

Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogია küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“)

[COM(2017) 477 final/2 2017/0225 (COD)]

(2018/C 227/13)

Raportöör: **Alberto MAZZOLA**

Kaasraportöör: **Antonio LONGO**

Konsulteerimistaotlus	Euroopa Parlament, 23.10.2017
	Euroopa Liidu Nõukogu, 25.10.2017
Õiguslik alus	Euroopa Liidu toimimise lepingu artikkel 114
Vastutav sektsioon	transpordi, energeetika, infrastruktuuri ja infoühiskonna sektsioon
Vastuvõtmine sektsioonis	5.2.2018
Vastuvõtmine täiskogus	14.2.2018
Täiskogu istungjärk nr	532
Hääletuse tulemus	206/1/2
(poolt/vastu/erapooletuid)	

1. Järeldused ja soovitused

1.1. Euroopa Majandus- ja Sotsiaalkomitee leiab, et Euroopa Komisjoni ettepaneku kohaselt Euroopa Liidu Võrgu- ja Infoturbeametile (ENISA) antav alaline mandaat aitab olulisel määral kaasa Euroopa süsteemide vastupanuvõime suurendamisele. Siiski ei piisa ettepanekuga esitatud esialgsest eelarvest ja ENISA-le eraldatud vahenditest selleks, et amet saaks oma volitusi täita.

1.2. Komitee soovib kõigil liikmesriikidel luua ENISA-le selgelt vastava samaväärse asutuse, sest enamik neist ei ole seda veel teinud.

1.3. Samuti leiab komitee, et suutlikkuse arendamise seisukohalt peaks ENISA seadma prioriteediks e-valitsust toetavad meetmed ⁽¹⁾. ELi-ülene/ülevaailmne digitaalne identiteet isikutele, organisatsioonidele ja seadmetele on määrava tähtsusega ning identiteedivarguse ja internetipettuste ennetamine ja nende vastu võitlemine peaks olema esmatähtis.

1.4. Komitee soovib, et ENISA peaks esitama korrapäraseid aruandeid liikmesriikide kübervalmisoleku kohta, keskendudes eelkõige võrgu- ja infoturbe direktiivi II lisas määratletud sektoritele. Iga-aastane Euroopa küberõppus peaks hindama liikmesriikide valmisolekut ja Euroopa küberkriisidele reageerimise mehhanismi tõhusust, samuti peaksid sellele järgnema soovitused.

1.5. Komitee pooldab ettepanekut luua küberturvalisuse pädevusvõrgustik. Võrgustikku toetaks küberturvalisuse uurimis- ja pädevuskeskus. See võrgustik võiks toetada Euroopa digitaalset suveräänsust, luues keske tähtsusega tehnoloogilise võimekuse väljaarendamiseks konkurentsivõimelise Euroopa tööstusbaasi, mis tugineks lepingulise avaliku ja erasektori partnerluse raames tehtud tööle, millest peaks kujunema kolmepoolne ühisettevõte.

1.6. Inimtegur on üks olulisematest küberõnnetuste põhjustest. Komitee hinnangul on vajalik luua tugev küberoskuste baas ja parandada teadlikkuse suurendamise kampaaniate abil küberhügieeni ka üksikisikute ja ettevõtjate seas. Komitee toetab ELi sertifitseeritud õppekava loomist keskkoolidele ja töötavatele spetsialistidele.

⁽¹⁾ Digitaalse ühtse turu vahekokkuvõte.

1.7. Komitee usub, et Euroopa digitaalne ühtne turg vajab ka küberturvalisuse eeskirjade ühest tõlgendamist, sealhulgas liikmesriikide vastastikust tunnustamist, ning et sertifitseerimise raamistik ja eri sektorite sertifitseerimiskavad võivad tagada ühtse lähtealuse. Eri sektoritele tuleb aga nende toimimisviiside tõttu pakkuda erinevaid lähenemisviise. Seepärast leiab komitee, et antud protsessi peaksid olema kaasatud valdkondlikud ELi ametid (Euroopa Lennundusohutusamet, Euroopa Liidu Raudteeamet, Euroopa Ravimiamet jne) ning et mõnel juhul tuleks – ENISA nõusolekul sidususe tagamiseks – delegeerida küberturvalisuse kavade koostamine neile. Euroopa IT-turbe miinimumnõuded tuleks vastu võtta koostöös Euroopa Standardikomitee/Euroopa Elektrotehnika Standardikomitee/Euroopa Telekommunikatsioonistandardite Instituudiga.

1.8. Kavandatav Euroopa küberturvalisuse sertifitseerimise rühm, mida toetab ENISA, peaks koosnema riiklikest sertifitseerimise järelevalveasutustest, erasektori sidusrühmadest, sealhulgas eri rakendusvaldkondades tegutsevatest operaatoritest, ning teadusringkondade ja kodanikuühiskonna esindajatest.

1.9. Komitee on arvamusel, et amet peaks Euroopa Komisjoni nimel jälgima riiklike sertifitseerimise järelevalveasutuste tegevust ja otsuste langetamist, viies läbi auditeid ja kontrole, ning et määruses tuleks sätestada vastutus ja sanktsioonid standarditele mittevastavuse korral.

1.10. Komitee leiab, et sertifitseerimistegevusest ei saa välja jätta korralikku märgistamissüsteemi, mida tuleb rakendada ka imporditud toodete suhtes, et suurendada tarbijate usaldust.

