Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Ettepanek: Euroopa Parlamendi ja nõukogu määrus Euroopa Võrgu- ja Infoturbeameti (ENISA) kohta"

KOM(2010) 521 lõplik

(2011/C 107/12)

Raportöör: **Peter MORGAN**

19. oktoobril 2010 otsustas nõukogu vastavalt Euroopa Liidu toimimise lepingu artiklile 114 konsulteerida Euroopa Majandus- ja Sotsiaalkomiteega järgmises küsimuses:

„*Ettepanek: Euroopa Parlamendi ja nõukogu määrus Euroopa Võrgu- ja Infoturbeameti (ENISA) kohta*"

KOM(2010) 521 lõplik.

Asjaomase töö ettevalmistamise eest vastutav transpordi, energeetika, infrastruktuuri ja infoühiskonna sektsioon võttis arvamuse vastu 2. veebruaril 2011.

Euroopa Majandus- ja Sotsiaalkomitee võttis täiskogu 469. istungjärgul 16.–17. veebruaril 2011 (17. veebruari istungil) vastu järgmise arvamuse. Poolt hääletas 173, erapooletuks jäi 5.

1. **Järeldused ja soovitused**

1.1 Komitee on väga teadlik sellest, kuivõrd suures ulatuses sõltub kodanikuühiskond praegu interneti kaudu pakutavatest teenustest. Samuti on komitee mures kodanikuühiskonna suhtelise teadmatuse pärast küberturbest. Komitee arvates on Euroopa Võrgu- ja Infoturbeamet (ENISA) see asutus, mis vastutab liikmesriikide ja teenuseosutajate abistamise eest nende üldiste turbestandardite tõstmisel nii, et kõik internetikasutajad võtavad meetmeid, mis on vajalikud nende isikliku küberturbe tagamiseks.

1.2 Seega toetab komitee ettepanekut arendada ENISAt eesmärgiga edendada kõrgetasemelist võrgu- ja infoturvet Euroopa Liidus, suurendada teadlikkust ning luua ühiskonnas ELi kodanike, tarbijate, ettevõtete ja avaliku sektori organisatsioonide jaoks võrgu- ja infoturbe kultuur, aidates sellega kaasa siseturu sujuvale toimimisele.

1.3 ENISA ülesanne on väga oluline ELi valitsus-, tööstus- ja kaubandussektori ning kodanikuühiskonna võrguinfrastruktuuri turvaliseks arenguks. Komitee eeldab, et Euroopa Komisjon seab ENISA jaoks kõrgeimad tulemuslikkusstandardid ning jälgib selle tulemuslikkust küberturbega seotud arenevate ja üha uute ohtude kontekstis.

1.4 Kõik NATO, Europoli ja Euroopa Komisjoni koostatud küberstrateegiad sõltuvad tulemuslikust koostööst liikmesriikidega, kellel on endal rohkelt riigisiseseid küberturbe küsimustega tegelevaid asutusi. NATO ja Europoli strateegiad on kavandatud ennetavate ja praktilistena. Euroopa Komisjoni strateegias on ENISA selgelt oluline osa elutähtsa sideinfrastruktuuri kaitsega tegelevate arvukate asutuste keerukast kogumist. Kuigi uues määruses ei anta ENISA-le operatiivrolli, näeb komitee ENISAt siiski ametina, millel on peamine vastutus ELi kodanikuühiskonna elutähtsa sideinfrastruktuuri kaitse eest.

1.5 Praktiline vastutus küberturbe eest liikmesriikide tasandil lasub liikmesriikidel, kuid elutähtsa sideinfrastruktuuri kaitse standardid on 27 liikmesriigis selgelt erinevad. ENISA ülesanne on aidata väiksema valmisolekuga liikmesriikidel saavutada vastuvõetav turbetase. ENISA peab tagama liikmesriikide koostöö ning aitama neid hea tava rakendamisel. Seoses piiriüleste ohtudega peab ENISA-l olema hoiatav ja ennetav roll.

1.6 Samuti tuleb ENISA kaasata kolmandate riikidega tehtavasse rahvusvahelisse koostöösse. Selline koostöö on väga poliitiline, hõlmates paljusid ELi allüksusi, kuid komitee arvates peab ENISA leidma koha rahvusvahelisel areenil.

