EUROOPA
KOMISJON

EUROOPA LIIDU VÄLISASJADE
JA JULGEOLEKUPOLIITIKA
KÕRGE ESINDAJA

Brüssel, 7.2.2013
JOIN(2013) 1 final

ÜHISTEATIS EUROOPA PARLAMENDILE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE

Euroopa Liidu küberjulgeoleku strateegia:

avatud, ohutu ja turvaline küberruum

ÜHISTEATIS EUROOPA PARLAMENDILE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE

Euroopa Liidu küberjulgeoleku strateegia:

avatud, ohutu ja turvaline küberruum

1. SISSEJUHATUS

1.1. Taust

Viimase kahekümne aasta jooksul on internet ja laiemalt küberruum avaldanud tohutut mõju ühiskonna kõikidele osadele. Meie igapäevaelu, põhiõigused, sotsiaalsed suhted ja majandus sõltuvad info- ja kommunikatsioonitehnoloogia (IKT) sujuvast toimimisest. Avatud ja vaba küberruum on edendanud üleilmset poliitilist ja sotsiaalset kaasatust; see on kõrvaldanud riikide, ühiskondade ja kodanike vahelised tõkked, võimaldades suhelda ning jagada teavet ja ideid üle laia ilma; see on loonud keskkonna, kus ennast vabalt väljendada ja oma põhiõigusi teostada ning on andnud inimestele vahendid, mille abil püüelda demokraatliku ja õiglasema ühiskonna poole – eriti selgelt oli seda näha araabia kevade ajal.

Selleks, et küberruum jääks avatuks ja vabaks, tuleks ka internetis kohaldada samu norme, põhimõtteid ja väärtusi, mille austamist toetab EL reaalses maailmas. Põhiõigusi, demokraatiat ja õigusriigi põhimõtet tuleb kaitsta ka küberruumis. Meie vabadus ja heaolu sõltuvad üha rohkem töökindlast ja uuenduslikust internetist, mille areng jätkub siis, kui seda soodustavad erasektori uuendustegevus ja kodanikuühiskond. Kuid ka internetivabaduse eeldusteks on ohutus ja turvalisus. Küberruumi tuleks kaitsta intsidentide, pahatahtliku tegevuse ja väärkasutuse eest ning valitsustel on täita märkimisväärne roll seoses vaba ja ohutu küberruumi tagamisega. Valitustel tuleb täita mitu ülesannet: kaitsta juurdepääsu ja avatust, austada ja kaitsta internetis põhiõigusi ning tagada interneti usaldusväärsus ja koostalitlusvõime. Kuna aga märkimisväärset osa küberruumist omab ja haldab erasektor, tuleks mis tahes valdkondlikes algatustes edu saavutamiseks tunnustada erasektori juhtrolli.

IKTst on saanud majanduskasvu alustala ning see on otsustava tähtsusega ressurss, millest sõltuvad kõik majandussektorid. IKT-l põhinevad keerukad süsteemid, mis tagavad majanduse toimimise võtmetähtsusega sektorites nagu rahandus, tervishoid, energeetika ja transport. Paljud ärimudelid tuginevad interneti katkematule kättesaadavusele ning infosüsteemide tõrgeteta toimimisele.

Digitaalse ühtse turu lõplik väljakujundamine võiks suurendada Euroopa SKPd ligikaudu 500 miljardi euro võrra aastas[1] ehk keskmiselt 1 000 euro võrra inimese kohta. Selleks et leiaksid kasutust uued võrgutehnoloogiad, sealhulgas e-maksed, pilvandmetöötlus või masinatevaheline andmevahetus,[2] on tarvis kodanike usaldust. Kahjuks ilmnes 2012. aasta Eurobaromeetri uuringust,[3] et ligikaudu kolmandik eurooplasi kahtleb oma oskustes kasutada internetti panganduseks või ostude tegemiseks. Suur enamik vastanutest väldib isikuandmete avaldamist võrgus, kuna tunneb muret turvalisuse pärast. Võrgupettuse ohvriks on ELis langenud juba üle kümne protsendi internetikasutajatest.

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf.

[2] Näiteks taimedele paigutatavad sensorid, mis teavitavad sprinklersüsteemi, kui taimed vajavad kastmist.

[3] Küberturvet käsitlev 2012. aasta Eurobaromeetri eriuuring 390.

Viimased aastad on näidanud, et kuigi digitaalmaailm toob suurt kasu, on see ka haavatav. Küberjulgeolekut[4] kahjustavate tahtlike või juhuslike turvaintsidentide arv kasvab hirmuäratava kiirusega ning need võivad häirida esmatähtsate ja endastmõistetavaks peetavate teenuste (nt veevarustus-, tervishoiu-, elektri- või mobiilsideteenused) osutamist. Ohud võivad olla eri päritolu – ajend võib olla näiteks kuritegelik või poliitiline või tegemist võib olla terrorirünnaku või mõne riigi mahitatud rünnakuga, samuti loodusõnnetuste või tahtmatu veaga.

ELi majandus kannatab juba praegu erasektori ja üksikisikute vastu suunatud küberkuritegevuse[5] all. Küberkurjategijad kasutavad üha keerukamaid meetodeid infosüsteemidesse sissetungimiseks, oluliste andmete varastamiseks või ettevõtetelt lunaraha nõudmiseks. Asjaolu, et suurenenud on nii majandusspionaaž kui ka riikide rahastatav tegevus küberruumis, tekitab ELi valitsuste ja ettevõtete jaoks uue ohukategooria.

ELi mittekuuluvates riikides võib ette tulla ka küberruumi väärkasutust, et oma kodanike järele valvata või neid kontrollida. EL saab sellisele tegevusele vastu seista internetivabaduse edendamisega ning põhiõiguste austamise tagamisega internetis.

See kõik on põhjuseks, miks valitsused on kogu maailmas asunud välja töötama küberjulgeoleku strateegiaid ning käsitavad küberruumi aina olulisema rahvusvahelise küsimusena. On aeg, et EL tõhustaks oma sellekohaseid meetmeid. Käesolevas ettepanekus Euroopa Liidu küberjulgeoleku strateegia kohta, mille esitajateks on komisjon ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja (kõrge esindaja), visandatakse ELi valdkondlik nägemus, selgitatakse ülesandeid ja vastutusalasid ning kehtestatakse vajalikud meetmed. Seejuures tuginetakse kodanike õiguste tugevale ja tõhusale kaitsele ja edendamisele, et muuta ELi veebikeskkond maailma ohutuimaks.

1.2. Küberjulgeoleku põhimõtted

Piirideta ja mitmekihilisest internetist on saanud üleilmse edu saavutamise üks olulisimaid vahendeid, mis ei ole valitsuste järelevalve all ega selle poolt reguleeritav. Kuigi erasektor peaks etendama jätkuvalt juhtivat osa interneti ülesehitamisel ja igapäevasel juhtimisel, on aina selgemaks saanud vajadus läbipaistvuse, vastutuse ja turvalisusega seotud nõuete järele. Käesolevas strateegias täpsustatakse põhimõtteid, millele peaks tuginema nii ELi kui ka rahvusvaheline küberjulgeolekupoliitika.

ELi põhiväärtused kehtivad nii digitaalses kui ka füüsilises maailmas

Igapäevaelu valdkondades kohaldatavad õigusnormid ja eeskirjad peaksid kehtima ka kübervaldkonna puhul.

---

[4] Küberjulgeolek viitab tavaliselt kaitse- ja muudele meetmetele, mida saab nii tsiviil- kui ka sõjalises valdkonnas kasutada küberruumi kaitsmiseks ohtude eest, mis seonduvad selle üksteisest sõltuvate võrkudega ja infotaristuga või võivad neid kahjustada. Küberjulgeoleku eesmärk on tagada võrkude ja taristu käideldavus ja terviklus ning neis sisalduva teabe konfidentsiaalsus.

[5] Küberkuritegevus viitab tavaliselt suurele hulgale erinevatele kuritegudele, mille puhul on arvutid ja infosüsteemid kas põhivahendiks või põhiliseks sihtmärgiks. Küberkuritegevus hõlmab tavapäraseid süütegusid (nt pettus, võltsimine ja identiteedivargus), infosisuga seotud õigusrikkumisi (nt lapsporno levitamine internetis või rassiviha õhutamine) ning üksnes arvutite ja infosüsteemiga seotud süütegusid (nt infosüsteemide vastu suunatud ründed, teenusetõkestamine, pahavara).

Põhiõiguste, sõnavabaduse, isikuandmete ja eraelu puutumatuse kaitse

Küberjulgeoleku kindlaks ja tulemuslikuks toimimiseks peaks see põhinema Euroopa Liidu põhiõiguste hartas sätestatud põhiõigustel ja ELi põhiväärtustel. Niisamuti ei saa üksikisikute õigusi tagada ilma ohutute võrkude ja süsteemideta. Juhul kui tegemist on isikuandmetega, peaks küberjulgeoleku eesmärgil toimuv teabejagamine toimuma kooskõlas ELi andmekaitseõigusega ning selle puhul tuleb täiel määral arvestada selles valdkonnas kehtivaid üksikisikute õigusi.