1.11. Euroopa peaks suurendama investeeringuid, koondades erinevaid ELi ja riiklike vahendeid ning erasektori investeeringuid, et aidata saavutada strateegilised eesmärgid tugevas avaliku ja erasektori koostöös, muu hulgas ELi fondi loomisega küberturvalisuse valdkonna innovatsiooniks ning teadus- ja arendustegevuseks teadusuuringute praeguse ja tulevase raamprogrammi raames. Lisaks peaks Euroopa Liit looma fondi küberturbe elluviimiseks, avades uue akna praeguses ja tulevas Euroopa ühendamise rahastus ning Euroopa Strateegiliste Investeeringute Fondis 3.0.

1.12. Komitee leiab, et tavalise, n-ö inimeste interneti seadmete puhul on vajalik minimaalne turbeaste. Nende seadmete korral on sertifitseerimine peamine meetod kõrgema turvalisuse taseme pakkumiseks. Asjade interneti turvalisus peaks olema esmatähtis.

2. Küberturvalisuse sertifitseerimise raamistik

2.1. Küberturvalisus on äärmiselt oluline nii heaolu kui ka riikliku julgeoleku seisukohast, samuti meie demokraatia toimumise, vabaduste ja väärtuste kaitseks. ÜRO ülemaailmse küberturvalisuse indeksi kohaselt on küberturvalisus „ökosüsteem, kus seadused, organisatsioonid, oskused, koostöö ja tehniline rakendamine peavad parimaks toimimiseks olema omavahel kooskõlas“ ning küberturvalisus on „riikide otsuselangetajate kaalutlustes muutumas üha olulisemaks“.

2.2. Vajadus turvalise ökosüsteemi järele on internetirevolutsiooni tõttu muutumas hädavajalikuks. See revolutsioon ei ole mitte ainult määratlenud uuesti ettevõtjalt tarbijale suunatud tööstusharusid, nagu meedia, jaekaubandus ja finantsteenused, vaid see kujundab ümber ka tootmist, energeetikat, põllumajandust, transporti ja teisi majanduse tööstusharusid, mis ühtekokku moodustavad ligi kaks kolmandikku maailma sisemajanduse koguproduktist, samuti kommunaalteenuste infrastruktuuri ja inimeste suhteid avaliku sektori haldusasutustega.

2.3. Digitaalse ühtse turu strateegia põhineb paremal ligipääsul kaupadele, teenustele ja infosivale, luues asjakohase õigusraamistiku digitaalvõrkude ja teenuste jaoks ning saades kasu andmetepõhisest majandusest. Hinnangute kohaselt võib antud strateegia tuua ELi majandusse 415 miljardit eurot aastas. Küberturvalisuse alaste oskustega spetsialistide puudus erasektoris on Euroopas 2022. aastaks ennustuste kohaselt 350 000 inimest⁽²⁾.

⁽²⁾ ELT JOIN(2017) 450 final.

2.4. 2014. aasta uuringu kohaselt oli küberkuritegevuse majanduslik mõju Euroopa Liidule 2013. aastal hinnanguliselt 0,41 % ELi SKPst (st umbes 55 miljardit eurot) ⁽³⁾.

2.5. Vastavalt Eurobaromeetri eriuuringule nr 464a eurooplaste suhtumise kohta küberturvalisusesse on 73 % internetikasutajatest mures, et veebilehed ei pruugi hoida nende isikuandmeid internetis turvaliselt, ning 65 % kardab, et avaliku sektori asutused ei pruugi hoida nende andmeid turvaliselt. Enamik vastanutest muretsseb erinevate küberkuritegevuse vormide ohvriks langemise pärast, eriti kardetakse pahavara oma seadmetes (69 %), identiteedivargust (69 %) ning pangakaardi- ja internetipangandusega seotud pettusi (66 %) ⁽⁴⁾.

2.6. Siiani ei ole ükski õigusraamistik jõudnud pidada sammu digitaalse innovatsiooniga ning mitmed õigusaktid aitavad ükshaaval kaasa asjakohase raamistiku loomisele: telekommunikatsiooniseadustiku läbivaatamine, isikuandmete kaitse üldmäärus, võrgu ja infosüsteemide turvalisuse direktiiv (võrgu- ja infoturbe direktiiv ehk küberturvalisuse direktiiv), määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (eIDASe määrus), ELi ja USA andmekaitseraamistik Privacy Shield, mittesularahaliste maksevahenditega seotud pettusi käsitlev direktiiv jne.

2.7. Lisaks ENISA-le ehk ELi küberturvalisuse ametile tegelevad küberturvalisuse küsimustega ka paljud teised organisatsioonid: Europol, CERT-EU (ELi institutsioonide ja ametite infoturbeentsidentidega tegelev rühm), ELi luure- ja situatsioonikeskus (EU INTCEN), vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimise Euroopa amet (eu-LISA), teabe jagamise ja analüüsimise keskused (ISACid), Euroopa küberjulgeoleku organisatsioon (ECISO), Euroopa Kaitseagentuur (EDA), NATO Küberkaitsekoostöö Keskus, ÜRO valitsusekspertide rühm (ÜRO info- ja kommunikatsioonitehnoloogia valdkonna rahvusvahelise julgeoleku raames toimuvate arengute valitsusekspertide rühm).