1.7 Komitee leiab, et ENISA saab täita väga väärtuslikku rolli turbevaldkonna uurimisprojektide käivitamisel ja neis osalemisel.

1.8 Mõjuhindamise raamistikus ei toeta komitee praegusel hetkel 4. ja 5. valikuvõimaluse täiemahulist rakendamist, mis teeks ENISAst operatiivasutuse. Küberturve on tohutult mahukas probleemivaldkond, kus ilmnevad pidevalt uued ohud, ning liikmesriikidel peab säilima võime neile ennetavalt reageerida. ELi

operatiivasutuste väljaarendamine lõpeb tavaliselt oskuste vähenemisega liikmesriikides. Küberturbe valdkonnas on olukord vastupidine – liikmesriikide pädevust tuleb suurendada.

1.9 Komitee mõistab komisjoni seisukohta, et ENISA-l peaksid olema määratletud ja hästi kontrollitud ülesanded koos neile vastavate vahenditega. Siiski on komitee mures selle pärast, et ENISA volituste kehtivusaja piiramine viie aastaga võib takistada pikaajalisi projekte ning ohustada inimkapitali ja teadmiste arengut ameti sees. ENISA on üsna väike asutus, mis tegeleb suure ja kasvava probleemiga. ENISA ülesannete ulatus tähendab seda, et asutus peab kasutama eksperdirühmi. Ameti töö on mitmekesine: ta tegeleb nii lühiajaliste ülesannete kui ka pikaajaliste projektidega. Seda arvestades eelistaks komitee, et ENISA volitused oleksid dünaamilised ja tähtajatud ning neid kinnitataks jooksvalt perioodiliste hindamiste alusel. Sel juhul võiks vahendeid eraldada järk-järgult ja vastavalt vajadusele.

2. **Sissejuhatus**

2.1 Käesolevas arvamuses käsitletakse määrust ENISA edasise arendamise kohta.

2.2 Komisjon esitas oma esimese ettepaneku võrgu- ja infoturbe küsimuste puhul kasutatava poliitilise lähenemisviisi kohta 2001. aasta teatises (KOM(2001) 298 lõplik). Vastuseks teatisele koostas Daniel Retureau põhjaliku arvamuse ([1]).

2.3 Seejärel esitas komisjon määruse ettepaneku ENISA loomiseks (KOM(2003) 63 lõplik). Komitee arvamuse ([2]) kõnealuse määruse kohta koostas Göran Lagerholm. Asutus loodigi määrusega (EÜ) nr 460/2004.

2.4 Koos internetikasutuse märkimisväärse kasvuga muutusid infoturbe küsimused üha suuremaks probleemiks. 2006. aastal avaldatud teatises (KOM(2006) 251 lõplik) esitas komisjon turvalise infoühiskonna strateegia. Komitee arvamuse selle teatise kohta koostas Antonello Pezzini ([3]).

2.5 Infoturbega seotud mure kasvades esitas komisjon 2009. aastal ettepaneku elutähtsa sideinfrastruktuuri kaitse kohta (KOM(2009) 149 lõplik). Thomas McDonogh koostas ettepaneku kohta arvamuse, ([4]) mis kiideti heaks komitee täiskogu 2009. aasta detsembri istungjärgul.

([1]) EÜT C 48, 21.2.2002, lk 33.
([2]) ELT C 220, 16.9.2003, lk 33.
([3]) ELT C 97, 28.4.2007, lk 21.
([4]) ELT C 255, 22.9.2010, lk 98.

2.6 Nüüd on tehtud ettepanek tugevdada ja täiustada ENISAt, et edendada kõrgetasemelist võrgu- ja infoturvet ELis, suurendada teadlikkust ning luua ühiskonnas ELi kodanike, tarbijate, ettevõtete ja avaliku sektori organisatsioonide jaoks võrgu- ja infoturbe kultuur, aidates sellega kaasa siseturu sujuvale toimimisele.