Kõigile tagatud juurdepääs

Arvestades seda, kui tihedalt on digimaailm ühiskonnaga põimunud, asetab piiratud juurdepääs või juurdepääsu puudumine internetile ning digitaalne kirjaoskamatus kodanikud ebasoodsasse olukorda. Kõigil peaks olema juurdepääs internetile ja takistamata teabevoole. Kõigile ohutu juurdepääsu võimaldamiseks tuleks tagada interneti terviklikkus ja turvalisus.

Demokraatlik, tõhus ja paljusid sidusrühmi hõlmav haldamine

Digitaalset maailma ei kontrolli vaid üks üksus. Internetiressursside, vastavate protokollide ja standardite igapäevase haldamise ning interneti arendamisega on hetkel seotud mitmed sidusrühmad, kellest paljud on äriettevõtted ja valitsusvälised üksused. EL kinnitab veel kord, kui tähtis on kõigi sidusrühmade kaasatus interneti haldamise praegusse mudelisse ning toetab sellist paljusid sidusrühmi hõlmavat haldusstrateegiat[6].

Jagatud vastutus turvalisuse tagamiseks

Kõigi eluvaldkondade suurenev sõltuvus IKTst on tekitanud nõrkusi, mida tuleks täpselt määratleda, põhjalikult analüüsida, leevendada või vähendada. Kõik asjaosalised – riigiasutused, erasektor ja üksikisikud – peavad tunnustama jagatud vastutuse olulisust, võtma meetmeid endi kaitseks ning tagama vajaduse korral kooskõlastatud tegutsemise küberjulgeoleku tugevdamiseks.

2. STRATEEGILISED PRIORITEEDID JA MEETMED

EL peaks kaitsma veebikeskkonda, mis pakub kõigi hüvanguks suurimat võimalikku vabadust ja turvalisust. Ehkki küberruumi turvalisuse probleemidega tegelemine on peaasjalikult liikmesriikide ülesanne, pakutakse käesolevas strateegias välja konkreetsed meetmed, mis saaksid edendada ELi üldist tulemuslikkust. Kõnealuseid meetmeid on nii lühi- kui ka pikaajalisi, need hõlmavad erinevaid poliitikavahendeid[7] ning eri osapooli – ELi institutsioone, liikmesriike ja tööstust.

Käesolevas strateegias esitatud ELi nägemust väljendavad viis strateegilist prioriteeti, mis on suunatud eespool väljatoodud probleemide lahendamisele:

- küberturve;
- küberkuritegevuse radikaalne vähendamine;

[6] Vt ka KOM(2009) 277, komisjoni teatis Euroopa Parlamendile ja nõukogule „Interneti haldamine: järgmised sammud".

[7] Juhul kui tegemist on isikuandmetega, peaksid teabe jagamisega seotud meetmed olema kooskõlas ELi andmekaitseõigusega.

- küberkaitsepoliitika väljatöötamine ning ühise julgeoleku- ja kaitsepoliitika (ÜJKP) raamistikuga seonduva suutlikkuse arendamine;
- tööstuslike ja tehnoloogiliste vahendite arendamine küberjulgeoleku jaoks;
- sidusa rahvusvahelise küberruumipoliitika kehtestamine Euroopa Liidu jaoks ning ELi põhiväärtuste edendamine.

2.1. Küberturve

Selleks et edendada küberturvet ELis, peavad nii riigiasutused kui ka erasektor arendama oma sellekohast suutlikkust ning tegema tõhusat koostööd. Tuginedes seni elluviidud meetmete[8] positiivsetele tulemustele, saaksid ELi täiendavad meetmed olla abiks eelkõige piiriülese mõõtmega küberriskide ja -ohtudega toimetulekul ning koordineeritud reageerimisel hädaolukordadele. Seeläbi toetatakse tugevalt siseturu sujuvat toimimist ning parandatakse ELi sisejulgeolekut.

Kui küberjulgeolekut kahjustavate intsidentide ennetamise, avastamise ja käsitlemise nimel ei tehta ulatuslikke jõupingutusi, et tõhustada avaliku ja erasektori suutlikkust, asjaomaseid vahendeid ja protsesse, püsib Euroopa haavatavana. Sel põhjusel on komisjon töötanud välja võrgu- ja infoturbe poliitika[9]. 2004. aastal loodi **Euroopa Võrgu- ja Infoturbeamet** (**ENISA**)[10] ning nõukogus ja Euroopa Parlamendis peetakse praegu läbirääkimisi uue määruse üle, et tugevdada ENISAt ja ajakohastada selle volitusi[11]. Lisaks on elektroonilise side raamdirektiiviga[12] nõutud, et elektrooniliste sideteenuste osutajad haldaksid asjakohaselt oma võrkudega seotud riske ning teataksid olulistest turvalisuse rikkumistest. Lisaks on andmekaitset käsitlevate ELi õigusaktidega[13] nõutud, et vastutavad töötlejad tagavad andmekaitsenõuete täitmise ja kaitsemeetmete, sealhulgas turvameetmete võtmise ning teavitavad pädevaid riigiasutusi üldkasutatavate elektrooniliste sideteenustega seotud intsidentidest, millega kaasneb isikuandmete rikkumine.

Hoolimata vabatahtlike kohustustega seoses saavutatud edusammudest, esineb ELis siiski veel puudujääke, eelkõige seoses riikliku suutlikkusega, tegevuse kooskõlastamisega piiriüleste intsidentide puhul ning erasektori kaasatuse ja valmisolekuga. Käesolevale strateegiale on lisatud **õigusakti** ettepanek, et eelkõige teha järgmist:

- kehtestada riigi tasandil võrgu- ja infoturbe ühised miinimumnõuded, mis kohustaksid liikmesriike nimetama võrgu- ja infoturbe vallas riigi pädeva asutuse, looma hästitoimiva infoturbeintsidentidega tegeleva rühma (CERT) ning võtma vastu riikliku võrgu- ja infoturbe strateegia ning riikliku võrgu- ja infoturbe koostöökava. Suutlikkuse suurendamine ja tegevuse koordineerimine puudutab ka ELi institutsioone. 2012. aastal loodi alalise organina infoturbeintsidentidega tegelev rühm, mis vastutab ELi institutsioonide, asutuste ja organite IT-süsteemide turvalisuse eest („CERT-EU”);

---

8 Vt käesolevas teatises esitatud viited ning ka komisjoni talituste töödokumendi mõjuhinnang, mis on lisatud komisjoni ettepanekule võrgu- ja infoturbe direktiivi kohta, eelkõige jaotised 4.1.4, 5.2, 2. lisa, 6. lisa, 8. lisa.

9 2001. aastal võttis komisjon vastu teatise „Võrgu- ja infoturve: Euroopa lähenemisviisi ettepanek” (KOM(2011) 298); 2006. aastal võttis komisjon vastu turvalise infoühiskonna strateegia (KOM(2006) 251). 2009. aastast alates on komisjon vastu võtnud ka tegevuskava ja teatise elutähtsate infrastruktuuride kaitse kohta (KOM(2009) 149, mis kiideti heaks nõukogu resolutsiooniga 2009/C 321/01, ning KOM(2011) 163, mis kiideti heaks nõukogu järeldustega 10299/11).

10 Määrus (EÜ) nr 460/2004.

11 KOM(2010) 521. Käesolevas strateegias väljapakutud meetmeid ei hõlma ENISA kehtivate või tulevaste volituste muutmist.

12 Direktiivi 2002/21/EÜ artiklid 13a ja 13b.

13 Direktiivi 95/46/EÜ artikkel 17; direktiivi 2002/58/EÜ artikkel 4.

- luua kooskõlastatud ennetus-, avastamis-, leevendus- ja reageerimismehhanismid, mis võimaldavad võrgu- ja infoturbe valdkonna riigi pädevatel asutustel jagada teavet ja osutada vastastikust abi. Võrgu- ja infoturbe valdkonna riigi pädevate asutuste ülesanne on tagada tegevuse koordineerimine kogu ELis, eelkõige ELi võrgu- ja infoturbe koostöökava alusel, et reageerida piiriülese mõõtmega küberintsidentidele. Tegevuse koordineerimisel tuginetakse liikmesriikide Euroopa foorumi (EFMS) tööle,[14] mille raames on peetud viljakaid arutelusid ja vahetatud arvamusi riikliku võrgu- ja infoturbepoliitika kohta; pärast koostöömehhanismi loomist saab foorumi sellega liita;
- parandada erasektori valmisolekut ja suurendada selle kaasatust. Kuna suurem enamik võrgu- ja infosüsteeme on eraomandis ja eraomanike hallatavad, on küberjulgeoleku edendamiseks ülioluline tihendada koostööd erasektoriga. Erasektor peaks arendama oma tehnilist küberturbesuutlikkust ning jagama sektorite vahel parimaid tavasid. Tööstuse poolt väljatöötatud vahendid intsidentidele reageerimiseks, põhjuste tuvastamiseks ja kriminalistikaalaste uurimiste läbiviimiseks peaksid tooma kasu ka erasektorile.