2.8. Sisseprojekteeritud turve on kvaliteetsete kaupade ja teenuste pakkumisel määrava tähtsusega: nutiseadmed ei ole nutikad, kui need ei ole kaitstud, sama kehtib ka arukate autode, linnade ja haiglate kohta – nende kõigi puhul on vajalik sisseehitatud turve seadmete, süsteemide, võrguarhitektuuri ja teenuste jaoks.

2.9. 19.–20. oktoobril 2017. aastal palus Euroopa Ülemkogu võtta vastu ühise lähenemise küberturvalisusele ELis tulenevalt esitatud reformipaketist ning taotles „ühist lähenemist küberturvalisusele: digimaailm vajab usaldust ja usaldust on võimalik saavutada ainult siis, kui tagame ennetavama sisseprojekteeritud turbe kõigis digitaalpoliitika valdkondades ning toodete ja teenuste piisava turvasertifitseerimise ning suurendame oma võimekust ennetada, takistada ja tuvastada küberrünnakuid ning neile reageerida“ ⁽⁵⁾.

2.10. Euroopa Parlament rõhutab oma 17. mai 2017. aasta resolutsioonis „vajadust otspunktturbe järele kogu finantsteenuste väärtusahelas; osutab suurtele ja mitmekesistele riskidele, mida kujutavad endast küberrünnakud, mille sihtmärgiks on meie finantsturgude taristu, asjade internet, valuutad ja andmed; [...] palub Euroopa järelevalveasutustel korrapäraselt läbi vaadata finantseerimisasutuste IKT-riskidega seotud olemasolevad tegevusstandardid; nõuab lisaks Euroopa järelevalveasutuste suuniseid nende riskide järelevalve kohta; rõhutab Euroopa järelevalveasutuste tehnilise oskusteabe tähtsust nende ülesannete täitmisel“ ⁽⁶⁾.

2.11. Komiteel on mitmel varasemal juhul olnud võimalus selle küsimusega tegeleda, ⁽⁷⁾ sh Tallinna tippkohtumisel toimunud konverentsil „E-valitsuse edasine areng“, ⁽⁸⁾ ning komitee on loonud alalise uurimisrühma „Digitaalarengu tegevuskava“.

⁽³⁾ Komisjoni talituste töödokument – mõjuhindang, mis on lisatud ettepanekule võtta vastu Euroopa Parlamendi ja nõukogu määrus, osa 1/6, lk 21, Brüssel, 13. september 2017.

⁽⁴⁾ Eurobaromeetri eriuuring nr 464a – küsitlus EB87.4 – „Eurooplaste suhtumine küberturvalisusesse“, september 2017.

⁽⁵⁾ Euroopa Ülemkogu järeldused, 19. oktoober 2017.

⁽⁶⁾ Euroopa Parlamendi resolutsioon, 17.5.2017 – A8-0176/2017.

⁽⁷⁾ Digitaalse ühtse turu vahekokkuvõte, ELT C 75, 10.3.2017, lk 124, ELT C 246, 28.7.2017, lk 8, ELT C 345, 13.10.2017, lk 52, ELT C 288, 31.8.2017, lk 62, ELT C 271, 19.9.2013, lk 133.

⁽⁸⁾ Euroopa Majandus- ja Sotsiaalkomitee pressidetade nr 31/2017: <https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incomingestonian-presidency>.

3. Komisjoni ettepanekud

3.1. Küberturvalisuse pakett sisaldab ühisteatist, kus vaadatakse läbi eelmine Euroopa küberturvalisuse strateegia (2013), ning küberturvalisust käsitlevat õigusakti, mis keskendub ENISA uuele mandaadile ja kavandatud küberturvalisuse raamistikule.

3.2. Strateegia on jagatud kolme peamisse ossa: vastupidavusvõime, heidutus ja rahvusvaheline koostöö. Heidutuse osas keskendutakse peamiselt küberkuritegevuse küsimustele, sealhulgas Budapesti konventsioonile, ning rahvusvahelise koostöö osas vaadeldakse küberkaitset, küberdiplomaatiat ja koostööd NATOga.

3.3. Ettepanekus on esitatud uued algatused, nagu:

- tugevama ELi küberturvalisuse ameti loomine;
- kogu ELi hõlmava küberturvalisuse sertifitseerimise kava kehtestamine;
- võrgu- ja infoturbe direktiivi kiire rakendamine.

3.4. Vastupidavusvõime osas esitatakse küberturvalisusega seotud tegevustega seotud soovitusi, mis käsitlevad eelkõige järgmisi küsimusi: turuprobleemid, võrgu- ja infoturbe direktiiv, kiire reageerimine hädaolukordades, ELi pädevuse arendamine, haridus, küberoskuste ja küberhügieeni teemaline kooolitus ja teadlikkus.

3.5. Lisaks sellele tehakse küberturvalisust käsitlevas õigusaktis ettepanek küberturvalisuse sertifitseerimise raamistiku loomiseks IKT toodetele ja teenustele.