2.7 Siiski ei ole ENISA ainus ELi küberruumi jaoks kavandatud julgeolekuasutus. Küberrünnakutele ja küberterrorismile reageerimine on sõjaväe ülesanne. Kõnealuses valdkonnas on peamine organisatsioon NATO. Vastavalt 2010. aasta novembris Lissabonis avaldatud uuele strateegilisele kontseptsioonile (kättesaadav aadressil http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf) arendab NATO edasi võimet avastada ja tõkestada küberründeid, end nende eest kaitsta ning nende tagajärgedest taastuda, muu hulgas kasutades riikide küberkaitsevõime tõhustamiseks ja koordineerimiseks NATO planeerimisprotsessi, mis koondab kõik NATO organid keskse küberkaitse alla ning parandab küberteadlikkuse, küberrünnete eest hoiatamise ja nendele reageerimise lõimitust liikmesriikides.

2.8 Pärast 2007. aasta küberrünnakut Eesti vastu loodi 14. mail 2008 ametlikult kooperatiivse küberkaitse kompetentsikeskus, et parandada NATO küberkaitse võimet. Eesti pealinnas Tallinnas asuv keskus on rahvusvahelise jõupingutuse tulemus, mida praegu rahastavad Eesti, Läti, Leedu, Saksamaa, Ungari, Itaalia, Slovakkia ja Hispaania.

2.9 ELi tasandil toime pandud elektrooniline kuritegevus kuulub Europoli vastutusalasse. Järgnev on väljavõte Europoli poolt Ühendkuningriigi ülemkojale esitatud kirjalikust tõendist (vt http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm):

On selge, et õiguskaitseorganid peavad pidama sammu kurjategijate käsutuses oleva tehnoloogia arenguga, tagamaks, et toimepandud kuritegusid on võimalik tulemuslikult ennetada või avastada. Lisaks, arvestades, et kõrgtehnoloogia ei tunne piire, peab tehnilise võimekuse standard kogu ELis olema ühtlaselt kõrge, vältimaks nõrkade kohtade teket, kus kõrgtehnoloogiline kuritegevus saab karistamatult lokata. See suutlikkus ei ole ELis kaugeltki ühtlane. Tegelikult on areng selgelt asümmeetriline; mõned liikmesriigid liiguvad edasi, tehes teatud valdkondades suuri edusamme, samas kui teised jäävad neist tehnoloogia osas maha. See loob vajaduse tsentraliseeritud teenuse järele, mille kaudu aidata kõigil liikmesriikidel koordineerida ühist tegevust, edendada lähenemisviiside ja kvaliteedistandardite standardimist ning teha kindlaks hea tava ja seda tutvustada; ainult nii on võimalik tagada ELi õiguskaitseorganite ühtlaselt jõuline tegevus kõrgtehnoloogilise kuritegevusega võitlemisel.

2.10 Kõrgtehnoloogilise kuritegevuse keskus loodi Europoli juures 2002. aastal. See on suhteliselt väike üksus, kuid peaks tulevikus kasvama kui Europoli kõnealuses valdkonnas tehtava töö keskpunkt. Kõrgtehnoloogilise kuritegevuse keskusel on suur roll kooskõlastamisel, praktilisel toetusel, strateegilisel analüüsil ja koolituses. Eriti tähtis on koolituse funktsioon. Lisaks on Europol loonud Euroopa küberkuritegevuse vastase platvormi. See keskendub järgmistele teemadele:

— internetikuritegevusest teatamise sidussüsteem (I-CROS);

— analüüsifail (Cyborg);

— interneti- ja kriminalistika eksperdifoorum (I-FOREX).

2.11 ELi küberjulgeoleku strateegia on esitatud Euroopa digitaalse tegevuskava peatükis „Usaldus ja turvalisus". Väljakutsed on määratletud järgmiselt:

Siiani on internet olnud äärmiselt turvaline, vastupidav ja stabiilne, kuid IT-võrgud ja lõppkasutajate terminalid on jätkuvalt haavatavad terve hulga ohtude tõttu: viimastel aastatel on rämpsposti hulk kasvanud sellise määrani, et ummistab elektronpostivahetust internetis (eri allikate järgi on 80 % kuni 98 % kõikidest e-kirjadest rämpspost), ning sel teel levivad viirused ja kurivara. Kasvavaks probleemiks on identiteedivargus ja võrgupettused. Rünnakud muutuvad üha keerukamaks (Trooja hobused, robotivõrgud jne) ja sageli püütakse nende abil saada finantskasu. Hiljutised Eesti, Leedu ja Gruusia vastu suunatud küberrünnakud näitasid, et need võivad olla ka poliitilist laadi.