Kuid erasektoril on jätkuvalt vajaka mõjusatest stiimulitest, et esitada usaldusväärseid andmeid võrgu ja info turvalisusega seotud intsidentide toimumise ja mõju kohta, võtta omaks riskihalduskultuur või investeerida turvalahendustesse. Kavandatavate õigusnormide eesmärk on seega teha kindlaks, et mitmete põhivaldkondade (energeetika, transport, pangandus, väärtpaberibörsid, võtmetähtsusega internetiteenuste võimaldajad ning ka haldusasutused) osalised hindaksid endi ees olevaid küberjulgeoleku riske, tagaksid asjakohase riskihalduse kaudu võrkude ja infosüsteemide usaldusväärsuse ja vastupidavuse ning jagaksid kindlakstehtud teavet võrgu- ja infoturbe valdkonna riigi pädevate asutustega. Küberjulgeolekukultuuri levik võiks suurendada ettevõtlusvõimalusi ning erasektori konkurentsivõimet, mistõttu võiks küberjulgeolekust saada müügiargument.

Kõnealused üksused peaksid võrgu- ja infoturbe valdkonna riigi pädevatele asutustele teatama intsidentidest, millel on oluline mõju põhiteenuste osutamise järjepidevusele ning võrgu- ja infosüsteemidel tuginevale kaupade pakkumisele.

Võrgu- ja infoturbe valdkonna riigi pädevad asutused peaksid tegema koostööd ja vahetama teavet muude reguleerivate asutustega, eelkõige isikuandmete kaitse asutustega. Kui kahtlustatakse, et intsident on seotud raske kuriteoga, peaksid võrgu- ja infoturbe valdkonna riigi pädevad asutused teatama sellest omakorda õiguskaitseasutustele. Samuti peaksid riigi pädevad asutused selleks ettenähtud veebisaidil avaldama korrapäraselt salastamata teavet intsidente ja riske käsitlevate varajaste hoiatuste ning koordineeritud reageerimise kohta. Õiguslikud kohustused ei tohiks asendada ega takistada mitteametlikku ja vabatahtlikku koostööd, sealhulgas avaliku ja erasektori vahel, eesmärgiga tõsta turvalisuse taset ning vahetada teavet ja parimaid tavasid. Vastupidavust käsitlev Euroopa avaliku ja erasektori partnerlus (EP3R)[15] on ELi tasandil iseäranis hea ja asjakohane platvorm ning seda tuleks edasi arendada.

---

[14] Liikmesriikide Euroopa foorum käivitati teatisega KOM(2009) 149, et luua platvorm liikmesriikide riigiasutuste vaheliste arutelude soodustamiseks heade poliitiliste tavade ja elutähtsate infrastruktuuride vastupidavuse vallas.

[15] Vastupidavust käsitlev Euroopa avaliku ja erasektori partnerlus loodi teatisega KOM(2009) 149. Kõnealune platvorm edendas avaliku ja erasektori koostööd vastupidavuse vallas võtmetähtsusega vara, ressursside, funktsioonide ja põhinõuete tuvastamiseks ning esitas vastavaid algatusi. Samuti keskenduti koostöövajaduste ja laiaulatuslikele, elektroonilist sidet mõjutavatele häiretele reageerimise mehhanismide väljaselgitamisele.

Euroopa ühendamise rahastu[16] tagaks rahalise toetuse võtmetähtsusega infrastruktuurile, sidudes liikmesriikide võrgu- ja infoturbealase suutlikkuse ning lihtsustades ELi ülest koostööd.

Kõigele lisaks on liikmesriikide ja erasektori koostöö edendamiseks olulised ELi tasandil läbiviidavad küberõppused. Esimene liikmesriike hõlmav õppus viidi läbi 2010. aastal („Cyber Europe 2010") ning teine, ka erasektorit kaasav õppus toimus 2012. aasta oktoobris („Cyber Europe 2012"). ELi-USA õppus viidi läbi 2011. aasta novembris („Cyber Atlantic 2011"). Tulevasteks aastateks on kavandatud täiendavaid õppusi, sealhulgas rahvusvaheliste partneritega.

Komisjon kavatseb teha järgmist:

- jätkab tihedas koostöös liikmesriikide asutustega ning elutähtsate infrastruktuuride omanike ja operaatoritega Teadusuuringute Ühiskeskuse elluviidavaid meetmeid, mis on suunatud Euroopa elutähtsate infrastruktuuride võrgu- ja infoturbega seotud nõrkade kohtade kindlaksmääramisele ning vastupidavate süsteemide väljatöötamise soodustamisele;
- algatab 2013. aasta alguses ELi rahastatud katseprojekti[17] **robotivõrkude ja pahavaraga võitlemise kohta**, et luua koordineerimis- ja koostööraamistik ELi liikmesriikide, erasektori organisatsioonide (näiteks internetiteenuse osutajate) ja rahvusvaheliste partnerite vahel.

küberõppuste läbiviimisel, millele omakorda tugineb ELi osalemine **Komisjon palub ENISA-l teha järgmist:**

- abistada liikmesriike tugeva **riikliku küberturbesuutlikkuse** arendamisel, suurendades eelkõige teadmisi tööstuslike kontrollisüsteemide ning transpordi- ja energiataristu turvalisuse ja vastupidavuse kohta;
- uurida 2013. aastal ELi tööstuslike kontrollisüsteemide (ICS-CSIRT) jaoks arvutiturbe intsidentidele reageerimise meeskonna (meeskondade) loomise teostatavust.
- jätkata liikmesriikide ja ELi institutsioonide toetamist korrapäraste **üle-euroopaliste** rahvusvahelistes küberõppustes.

Komisjon kutsub Euroopa Parlamenti ja nõukogu üles tegema järgmist:

- **võtma** kiiresti **vastu** ettepanek direktiivi kohta, milles käsitletakse **võrgu- ja infoturbe ühtlaselt kõrge taseme tagamist** kogu Euroopa Liidus, riikide suutlikkust ja valmisolekut, ELi tasandi koostööd, riskihaldustavade juurutamist ja võrgu- ja infoturbealase teabe jagamist.

Komisjon palub tööstusel teha järgmist:

- võtta juhtroll küberjulgeoleku kõrgesse tasemesse **investeerimisel** ning töötada välja parimad tavad ja teabejagamissüsteem sektori tasandil ja riigiasutustega, et tagada vara ja üksikisikute tugev ja tõhus kaitse, eelkõige selliste avaliku ja erasektori partnerluste kaudu nagu EP3R ja Trust in Digital Life (TDL)[18].

---

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Euroopa ühendamise rahastu eelarverida 09.03.02 – telekommunikatsioonivõrgud (avalike elektrooniliste teenuste omavahelise ühendamise ja koostalitluse ning sellistele võrkudele juurdepääsu tagamine).

17 CIP-ICT PSP-2012-6, 325188. Projekti üldeelarve on 15 miljonit eurot, ELi toetus on 7,7 miljoni euro suurune.

18 http://www.trustindigitallife.eu/.

Teadlikkuse suurendamine

Küberjulgeoleku tagamine on ühine ülesanne. Lõppkasutajatel on oluline roll võrkude ja infosüsteemide turvalisuse tagamisel. Seepärast tuleb neid teavitada riskidest, millega nad internetis kokku puutuvad ning neil peab olema võimalus võtta lihtsaid meetmeid, et end nende eest kaitsta.

Viimastel aastatel on töötatud välja mitu algatust ning nendega tuleks jätkata. Teadlikkuse suurendamisega on eelkõige olnud seotud ENISA kes on avaldanud vastavaid aruandeid, korraldanud ekspertidega seminare ning arendanud avaliku ja erasektori partnerlusi. Euroopa Politseiamet (Europol), Euroopa Õigusalase Koostöö Üksus (Eurojust) ja riiklikud andmekaitseasutused teevad samuti tõhusat tööd teadlikkuse suurendamiseks. 2012. aasta oktoobris organiseeris ENISA koos mõne liikmesriigiga esmakordselt Euroopa küberjulgeoleku kuu. Teadlikkuse suurendamine on üks valdkondi, mille arendamise kallal teeb tööd ka ELi ja USA ühine küberjulgeoleku ja küberkuritegevuse töörühm[19]. Samuti on see laste turvalisust internetis käsitleva programmi „Turvalisem internet"[20] oluline teema.

[19] 2010. aasta novembris ELi ja USA tippkohtumisel (MEMO/10/597) loodud töörühma ülesanne on koostööstrateegiate väljatöötamine erinevates küberturbe ja küberkuritegevuse küsimustes.

[20] Programmi „Turvaline internet" raames rahastatakse vabaühenduste võrgustikku, kes teeb aktiivset tööd laste heaolu tagamise nimel internetis, õiguskaitseasutuste võrgustikku, kus jagatakse teavet ja parimaid tavasid seoses interneti ärakasutamisega kuritegevuslikel eesmärkidel laste seksuaalset kuritarvitamist kujutava materjali levitamiseks ning teadlaste võrgustikku, kes kogub teavet veebitehnoloogia kasutamise ning selle ohtude ja tagajärgede mõju kohta laste elule.

Komisjon palub ENISA-l teha järgmist:

- esitada 2013. aastal tegevuskava võrgu- ja infoturbe oskustunnistuse kohta, mis kujutab endast vabatahtlikku sertifitseerimiskava IT-ekspertide (nt veebiadministraatorid) oskuste ja pädevuse edendamiseks.