3.6. Küberturvalisust käsitlev õigusakt sisaldab ka ettepanekut suurendada ENISA rolli ELi küberturvalisuse ametina, mis annaks ENISA-le alalise mandaadi. Lisaks praegustele tööülesannetele kuuluksid ENISA vastutusalasse uued tugi- ja koordineerivad ülesanded, mis on seotud võrgu- ja infoturbe direktiivi rakendamise toetamise, ELi küberturvalisuse strateegia, tegevuskava, suutlikkuse arendamise, teadmiste ja teabe, teadlikkuse suurendamise, selliste turuga seotud ülesannetega nagu standardimine ja sertifitseerimine, teadusuuringute ja innovatsiooni, üleeuroopaliste küberturvalisuse õppuste ning küberturbe intsidentide lahendamise üksuste (CSIRTide) võrgustiku sekretariaadiga.

4. Üldised märkused – ülevaade

4.1. **Valdkond: vastupidavusvõime**

4.1.1. Ühtne küberturvalisuse turg

Hoolsuskohustus: ühisteatistes mainitud kavandatava hoolsuskohustuse põhimõtte edasiarendamine, mida kasutatakse turvalise arenduse olulusringi protsessides, on huvitav kontseptsioon, mida koos ELi tööstusega edasi vormitakse ning mis võib viia tervikliku lähenemisviisini ELi õigusaktidele vastavuse osas. Edasises arengus tuleks kaaluda vaikimisi turvet.

Vastutus: sertifitseerimine lihtsustab vaidluste korral vastutuse kohaldamist.

4.1.2. Võrgu- ja infoturbe direktiiv: energeetika, transport, pangandus/finantssektor, tervishoid, vesi, digitaalne taristu, e-kaubandus.

Komitee jaoks on elutähtsates sektorites vastupidavusvõime tagamiseks oluline võrgu- ja infoturbe direktiivi täielik ja tõhus rakendamine.

Komitee leiab, et teabe jagamist avaliku ja erasektori asutuste vahel tuleks tugevdada valdkondlike teabe jagamise ja analüüsimise keskuste kaudu. Välja tuleks töötada sobiv mehhanism usaldusväärse teabe turvaliseks jagamiseks teabe jagamise ja analüüsimise keskuste siseselt ning küberturbe intsidentide lahendamise üksuste ja teabe jagamise ja analüüsimise keskuste vahel, tuginedes hinnangule/analüüsile praegu kasutusel oleva mehhanismi kohta.

4.1.3. Kiirreageerimine

Tegevuskavapõhine lähenemisviis looks tõhusa protsessi operatiivseks reageerimiseks liidu ja liikmesriikide tasandil ulatuslike küberintsidentide korral. Komitee rõhutab erasektori kaasamise vajadust; arvesse tuleks võtta ka oluliste teenuste operaatorite kaasamist operatiivse reageerimise mehhanismi, kuna nad võiksid anda väärtuslikku teavet ohtude kohta ja/või aidata ohtude ja ulatuslike kriiside tuvastamisel ja neile reageerimisel.

Ühisteatistes tehakse ettepanek küberintsidentide integreerimiseks ELi tasandi kriisiohjeme mehhanismidesse. Kuigi komitee mõistab ühise tegutsemise ja solidaarsuse vajadust rünnaku korral, on vaja paremat arusaamist sellest, kuidas seda võiks rakendada, kuna küberohud levivad tavaliselt üle mitme riigi. Riiklikes hädaolukordades kasutatavaid vahendeid saaks kohaliku vajaduse tekkimisel ainult osaliselt jagada.

4.1.4. ELi pädevuse arendamine

Et EL suudaks olla ülemaailmselt tõesti konkurentsivõimeline ja luua tugeva tehnoloogilise baasi, on hädavajalik töötada välja sidus pikaajaline raamistik, mis hõlmaks küberturvalisuse väärtusahela kõiki etappe. Seega on koostöö edendamine Euroopa piirkondlike ökosüsteemide vahel määrava tähtsusega Euroopa küberturvalisuse väärtusahela arendamisel. Komitee avaldab heameelt ettepaneku üle luua küberturvalisuse pädevusvõrgustik.

Võrgustik võiks toetada Euroopa digitaalset suveräänsust, töötades välja konkurentsivõimelise Euroopa tööstusbaasi ja vähendades sõltuvust väljaspool ELi loodud oskusteabest, mis on seotud olulise tehnoloogilise võimekusega, korraldada tehnilisi õppusi, õpikodasid ja pakkuda isegi vajalikku küberhügieenialast koolitust spetsialistidele ja mitte-kutseala esindajatele, samuti – tuginedes küberturvalisuse alase lepingulise avaliku ja erasektori partnerluse raames tehtud tööle – edendada riikide avaliku ja erasektori ühisorganisatsioonide võrgustiku arendamist, et toetada turu väljaarendamist Euroopas. „Küberturvalisuse alase lepingulise avaliku ja erasektori partnerluse areng peaks viima selle optimeerimise, kohandamise või laiendamiseni“ (eesistujariikide kolmiku Eesti, Bulgaaria ja Austria küberturvalisuse tööprogramm) kolmepoolse (Euroopa Komisjon, liikmesriigid, ettevõtted) ühisettevõtte loomise kaudu.

Tõhusaks tööks ja kavandavate eesmärkide saavutamiseks Euroopa tasandil peaks võrgustik tuginema selgelt määratletud juhtimissüsteemile.

Võrgustikku toetaks Euroopa tasandil küberturvalisuse uurimis- ja pädevuskeskus, mis ühendab kogu Euroopas olemasolevaid riiklikke pädevuskeskusi. Küberturvalisuse uurimis- ja pädevuskeskus mitte ainult ei koordineeriks ja juhiks teadustööd, nagu teistes ühisettevõtetes, vaid võimaldaks ka tõhusalt välja arendada Euroopa küberturvalisuse ökosüsteemi, mis toetaks ELi innovatsiooni rakendamist ja kasutuselevõtmist.

