Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine““

[COM(2016) 410 final]

(2017/C 075/21)

Raportöör: **Thomas McDONOGH**

Konsulteerimistaotlus	Euroopa Komisjon, 18.8.2016
Õiguslik alus	Euroopa Liidu toimimise lepingu artikkel 304
Vastutav sektsioon	transpordi, energeetika, infrastruktuuri ja infoühiskonna sektsioon
Vastuvõtmine sektsioonis	15.11.2016
Vastuvõtmine täiskogus	14.12.2016
Täiskogu istungjärk nr	521
Hääletuse tulemus	148/0/1
(poolt/vastu/erapooletuid):	

1. **Järeldused ja soovitused**

1.1. Euroopa Majandus- ja Sotisaalkomitee tervitab komisjoni teatist teemal „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“. Komitee jagab komisjoni muret, et Euroopa on jätkuvalt haavatav küberrünnakute suhtes, märkides, et vähemalt 80 % Euroopa ettevõtetest on viimase aasta jooksul olnud vähemalt üks küberjulgeoleku intsident ja et 2015. aastal suurenes kõigis tööstusharudes küberjulgeoleku intsidentide arv 38 % (*The Global State of Information Security Survey 2016, PWC*). Komitee nõustub komisjoniga, et tarvis on erinevaid meetmeid, tugevdamaks Euroopa kübervastupidavusvõime süsteemi ning edendamaks konkurentsivõimelist ja uuenduslikku küberjulgeolekutööstust Euroopas.

1.2. Komitee tervitab seda ettepanekut eelkõige seoses hiljuti vastu võetud küberjulgeoleku direktiiviga, ([1]) mille eesmärk on ühtlustada küberjulgeoleku käsitlusviisi Euroopa Liidus, ning ulatuslikumat küberjulgeoleku strateegiat, ([2]) milles antakse ülevaade praegusest arusaamast selle kohta, kuidas on kõige parem ära hoida küberhäireid ja -rünnakuid, edendada selliseid Euroopa väärtusi nagu vabadus ja demokraatia ning tagada digitaalmajanduse turvaline kasv.

1.3. Komitee nõustub, et tarvis on ulatuslikke meetmeid, et kaitsta täiendavalt Euroopa elutähtsaid digitaalteenuseid ja -taristut julgeolekuohtude eest, ning tunneb heameelt, et pakutud meetmed aitavad märkimisväärselt kaasa hulga soovituste rakendamisele, mis on esitatud komitee mitmes varasemas arvamuses ([3]) liidu küberjulgeoleku edendamise kohta.

([1]) ELT L 194, 19.7.2016, lk 1.
([2]) JOIN(2013) 1.
([3]) ELT C 97, 28.4.2007, lk 21;
ELT C 175, 28.7.2009, lk 92;
ELT C 255, 22.9.2010, lk 98;
ELT C 54, 19.2.2011, lk 58;
ELT C 107, 6.4.2011, lk 58;
ELT C 229, 31.7.2012, lk 90;
ELT C 218, 23.7.2011, lk 130;
ELT C 24, 28.1.2012, lk 40;
ELT C 229, 31.7.2012, lk 1;
ELT C 351, 15.11.2012, lk 73;
ELT C 76, 14.3.2013, lk 59;
ELT C 271, 19.9.2013, lk 127;
ELT C 271, 19.9.2013, lk 133;
ELT C 451, 16.12.2014, lk 31.

1.4. Komitee väljendab heameelt, et komisjon on allkirjastanud küberjulgeoleku avaliku ja erasektori lepingulise partnerluse, mis eeldatavasti avab 1,8 miljardi euro suuruse investeeringu ELi küberjulgeolekutööstusesse, et soodustada koostööd teadusuuringute ja innovatsiooniprotsessi varastes etappides ning luua küberjulgeolekulahendused eri sektorites, nagu energia, tervishoid, transport ja rahandus. Eriti loodab komitee, et selle avaliku ja erasektori lepingulise partnerluse kaudu toetatakse äsja loodud küberjulgeolekualaste ettevõtete arengut kogu ELis.