2.12 Tegevuskavas loetletud komisjoni lubatud meetmed on järgmised:

6. põhimeede: esitab 2010. aastal meetmed, mille eesmärk on **tõhusam ja kõrgetasemeline võrgu- ja infoturbepoliitika**, sealhulgas seadusandlikud algatused, mis käsitlevad Euroopa Võrgu- ja Infoturbeameti (ENISA) ajakohastamist, ja meetmed, mis võimaldavad küberrünnakute korral kiiremini reageerida, sh CERT ja ELi institutsioonid;

7. põhimeede: esitab 2010. aastaks meetmed, sealhulgas seadusandlikud algatused, **infosüsteemide vastu suunatud küberrünnakutega võitlemiseks**, ja 2013. aastaks küberruumi käsitleva kohtualluvuse eeskirjad nii Euroopa kui ka rahvusvahelisel tasandil.

2.13 2010. aasta novembri teatises (KOM(2010) 673 lõplik) arendas komisjon tegevuskava edasi, esitades ELi sisejulgeoleku strateegia. Strateegial on viis eesmärki ja kolmas neist on tõsta kodanike ja ettevõtjate jaoks turvalisuse taset küberruumis. Tabelis antakse ülevaade kolmest tegevuskavast ning esitatakse meetmete üksikasjad (allikas: KOM(2010) 673 lõplik; kättesaadav aadressil: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:ET:pdf)

EESMÄRGID JA MEETMED	VASTUTAJA	AJAKAVA
EESMÄRK 3: tõsta küberruumis kodanike ja ettevõtjate jaoks turvalisuse taset		
Meede 1: suurendada õiguskaitseasutuste ja kohtute suutlikkust		
ELi küberkuritegevuse keskuse loomine	Sõltub KOMi 2011. aasta teostatavusuuringust	2013
Luua suutlikkus küberkuritegude uurimiseks ja nende eest süüdistuse esitamiseks	LR koos Euroopa Politseikolledži, Europoli ja Eurojustiga	2013
Meede 2: teha koostööd tööstussektoriga, et anda kodanikele paremad võimalused ja neid kaitsta		
Küberkuritegevuse juhtudest teatamise korra loomine ja kodanikele küberturbe- ja küberkuritegevusealase nõustamise pakkumine	LR, KOM, Europol, **ENISA** ja erasektor	Pidev
Suunised ebaseadusliku internetisisu käsitamisel tehtava koostöö kohta	KOM koos LRi ja erasektoriga	2011
Meede 3: parandada võimet tulla toime küberrünnakutega		
Võrgustiku loomine infoturbeintsidentidega tegelevatest rühmadest igas liikmesriigis ja ühes ELi institutsioonis, samuti korrapäraste riiklike situatsiooniplaanide koostamine ning juhtumitele reageerimise ja katastroofijärgse taastamise harjutamine	LR ja ELi institutsioon koos **ENISA** ga	2012
Euroopa teabe jagamise ja hoiatussüsteemi (EISAS) loomine	LR koos KOMi ja **ENISA** ga	2013

2.14 Kõik NATO, Europoli ja Euroopa Komisjoni koostatud küberstrateegiad sõltuvad tulemuslikust koostööst liikmesriikidega, kellel on endal rohkelt riigisiseseid küberturbe küsimustega tegelevaid asutusi. NATO ja Europoli strateegiad on kavandatud ennetavate ja praktilistena. Euroopa Komisjoni strateegias on ENISA selgelt oluline osa elutähtsa sideinfrastruktuuri kaitsega tegelevate arvukate asutuste keerukast kogumist. Kuigi uues määruses ei anta ENISA-le operatiivrolli, näeb komitee ENISAt siiski ametina, millel on peamine vastutus ELi kodanikuühiskonna elutähtsa sideinfrastruktuuri kaitse eest.

