EUROOPA
KOMISJON

LIIDU VÄLISASJADE
JA JULGEOLEKUPOLIITIKA
KÕRGE ESINDAJA

Brüssel, 13.9.2017
JOIN(2017) 450 final

ÜHISTEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis

1. SISSEJUHATUS

Küberturvalisus on äärmiselt oluline nii meie heaolu kui ka turvalisuse jaoks. Mida rohkem meie igapäevaelu ja majandus sõltuvad digitehnoloogiatest, seda haavatavamad me oleme. Küberturvalisuse intsidendid (edaspidi „küberintsidendid“) mitmekesistuvad nii toimepanijate kui ka taotletavate eesmärkide poolest. Kuritahtlik kübertegevus ei kujuta endast ohtu mitte üksnes meie majandusele ja digitaalse ühtse turu poole liikumisele, vaid ka meie demokraatiate toimimisele, vabadustele ja väärtustele. Tulevikus sõltub meie turvalisus sellest, mil viisil kohandame oma võimet kaitsta ELi küberintsidentide eest: nii tsiviiltaristu kui ka sõjaline suutlikkus sõltuvad turvalistest digisüsteemidest. Seda on tunnistatud nii Euroopa Ülemkogu 2017. aasta juuni kohtumisel[1] kui ka Euroopa Liidu üldise välis- ja julgeolekupoliitika strateegias[2].

Ohud kasvavad kiiresti. Uuringute järgi on küberkuritegevuse majanduslik mõju kasvanud vahemikus 2013 kuni 2017 viis korda ja 2019. aastaks võib see suureneda veel neli korda[3]. Lunavara[4] kasutamine on oluliselt suurenenud ja hiljutised ründed[5] viitavad küberkuritegevuse järsule kasvule. Kuid lunavara ei ole kaugeltki ainus oht.

Küberohu taga võivad olla nii riikidega mitte seotud osalejad kui ka riigid: sageli on tegemist kuritegeliku tegevusega, mis on kannustatud kasusaamisest, kuid mis võib olla ka poliitiline ja strateegiline. Kuritegevusega seotud ohtu võimendab piiri ähmastumine küberkuritegevuse ja nn traditsioonilise kuritegevuse vahel, sest kurjategijad kasutavad internetti nii oma tegevuse laiendamiseks kui ka selleks, et leida oma kuritegude toimepanemiseks uusi võtteid ja vahendeid[6]. Samas on enamikul juhtudel tõenäosus kurjategijale jälile saada väga väike ja võimalused tema vastutuselevõtmiseks veelgi väiksemad.

Samal ajal kasutavad riigid oma geopoliitiliste eesmärkide saavutamiseks traditsiooniliste vahendite kõrval, nagu sõjaline jõud, üha enam ka diskreetsemaid kübervahendeid, sealhulgas sekkumist riigisisestesse demokraatlikesse protsessidesse. Küberruumi kasutamine sõjatandrina kas eraldiseisvalt või osana hübriidlähenemisest on tänapäeval kõigile teada. Järjest levinumad on väärteabe levitamise kampaaniad, libauudised ja küberründed, mis on suunatud elutähtsa taristu vastu, ning neile tuleb reageerida. Sel põhjusel rõhutas komisjon oma aruteludokumendis Euroopa kaitse tuleviku kohta[7] küberkaitsealase koostöö olulisust.

Kui me ei paranda oluliselt oma küberturvalisust, kasvab oht koos digitaliseerumisega. 2020. aastaks tahetakse asjade internetti ühendada kümneid miljardeid seadmeid, kuid küberturvalisus ei ole nende projekteerimises olnud esmatähtsal kohal[8]. Suutmatusel kaitsta seadmeid, mis kontrollivad meie elektrivõrke, autosid ja transpordivõrke, tehaseid, rahandust, haiglaid ja kodusid, võivad olla laastavad tagajärjed ja see võib oluliselt vähendada tarbijate usaldust kujunemisjärgus tehnoloogiatesse. Oht poliitiliselt motiveeritud rünneteks tsiviilsihtmärkide vastu ja puudused sõjalises küberkaitses suurendavad seda riski veelgi.