1.5. Komitee kiidab heaks komisjoni kavatsuse hinnata vajadust muuta või laiendada Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) volitusi 2017. aasta lõpuks ning ootab huviga, et komisjon peaks komiteega selles küsimuses nõu. Komitee on veendunud, et ENISA volituste laiendamisega peaks kaasnema kõnealuse ameti suurem operatiivfunktsioon, et suurendada tõhusamalt teadlikkust küberrünnakuohust ja reageerimisvõimet kogu ELis, ning otsesem vastutus küberjulgeolekualase koolituse ja teadlikkuse suurendamise programmide eest, mis on eelkõige suunatud kodanikele ning väikestele ja keskmise suurusega ettevõtjatele (VKEd).

1.6. Selleks, et tagada vajalik tugev juhtimine ja integratsioon ELi tasandil, tegelemaks tõhusa üleeuroopalise küberjulgeolekupoliitika rakendamise probleemkohtadega, kutsub komitee komisjoni üles hindama võimalust ENISA staatuse muutmiseks, et kujundada see ELi tasandil küberjulgeoleku eest vastutavaks asutuseks sarnaselt lennundustööstuse kesksele ametile, Euroopa Lennundusohutusametile (EASA). Kui ENISA mandaadi selline muutmine ei ole võimalik, pooldab komitee seda tüüpi täiesti uue asutuse loomist.

1.7. Komitee kutsub komisjoni üles kaaluma sarnaselt IT-tööstuses kasutatavale mudelile *Capability Maturity Model* (CMM) küberjulgeoleku mudeli loomist riikliku küberjulgeoleku arendamiseks ja hindamiseks, et objektiivselt mõõta küberjulgeoleku vastupidavusvõime olukorda igas liikmesriigis.

1.8. Komitee märgib, et komisjon kaalub 2013. aasta Euroopa Liidu küberjulgeoleku strateegia ajakohastamise vajadust lähitulevikus, ja ootame huviga, et komisjon arutaks meiega oma seisukohti õigeaegselt.

1.9. Arvestades küberjulgeoleku olulisust ja üha suurenevat küberkuritegevuse ohtu, kutsub komitee üles eraldama piisavaid rahalisi vahendeid ja ressursse Europoli küberkuritegevuse vastase võitluse Euroopa keskusele ja Euroopa Kaitseagentuurile.

1.10. Arvestades avaliku halduse asutustes salvestatud isikuandmete kaitsmise suurt olulisust, kutsub komitee üles pakkuma avaliku haldusstruktuuri töötajatele spetsiaalset koolitust teabehalduse, andmekaitse ja küberjulgeoleku valdkonnas.

1.11. ELi küberjulgeoleku strateegia ja poliitika, millega lähenetakse terviklikult ELi kaitsmisele küberkuritegevuse ja -rünnakute eest ning rajatakse Euroopas tugev küberjulgeolekutööstus, peab komitee arvates saavutama tulemusi ennekõike järgmistes aspektides: ELi tugev juhtroll; küberjulgeolekupoliitika, mis suurendab turvalisust, säilitades samas eraelu puutumatuse ja muud põhiõigused; kodanike teadlikkuse suurendamine ja ennetavale kaitsele suunatud lähenemisviiside julgustamine; terviklik valitsemine liikmesriikides; ettevõtjate teadlik ja vastutustundlik tegutsemine; tihe partnerlus valitsuste, erasektori ja kodanike vahel; piisav investeeringute tase; head tehnilised standardid ning piisavad investeeringud teadus- ja arendustegevusse ning innovatsiooni; tegutsemine rahvusvahelisel tasandil.

2. **Komisjoni teatise põhisisu**

2.1. Teatises tutvustatakse meetmeid, millega tugevdada Euroopa kübervastupidavusvõime süsteemi ning soodustada Euroopas konkurentsivõimelist ja uuenduslikku küberjulgeolekutööstust, nagu on kuulutatud ELi küberjulgeoleku strateegias ja digitaalse ühtse turu strateegias.

2.2. Selle saavutamiseks võimendatakse komisjoni esitatud meetmetega küberjulgeoleku direktiivi, et tugevdada liidus küberjulgeolekualast koostööd, teabe jagamist ning koolitus- ja julgeolekumeetmete korraldust. Komisjon lõpetab 2017. aasta lõpuks ka ENISA hindamise ning kaalub vajadust muuta või laiendada ENISA volitusi.

