsiaalse töörühma, mis hakkab tegelema IKT-toodete ja -teenuste turvalisuse sertifitseerimisega ning koosneb liikmesriikide ja tööstussektori ekspertidest. Selle töörühma eesmärk on töötada koostöös ENISA ja Teadusuuringute Ühiskeskusega 2016. aasta lõpuks välja tegevuskava, milles analüüsitakse 2017. aasta lõpuks sellise Euroopa IKT turvalisuse sertifitseerimise raamistiku ettepaneku koostamise võimalikkust. Selles kontekstis vaatab komisjon ka määrust (EÜ) nr 2008/765 ja isikuandmete üldmääruses 2016/679[29] sätestatud sertifitseerimisnõudeid.

Protsess hõlmab laiapinnalist konsulteerimist ja mõjuhinnangut. See võimaldab komisjonil uurida mitmesuguseid IKT-toodete ja -teenuste sertifitseerimise raamistiku loomise variante. Komisjon uurib ka IKT turvalisuse sertifitseerimist taristusektorites (nt lennundus, raudtee, sõidukid) ja kasutusvalmi tehnoloogia korral (nt tööstuslike automatiseeritud juhtimissüsteemide küberjulgeolek[30], asjade internet, pilveteenused) kasutatavaid spetsiaalseid sertifitseerimis- ja valideerimismehhanisme. Samuti käsitletakse eespool nimetatud Euroopa IKT turvalisuse sertifitseerimise raamistiku kaudu tuvastatud puudujääke.

Sertifitseerimistöös toetutakse niivõrd kui võimalik rahvusvaheliselt tunnustatud standarditele ja arendus toimub koostöös rahvusvaheliste partneritega.

Komisjon uurib ka võimalikke variante, kuidas IKT turvalisuse sertifitseerimist, sh ohutuse aspekte, oleks kõige parem tulevikus valdkondlikesse õigusaktidesse integreerida.

Lisaks võimalikele regulatiivsetele variantidele uurib komisjon IKT-toodete turvalisuse märgistamiseks ka Euroopa oma kaubandusliku, vabatahtliku ja vähenõudliku süsteemi loomist. Sertifitseerimist täiendavana on selle eesmärk parandada kaubanduslike toodete küberjulgeoleku arusaadavust, et suurendada nende konkurentsivõimet ühtsel turul ja üleilmselt. Vajalikul määral kaalutakse ka käimasolevaid valdkondlikke ja horisontaalseid tööstusharude algatusi nii tarne kui ka nõudluse poolelt.

Haldusasutused osalevad aktiivselt, et riigihangetes oleks võimalik kasutada ühiseid tehnilisi kirjeldusi ja osutada sertifitseerimisele. Samuti jälgib komisjon riigihangete tasandil ja eriti valdkondlike süsteemide puhul (energia, transport, tervis, avalik haldus jne) asjakohaste sertifitseerimisnõuete kasutamist ning esitab selle kohta aruande.

Komisjon teeb järgmist:

- töötab 2016. aasta lõpuks välja tegevuskava, mille alusel liikuda 2017. aasta lõpuks esitatava Euroopa IKT turvalisuse sertifitseerimise võimaliku raamistiku suunas, et hinnata Euroopa küberjulgeoleku märgistamise vähenõudliku raamistiku teostatavust ja mõju;
- uurib praeguste valdkondlike sertifitseerimis-/valideerimismehhanismide puhul IKT turvalisuse sertifitseerimise vajadust ning pakub puudujääkide korral välja

[29] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruses (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta on sätestatud nii toimimisjuhendid, millega aidata kaasa nõuetekohasele andmekaitse-eeskirjade kohaldamisele, kui ka sertifitseerimismehhanismid, mis hõlmavad kõiki andmekaitsepõhimõtteid, sh eriti andmeturvet isikuandmete töötlemisel.

[30] Vt ERNCIPi temaatilise „Tööstuslike juhtimissüsteemide küberjulgeoleku“ rühma kohta https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

lahendusi;
- juhul kui see on asjakohane, käsitleb IKT-toodete turvalisuse sertifitseerimist tulevaste valdkondlike õigusaktide ettepanekutes;
- stimuleerib haldusasutuste osalemist, et hõlbustada riigihangetes sertifitseerimise ja ühiste tehniliste kirjelduste kasutamist, ning
- jälgib asjakohaste sertifitseerimisnõuete kasutamist riigi- ja erasektori hangetes ning esitab kolme aasta pärast turu olukorra aruande.