3. **ENISAt käsitlev ettepanek**

3.1 Probleemil, mida ENISA peab aitama lahendada, on seitse tahku:

(1) riiklike lähenemisviiside erinevus ja mitmekesisus;

(2) varajase hoiatamise ja reageerimise piiratud võime Euroopas;

(3) usaldusväärsete andmete puudumine ja piiratud teadmised üha keerukamatest probleemidest;

(4) vähene teadlikkus võrgu- ja infoturberiskidest ja -probleemidest;

(5) võrgu-ja infoturbe probleemide rahvusvaheline mõõde;

(6) vajadus koostöömudelite järele poliitika asjakohase rakendamise tagamiseks;

(7) vajadus tõhusamate küberkuritegevuse vastaste meetmete järele.

3.2 ENISAt käsitlev ettepanek on kesksel kohal nii olemasolevat poliitikat puudutavate sätete kui ka ELi digitaalses tegevuskavas esitatud uute algatuste jaoks.

3.3 Olemasolevad poliitikasuunad, mida ENISA peab toetama, on järgmised:

(i) Euroopa liikmesriikide foorum (EFMS – *European Forum of Member States*), et soodustada arutelu heade poliitiliste tavade üle ja nende levitamist eesmärgiga võtta IKT-infrastruktuuri turvalisuse ja vastupidavuse valdkonnas vastu ühised poliitilised eesmärgid ja prioriteedid;

(ii) vastupidavust käsitlev Euroopa avaliku ja erasektori partnerlus (EP3R), mis on üleeuroopaline paindlik juhtimisraamistik IKT-infrastruktuuri vastupidavuse tagamiseks ning mis soodustab avaliku ja erasektori koostööd turvalisuse ja vastupidavuse küsimuste valdkonnas;

(iii) Euroopa Ülemkogul 11. detsembril 2009 vastu võetud Stockholmi programm, edendamaks poliitikameetmeid, millega tagatakse võrguturve ning mis võimaldavad küberrünnakute korral ELis kiiremini reageerida.

3.4 Uued poliitikasuunad, mida ENISA peab toetama, on järgmised:

(i) Euroopa liikmesriikide foorumi tegevuse intensiivistamine;

(ii) vastupidavust käsitleva Euroopa avaliku ja erasektori partnerluse (EP3R) toetamine, arutades uuendusmeetmeid ja -vahendeid turvalisuse ja vastupidavuse parandamiseks;

(iii) elektroonilist sidet reguleeriva raamistiku turbenõuete praktikas rakendamine;

(iv) kogu ELi hõlmavate küberturbe valmisolekuõppuste toetamine;

(v) ELi institutsioonide jaoks infoturbeintsidentidega tegelevate rühmade (CERT – *Computer Emergency Response Team*) asutamine;

(vi) liikmesriikide mobiliseerimine ja toetamine riikide või valitsuste CERTide koostamisel ja vajaduse korral asutamisel, et luua hästi toimiv CERTide võrgustik, mis katab kogu Euroopat;

(vii) võrgu- ja infoturbeprobleemidest teadlikkuse tõstmine.

3.5 Enne kõnealuse ettepaneku esitamist analüüsiti viit erinevat poliitikavalikut. Iga valikuvõimalusega seondusid valikud ülesannete ja vahendite osas. Valiti kolmas valikuvõimalus. See tähendab ENISA ülesannete laiendamist, lisades sidusrühmadena õiguskaitseasutused ja eraelu puutumatuse kaitse asutused.