Komisjon kavatseb teha järgmist:

- korraldab ENISA toel 2014. aastal küberjulgeoleku **võistlused**, kus tudengid võistleksid võrgu- ja infoturbega seotud lahenduste väljapakkumises.

Komisjon kutsub liikmesriike[21] üles tegema järgmist:

- korraldama igal aastal ENISA toel **küberjulgeoleku kuud**, kaasates sinna 2013. aastast ka erasektori, et suurendada lõppkasutajate teadlikkust. alates 2014. aastast hakatakse kooskõlastatult läbi viima ELi ja USA küberjulgeoleku kuud;
- **tugevdama võrgu- ja infoturbe vallas riigi tasandil võetavaid haridus- ja koolitusmeetmeid**, võttes kasutusele järgmised koolitused: 2014. aastaks koolides toimuv võrgu- ja infoturbealane koolitus; informaatikatudengitele mõeldud koolitus võrgu- ja infoturbe, turvalise tarkvaraarenduse ning isikuandmete kaitse kohta; riigiasutuste töötajatele suunatud võrgu- ja infoturbealane baaskoolitus.

Komisjon kutsub tööstust üles tegema järgmist:

- edendama kõigil tasanditel küberjulgeolekualast teadlikkust, nii äritavades kui ka klientidega suhtlemisel. Tööstus peaks eelkõige kaaluma seda, kuidas suurendada tegevjuhtide ja nõukogude vastutust küberjulgeoleku tagamise eest.

2.2. Küberkuritegevuse oluline vähendamine

Mida digitaalsem on meie maailm, seda rohkem on küberkurjategijatel võimalusi selle ärakasutamiseks. Küberkuritegevus on üks kiiremini kasvavaid kuritegevuse vorme, mille ohvriks langeb maailmas iga päev üle miljoni inimese. Küberkurjategijad muutuvad üha osavamaks ja nende võrgustikud aina keerukamaks. Nendega toimetulekuks on vaja vastavaid vahendeid ja oskusi. Küberkuritegevus on väga tulutoov ja madala riskiastmega ning kurjategijad kasutavad sageli ära veebidomeenide anonüümsust. Küberkuritegevus ei tunne piire – interneti üleilmne levik tähendab seda, et õiguskaitseasutused peavad kehtestama koordineeritud piiriülese strateegia kasvava ohuga ühiselt silmitsi seismiseks.

Ranged ja tõhusad õigusaktid

EL ja liikmesriigid vajavad küberkuritegevusega võitlemiseks rangeid ja tõhusaid õigusakte. Euroopa Nõukogu küberkuritegevuse konventsioon, mida nimetatakse ka Budapesti konventsiooniks, on siduv rahvusvaheline leping, millega on ette nähtud tõhus raamistik riiklike õigusaktide vastuvõtmiseks.

EL on juba võtnud vastu küberkuritegevust käsitlevaid õigusakte, sealhulgas direktiivi, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust[22].

[21] Kaasatud oleksid ka asjaomased riigiasutused, sealhulgas võrgu- ja infoturbe valdkonna pädevad asutused ja andmekaitseasutused.

[22] Direktiiv 2011/93/EL, millega asendatakse nõukogu raamotsus 2004/68/JSK.

EL on ka jõudmas kokkuleppele direktiivi üle, milles käsitletakse infosüsteemide vastu suunatud ründeid, ennekõike robotivõrkude kasutamise abil.

Komisjon kavatseb teha järgmist:

- tagab küberkuritegevusega seotud õigusaktide kiire ülevõtmise ja rakendamise;
- soovitab tungivalt liikmesriikidel, kes ei ole veel ratifitseerinud **Euroopa Nõukogu küberkuritegevust käsitlevat Budapesti konventsiooni**, seda võimalikult kiiresti teha ning konventsiooni sätted rakendada.

Küberkuritegevusega võitlemise operatiivsuutlikkuse suurendamine

Küberkuritegevuse tehnilised vahendid arenevad üha kiiremini. Õiguskaitseasutused ei suuda küberkuritegevusega võidelda vananenud vahenditega. Kõigil ELi liikmesriikidel ei ole praegu veel vajalikku operatiivsuutlikkust tõhusaks võitluseks küberkuritegevusega. Kõigil liikmesriikidel on tarvis tõhusaid riiklikke küberkuritegevuse üksuseid.

Komisjon kavatseb teha järgmist:

- toetab oma rahastamisprogrammide[23] kaudu liikmesriike, et **tuvastada puudused ja suurendada nende suutlikkust** uurida küberkuritegevust ja sellega võidelda. Komisjon toetab täiendavalt asutusi, kes seostavad teadustöö / akadeemilised ringkonnad, õiguskaitseasutused ja erasektori, nagu juba tehakse komisjoni rahastatavates küberkuritegevust käsitlevates tippkeskustes, mis on mõnes liikmesriigis juba loodud;
- kooskõlastab koos liikmesriikidega püüdlusi, et tuvastada teiste hulgas Teadusuuringute Ühiskeskuse abil parimad tavad ja parimad olemasolevad meetodid küberkuritegevusega võitlemiseks (nt seoses kriminalistikavahendite arendamise ja kasutuse või ohuanalüüsiga);
- teeb tihedat koostööd hiljuti **Europoli juurde loodud küberkuritegevuse vastase võitluse Euroopa keskusega (EC3) ning Eurojustiga**, et saavutada kooskõla poliitiliste strateegiate ja parimate tegevustavade vahel.

parem koordineerimine ELi tasandil

EL saab täiendada liikmesriikide tööd sellega, et soodustab koordineeritud ja kooskõlastatud strateegia väljatöötamist, mis koondab õiguskaitseasutused, õigusasutused ning avaliku ja erasektori sidusrühmad nii EList kui ka mujalt.

Komisjon kavatseb teha järgmist:

- toetab hiljuti loodud **küberkuritegevuse vastase võitluse Euroopa keskust** (EC3) kui Euroopa keskset asutust võitluses küberkuritegevusega. EC3 esitab analüüse ja andmeid, toetab uurimist, teeb kõrgetasemelist kriminalistikaalast tööd, soodustab koostööd, loob teabevahetuskanaleid liikmesriikide pädevate asutuste, erasektori ja muude sidusrühmade vahel ning saab aja möödudes õiguskaitseasutuste eestkõnelejaks[24];
- toetab jõupingutusi, et suurendada domeeninimede registripidajate vastutust ja tagada veebisaitide omanikke käsitleva teabe täpsus, võttes aluseks Interneti nimede ja numbrite määramise korporatsiooni (ICANN) õiguskaitsealased soovitused ning tegutsedes kooskõlas liidu õigusega, sealhulgas andmekaitseeeskirjadega;
- tugineb hiljuti vastuvõetud õigusaktidele, et jätkuvalt tugevdada ELi pingutusi seoses võitlusega internetis toimuva laste seksuaalse kuritarvitamise vastu. Komisjon on võtnud vastu lastele parema interneti loomise Euroopa strateegia[25]

[23] 2013. aastal programmist „Kuritegevuse ennetamine ja kuritegevuse vastu võitlemine" (ISEC). Pärast 2013. aastat sisejulgeoleku fondist (mitmeaastase finantsraamistiku alla kuuluv uus vahend).

[24] 28. märtsil 2012 võttis Euroopa Komisjon vastu teatise „Võitlus kuritegevusega digitaalajastul: küberkuritegevuse vastase võitluse Euroopa keskuse loomine".

[25] COM(2012) 196 (final).

ning on koos ELi liikmesriikide ja ELi mittekuuluvate riikidega loonud **internetis toimuva laste seksuaalse kuritarvitamise vastu võitlemise ülemaailmse liidu**[26]. Liit on vahend mille kaudu liikmesriigid saavad komisjoni ja EC3 toel võtta täiendavaid meetmeid.

Komisjon palub Europolil (EC3) teha järgmist:

- keskenduda oma analüütilise ja operatiivse toe pakkumisel küberkuritegude uurimisele liikmesriikides, et küberkurjategijate võrgustikke tõkestada ja need likvideerida eelkõige järgmistes valdkondades: laste seksuaalne kuritarvitamine, maksepettused, robotivõrgud ja sissetung;
- esitada regulaarselt strateegilisi ja tegevusaruandeid suundumuste ja tekkivate ohtude kohta, et määrata kindlaks prioriteedid ning anda suund liikmesriikides küberkuritegude uurimisega tegelevate rühmade tööle.

Komisjon palub Euroopa Politseikolledžil (CEPOL) koostöös Europoliga teha järgmist:

- koordineerida koolituste kavandamist ja läbiviimist, et varustada õiguskaitseasutused küberkuritegude tõhusaks lahendamiseks vajalike teadmiste ja oskusteabega.

Komisjon palub Eurojustil teha järgmist:

- teha kindlaks peamised takistused õigusalases koostöös küberkuritegude uurimise vallas ning töö koordineerimises liikmesriikide vahel ja kolmandate riikidega ning toetada küberkuritegude uurimist ja nende eest vastutusele võtmist nii operatiiv- kui ka strateegilisel tasandil ning ka valdkondlikke koolitusmeetmeid.