4.2. **Valdkond: heidutus**

4.2.1. Küberkuritegevuse vastane võitlus on riiklikul ja Euroopa tasandil esmatähtis valdkond, mis eeldab suurt poliitilist pühendumist. Heidutustegevuse elluviimisel tuleks tugineda kindlale avaliku ja erasektori partnerlusele, millega tagatakse tõhus teabejagamine ja oskusteave nii riiklikul kui ka Euroopa tasandil. Võimalik oleks ka Europoli tegevuse laiendamine küberkriminalistika ja järelevalve alal.

4.3. **Valdkond: rahvusvaheline koostöö**

4.3.1. Usaldava koostöö ülesehitamine ja alalhoidmine kolmandate riikidega kübertehnoloogia ja ettevõtjate partnerluste kaudu on määrava tähtsusega, et suurendada Euroopa suutlikkust suuremahuliste küberrünnete ennetamisel ja takistamisel ning neile reageerimisel. Euroopa peaks edendama koostööd USA, Hiina, Iisraeli, India ja Jaapaniga. ELi ekspordikontrolli kaasajastamine peaks ennetama inimõiguste rikkumisi ja tehnoloogiate väärkasutamist Euroopa Liidu enda turvalisuse vastu, kuid peaks samas tagama ka selle, et seoses pakkumistega kolmandatest riikidest ELi tööstus ebaõiglaselt ei kannataks. Kandidaatriikide jaoks tuleks ette näha sihtotstarbeline strateegia, et valmistuda tundlike piiriüleste andmete vahetamiseks. See hõlmaks võimalust osaleda vaatlejatena ENISA riikide teatud tegevuses, kusjuures riigid tuleks seada paremusjärjekorda vastavalt nende valmidusele võidelda küberkuritegevuse vastu, samuti võiks kavandada musta nimekirja koostamist.

4.3.2. Komitee tunneb heameelt küberkaitse kaasamise üle võimaliku tulevase ELi küberturvalisuse pädevuskeskuse kavandatavasse teise etappi. Seepärast võiks Euroopa vahepealsel perioodil jälgida kahesuguse kasutusega pädevuste arengut, sealhulgas finantsvõimenduse kasutamist Euroopa Kaitsefondis ja kavandatava küberkaitsealase koolituse ja hariduse platvormi loomist 2018. aastaks. Pidades silmas vastastikku tunnistatud potentsiaali ja ohte, peab komitee vajalikuks arendada ELi ja NATO koostööd. Samuti peaks Euroopa tööstus tähelepanelikult jälgima arengut, mis toimub ELi ja NATO koostöös küberturvalisuse standardite suurema koostalitlusvõime vallas ning teistes koostöövormides ELi lähenemisviisi raames küberkaitsele.

4.4. ELi sertifitseerimisraamistik

4.4.1. Komitee on veendunud, et Euroopa peab tegelema küberturvalisuse killustatuse probleemiga eeskirjade ühese tõlgendamise kaudu, sh on vaja liikmesriikide vastastikust tunnustamist ühtses raamistikus, et lihtsustada digitaalse ühtse turu kaitsmist. Sertifitseerimisraamistik võiks tagada ühtse lähtealuse (vajaduse korral erieeskirjadega kõrgematel tasanditel), mis tagab vertikaalsete valdkondade koostoime ja vähendab praegust killustatust.

4.4.2. Komitee väljendab heameelt ELi küberturvalisuse sertifitseerimise raamistiku ja eri sektorite sertifitseerimiskavade loomise üle, mis põhinevad asjakohastel nõuetel ja mida tehakse koostöös peamiste sidusrühmadega. Turustamiseks vajaminev aeg ja sertifitseerimiskulud, samuti kvaliteet ja turvalisus on aga peamised elemendid, millega tuleb arvestada. Et suurendada turvalisust vastavalt praegustele vajadustele ja teadmiste ohtudest, luuakse sertifitseerimiskavad, mille juures tuleks arvesse võtta nende paindlikkust ja arendusvõimalusi, et võimaldada vajalik ajakohastamine. Eri sektoritele tuleb nende toimumisviiside tõttu pakkuda erinevaid lähenemisviise. Seepärast leiab komitee, et antud protsessi peaksid olema kaasatud valdkondlikud ELi ametid (Euroopa Lennundusohutusamet, Euroopa Pangandusjärelevalve, Euroopa Liidu Raudteeamet, Euroopa Raviamet jne) ning et mõnel juhul tuleks – ENISA nõusolekul, et ära hoida dubleerimist ja sidususe puudumist – delegerida küberturvalisuse kavade koostamine neile.

4.4.3. Komitee jaoks on oluline, et sertifitseerimisraamistiku loomisel tuginetaks ühiselt määratletud ja võimalusel rahvusvaheliselt tunnustatud Euroopa küberturvalisuse ja IKT standarditele. Arvestades ajakava ja liikmesriikide õigusi, tuleks Euroopa IT-turbe miinimumnõuded vastu võtta koostöös Euroopa Standardikomitee/Euroopa Elektrotehnika Standardikomitee/Euroopa Telekommunikatsioonistandardite Instituudiga. Kutsestandardeid tuleks positiivselt arvesse võtta, kuid need ei tohiks olla õiguslikult siduvad ega takistada konkurentsi.