3.6 Vastavalt 3. valikuvõimalusele annaks ajakohastatud võrgu- ja infoturbeamet oma panuse järgmistes valdkondades:

— riiklike lähenemisviiside erinevuse vähendamine (probleemi esimene tahk), andmetel ja teadmistel/teabel põhineva poliitika ja otsustamise osakaalu suurendamine (probleemi kolmas tahk) ning üldise teadlikkuse tõstmine võrgu- ja infoturbe ohtude ja probleemidega võitlemisest (probleemi neljas tahk), aidates kaasa järgmiste aspektide saavutamisele:

  — tõhusam asjakohase teabe kogumine iga liikmesriigi riskide, ohtude ja puuduste kohta;

  — teabe parem kättesaadavus võrgu- ja infoturbega seotud praeguste ning tulevaste probleemide ja ohtude kohta;

  — võrgu- ja infoturbe poliitika kujundamise kõrgem kvaliteet liikmesriikides;

— varajase hoiatamise ja reageerimise võime parandamine Euroopas (probleemi teine tahk) järgmiste meetmete kaudu:

  — komisjoni ja liikmesriikide aitamine üleeuroopaliste õppuste korraldamisel, saavutades sellega mastaabisäästu kogu ELi hõlmavatele juhtumitele reageerimisel;

  — vastupidavust käsitleva Euroopa avaliku ja erasektori partnerluse toimimise soodustamine, mis võib lõppkokkuvõttes viia suuremate investeeringuteni, mille käivitajaks on ühised poliitilised eesmärgid ja kogu ELi hõlmavad turbe- ja vastupidavuse standardid;

— ühise ülemaailmse lähenemisviisi edendamine võrgu- ja infoturbe küsimustes (probleemi viies tahk) järgmise meetme kaudu:

  — teabe ja teadmiste vahetuse suurendamine kolmandate riikidega;

— tõhusam ja tulemuslikum küberkuritegevuse vastu võitlemine (probleemi seitsmes tahk) järgmise meetme kaudu:

  — osalemine õiguskaitseorganite ja kohtute vahelise koostöö võrgu- ja infoturbe aspektidega seotud mitteoperatiivsete ülesannete täitmises, näiteks kahesuunalises teabevahetuses ja koolituses (nt koostöös Euroopa Politseikolledžiga).

3.7 Vastavalt 3. valikuvõimalusele oleksid ENISA käsutuses kõik vahendid, mis on vajalikud ENISA ülesannete piisavalt põhjalikuks täitmiseks, s.o võimaldades sel avaldada tegelikku mõju. Suuremate ressursside olemasolu korral ([5]) saab ENISA võtta palju proaktiivsema rolli ning teha algatusi sidusrühmade aktiivse osalemise stimuleerimiseks. Lisaks sellele võimaldaks see uus olukord suuremat paindlikkust, et kiiresti reageerida pidevalt areneva võrgu- ja infoturbe keskkonna muutustele.

3.8 4. valikuvõimalus sisaldab ka operatiivülesandeid küberrünnakute vastu võitlemisel ja küberjuhtumitele reageerimisel. Lisaks eespool kirjeldatud tegevusele oleksid ametil ka operatiivülesanded, nagu aktiivsem roll ELi elutähtsa sideinfrastruktuuri kaitsel, nt juhtumite ennetamisel ja neile reageerimisel, tegutsedes konkreetselt kui ELi infoturbeintsidentidega tegelev rühm ning kooskõlastades ELi võrgu- ja infoturbe hädaabikeskusena liikmesriikide infoturbeintsidentidega tegelevate rühmade tööd, sh nii igapäevast juhtimist kui ka hädaabiteenuste osutamist.

3.9 4. valikuvõimalus avaldaks operatiivtasandil suuremat mõju – seda lisaks mõjule, mis saavutataks vastavalt 3. valikuvõimalusele. Tegutsedes ELi võrgu- ja infoturbe infoturbeintsidentidega tegeleva rühmana ja kooskõlastades riiklike infoturbeintsidentidega tegelevate rühmade tegevust, aitaks amet saavutada suuremat mastaabisäästu kogu ELi hõlmavatele juhtumitele reageerimisel ning vähendada näiteks kõrgemast infoturbe ja vastupidavuse tasemest tulenevaid tegevusriske ettevõtjate jaoks. 4. valikuvõimalus nõuaks ameti eelarve ja inimressursside olulist suurendamist, mis tekitab küsimusi selle vastuvõtusuutlikkuse ja eelarve tulemusliku kasutamise võime suhtes võrreldes saadava kasuga.