3.2. Euroopas küberjulgeoleku investeeringute laiendamine ja VKEde toetamine

Kuigi Euroopas ei tule küberjulgeoleku sektoris uuenduslikkusest puudu, jätab ELi kultuur küberjulgeolekusse investeerimisel endiselt soovida. Valdkonnas on palju uuenduslikke VKEsid, kuid nad ei ole tihti suutelised oma tegevust laiendama. Muu hulgas seetõttu, et arengu varastes etappides ei ole võimalik hõlpsalt ligi pääseda arengut toetavale rahastamisele. Samuti on Euroopas ettevõtjate juurdepääs riskikapitalile piiratud ning turunduse kaudu nähtavuse parandamiseks või erinevate standardimiseeskirjade ja vastavusnõuetega töötamiseks saadaolev võimalik eelarve ei ole piisav.

Samas on erinevate küberjulgeoleku valdkonnas tegutsejate vaheline koostöö lünklik ning on vaja veel pingutada, et suurendada majanduslikku koondumist ja arendada uusi väärtusahelaid[31].

Euroopas küberjulgeoleku investeeringute laiendamiseks ja VKEde toetamiseks on vaja hõlbustada rahastamisele juurdepääsu. Samuti tuleb digitaalarengut soodustavate piirkondlike ökosüsteemide kaudu toetada üleilmselt konkurentsivõimeliste küberjulgeoleku klastrite ja tippkeskuste arendamist. See tugi tuleb seostada aruka spetsialiseerumise strateegiate ja muude ELi instrumentide rakendamisega, et Euroopa küberjulgeolekutööstus neid paremini ära kasutaks.

Komisjoni põhimõtteline eesmärk on, et küberjulgeolekukogukond võimalikult hästi teadvustaks, millised on rahastamisvõimalused Euroopa, riiklikul ja piirkondlikul tasandil (nii seoses horisontaalsete instrumentide kui ka konkreetsete konkursikutsetega[32]), kasutades selleks olemasolevaid instrumente ja kanaleid, nt Euroopa ettevõtlusvõrgustikku.

Komisjon panustab lisaks seeläbi, et uurib koos Euroopa Investeerimispanga ja Euroopa Investeerimisfondiga rahastamisele juurdepääsu lihtsustamise võimalusi. See võib toimuda omakapitali- või kvaasiomakapitali investeeringute, laenude, projektidele antavate laenutagatiste või vahendajatele vastutagatiste andmisega, nt Euroopa Strateegiliste Investeeringute Fondi[33] raames küberjulgeoleku investeeringute platvormi loomise kaudu.

[31] Vt SWD(2016) 216.

[32] Vt nt Euroopa ühendamise rahastu programmi alla kuuluvad mitut sektorit hõlmavad 2016. aasta konkursikutsed, klastrite rahvusvahelistumise programmiga seotud COSMO 2016. aasta konkursikutsed.

[33] Euroopa Strateegiliste Investeeringute Fondi raames võib individuaalsete projektide jaoks investeerimisplatvormide kaudu toetust saada otseselt või kaudselt. Selliste platvormide abil saab finantseerida väiksemaid projekte ja koondada eri allikatest pärinevaid vahendeid, et oleks võimalik teha mitmekesiseid investeeringuid, keskendudes mõnele geograafilisele alale või teemavaldkonnale.

Lisaks kaaluks komisjon võimalust töötada koos huvitatud liikmesriikide ja piirkondadega välja küberjulgeoleku aruka spetsialiseerumise platvorm[34]. See aitaks küberjulgeoleku strateegiaid kooskõlastada ja planeerida ning huvitatud poolte strateegilist koostööd piirkondlikes ökosüsteemides käima lükata. See lähenemisviis peaks ka aitama küberjulgeolekusektoril pääseda olemasolevate Euroopa struktuuri- ja investeerimisfondide pakutavate võimalusteni.