Komisjon palub Eurojustil ja Europolil (EC3) teha järgmist:

- teha tihedat koostööd, muu hulgas teabevahetuse kaudu, et suurendada nende küberkuritegevusega võitlemise tõhusust, vastavalt oma volitustele ja pädevusele.
-

2.3. Küberkaitsepoliitika väljatöötamine ning ühise julgeoleku- ja kaitsepoliitika (ÜJKP) raamistikuga seonduva suutlikkuse arendamine

ELis tehtavad küberjulgeoleku valdkonna jõupingutused hõlmavad ka küberkaitse mõõdet. Selleks et suurendada liikmesriikide kaitse- ja julgeolekualaseid huvisid toetavate kommunikatsiooni- ja infosüsteemide vastupidavust, peaks küberkaitsealase suutlikkuse arendamine olema orienteeritud keerukate küberohtude avastamisele, nendele reageerimisele ning nendest taastumisele.

Arvestades, et ohud on mitmetahulised, tuleks tõhustada koostoimet tsiviil- ja sõjandussektoris elutähtsa kübervara kaitsmiseks väljatöötatud lahenduste vahel. Selle nimel tehtavat tööd peaksid toetama teadus- ja arendustegevus ning tihedam koostöö ELi valitsuste,

[26] Nõukogu 7. ja 8. juuni 2012. aasta järeldused internetis toimuva laste seksuaalse kuritarvitamise vastu võitlemise ülemaailmse liidu kohta (ELi ja USA ühisavaldus) ning internetis toimuva laste seksuaalse kuritarvitamise vastu võitlemise ülemaailmse liidu loomise deklaratsioon (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

erasektori ja akadeemiliste ringkondade vahel. Dubleerimise vältimiseks uurib EL võimalusi, kuidas saavad EL ja NATO vastastiku täiendada oma püüdlusi, et suurendada selliste elutähtsate valitsus-, kaitse- ja muude teabeinfrastruktuuride vastupidavust, millest mõlema organisatsiooni liikmed sõltuvad.

Kõrge esindaja keskendub järgmistele olulistele meetmetele ning kutsub liikmesriike ja Euroopa Kaitseagentuuri üles tegema koostööd, et:

- hinnata ELi küberkaitse operatiivnõudeid ning edendada ELi küberkaitsealast suutlikkust ja tehnoloogiat, käsitledes suutlikkuse arendamise kõiki aspekte, nagu näiteks doktriin, juhtimine, korraldus, personal, koolitus, tehnoloogia, infrastruktuur, logistika ja koostalitlusvõime;

- arendada ELi küberkaitsepoliitika raamistikku, eesmärgiga kaitsta ÜJKP missioonide ja operatsioonidega seotud võrgustikke, pöörates tähelepanu ka dünaamilisele riskihaldusele, tõhustatud ohuanalüüsile ja teabe jagamisele. Eesmärk on parandada sõjaväe küberkaitsealase koolituse ja õppuste võimalusi Euroopa ja rahvusvahelises kontekstis ning lisada küberkaitsealased elemendid olemasolevatesse õppuseprogrammidesse;

- edendada dialoogi ja koostööd ELi tsiviil- ja sõjaväeliste osapoolte vahel, pöörates suurt tähelepanu heade tavade vahetusele, teabevahetusele ja varajasele hoiatamisele, intsidentidele reageerimisele, riskihindamisele, teadlikkuse suurendamisele ning küberjulgeoleku prioriteediks seadmisele;

- tagada dialoogi pidamine rahvusvaheliste partnerite, sealhulgas NATO, muude rahvusvaheliste organisatsioonide ja rahvusvaheliste tippkeskustega, et tagada toimiv kaitsealane suutlikkus, määrata kindlaks koostöövaldkonnad ja vältida töö dubleerimist.

2.4. Tööstuslike ja tehnoloogiliste vahendite arendamine küberjulgeoleku jaoks

Euroopa teadus- ja arendustöö suutlikkus on suurepärane, kuid paljud maailma juhtivad uuenduslike IKT-toodete ja -teenuste pakkujad asuvad EList väljaspool. Euroopal on oht saada ülemääraselt sõltuvaks nii mujal toodetud IKT-st kui ka piiri taga arendatud turvalahendustest. Oluline on tagada, et ELis ja kolmandates riikides toodetud riist- ja tarkvarakomponendid, mida kasutatakse elutähtsate teenuste ja infrastruktuuride puhul ning üha enam mobiilsetes seadmetes, oleksid usaldusväärsed, turvalised ja tagaksid isikuandmete kaitse.

Küberturbetoodete ühtse turu edendamine

Kõrge turvalisuse taseme saab tagada üksnes siis, kui väärtusahela kõik osalised (nt seadmete tootjad, tarkvaraarendajad, infoühiskonna teenuste pakkujad) seavad turvalisuse prioriteediks. Siiski näib,[27] et paljud osapooled peavad turvalisust üksnes lisakoormaks ning nõudlus turvalahenduste järele on piiratud. Euroopas kasutatavate IKT-toodete väärtusahela lõikes tuleks rakendada asjakohaseid küberjulgeolekualaseid toimivusnõudeid. Erasektoril on tarvis stiimuleid küberjulgeoleku kõrge taseme tagamiseks. Näiteks asjakohast küberjulgeolekualast toimivust osutavad märgised võimaldaksid küberturbealal hästi toimivatel ja vastava kogemusega ettevõtetel teha sellest turustusargumendi ning saavutada konkurentsieelise.

[27] Vt komisjoni talituste töödokumendi mõjuhinnang, mis on lisatud komisjoni ettepanekule võrgu- ja infoturbe direktiivi kohta, jaotis 4.1.5.2.

Võrgu- ja infoturbe direktiivi ettepanekus sätestatud kohustused annaksid märkimisväärse panuse ettevõtjate konkurentsivõime suurendamisele asjaomastes sektorites.

Samuti tuleks stimuleerida üle-euroopalist turunõudlust äärmiselt turvaliste toodete järele. Esiteks on kõnealuse strateegia eesmärk suurendada koostööd ja läbipaistvust IKT-toodete turvalisuse vallas. Selles kutsutakse üles looma platvormi, mis koondab asjaomased Euroopa avaliku ja erasektori sidusrühmad, et teha terve väärtusahela ulatuses kindlaks head küberjulgeoleku tavad ning luua soodsad turutingimused turvaliste IKT-lahenduste arendamiseks ja kasutuselevõtmiseks. Tähelepanu keskmes peaks olema stiimulite loomine asjaomase riskihaldusega tegelemiseks ning turvastandardite ja -lahenduste kehtestamine, samuti võimaluse korral ELi üleste vabatahtlike sertifitseerimiskavade loomine, mis tugineks olemasolevatele ELi ja rahvusvahelistele kavadele. Komisjon edendab sidusate strateegiate vastuvõtmist liikmesriikides, et ära hoida erinevusi, mis võiksid seada ettevõtted ebasoodsamasse olukorda nende asukoha tõttu.

Teiseks toetab komisjon turvastandardite väljatöötamist ning aitab kaasa ELi ülestele vabatahtlikele sertifitseerimiskavadele pilvandmetöötluse valdkonnas, võttes samas arvesse vajadust tagada andmete kaitse. Tähelepanu tuleks pöörata tarneahela turvalisusele, eelkõige elutähtsates majandussektorites (tööstuslikud kontrollisüsteemid, energia- ja transporditaristud). Seejuures tuleks tugineda käimasolevale standardimistööle Euroopa standardiorganisatsioonides (CEN, CENELEC ja ETSI)[28] ja küberjulgeolekualases koordineerimisrühmas (CSCG) ning ka ENISA, komisjoni ja muude asjakohaste osaliste ekspertteadmistele.

Komisjon kavatseb teha järgmist:

- käivitab 2013. aastal avaliku ja erasektori platvormi võrgu- ja infoturbelahenduste jaoks, et arendada stiimuleid turvaliste IKT-lahenduste kasutuselevõtmiseks ning heaks küberjulgeolekualaseks toimivuseks, mida tuleks kohaldada Euroopas kasutatavate IKT-toodete suhtes;
- esitab 2014. aastal soovitused küberjulgeoleku tagamiseks kogu IKT väärtusahelas, tuginedes kõnealuse platvormi tööle;
- uurib, kuidas olulised IKT riist- ja tarkvara pakkujad võiksid teavitada riigi pädevaid asutusi avastatud nõrkustest, millel võivad olla märkimisväärsed turvalisusega seotud tagajärjed.

Komisjon palub ENISA-l teha järgmist:

- töötada koostöös asjaomaste riigi pädevate asutuste, asjaomaste sidusrühmade, rahvusvaheliste ja Euroopa standardiorganisatsioonide ning Euroopa Komisjoni Teadusuuringute Ühiskeskusega välja **tehnilised suunised ja soovitused võrgu- ja infoturbealaste standardite ja heade tavade vastuvõtmiseks** avalikus ja erasektoris.