---

1 http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Vt McAfee & Centre for Strategic and International Studies „Net losses: Estimating the Global Cost of Cybercrime“ 2014.

4 Lunavara on pahavara, mis takistab või piirab kasutajate juurdepääsu oma süsteemile, lukustades süsteemi ekraani või kasutajate failid kuniks tasutud on lunaraha.

5 2017. aasta mais mõjutas lunavararünne WannaCry rohkem kui 400 000 arvutit üle 150 riigis. Kuu hiljem tabas Ukrainat ja mitmeid ettevõtjaid maailmas lunavararünne „Petya“.

6 Europol, Raske ja organiseeritud kuritegevuse põhjustatud ohtude hinnang, 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_et.pdf.

8 *IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination*, komisjoni tellimusel läbiviidud uuring.

Käesolevas ühisteatises kirjeldatud lähenemisviis loob ELile paremad väljavaated nende ohtudega toimetulemiseks. See aitab suurendada vastupidavusvõimet ja strateegilist sõltumatust, parandades tehnoloogia ja oskustega seotud suutlikkust ning aidates kujundada tugeva ühtse turu. Selleks peavad paigas olema õiged struktuurid, et tagada kõrge küberturvalisus ja olla valmis vajaduse korral reageerima, kaasates täies ulatuses kõik võtmeosalejad. Valitud lähenemisviis aitab ka tagada küberrünnete suhtes parema heidutuse, parandades nende eest vastutajate kindlaks tegemist, neile jälile jõudmist ja nende vastutusele võtmist. Selles tunnistatakse ka nähtuse üleilmset mõõdet ning arendatakse rahvusvahelist koostööd kui platvormi, kus ELil on küberturvalisuse küsimustes juhtpositsioon. Nende sammude aluseks on lähenemisviisid, mida kasutatakse digitaalse ühtse turu, üldise välis- ja julgeolekupoliitika strateegia, Euroopa julgeoleku tegevuskava,[9] hübriidohtudega võitlemise ühise raamistiku[10] ja Euroopa Kaitsefondi käivitamist käsitleva teatise puhul[11,12].

EL töötab juba mitme nimetatud teemaga: nüüd on aeg hakata eri otsi omavahel kokku viima. 2013. aastal koostas EL küberjulgeoleku strateegia, millega käivitas kübervastupidavuse parandamiseks peamised töösuunad[13]. Selle peamised eesmärgid ja põhimõtted – edendada usaldusväärset, turvalist ja avatud küberökosüsteemi – on endiselt asjakohased. Kuid pidevalt arenevad ja süvenevad ohud nõuavad uusi meetmeid, kui tahame tulevastele rünnetele vastu seista ja tagada nende suhtes heidutuse[14].

Arvestades ELi eri valdkondade poliitika ulatust ja tema käsutuses olevaid vahendeid, struktuure ja võimeid, on ELil küberturvalisusega tegelemiseks head eeldused. Liikmesriigid vastutavad ka edaspidi riigi julgeoleku eest, kuid ohtude ulatus ja piiriülene olemus on tugevad argumendid, mis räägivad ELi meetme võtmise kasuks, pakkudes liikmesriikidele stiimuleid ja tuge, et arendada ja säilitada suuremat ja paremat riiklikku suutlikkust küberturvalisuse valdkonnas, luues samal ajal ELi tasandi võimeid. Selle lähenemisviisi eesmärk on kaasata kõik osalejad – EL, liikmesriigid, tööstus ja üksikisikud –, et seada küberturvalisus esmatähtsale kohal. See on vajalik selleks, et arendada küberrünnete suhtes vastupidavust ja suuta ELi tasandil neile paremini reageerida. Selles esitatakse konkreetsed sammud, mis aitavad avastada ja uurida mis tahes vormis ELi ja selle liikmesriikide vastu suunatud küberintsidente ning neile kohaselt reageerida, sh andes kurjategijad kohtu alla. See annab ELi välisteenistusele võimaluse tõhusalt edendada küberturvalisust ülemaailmsel areenil. Selle tulemusena saab EL vahetada tagantjärele reageeriva lähenemisviisi ennetava vastu, et kaitsta Euroopa heaolu, ühiskonda ja väärtusi ning ka põhiõigusi ja -vabadusi, tegeledes nii olemasolevate kui ka tulevaste ohtudega.