Üldisemalt edendab komisjon projekteeritud turvalisuse lähenemisviisi. Eesmärk on tagada, et küberjulgeolekunõudeid arvestataks jooksvalt kõikides digitaalset komponenti sisaldavates ELi fondidest kaasrahastavates suurtes taristuinvesteeringutes. Selleks võetakse riigihanke- ja programmieeskirjades järk-järgult kasutusele asjakohased nõuded.

Komisjon teeb järgmist:

- kasutab olemasolevaid VKEde toetamise vahendeid, et kübejulgeolekukogukonnas suurendada teadlikkust olemasolevatest rahastamismehhanismidest;
- rakendab ulatuslikumalt ELi vahendeid ja instrumente, millega toetada uuenduslikke VKEsid tsiviilvaldkonna ja kaitsevaldkonna sünergia otsimisel[35];
- uurib koos Euroopa Investeerimispanga ja Euroopa Investeerimisfondiga, rahastamisele juurdepääsu lihtsustamise (nt spetsiaalse küberjulgeoleku investeeringute platvormi või muude vahendite kaudu) teostatavust;
- arendab küberjulgeolekusektorisse investeerimisest huvitatud liikmesriikide ja piirkondade jaoks küberjulgeoleku aruka spetsialiseerumise platvormi (RIS3) ning
- edendab digitaalset komponenti sisaldavates ELi fondidest kaasrahastavates suurtes taristuinvesteeringutes projekteeritud turvalisuse lähenemisviisi kasutamist.

4. UUENDUSLIKKUS KUI EUROOPA KÜBERJULGEOLEKUTÖÖSTUSE STIMULEERIMISE JA ARENDAMISE VAHEND – KÜBERJULGEOLEKU AVALIKU JA ERASEKTORI LEPINGULISE PARTNERLUSE LOOMINE

Euroopa küberjulgeolekutööstuse konkurentsivõime ja uuenduslikkuse stimuleerimiseks allkirjastatakse küberjulgeoleku avaliku ja erasektori lepinguline partnerlus. Avaliku ja erasektori lepingulise partnerlusega koondatakse teadusuuringutes ja uuenduslikkuses parimate tulemuste saamiseks tööstus- ja avaliku sektori ressursid.

Avaliku ja erasektori lepingulise partnerluse eesmärk on suurendada liikmesriikide ja tööstussektori vahelist usaldust seeläbi, et koostööd soodustatakse juba teadusuuringute ja uuendusprotsessi varastes etappides. Selle eesmärk on ka aidata kooskõlla viia nõudlus- ja tarnesektorit. See peaks andma tööstusele võimaluse välja selgitada, mis on küberjulgeolekulahenduste jaoks oluliste kasutajate ja sektorite (nt energia, tervis, transport,

[34] Vt aruka spetsialiseerumise instrumendid (RIS3): http://s3platform.jrc.ec.europa.eu/.
[35] Näiteks Euroopa ettevõtlusvõrgustik ja kaitsevaldkonnaga seotud piirkondade Euroopa võrgustik pakuvad piirkondadele kahese kasutuse valdkonnas piiriülese koostöö võimaluste otsimisel uusi võimalusi, sh küberjulgeoleku vallas, ja võimaldavad VKEdel kontakte luua.

rahandus) tulevikuvajadused. See hõlbustab nende kaasamist vastavates sektorites ühiste digitaalse turvalisuse, privaatsus- ja andmekaitsenõuete kindlaks määramise protsessi.

Küberjulgeoleku avaliku ja erasektori lepinguline partnerlus aitab ka saadaolevate vahendite kasutamist maksimeerida. See saavutatakse esiteks liikmeriikidega rohkem kooskõlastades. Teiseks saab paremini keskenduda paarile tehnilisele prioriteedile, et aidata küberjulgeolekutööstusel saavutada tehnoloogilisi läbimurdeid ja vilumus tuleviku tähtsaimas küberjulgeolekutehnoloogias. Selles kontekstis saab lähtekoodtarkvara ja avatud standardite arendamine soodustada usaldust, läbipaistvust ja murrangulist uuenduslikkust ning peaks seega kuuluma kõnealuse avaliku ja erasektori lepingulise partnerluse huvides tehtavate investeeringute ringi.