3.10 5. valikuvõimalus sisaldab operatiivülesandeid õiguskaitseasutuste ja kohtute toetamiseks küberkuritegevuse vastu võitlemisel. Lisaks neljandas valikuvõimaluses loetletud tegevustele võimaldaks kõnealune valikuvõimalus ENISA-l

— pakkuda toetust menetlusõiguse alusel (vrd küberkuritegevuse konventsioon): näiteks võrguliikluse kohta andmete kogumine, sisuandmete kinnipüüdmine, liikluse jälgimine teenust tõkestavate rünnakute korral;

— toimida kriminaaluurimise eksperdikeskusena, sh võrgu- ja infoturbe seisukohalt.

3.11 5. valikuvõimalus oleks 3. ja 4. valikuvõimalusega võrreldes küberkuritegevusega võitlemisel tõhusam, kuna lisanduksid operatiivülesanded ning õiguskaitseorganite ja kohtute toetamine.

3.12 5. valikuvõimalus eeldaks ameti ressursside olulist suurendamist ning tekitaks taas küsimusi ameti vastuvõtusuutlikkuse ja eelarve tulemusliku kasutamise võime kohta.

3.13 Ehkki nii 4. kui ka 5. valikuvõimalusega saavutataks 3. valikuvõimalusega võrreldes suurem positiivne mõju, leiab komisjon, et on mitu põhjust neist valikutest loobumiseks.

— Seoses liikmesriikide elutähtsa sideinfrastruktuuri kaitse pädevusega oleks tegemist liikmesriikide jaoks poliitiliselt tundlike lahendustega (st mitmed liikmesriigid ei pooldaks operatiivülesannete tsentraliseerimist).

— Volituste laiendamine vastavalt 4. ja 5. valikuvõimalusele võib muuta ameti staatuse ebaselgeks.

— Nende uute ja täiesti erinevate operatiivülesannete lisamine asutuse pädevusvaldkonda võib olla lühikeses perspektiivis väga raske ning on märkimisväärne oht, et amet ei suuda mõistliku aja jooksul selliseid ülesandeid nõuetekohaselt täitma asuda.

— Sama oluline on ka asjaolu, et 4. ja 5. valikuvõimaluse rakendamise kulud on liiga suured. Selleks vajalik eelarve ületaks ENISA praegust eelarvet nelja- kuni viiekordselt.

([5]) Viide enamatele vahenditele sõltub ENISAt käsitleva ettepaneku vastuvõtmisest selle praegusel kujul.

4. **Määruse sätted**

4.1 Amet aitab komisjonil ja liikmesriikidel vastata õiguslikele ja regulatiivsetele võrgu- ja infoturbenõuetele.

4.2 Juhatus määratleb ameti tegevuse üldise suuna.

4.3 Juhatusse kuulub igast liikmesriigist üks esindaja, komisjoni poolt määratud kolm esindajat ning üks info- ja kommunikatsioonitehnoloogiatööstuse, üks tarbijarühmade ja üks akadeemiliste võrgu- ja infoturbe ekspertide esindaja.

4.4 Ametit juhib sõltumatu tegevdirektor, kes vastutab ameti tööprogrammi koostamise eest, mille juhatus peab heaks kiitma.

4.5 Tegevdirektor vastutab ka tööprogrammi toetava aasta-eelarve koostamise eest. Juhatus peab esitama nii eelarve kui ka tööprogrammi komisjonile ja liikmesriikidele heakskiitmiseks.

4.6 Juhatus asutab tegevdirektori ettepanekul alalise sidusrühma, millesse kuuluvad IKT-tööstust, tarbijarühmi, ülikoole, õiguskaitseasutusi ja eraelu puutumatuse kaitse asutusi esindavad eksperdid.

4.7 Kuna määrus on alles ettepaneku etapis, siis valitseb arvude osas teatud ebakindlus. Praegu on ametile ette nähtud 44–50 töötajat ja eelarve maht on 8 miljonit eurot. 3. valikuvõimaluse kontseptsiooni järgimine võiks tähendada 99 töötajat ja eelarvet mahuga 17 miljonit eurot.

4.8 Määruses tehakse ettepanek kinnitada volituste kehtivusajaks viis aastat.

Brüssel, 17. veebruar 2011

Euroopa Majandus- ja Sotsiaalkomitee president

Staffan NILSSON