Komisjon kutsub avaliku ja erasektori sidusrühmi üles tegema järgmist:

- stimuleerima tööstuse algatatavate **turvastandardite**, tehniliste normide ning lõimturvalisusele ja lõimprivaatsusele orienteeritud põhimõtete väljatöötamist ja kasutuselevõtmist IKT-toodete valmistajate ja teenuseosutajate, sealhulgas

[28] Eelkõige arukate võrkude standardi M/490 raames (esimene standardikogum seoses arukate võrkude ja etalonarhitektuuriga).

pilveteenuste pakkujate poolt. Uue põlvkonna tark- ja riistvara peaks olema varustatud **tugevamate, integreeritud ja kasutajasõbralike turbe**vahenditega;

- töötama välja tööstuse algatatud standardid seoses ettevõtete küberjulgeolekualase toimivusega ning parandama avalikkusele suunatud teavet, arendades välja **turvamärgistused** või kvaliteedimärgid, mis aitaksid tarbijal turul orienteeruda.

Teadus- ja arendustegevuse investeeringute ja innovatsiooni soodustamine

Teadus- ja arendustegevusega saab toetada tugevat tööstuspoliitikat, edendada usaldusväärset Euroopa IKT-tööstust, parandada siseturu toimimist ja vähendada Euroopa sõltuvust välismaisest tehnoloogiast. Teadus- ja arendustegevus peaks täitma tehnoloogialüngad IKT turbes, valmistama pinda ette järgmise põlvkonna turvaprobleemide lahendamiseks, võtma arvesse kasutajate vajaduste pidevat arengut ning võimaldama kasu saada nn kahese kasutusega tehnoloogiatest. Samuti peaks see jätkama krüptograafia arendamise toetamist. Seda peaksid täiendama pingutused realiseerida teadus- ja arendustegevuse vallas saavutatud tulemused ärilahendustes, pakkudes vajalikke suuniseid ning kehtestades asjakohased poliitilised tingimused.

EL peaks maksimaalselt ära kasutama 2014. aastal algatavat teadusuuringute ja innovatsiooni raamprogrammi Horisont 2020[29]. Komisjoni ettepanek hõlmab konkreetseid, käesolevale strateegiale vastavaid eesmärke seoses usaldusväärse IKTga ning ka küberkuritegevuse vastu suunatud võitlusega. Programmi Horisont 2020 raames toetatakse kujunemisjärgus info- ja sidetehnoloogiaga seonduvaid turvalisusuuringud; sellega pakutakse välja lahendusi seoses läbivalt turvaliste IKT-süsteemide, -teenuste ja -rakendustega; sellega pakutakse välja stiimuleid olemasolevate lahenduste rakendamiseks ja kasutuselevõtuks ning selles käsitletakse võrgu- ja infosüsteemide koostalitlusvõimet. ELi tasandil pööratakse erilist tähelepanu erinevate rahastamisprogrammide (Horisont 2020, sisejulgeoleku fond, Euroopa Kaitseagentuuri (EDA) uuringud, sealhulgas koostöö Euroopa raamistik) optimeerimisele ja paremale koordineerimisele.

Komisjon kavatseb teha järgmist:

- kasutab programmi Horisont 2020 mitmete eraelu puutumatuse ja turvalisusega seotud küsimuste käsitlemiseks IKT valdkonnas, alates teadus- ja arendustegevusest kuni innovatsiooni ja juurutamiseni. Horisont 2020 raames töötatakse ka välja vahendid, et võidelda küberkeskkonna vastu suunatud kuritegeliku ja terroristliku tegevusega;
- loob mehhanismid Euroopa Liidu institutsioonide ja liikmesriikide teadusuuringute kavade paremaks koordineerimiseks ning innustab liikmesriike suurendama teadus- ja arendustegevusse tehtavaid investeeringuid.

Komisjon kutsub liikmesriike üles tegema järgmist:

- töötama 2013. aasta lõpuks välja tead tavad **haldusasutuste ostujõu** kasutamiseks

[29] Horisont 2020 on rahastamisvahend, millega viiakse ellu STRATEEGIA „EUROOPA 2020" juhtalgatus „INNOVATIIVNE LIIT", mille eesmärk on tagada Euroopa globaalne konkurentsivõime. ELi uus teadusuuringute ja innovatsiooni raamprogramm aastateks 2014–2020 on osa majanduskasvu hoogustamise ja uute töökohtade loomise strateegiast Euroopas.

(nt riigihangete kaudu), et kannustada turbevahendite arendamist ja juurutamist IKT-toodetes ja -teenustes;

- soodustama tööstuse ja teadusringkondade varast kaasamist lahenduste väljatöötamisse ja selle töö kooskõlastamisse. Sellega seoses tuleks võimalikult suurel määral ära kasutada Euroopa tööstusbaasi ning asjaomaseid tehnoloogilisi uuendusi teadus- ja arendustegevuse vallas, seejuures tuleks koordineerida tsiviil- ja sõjaväeliste organisatsioonide teadusuuringute kavasid.

Komisjon palub Europolil ja ENISA-l teha järgmist:

- tuvastada uued suundumused ja vajadused, pidades silmas muutusi küberkuritegevuse ja küberturbe vallas, et töötada välja asjakohased digitaalkriminalistika vahendid ja tehnoloogiad.

Komisjon kutsub avaliku ja erasektori sidusrühmi üles tegema järgmist:

- töötama koostöös kindlustussektoriga välja **riskipreemiate arvutamise ühtsed parameetrid**, mis võimaldaksid turvalisusse investeerinud ettevõtetel saada kasu madalamatest riskipreemiatest.

2.5. Sidusa rahvusvahelise küberruumipoliitika kehtestamine Euroopa Liidu jaoks ning ELi põhiväärtuste edendamine

Küberuumi hoidmine avatuna, vabana ja turvalisena on ülemaailmne ülesanne, mida EL peaks lahendama koostöös asjaomaste rahvusvaheliste partnerite ja organisatsioonide, erasektori ja kodanikuühiskonnaga.

Rahvusvahelise küberruumipoliitika kehtestamisega soovib EL edendada interneti avatust ja vabadust, soodustada käitumisnormide kehtestamist ning kohaldada kehtivat rahvusvahelist õigust küberruumis. EL teeb ka tööd digitaalse lõhe kaotamise nimel ning osaleb innukalt rahvusvahelistes püüdlustes küberjulgeolekualase suutlikkuse suurendamiseks. ELi rahvusvaheliste kohustuste puhul juhindutakse ELi põhiväärtustest, milleks on inimväärikus, vabadus, demokraatia, võrdsus, õigusriigi põhimõte ja põhiõiguste austamine.

Küberruumi temaatika arvestamine ELi välissuhete ning ühise välis- ja julgeolekupoliitika puhul

Komisjon, kõrge esindaja ja liikmesriigid peaksid kujundama Euroopa Liidu jaoks sidusa rahvusvahelise küberruumipoliitika, mis oleks suunatud tugevamale koostööle võtmetähtsusega rahvusvaheliste partnerite ja organisatsioonide ning ka kodanikuühiskonna ja erasektoriga ning nimetatud osapoolte suuremale kaasamisele. Kübertemaatikat käsitlevad ELi konsultatsioonid rahvusvaheliste partneritega peaksid olema hästi kavandatud, koordineeritud ja rakendatud, et anda ELi liikmesriikide ja kolmandate riikide vahel käimasolevatele kahepoolsetele dialoogidele lisaväärtust. EL paneb senisest enam rõhku kolmandate riikidega peetavatele aruteludele, keskendudes iseäranis samu seisukohti ja ELi väärtusi jagavatele partneritele. EL edendab andmekaitse kõrge taseme saavutamist, kaasa arvatud juhul, kui isikuandmeid edastatakse kolmandatele riikidele. Küberruumiga seotud üleilmsete probleemide lahendamiseks püüab EL teha tihedamat koostööd selles valdkonnas energiliselt tegutsevate organisatsioonidega nagu Euroopa Nõukogu, OECD, ÜRO, OSCE, NATO, AL, ASEAN ja ARO. Kahepoolsel tasandil peetakse eriti oluliseks koostööd USAga ning seda arendatakse edasi, eelkõige ELi ja USA küberjulgeoleku ja küberkuritegevuse töörühma raames.

ELi rahvusvahelise küberruumipoliitika üks olulisemaid ülesandeid saab olema küberruumi kui vabadusel rajaneva ja põhiõigusi austava ala edendamine. Interneti kättesaadavuse laiendamine peaks kõikjal maailmas toetama ja edendama demokraatlikke reforme. Võrguühenduste üha suurema levikuga ei peaks kaasnema tsensuur ega massijälgimine. EL peaks edendama ettevõtjate sotsiaalset vastutust[30] ning käivitama rahvusvahelisi algatusi üleilmse koordineerimise parandamiseks selles valdkonnas.

Vastutust turvalisema küberruumi eest kannavad kõik üleilmse infoühiskonna osapooled, kodanikest valitsusteni. EL toetab tööd, mida tehakse selle nimel, et määrata kindlaks küberruumi käitumisnormid, mida peaksid järgima kõik sidusrühmad. Just nii nagu EL ootab kodanikelt võrgus kodanikukohuse täitmist, sotsiaalse vastutuse kandmist ja õigusaktide järgmist, nii peaksid ka riigid pidama kinni normidest ja kehtivatest õigusaktidest. Rahvusvahelise julgeoleku vallas julgustab EL küberjulgeolekualast usaldust suurendavate meetmete väljatöötamist, et suurendada läbipaistvust ning vähendada riigi käitumise vääritimõistmise ohtu.