2. PARANDAME ELi VASTUPIDAVUSVÕIMET KÜBERRÜNNETELE

Tugev kübervastupidavusvõime eeldab kollektiivset ja laiaulatuslikku lähenemisviisi. Selleks on vaja stabiilsemaid ja tõhusamaid struktuure, et edendada küberturvalisust ja reageerida küberrünnetele liikmesriikides, kuid ka ELi enda institutsioonides, asutustes ja organites. Samuti eeldab see terviklikumat, eri poliitikavaldkondi hõlmavat lähenemisviisi, et parandada

[9] COM(2015) 185 final.
[10] JOIN(2016) 18 final.
[11] COM(2017) 295.
[12] Lähenemisviisis on kasutatud ka sõltumatuid teaduslikke nõuandeid, mille Euroopa Komisjon on saanud teadusnõustamise mehhanismi teadusnõustajate kõrgetasemeliselt töörühmalt (vt viide allpool).
[13] JOIN(2013) 1 final. Selle strateegia hinnang on kättesaadav dokumendis SWD(2017) 295.
[14] Käesoleva teatise ettepanekud on eelarve seisukohast neutraalsed, kui ei ole märgitud teisiti. Iga algatuse puhul, millel on mõju eelarvele, järgitakse nõuetekohaselt iga-aastast eelarve menetlust ja see ei mõjuta järgmist 2020. aasta järgset mitmeaastast finantsraamistikku.

kübervastupanuvõimet ja strateegilist sõltumatust, tugevat ühtset turgu, suurt edasiminekut ELi tehnoloogilises võimes ja oluliselt suuremat kvalifitseeritud ekspertide arvu. Kesksel kohal on sealjuures laialdasem tõdemus, et küberturvalisuse näol on tegemist ühiskonna ees seisva ühise probleemiga, mille lahendamisse tuleks kaasata valitsuse, majanduse ja ühiskonna eri tasandid.

2.1 Euroopa Liidu Võrgu- ja Infoturbeameti tugevdamine

Euroopa Liidu Võrgu- ja Infoturbeametil (ENISA) on ELi kübervastupidavusvõime ja reageerimise parandamisel keskne koht, kuid praegune mandaat piirab tema tegevust. Seepärast esitab komisjon põhjaliku reformiettepaneku, mis hõlmab ka **ametile alalise mandaadi andmist**[15]. Sellega tagatakse, et ENISA saab pakkuda tuge liikmesriikidele, ELi institutsioonidele ja ettevõtetele olulistes valdkondades, sh võrgu- ja infosüsteemide turvalisuse direktiivi[16] (edaspidi „võrgu- ja infoturbe direktiiv“) ning kavandatud küberturvalisuse sertifitseerimise raamistiku rakendamisel.

Reformitud ENISA-l on tugev nõuandev roll poliitikakujundamisel ja rakendamisel, sh valdkondlike algatuste ning võrgu- ja infoturbe direktiivi vahelise ühtsuse edendamisel ning valdkondlike teabe jagamise ja analüüsimise keskuste loomisele kaasa aitamisel elutähtsates sektorites. ENISA tõstab lati kõrgemale ja parandab Euroopa valmisolekut, korraldades iga-aastaseid üle-Euroopalisi küberturvalisuse õppuseid, milles ühendatakse eri tasandite reageerimisvõtted. Ta toetab ELi poliitika kujundamist info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimise valdkonnas ja mängib olulist rolli nii operatiivkoostöö kui ka kriisihalduse parandamisel ELis. Ameti ülesanne on toimida ka küberturvalisusekogukonna teabe ja teadmiste teabekeskusena.