2.2.1. Komisjon teeb küberjulgeoleku koolitusplatvormi loomiseks tihedat koostööd liikmesriikide, Euroopa Liidu Võrgu- ja Infoturbeameti, Euroopa välisteenistuse ja muude asjakohaste ELi asutustega.

2.2.2. On olemas rida meetmeid, et tegeleda sektoritevahelise seotusega ja tugevdada olulise avaliku võrgutaristu vastupidavusvõimet, sh Euroopa valdkondlike teabe jagamise ja analüüsimise koostöökeskuste arendamine ning nende koostöö küberturbe intsidentide lahendamise üksustega (CSIRT). Samuti teeb komitee ettepaneku, et liikmesriikide ametiasutustel oleks olulise võrgutaristu regulaarseks kontrollimiseks võimalik rakendada CSIRTe.

2.3. Komisjoni esitatud meetmetega käsitletakse ühtlasi vajadust suurendada tugeva Euroopa küberjulgeolekutööstuse kasvu ja arengut koolituse, investeeringute, ühtse turu nõuete ning uue küberjulgeoleku avaliku ja erasektori partnerluse loomise abil, mis eeldatavasti võimaldab teha 2020. aastaks 1,8 miljardi euro suuruse investeeringu.

2.3.1. Samuti tehakse ettepanek töötada välja ettepanek Euroopa IKT turvalisuse sertifitseerimise raamistiku jaoks, mida esitletakse 2017. aasta lõpus, ning hinnata Euroopa küberjulgeoleku märgistamise vähenõudliku raamistiku teostatavust ja mõju.

2.3.2. Euroopas küberjulgeoleku investeeringute laiendamiseks ning väikeste ja keskmise suurusega ettevõtjate toetamiseks teeb komisjon järgmist: suurendab küberjulgeolekukogukonnas teadlikkust olemasolevatest rahastamismehhanismidest; rakendab ulatuslikumalt ELi vahendeid ja instrumente, millega toetada uuenduslikke väikeseid ja keskmise suurusega ettevõtjaid tsiviil- ja kaitsevaldkonna küberjulgeolekuturgude sünergia otsimisel (nt Euroopa ettevõtlusvõrgustik ja kaitsevaldkonnaga seotud piirkondade Euroopa võrgustik pakuvad piirkondadele kahesuguse kasutuse valdkonnas piiriülese koostöö võimaluste otsimisel uusi võimalusi, sh küberjulgeoleku vallas, ning võimaldavad VKEdel kontakte luua); uurib 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).

2.3.3. Lisaks kavatseb komisjon Euroopa küberjulgeolekutööstuse stimuleerimiseks ja arendamiseks uuenduslikkuse abil allkirjastada tööstusega küberjulgeoleku avaliku ja erasektori lepingulise partnerluse, algatada programmi „Horisont 2020“ raames küberjulgeoleku avaliku ja erasektori lepingulise partnerlusega seonduvad konkursikutsed ning tagada küberjulgeoleku avaliku ja erasektori lepingulise partnerluse kooskõlastamise asjakohaste valdkondlike strateegiate, programmi „Horisont 2020“ instrumentide ning valdkondlike avaliku ja erasektori lepinguliste partnerlustega.

3. **Üldised märkused**

3.1. ELis on digitaalmajandus toonud kaasa rohkem kui ühe viiendiku suuruse SKP kasvu ning igal aastal teeb enamik eurooplasi oste veebis. Oleme sõltuvad internetist ja ühendatud digitaaltehnoloogiast, mis toetavad eluliselt olulisi energeetika-, tervishoiu-, valitsus- ja finantsteenuseid. Ent elutähtsad digitaalteenused ja -taristu, millel on keskne roll meie majanduslikus ja ühiskondlikus elus, on üha rohkem haavatavad küberkuritegevuse ja küberrünnakute suhtes, mis ohustavad meie heaolu ja elukvaliteeti.