EL ei kutsu üles looma uusi rahvusvahelisi õigusakte kübertemaatika vallas.

Kodaniku- ja poliitiliste õiguste rahvusvahelises paktis, Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis ja Euroopa Liidu põhiõiguste hartas sätestatud õiguslikke kohustusi tuleks järgida ka internetis. EL koondab oma tähelepanu sellele, kuidas tagada nimetatud meetmete jõustamine ka küberruumis.

Küberkuritegevusega võitlemiseks on Budapesti konventsioon vahend, mille kolmandad riigid võivad vabalt vastu võtta. Selles on esitatud küberkuritegevust käsitlevate riiklike õigusaktide koostamise mudel ning konventsioon on aluseks rahvusvahelisele koostööle selles valdkonnas.

Relvastatud konflikti laienemisel küberruumi kohaldatakse vastava juhtumi suhtes rahvusvahelist humanitaarõigust ning vajaduse korral inimõigusi käsitlevat õigust.

Küberjulgeoleku ja teabetaristute turbe alase suutlikkuse arendamine kolmandates riikides

Rahvusvahelise koostöö laiendamine aitab kaasa kommunikatsiooniteenuseid osutavate ja soodustavate baastaristute sujuvale toimimisele. See hõlmab parimate tavade ja teabe vahetust, varajast hoiatamist, intsidentide haldamist käsitlevaid ühisõppuseid jms. EL aitab selle eesmärgi saavutamisele kaasa, tõhustades rahvusvahelisel tasandil tehtavaid jõupingutusi, et tugevdada elutähtsate infrastruktuuride kaitse alaseid koostöövõrgustikke, kuhu on kaasatud valitsused ja erasektor.

Kahjuks ei saa kõik maailma piirkonnad nautida interneti positiivset mõju, kuna puudub avatud, turvaline, koostalitlusvõimeline ja usaldusväärne juurdepääs. Seepärast toetab Euroopa Liit jätkuvalt riikide püüdlusi seoses internetile juurdepääsu ja selle kasutamise arendamisega oma kodanike hüvanguks, interneti terviklikkuse ja turvalisuse tagamisega ning tõhusa võitlusega küberkuritegevuse vastu.

[30] ELi uuendatud strateegia aastateks 2011–2014 ettevõtja sotsiaalse vastutuse valdkonnas; KOM(2011) 681 (lõplik).

Komisjon ja kõrge esindaja kavatsevad koostöös liikmesriikidega teha järgmist:

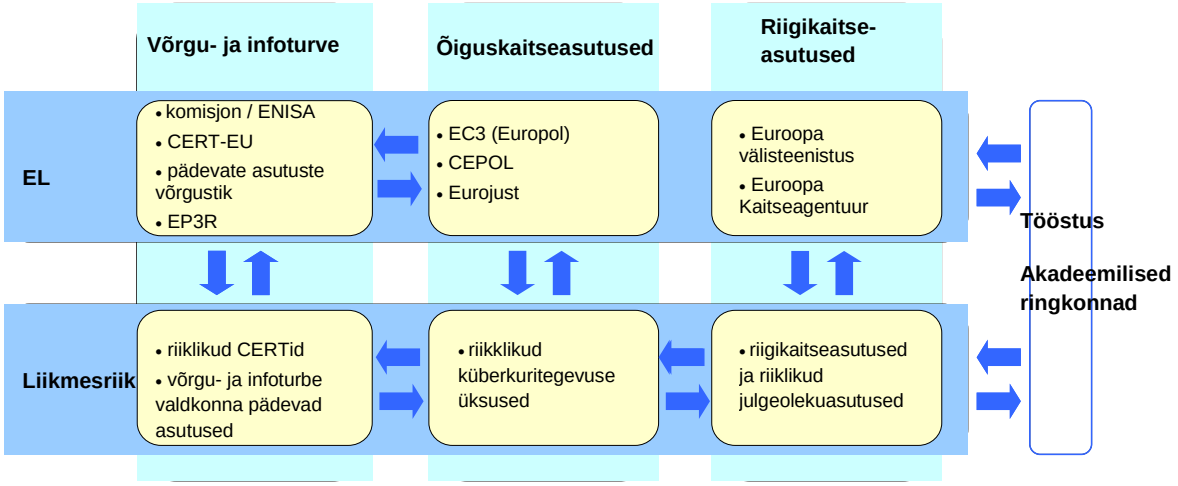
- töötavad ELi sidusa rahvusvahelise küberruumipoliitika loomise nimel, et suurendada võtmetähtsusega rahvusvaheliste partnerite ja organisatsioonide kaasatust, suurendada kübertemaatikaga arvestamist ühises välis- ja julgeolekupoliitikas (ÜVJP) ning parandada üleilmse tähtsusega küberküsimuste koordineerimist;
- toetavad käitumisnormide kehtestamist ja usaldust suurendavate meetmete väljatöötamist küberjulgeoleku vallas. Hõlbustavad dialooge selles vallas, kuidas kohaldada kehtivat rahvusvahelist õigust küberruumis ning edendada Budapesti konventsiooni kasutamist küberkuritegevusega võitlemiseks;
- toetavad põhiõiguste edendamist ja kaitset, sealhulgas juurdepääsu teabele ja sõnavabadust, keskendudes järgmisele: a) uute avalike suuniste väljatöötamine sõnavabaduse kohta veebikeskkonnas ja väljaspool seda; b) selliste toodete või teenuste ekspordi järelevalve, mida võidaks kasutada võrgus materjalide tsenseerimiseks või massijälgimiseks; c) meetmete ja vahendite arendamine, eesmärgiga suurendada juurdepääsu internetile, avatust ja vastupidavust, et seista vastu kommunikatsioonitehnoloogia abil toimuvale tsensuurile ja massijälgimisele; d) kommunikatsioonitehnoloogia kasutamise võimaldamine sidusrühmadele põhiõiguste kaitse eesmärgil;
- teevad koostööd rahvusvaheliste partnerite ja organisatsioonide, erasektori ja kodanikuühiskonnaga, et toetada ülemaailmse suutlikkuse arendamist kolmandates riikides, eesmärgiga parandada juurdepääsu teabele ja avatud internetile, ennetada küberohte (sealhulgas õnnetusjuhtumeid, küberkuritegusid ja küberterrorismi) ja neile reageerida ning arendada rahastamise koordineerimist, et suunata suutlikkuse suurendamise vallas võetavaid meetmeid;
- kasutavad küberjulgeolekualase suutlikkuse suurendamiseks ELi erinevaid abivahendeid, sealhulgas toetades õiguskaitsealal, kohtuasutustes ja tehnilistes valdkondades töötavate isikute koolitamist, et küberohtudega toime tulla ning toetades samuti asjaomaste riiklike poliitikate, strateegiate ja institutsioonide loomist kolmandates riikides;
- suurendavad poliitilist koordineerimist ja teabe jagamist rahvusvaheliste elutähtsate infrastruktuuride kaitse alaste võrgustike kaudu (nt Meridian) ning võrgu- ja infoturbe valdkonna pädevate asutuste ja muude asutuste koostööd.

3. ÜLESANDED JA VASTUTUSALAD

Küberintsidendid ei tunne omavahel ühendatud digitaalmajanduses ja -ühiskonnas riigipiire. Kõik osapooled, alates võrgu- ja infoturbe valdkonna pädevatest asutustest, CERTidest ja õiguskaitseasutustest kuni tööstuseni, peavad võtma vastutuse nii riigi kui ka ELi tasandil ja tegema koostööd küberjulgeoleku tugevdamiseks. Kuna see võib hõlmata erinevaid õigusraamistikke ja jurisdiktsioone, on ELi suurim ülesanne teha selgeks paljude asjaomaste osapoolte ülesanded ja vastutusalad.

Arvestades teema keerukust ning asjaosaliste laia spektrit, ei ole lahenduseks tsentraliseeritud järelevalve ELi tasandil. Riikide valitsused oskavad kõige paremini korraldada küberintsidentide ja -rünnete vältimist ja neile reageerimist ning luua enda kehtestatud

õigusraamistike ja poliitikastrateegiate raames kontakte ja võrgustikke erasektori ja üldsusega. Tulenevalt riskide võimalikust või tegelikust piiriülesusest eeldab riigi tõhus reageerimine sageli ka sekkumist ELi tasandil. Küberjulgeolekuga ulatuslikult tegelemiseks peaksid meetmed hõlmama kolme põhivaldkonda – võrgu- ja infoturve, õiguskaitse ja riigikaitse – mis on reguleeritud ka erinevate õigusraamistikega.



3.1. Töö koordineerimine võrgu- ja infoturbe valdkonna pädevate asutuste /CERTide, õiguskaitse- ja riigikaitseasutuste vahel

Liikmesriigi tasand

Liikmesriikidel peaks juba olema küberturbe, küberkuritegevuse ja riigikaitse eest vastutavad struktuurid või nad peaksid need käesoleva strateegia tulemusena looma. Kõnealused struktuurid peaksid saavutama küberintsidentidega tegelemiseks vajaliku suutlikkuse. Võttes aga arvesse, et paljud üksused võivad tegevuse poole pealt vastutada küberjulgeoleku erinevate valdkondade eest, ning arvestades erasektori kaasamise olulisust, tuleks liikmesriigi tasandil optimeerida koordineerimist ministeeriumide vahel. Liikmesriigid peaksid oma riiklikes küberjulgeoleku strateegiates sätestama erinevate riiklike üksuste ülesanded ja vastutusalad.