Kiiresti kujundatud ühtne arusaam ohtudest ja intsidentidest ning nende arengutest on eelduseks, et teha otsus selle kohta, kas ühine leevendamise meede või reageerimine ELi tasandil on vajalik. Selline teabevahetus eeldab kõigi asjaomaste osalejate – ELi asutused ja organid ning ka liikmesriigid – kaasatust tehnilisel, operatiivsel ja strateegilisel tasandil. Ka ENISA osaleb ELi tasandi olukorrateadlikkuse loomises koostöös asjaomaste asutustega liikmesriikides ja ELis, eelkõige küberturbe intsidentide lahendamise üksuste,[17] CERT-EU, Europoli ja Euroopa Liidu luureandmete analüüsi keskusega (INTCEN). Seda saab kasutada ohtude kohta teabe kogumisel ja poliitika kujundamisel korrapärase ohtude seire ja tõhusa operatiivkoostöö raames ning ulatuslikele piiriülestele intsidentidele reageerimisel.

2.2 Ühtse küberturvalisuse turu suunas

Mitmed tegurid pidurdavad küberturvalisuse turu kasvu ELis nii toodete, teenuste kui ka protsesside mõttes. Peamine nendest on kõikjal ELis tunnustatud küberturvalisuse sertifitseerimise kavade puudumine. Selliste kavade abil saaks tootele seada vastupidavusvõime suhtes rangemad nõuded ja parandada usaldust ELi-ülese turu vastu. Seepärast teeb komisjon ettepaneku luua **ELi küberturvalisuse sertifitseerimise**

[15] COM(2017) 477.

[16] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.

[17] Nagu sätestatud võrgu- ja infoturbe direktiivi artiklis 9.

raamistik[18]. Raamistikus kehtestataks menetlus kogu ELi küberturvalisuse sertifitseerimise kavade loomiseks, mis hõlmaks tooteid, teenuseid ja/või süsteeme, mille puhul kohandatakse usaldusväärsuse taset vastavalt kasutusele (olgu siis tegemist elutähtsa taristu või tarbeseadmega)[19]. Ettevõtetele oleks see kindlasti kasulik, sest nõnda ei oleks neil vaja piiriüleselt kaubeldes läbida mitut sertifitseerimisprotsessi, misläbi piiratakse nii halduskoormust kui ka kulusid. Selles raamistikus loodud kavad aitaksid ka suurendada tarbijate usaldust, sest vastavussertifikaat annaks ostjatele ja kasutajatele teavet ja kindlustunde toodete ja teenuste turvaomadustest. Tänu sellele saaks küberturvalisuse rangetest nõuetest konkurentsieelis. Tulemuseks oleks suurem vastupidavusvõime, sest IKT-tooteid ja -teenuseid hinnataks ametlikult kindlaksmääratud küberturvalisuse standardite alusel, mida saaks koostada IKT-standarditega seoses toimuvast üldisemast tööst[20] eeskuju võttes.

Raamistiku kavad oleks vabatahtlikud ja müüjate või teenuse osutajate jaoks ei kaasneks nendega kohe mingit õiguslikku kohustust. Kavad ei oleks vastuolus ühegi õigusaktides kehtestatud nõudega, nt ELi õigusaktiga andmekaitse kohta.

Pärast raamistiku loomist kutsub komisjon sidusrühmi üles keskenduma kolmele prioriteetsele valdkonnale.

- Elutähtsate või kõrge riskiga rakenduste turvalisus[21]: süsteemid, millest me sõltume oma igapäevatoimingutes ja mis digitaliseeruvad järjest enam ja on omavahel järjest rohkem ühendatud, alates autodest ja tehaseseadmetest, suurimatest süsteemidest, nagu lennukid või elektrijaamad, väiksemate süsteemideni, nagu meditsiiniseadmed. Seepärast tuleks selliste toodete ja süsteemide IKT-tuumkomponentide turvalisust põhjalikult hinnata.

- Küberturvalisus era- või avaliku sektori poolt laialdaselt kasutatavates digitoodetes, -võrkudes, -süsteemides ja -teenustes, et end kaitsta rünnete eest ja kohaldada õigusaktides kehtestatud nõudeid[22] – nt e-kirjade krüpteerimine, tulemüürid ja virtuaalsed privaatvõrgud. On oluline, et selliste tööriistade laialdasem kasutamine ei tooks kaasa uusi ohte või nõrkusi.