3.2. Valitsused ja avaliku sektori asutused hoiavad praegu suurt osa kõiki kodanikke puudutavaid isikuandmeid elektroonilisel moel. Seetõttu on hea teabehaldus, küberjulgeolek ja andmekaitse äärmiselt olulised kogu ELi kodanike jaoks, kellele on tarvis kinnitada, et nende isikuandmeid ja privaatsust kaitstakse vastavalt ELi direktiividele ja määrustele. Eriti kehtib see eraisiku tervise-, finants-, juriidiliste ja muude andmete kohta, mida saab kasutada identiteedi varastamiseks või sobimatul viisil kolmandatele isikutele edastamiseks. See on äärmiselt oluline, et kõigil avaliku sektori töötajatel on hea väljaõpe teabehalduse, küberjulgeoleku ja andmekaitse valdkonnas.

3.3. Isikliku küberjulgeoleku, sealhulgas andmeturbe õpetamine kodanikele peaks olema kõigi digikirjaoskuse õppekavade lahutamatu osa. ELi juhitav koolitusprogramm võib toetada vähemaktiivsete liikmesriikide jõupingutusi ja ühtlasi tagada, et strateegiast saadakse õigesti aru, vähendades seega eraelu puutumatusega seotud hirme ja suurendades usaldust digitaalmajanduse vastu. Sellist programmi võiks rakendada, kaasates üle kogu ELi tarbijate ühendusi ja kodanikuühiskonna organisatsioone ning eakate kodanike vajadustele vastavaid haridusasutusi.

3.4. Iga liikmesriik peaks volitama oma tööstusarengu eest vastutavaid organisatsioone pakkuma VKE-dele teavet, koolitust ning toetust küberjulgeoleku küsimustes. Suurtel ettevõtjatel on kergem saada vajalikke teadmisi, aga VKE-d vajavad toetamist.

3.5. Väga kasulik oleks objektiivselt mõõta küberjulgeoleku vastupidavusvõime taset igas liikmesriigis, et kasutada seda võrdlust nõrkade kohtade kõrvaldamiseks ja paranduste hoogustamiseks. Võiks luua riikliku küberjulgeoleku arengu mudeli sarnaselt IT-tööstuses kasutatavale mudelile *Capability Maturity Model* (CMM), et hinnata riikliku küberjulgeoleku ja vastupidavusvõime olukorda.

3.6. Terviklik küberjulgeoleku strateegia peaks hõlmama järgmisi meetmeid:

— ELi tugev juhtroll, mille raames kujundatakse poliitikameetmed, õigusaktid ja institutsioonid, et toetada küberjulgeoleku kõrget taset kogu ELis;

— küberjulgeolekupoliitika, mis suurendab üksikisikute ja üldist turvalisust, säilitades samas kodanike eraelu puutumatuse ning muud põhiväärtused ja -vabadused;

— kodanike head teadmised internetikasutuse ohtudest ning ennetava strateegia edendamine, et kaitsta nende digitaalseadmeid, identiteeti, eraelu ja veebitehinguid;

— kõikide liikmesriikide poolne kõikehõlmav reguleerimine, et tagada elutähtsa infotaristu turvalisus ja vastupanuvõime;

— kõigi ettevõtjate teavitatud ja vastutustundlik tegevus, et tagada oma IKT süsteemide turvalisus ja vastupanuvõime, kaitsmaks oma tehinguid ja klientide huve;

— internetiteenuse osutajate ennetav strateegia klientide kaitsmiseks küberrünnakute eest;

— küberjulgeoleku käsitlus, mis põhineb kogu ELi hõlmaval tihedal partnerlusel valitsuste, erasektori ja kodanike vahel strateegilistel ja tegevuslikel tasanditel;

— projekteerimispõhine lähenemisviis, et kavandada küberjulgeolek sisse juba veebitehnoloogia ja -teenuste arendamisel;

— piisavad investeeringud küberjulgeolekualaste teadmiste ja oskuste arendamisse, et luua küberjulgeoleku valdkonnas tugevad inimressursid;

— head tehnilised küberjulgeoleku standardid ja piisavad investeeringud teadus- ja arendustegevusse ning innovatsiooni, et toetada tugeva küberjulgeolekutööstuse ja maailmatasemel lahenduste arendamist;

— aktiivne tegutsemine rahvusvahelisel tasandil koos kolmandate riikidega, et arendada küberjulgeoleku ohtude valdkonnas välja kooskõlastatud ülemaailmne poliitika ja strateegia.