4.4.4. Selgesti on vaja siduda vastutus usaldusväärsuse eri tasemetega vastavalt ohtudest tulenevatele mõjudele. Dialoogi astumine kindlustusandjatega võib aidata kaasa tõhusate küberturvalisuse nõuete vastuvõtmisele vastavalt rakendusvaldkonnale. Komitee hinnangul tuleks toetada ja motiveerida ettevõtteid, kes on huvitatud kõrgest usaldusväärsuse tasemest, eriti mis puudutab elutähtsaid seadmeid ja süsteeme.

4.4.5. Arvestades aega, mis on möödunud direktiivi 85/374/EMÜ⁽⁹⁾ vastuvõtmisest, ning pidades silmas praegust tehnoloogilist arengut, kutsub komitee komisjoni üles uurima, kas tasuks lisada direktiivi kohaldamisalasse mõned kõnealuse määru ettepanekus esitatud stsenaariumid, et muuta tooted ohutumaks, tõstes kaitse taset.

4.4.6. Komitee leiab, et kavandatav Euroopa küberturvalisuse sertifitseerimise rühm, mida toetab ENISA, peaks koosnema riiklikest sertifitseerimise järelevalveasutustest, erasektori sidusrühmadest ja eri rakendusvaldkondades tegutsevatest operaatoritest, et tagada laiahaardeliste sertifitseerimiskavade väljatöötamine. Lisaks sellele tuleks ette näha koostöö antud rühma ja sektorit esindavate ühingute vahel EList/Euroopa Majanduspiirkonnast (nt küberturvalisuse alane lepinguline avaliku ja erasektori partnerlus, pangandus, transport, energeetika, liidud jne) ekspertide ametisse nimetamise kaudu. See rühm peaks olema võimeline hindama Euroopa saavutusi sertifitseerimise alal (mis põhinevad peamiselt kõrgemate ametnike infosüsteemide turbe rühma (SOG-IS) vastastikuse tunnustamise kokkuleppel ning riiklikel ja omandipõhistel kavadel) ja püüdma säilitada Euroopa konkurentsieeliseid.

⁽⁹⁾ EÜT L 210, 7.8.1985, lk 29.

4.4.7. Komitee teeb ettepaneku anda neile sidusrühmadele koos Euroopa Komisjoniga sertifitseerimiskavade ühise ettevalmistamise vastutus. Ka valdkondlikud nõuded tuleks välja töötada üksmeelse nõusoleku teel avaliku ja erasektori (tarbijate ja tarnijate) sidusrühmade vahel.

4.4.8. Lisaks sellele peaks sertifitseerimisrühm sertifitseerimiskavad korrapäraselt läbi vaatama, pidades silmas iga valdkonna nõudeid ja vajaduse korral kavasid kohandades.

4.4.9. Komitee toetab riiklike sertifitseerimiskavade järkjärgulist kaotamist, kui võetakse kasutusele Euroopa kava, nagu on ette nähtud määruse artiklis 49. Ühtne turg ei saa toimida erinevate ja omavahel konkureerivate riiklike eeskirjadega. Sellega seoses teeb komitee ettepaneku viia läbi riiklike kavade loendus.

4.4.10. Komitee soovib komisjonil algatada meede, millega edendada ELis küberturvalisuse sertifitseerimist ja sertifikaate ning toetada nende tunnustamist kõigis rahvusvahelistes kaubanduslepingutes.

4.5. Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA)

4.5.1. Komitee leiab, et komisjoni ettepaneku kohaselt ENISA-le antav alaline mandaat aitab olulisel määral kaasa Euroopa süsteemide vastupanuvõime suurendamisele. Siiski ei pruugi ettepanekuga esitatud esialgsest eelarvest ja reformitud ENISA-le eraldatud vahenditest piisata selleks, et amet saaks oma volitusi täita.

4.5.2. Komitee julgustab kõiki liikmesriike looma ENISA-le selgelt vastava sarnase asutuse, sest enamik neist ei ole seda veel teinud. Edendada tuleks struktureeritud programmi, millega lähetada riiklikke eksperte ENISASSE, et toetada heade tavade tutvustamist ja suurendada usaldust. Komitee soovib komisjonil tagada, et liikmesriikides käibel olevad head tavad ja toimivad meetmed kogutaks kokku ja neid tutvustataks üksteisele.

4.5.3. Samuti leiab komitee, et suutlikkuse arendamise seisukohalt peaks ENISA seadma prioriteediks e-valitsust toetavad meetmed⁽¹⁰⁾. ELi-ülene/ülemaailmne digitaalne identiteet isikutele, organisatsioonidele, ettevõtetele ja seadmetele on määrava tähtsusega ning identiteedivarguse ja internetipettuste ennetamine ja nende vastu võitlemine ning tööstus-intellektuaalomandi varguse vastu võitlemine peaks olema esmatähtis.

4.5.4. Samuti peaks ENISA esitama korrapäraseid aruandeid liikmesriikide kübervalmisoleku kohta, keskendudes eelkõige võrgu- ja infoturbe direktiivi II lisas määratletud sektoritele. Iga-aastane Euroopa küberõppus peaks hindama liikmesriikide valmisolekut ja Euroopa küberkriisidele reageerimise mehhanismi tõhusust, samuti peaksid sellele järgnema soovitusel.