Teabe vahetamist riiklike üksuste ja erasektori vahel tuleks soodustada, et mõlemale oleks jätkuvalt tagatud ülevaade erinevatest ohtudest ning nad mõistaksid paremini uusi suundumusi ja tehnikaid, mida kasutatakse nii küberrünnete läbiviimiseks kui ka nendele kiiremaks reageerimiseks. Küberintsidentide korral aktiveeritavate riiklike võrgu- ja infoturbe koostöökavade kehtestamisel peaksid liikmesriigid määrama selged ülesanded ja vastutusalad ning optimeerima reageerimismeetmeid.

ELi tasand

Nagu liikmesriigi tasandil, tegelevad ka ELi tasandil küberjulgeolekuga mitmed osapooled. Võrgu- ja infoturbe, õiguskaitse ja riigikaitse vallas kõige aktiivsemalt tegutsevad asutused on vastavalt ENISA, Europol/EC3 ja EDA. Kõnealuste, ELi tasandi koostöövõimalusi pakkuvate asutuste haldusnõukogudes on esindatud liikmesriigid.

ENISA, Europoli/EC3 ja EDA vahelist koordineerimist ja koostööd soodustatakse mitmetes valdkondades, millesse nad on kõik kaasatud, eelkõige seoses suundumuste analüüsiga, riskihindamise, koolituse ja parimate tavade vahetamisega. Koostöö tegemisel peaksid nad

siiski säilitama oma eripära. Koos CERT-EU, komisjoni ja liikmesriikidega peaksid kõnealused asutused toetama valdkonna tehniliste ja poliitiliste ekspertide usaldusväärse kogukonna loomist.

Mitteametlikke koordineerimis- ja koostöökanaleid täiendavad struktuursemad sidemed. ELi sõjalist staapi ning EDA küberkaitse projektimeeskonda saab kasutada kaitsemeetmete koordineerimiseks. Europoli/EC3e programminõukogu koondab muu hulgas Eurojusti, CEPOLi, liikmesriigid,[31] ENISA ja komisjoni, ning pakub võimalust erialaste teadmiste vahetamiseks ning selle kindlustamiseks, et EC3-e meetmed viiakse ellu partnerluses, tunnustades kõikide sidusrühmade ekspertiisi ja vastavaid volitusi. ENISA uued volitused peaksid võimaldama muuta tihedamaks selle sidemeid Europoliga ning tugevdada sidemeid tööstusvaldkonna sidusrühmadega. Olulisim on see, et võrgu- ja infoturvet käsitleva komisjoni õigusakti ettepanekuga plaanitakse kehtestada koostöövõrgustik võrgu- ja infoturbe valdkonna riigi pädevate asutuste võrgustiku raames ning reguleerida teabe jagamist võrgu- ja infoturbe valdkonna asutuste ja õiguskaitseasutuste vahel.

Rahvusvaheline tasand

Komisjon ja kõrge esindaja tagavad koos liikmesriikidega koordineeritud rahvusvaheliste meetmete võtmise küberjulgeoleku valdkonnas. Seda tehes kaitsevad komisjon ja kõrge esindaja ELi põhiväärtusi ning edendavad kübertehnoloogia rahumeelset, avatud ja läbipaistvat kasutamist. Komisjon, kõrge esindaja ja liikmesriigid peavad poliitilist dialoogi rahvusvaheliste partnerite ja rahvusvaheliste organisatsioonidega nagu Euroopa Nõukogu, OECD, OSCE, NATO ja ÜRO.

3.2. ELi toetus suure küberintsidendi või -ründe korral

Suured küberintsidendid või -ründed mõjutavad suure tõenäosusega ELi valitsusi, ettevõtjaid ja üksikisikuid. Käesoleva strateegia ning eelkõige võrgu- ja infoturvet käsitleva väljapakutud direktiivi tulemusel peaksid paranema küberintsidentide vältimine, avastamine ja neile reageerimine ning liikmesriigid ja komisjon peaksid üksteist põhjalikumalt teavitama suurtest küberintsidentidest või -rünnetest. Reageerimismehhanismid erinevad siiski sõltuvalt intsidendi laadist, ulatusest ja piirülesest mõjust.

Võrgu- ja infoturbe direktiivis on välja pakutud, et kui intsident mõjutab suurel määral talitluspidevust, võetakse olenevalt intsidendi piirülesest mõjust kasutusele kas liikmesriigi või ELi võrgu- ja infoturbe koostöökava. Võrgu- ja infoturbe valdkonna pädevate asutuste võrgustikku kasutataks sellisel juhul teabe jaotamiseks ja tugifunktsioonideks. See võimaldaks säilitada ja/või taastada kahjustatud võrgud ja teenused

Kui intsident näib olevat seotud kuriteoga, tuleks teavitada Europoli/EC3-e, et nad saaksid koos asjaomaste riikide õiguskaitseasutustega algatada uurimise, säilitada tõendusmaterjali, tuvastada süüdlased ning viimaks kindlustada nende kohtu alla andmise.

Kui intsident näib olevat seotud küberspionaaži või mõne riigi mahitatud ründega või kahjustab riigi julgeolekut, hoiatavad riiklikud julgeolekuasutused ja riigikaitseasutused asjaomaseid kolleege, et viimased oleksid teadlikud sellest, et neid rünnatakse ning saaksid end kaitsta. Seejärel käivitatakse varajase hoiatamise mehhanismid ning vajaduse korral ka kriisihaldus- või muud protseduurid. Eriti tõsine küberintsident või -rünne võib anda

[31] Esindatuse kaudu liikmesriikide küberkuritegevuse üksuste juhtidest koosnevas ELi küberkuritegevuse töörühmas.

liikmesriigile piisava aluse ELi solidaarsusklausli (Euroopa Liidu toimimise lepingu artikkel 222) rakendamiseks.

Kui intsident näib olevat rikkunud isikuandmete kaitstust, tuleks kaasata riiklikud andmekaitseasutused või riigi reguleeriv asutus vastavalt direktiivile 2002/58/EÜ.

Küberintsidentide ja -rünnete käsitlemisele aitavad palju kaasa kontaktvõrgustikud ja rahvusvaheliste partnerite toetus. Viimane võib hõlmata tehnilisi leevendusmeetmeid, kriminaaljuurdlust ja kriisihalduse reageerimismehhanisme.

4. KOKKUVÕTE JA JÄRELMEETMED

Komisjoni ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja poolt väljapakutud Euroopa Liidu küberjulgeoleku strateegias on visandatud ELi nägemus ning vajalikud meetmed. Seejuures tuginetakse kodanike õiguste tugevale kaitsele ja edendamisele, et muuta ELi veebikeskkond maailma ohutuimaks[32].

Selle nägemuse saab realiseerida üksnes paljusid osapooli hõlmava tõelise partnerlusega, mille raames võetakse endile kohustused ja püütakse toime tulla ees ootavate probleemidega.

Komisjon ja kõrge esindaja kutsuvad seega nõukogu ja Euroopa Parlamenti üles käesolevat strateegiat toetama ning ulatama oma abikäe kavandatud meetmete elluviimisel. Tugevat toetust ja pühendumust on vaja üles näidata ka erasektoril ja kodanikuühiskonnal, kes on olulised osapooled turvalisuse taseme suurendamisel ja kodanike õiguste kaitsmisel.

Käes on tegude aeg. Komisjon ja kõrge esindaja on kindlalt otsustanud teha kõigi osapooltega koostööd vajaliku turvalisuse taseme tagamiseks Euroopas. Selle tagamiseks, et käesolevat strateegiat rakendataks viivitamata ning seda hinnataks võimalike arengute valguses, palutakse kõigil asjaomastel osapooltel osaleda kõrgetasemelisel konverentsil ning saavutatud edusamme hinnatakse aasta möödudes.

[32] Strateegiat rahastatakse igale asjaomasele poliitikavaldkonnale (Euroopa ühendamise rahastu, Horisont 2020, sisejulgeoleku fond, ÜVJP ning väliskoostöö, eelkõige stabiliseerimise rahastamisvahend) ettenähtud summades, mis on sätestatud komisjoni ettepanekus mitmeaastase finantsraamistiku 2014–2020 kohta (sõltudes eelarvepädevate institutsioonide heakskiidust ning vastuvõetud 2014.–2020. aasta mitmeaastase finantsaamistikuga kehtestatud lõppsummadest). Seoses vajadusega mitte ületada detsentraliseeritud ametitele ettenähtud ametikohtade arvu ning pidada kinni detsentraliseeritud ametitele järgmises mitmeaastases finantsaamistikus igas kulurubriigis ettenähtud vaheülemmäärast, julgustatakse ameteid (CEPOL, EDA, ENISA, EUROJUST ja EUROPOL/EC3), kellel palutakse käesoleva teatisega võtta endale uusi ülesandeid, seda tegema, arvestades ameti tegelikku kindlaks määratud suutlikkust võtta vastu suurenevaid ressursse ning kõigi tuvastatud ümberpaigutamise võimaluste piires.