4. **Konkreetsed märkused**

4.1. Lähtuvalt küberjulgeoleku direktiivis kirjeldatud küberjulgeoleku juhtimisraamistikust ja kõnealusesse teatisesse kaasatud lisameetmetest peaks EL kaaluma killustunud lähenemisviisi selgitamist küberjulgeoleku parandamiseks kogu ELis, luues Euroopa Lennundusohutusametile (EASA) analoogse küberjulgeoleku eest vastutava tugeva keskse asutuse või ELi infoturbe eest vastutava vanemametniku ametikoha, nagu hiljuti loodi Ameerika Ühendriikides (küberjulgeoleku riiklik tegevuskava, Valge Maja, 9.2.2016). Nende vastutusalasse kuuluks küberjulgeolekupoliitika rakendamise jälgimine ELi tasandil ja kõnealuse valdkonna erinevate ametite edusammude integreerimine.

4.2. Komitee peab märkimisväärseks pädevust, mille ENISA on aastate jooksul omandanud, ning usub, et ENISA võiks anda veelgi suurema panuse Euroopa küberjulgeoleku vastupidavusvõimesse ja turvalisusse. ENISA operatiivvolitusi tuleks tugevdada, et tõhusamalt suurendada teadlikkust küberrünnakute ohust ja nendele reageerimist kogu liidus. Volituste läbivaatamine on ajakohane, arvestades seda, kui palju on küberjulgeoleku keskkond muutunud pärast ENISA asutamist. Küberjulgeoleku direktiivile toetudes võiks ENISA operatiivfunktsiooni laiendada nii, et suurendada tema antavat lisandväärtust ELile, liikmesriikidele, kodanikele ja ettevõtetele, võimendades tema pädevusi ja sünergiaid ELi ja liikmesriikide muude institutsioonide, asutuste ja organite tööga, nagu näiteks CERT-EU, küberkuritegevuse vastase võitluse Euroopa keskus ja Euroopa Kaitseagentuur. ENISA-le tuleks anda rohkem otsest vastutust küberjulgeolekualase koolituse ja teadlikkuse suurendamise programmide eest, mis on eelkõige suunatud kodanikele ja VKE-dele.

4.3. Kui küberkuritegevusevastase võitluse Euroopa keskus (EC3) 2013. aastal loodi, oli selle tegevuseelarve 7 miljonit eurot, mis on vähem kui 10 % kogu Europoli eelarvest (Euroopa Komisjoni teabekiri 13/6, 9.1.2012). 2014. aastal ütles EC3 direktor, et kärped on tõsiselt piiranud tema üksusele eraldatud vahendeid ning nad heitlevad selle nimel, et olla kursis kiirelt arenevate küberkuritegevuse ohtudega (*Security Magazine*, 1.11.2014). Komitee leiab, et Europolile küberkuritegevuse vastu võitlemiseks eraldatavaid vahendeid tuleb oluliselt suurendada, et pidada sammu areneva ohuga. Europoli 2016. aasta eelarve on ikka vaid 100 miljonit eurot ([4]).

4.4. Komitee tervitab küberjulgeoleku direktiivi meetmeid ja teatises esitatud tegevusi, mille eesmärk on parandada küberjulgeolekualast koostööd liikmesriikide vahel. Kõigi kodanike turvalisuse ja hea kübervastupidavusvõime saavutamiseks kogu ELis, kus elutähtsa taristu infosüsteemid on sageli omavahel ühendatud, on oluline, et koostöömeetmed on suunatud riikidevahelisele suurenevale lõhele kõige paremini arenenud küberjulgeolekualaste pädevustega liikmesriikide ja nende liikmesriikide vahel, kelle oskused on vähem arenenud.

Brüssel, 14. detsember 2016

Euroopa Majandus- ja Sotsiaalkomitee
president
Georges DASSIS

([4]) ELT C 113, 30.3.2016, lk 144.