4.5.5. Komitee kardab, et operatiivkoostööle, sealhulgas küberturbe intsidentide lahendamise üksuste võrgustikule määratud vahendid on liiga piiratud.

4.5.6. Turuga seotud ülesannete kohta leiab komitee, et koostöö tihendamine liikmesriikidega ja ametliku küberturvalisuse ametite võrgustiku loomine aitaks toetada sidusrühmadevahelist koostööd⁽¹¹⁾. Turustamiseks vajaminev aeg on väga lühike ja see on ELi ettevõtete jaoks antud alal konkureerimiseks elulise tähtsusega ning ka ENISA peab olema suuteline sellega kooskõlas tegutsema. Komitee leiab, et ENISA võiks tulevikus rakendada lõivude ja tasude süsteemi, nagu seda teevad teised ELi ametid. Komitee on mures, et ELi ja riiklike ametite vaheline pädevuse nimel konkureerimine võib, nagu on juhtunud teistes valdkondades, aeglustada ELi õigusraamistiku korralikku kehtestamist ja kahjustada ELi ühtset turgu.

4.5.7. Komitee märgib, et teadus- ja arendustöö ning rahvusvahelise koostööga seotud ülesanded on praegu minimaalsed.

⁽¹⁰⁾ Digitaalse ühtse turu vahekokkuvõte.

⁽¹¹⁾ ELT C 75, 10.3.2017, lk 124.

4.5.8. Komitee leiab, et küberturvalisus peaks olema korrapärane aruteluteema justiits- ja siseküsimuste ametite korralistel ühiskoosolekutel ning ENISA ja Europol peaksid korrapäraselt koostööd tegema.

4.5.9. Kuna kübermaailm on väga uuenduslik, peavad nõuded olema hoolikalt läbi mõeldud, et vältida takistuste seadmist innovatsioonile, mille toimumiseks on vaja dünaamilist raamistikku; võimalikult suures ulatuses tuleks tagada nii edasi- kui ka tagasiühilduvus, et kaitsta nii kodanike kui ka ettevõtjate investeeringuid.

4.5.10. Riiklike sertifitseerimise järelevalveasutuste olulisuse tõttu teeb komitee ettepaneku, et juba kõnealuse määrusega loodaks ametlik järelevalveasutuste võrgustik, millel on õigus ENISA abiga lahendada piiriüleseid küsimusi. Võrgustikust võiks hilisemas etapis areneda välja üks amet.

4.5.11. Usaldus on väga oluline, kuid ENISA-l ei ole õigust väljastada otsuseid ega auditeerimisaruandeid. Komitee on arvamisel, et amet peaks Euroopa Komisjoni nimel jälgima riiklike sertifitseerimise järelevalveasutuste tegevust ja otsuste langetamist, viies läbi auditeid ja kontrole.

4.5.12. ENISA juhatuses peaksid vaatelejatena osalema ka tööstus- ja tarbijaorganisatsioonid.

4.6. Tööstus, VKEd, rahastamine/investeeringud ja uuenduslikud ärimudelid

4.6.1. Tööstus ja investeeringud

IKT valdkonnas tegutsevate ELi ettevõtjate ülemaailmse konkurentsivõime suurendamiseks peab toimuma suunatud tegevus IKT valdkonna, sealhulgas VKEde kasvu ja konkurentsivõime toetamiseks.

Euroopa peaks suurendama investeeringuid, koondades erinevaid ELi ja riiklike vahendeid ning erasektori investeeringuid, et aidata saavutada strateegilised eesmärgid tugevas avaliku ja erasektori koostöös. Investeeringute taset olulistest valdkondades tuleks tõsta ning investeerimist toetada, luues ELi fondi küberturvalisuse valdkonna innovatsiooniks ning teadus- ja arendustegevuseks teadusuuringute praeguse ja tulevase raamprogrammi raames. Lisaks peaks Euroopa Liit looma fondi küberturbe elluviimiseks, avades uue akna praeguses ja tulevases Euroopa ühendamise rahastus ning Euroopa Strateegiliste Investeeringute Fondis 3.0.

ELi liikmesriikidele tuleks luua stiimuleid võimaluse korral Euroopa lahenduste ostmiseks ja Euroopa tarnijate valimiseks, eriti tundliku loomuga rakendusvaldkondade puhul. Euroopa peaks toetama edukate Euroopa suurettevõtete kasvu, kes on ülemaailmsel turul konkurentsivõimelised.

4.6.2. VKEd

Turu killustatuse tõttu on vaja suuremat selgust klientidepoolse nõudluse kohta, et turu vajadusi paremini täita. Ilma struktureeritud nõudlusest ei saa VKEd ja idufirmad kiiresti kasvada. Seepärast oleks positiivne, kui loodaks Euroopa VKEde küberturvalisuse keskus.

Küberturvalisuse tehnoloogia muutub kiiresti ja VKEd on suutelised tänu oma kiirele reageerimisvõimele pakkuma uusimaid lahendusi, mis on konkurentsivõime säilitamiseks olulised. Võrreldes kolmandate riikidega otsib Euroopa Liit ikka veel VKEdele sobilikku ärimudelit.