Küberjulgeoleku avaliku ja erasektori lepingulise partnerluse raames tehtavat tööd võimendab ka sünergia muude Euroopa projektidega, eelkõige sellistega, mis käsitlevad turvalisuse elemente. Need hõlmavad algatusi nagu „Tuleviku tehased“, energiatõhusad ehitised, 5G ja suurandmete valdkonna avaliku ja erasektori partnerlus[36] ja muud valdkondlikud avaliku ja erasektori partnerlused[37], samuti asjade internet[38]. Lisaks edendatakse kooskõlastamist Euroopa avatud teaduspilve ja Euroopa kvant-kübertehnoloogia superarvutirakenduste algatusega (nt kvantmehaanilise kodeerimise/dekodeerimise uuenduslikkus, kvantandmetöötluse teadustöö).

Küberjulgeoleku avaliku ja erasektori lepinguline partnerlus algatatakse programmi „Horisont 2020“[39] (ELi teadusuuringute ja innovatsiooni raamprogramm aastateks 2014–2020) raames. Selle rahastamisel tuleneb finantsvõimendus programmi kahest järgmisest sambast: „Juhtpositsioon progressi võimaldava ja tööstusliku tehnoloogia vallas“ (LEIT-ICT) ja „Ühiskondlikud väljakutsed – turvaline ühiskond“ (SC7). Avaliku ja erasektori lepingulise partnerluse kogueelarve on 450 miljonit eurot ja tööstusepoolne finantsvõimendustegur on kolm. Küberjulgeoleku käsitlemisel ja kooskõlastamisel tuleks arvestada ka programmi „Horisont 2020“ muid asjakohaseid komponente (nt energia, transport, tervise väljakutse ühiskonnas ning programmi „Horisont 2020“ tipptaseme komponent). See aitab kaasa küberjulgeoleku avaliku ja erasektori lepingulise partnerluse eesmärkide saavutamisele. Selline kooskõlastamine peaks toimuma juba valdkondlike strateegiate kavandamise alguses.

Avaliku ja erasektori lepinguline partnerlus rakendatakse läbipaistval viisil ja küberjulgeolekukeskkonna kiirele muutumisele kohandatud avatud ja paindliku juhtimisega. Selles arvestatakse, et liikmesriikidel on vaja arutada, kuidas tehnoloogia muutused mõjutavad riikliku ja piiriülese taristu turvalist tööd. Sama oluline on partnerluse eesmärkide saavutatavuse tagamiseks, et partnerlus oleks tulemuslik mitme aasta jooksul.

Avaliku ja erasektori lepingulist partnerlust toetab Euroopa küberjulgeoleku organisatsioon (ECSO), mille liikmelisus peegeldab Euroopa küberjulgeolekuturu mitmekesisust. Sinna kuuluvad ka riiklikud, piirkondlikud ja kohalikud haldusasutused, teaduskeskused, teadusringkonnad ja teised huvitatud isikud.

[36] 5G taristu avaliku ja erasektori partnerlus ning suurandmete väärtuse avaliku ja erasektori partnerlus.
[37] Näiteks SESARi või raudteetranspordile ülemineku avaliku ja erasektori partnerlus.
[38] Asjade interneti innovatsiooni liit (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

Komisjon teeb järgmist:

- allkirjastab tööstusega küberjulgeoleku avaliku ja erasektori lepingulise partnerluse arvestusega, et partnerlus hakkaks toimima alates 2016. aasta kolmandast kvartalist;
- algatab 2017. aasta esimeses pooles programmi „Horisont 2020“ raames küberjulgeoleku avaliku ja erasektori lepingulise partnerlusega seonduvad konkursikutsed ning
- tagab küberjulgeoleku avaliku ja erasektori lepingulise partnerluse kooskõlastamise asjakohaste valdkondlike strateegiate, programmi „Horisont 2020“ instrumentide ning valdkondlike avaliku ja erasektori lepinguliste partnerlustega.

5. JÄRELDUS

Käesolev teatis tutvustab meetmeid, millega tugevdada Euroopa kübervastupidavusvõime süsteemi ning soodustada Euroopas konkurentsivõimelist ja uuenduslikku küberjulgeolekutööstust, nagu on kuulutatud ELi küberjulgeoleku strateegias ja digitaalse ühtse turu strateegias. Komisjon kutsub Euroopa Parlamendi ja nõukogu üles käesolevat lähenemist toetama.