Välja võiks töötada idufirmadele ja VKEdele suunatud kavad, et pakkuda tuge sertifitseerimiskulude katmisel, arvestades, kui keeruline on neil koguda raha tehnoloogiliseks ja kaubanduslikuks arenguks.

4.7. Inimtegur: haridus ja kaitse

4.7.1. Komitee märgib, et komisjoni ettepanekus ei võeta piisavalt arvesse inimesi kui digitaalprotsesside mootorit kas neist kasusaajatena või peamiste küberintsidentide põhjustajatena.

4.7.2. Vaja on luua tugev kübersüsteemide baas ja parandada küberhügieeni ning suurendada teadlikkust üksikisikute ja ettevõtjate seas. Selle tulemuse saavutamiseks tuleks kaaluda sihtotstarbelisi investeeringuid, aja eraldamist kõrgetasemeliste juhendajate koolitamiseks ning tõhusate teadlikkuse suurendamise kampaaniate korraldamist. Nende kolme tegevussuuna rakendamiseks on vajalik riiklike ja piirkondlike ametiasutuste (kes vastutavad tõhusate haridusprogrammide loomise ja nendesse investeerimise eest) ning ettevõtete ja VKEdes kaasaamine ühise lähenemisviisi raames.

4.7.3. Plaanida tuleks võimalikku ELi sertifitseeritud õppekava loomist keskkoolidele ja töötavatele spetsialistidele, kaasates aktiivselt ENISA ja sellele vastavad riiklikud asutused. Lisaks sellele tuleb haridusprogramme välja töötades silmas pidada soolist võrdsuslikkust, et parandada tööhõive taset küberturvalisuse valdkonnas.

4.7.4. Komitee leiab, et sertifitseerimistegevusest ei saa välja jätta korralikku märgistamissüsteemi nii riistvara kui ka tarkvara jaoks, nagu juba tehakse paljude muude toodete (näiteks energiatooted) puhul. Sellisel vahendil oleks kolm eelist: vähendada ettevõtjate kulusid, kaotada turu praegune killustumine, mis tuleneb riiklike sertifitseerimissüsteemide erinevustest, ning aidata tarbijatel mõista ostetud toote kvaliteeti ja omadusi. Selles mõttes on oluline, et samu sertifitseerimis- ja märgistamissüsteeme rakendataks ka imporditud toodete suhtes. Lisaks usub komitee, et kasulik võiks olla *ad hoc* logo kasutuselevõtt, et kohe teavitada tarbijaid ja kasutajaid ostetud toote või veebipoe usaldusväärsusest või veebilehtedest, kus edastatakse tundlikke andmeid.

4.7.5. ENISA peaks juhtima olulist mitmetasandilist teabe- ja teadlikkuse suurendamise kampaaniat, et suurendada interneti kasutajate teadlikkust turvalisest käitumisest ja nende usaldust interneti suhtes. Seetõttu tuleks kaasata ettevõtjate ja tarbijate ühendused ning muud digitaalteenuste ettevõtjate organisatsioonid.

4.7.6. Lisaks küberjulgeolekut käsitlevale õigusaktile peab komitee esmatähtsaks – nagu juba väljendatud arvamuses INT/828 – käivitada võimalikult kiiresti ulatuslik Euroopa digitaalharidus- ja -koolitusprogramm, millega tagada kõigile kodanikele vahendid, et saada üleminekuga hakkama võimalikult hästi. Olles teadlik liikmesriikide konkreetsest pädevusest antud valdkonnas, loodab komitee eelkõige, et programm algab koolis ja sellega suurendatakse õpetajate teadmisi, kohandatakse õppekavasid ja õppemetoodikat digitaaltehnoloogiale (sh e-õpe) ning pakutakse kõigile õpilastele hea kvaliteediga koolitust. See programm laieneks loomulikult elukestvatele õppele, et töötajaid ümber õpetada või ajakohastada nende oskusi⁽¹²⁾.

5. Konkreetsed märkused

5.1. Kujunemisjärgus tehnoloogiad ja lahendused: asjade internet

Ühendatud seadmete hulk kasvab pidevalt, jõudes eelduste kohaselt tasemele, kus nende arv on mitu korda suurem maakeral elavate inimeste arvust, tingituna komponentide, süsteemide ja lahenduste üleminekust digitehnoloogiale ning paranenud ühenduvusest. See suundumus loob uusi võimalusi küberkurjategijatele, eriti seetõttu, et asjade interneti seadmed ei ole tihti nii hästi kaitstud kui traditsioonilised seadmed.

Euroopa turbestandardite kehtestamine eri tasanditel, kus asjade interneti seadmeid kasutatakse, võib vähendada jõupingutusi arendustöös, ajakulu ja eelarve suurust kõikides tööstustes võrgustatud toodete väärtusahelas osalejate jaoks.

Tavalise, n-ö inimeste interneti seadmete puhul on tõenäoliselt vajalik teatav minimaalne turbeaste identiteedi ja juurdepääsuõiguste haldamise, paikamise ja seadmehalduse teel. Kuna sertifitseerimine on peamine meetod kõrgema turvalisuse taseme pakkumiseks, siis uues ELi sertifitseerimise lähenemisviisis tuleks asetada suuremat rõhku asjade interneti turvalisusele.

Brüssel, 14. veebruar 2018

Euroopa Majandus- ja Sotsiaalkomitee
president
Georges DASSIS

⁽¹²⁾ Digitaalse ühtse turu vahekokkuvõte.