- Sisseprojekteeritud turbe kasutamine odavates, digitaalsetes, omavahel ühendatud laiatarbeseadmetes, millest koosneb asjade internet: raamistiku kohaseid kavu saaks kasutada selleks, et anda teada, et tooted on ehitatud uusimaid turvalisi arendusmeetodeid kasutades, et nad on läbinud piisava turvatestimise ja et müüjad on võtnud kohustuse uute nõrkuste või ohtude avastamise korral nende tarkvara ajakohastada.

---

18 COM(2017) 477.

19 Usaldusväärsuse tase näitab turvalisuse hindamise rangust, mis sõltub tavaliselt rakendusala ja funktsioonidega seotud riskitasemest (st IKT-toodetelt või teenustelt, mida kasutatakse kõrge riskiga valdkondades või funktsioonides, eeldatakse kõrgemat usaldusväärsuse taset).

20 COM(2016) 176.

21 Erandiks oleks olukorrad, kus kohustuslik või vabatahtlik sertifitseerimine on reguleeritud muude liidu õigusaktidega.

22 Näiteks direktiiv (EL) 2016/1148, määrus (EL) 2016/679, direktiiv (EL) 2015/2366 ja muud esildatud õigusaktid, nagu Euroopa elektroonilise side seadustik. Kõigis neis nõutakse, et organisatsioonid võtaksid asjaomaste küberturvalisuse riskide lahendamiseks vajalikud turbemeetmed.

Nendes prioriteetides tuleks eelkõige võtta arvesse küberturvalisuse ohtude pidevat muutumist ja ka selliste esmatähtsate teenuste olulisust nagu transport, energeetika, tervishoid, pangandus, finantsturutaristud, joogivesi või digistruktuurid[23].

Kuigi IKT-toote, -süsteemi või -teenuse puhul ei ole võimalik tagada, et see on 100 % turvaline, on IKT-toodete lahendustes mitu hästituntud ja hästidokumenteeritud puudust, mida saab rünneteks ära kasutada. Kui võrku ühendatud seadmete, IT-tarkvara ja -seadmete tootjad kasutaksid sisseprojekteeritud turbe lähenemisviisi, siis oleks võimalik tagada, et küberturvalisusega tegeletakse enne uute toodete turulelaskmist. See võiks kuuluda nn hoolsuskohustuse põhimõtte alla, mida saaks koos tööstusega edasi arendada ja millega saaks vähendada toote/tarkvara nõrkusi tänu mitmesugustele projekteerimisel, testimisel ja kontrollimisel kohaldatavatele meetoditele (sh ametlik kontroll, kui see on vajalik), tänu pikaajalisele hooldusele ja turvaliste elutsükli protsesside kasutamisele arenduses ning uuendite ja paikade väljatöötamisele, et lahendada varem avastamata nõrkused, ning teha kiire ajakohastus ja parandus[24]. See suurendaks ka tarbijate usaldust digitoodetesse.

Lisaks tuleb tunnistada kolmandatest osapooltest turvalisuse uurijate olulist rolli olemasolevates toodetes ja teenustes nõrkuste avastamisel. Liikmesriikides tuleks luua tingimused, mis võimaldaksid nõrkustest koordineeritult teada anda,[25] tuginedes parimatele tavadele[26] ja asjakohastele standarditele[27].

Samal ajal on igal **konkreetsel sektoril** oma spetsiifilised probleemid ja neid tuleks julgustada töötama välja oma lähenemisviisi. Nõnda täiendaksid valdkonnaspetsiifilised küberturvalisuse strateegiad üldiseid küberturvalisuse strateegiaid sellistes valdkondades nagu finantsteenused,[28] energeetika, transport ja tervishoid[29].

Komisjon on juba tõstatanud konkreetselt uute digitehnoloogiatega[30] seotud **vastutuse** küsimused. Mõju analüüsimine on pooleli. Järgmised etapid jõuavad lõpule 2018. aasta juuniks. Küberturvalisus tõstatab ettevõtete ja tarneahela jaoks küsimuse vastutusest kahju tekkimise korral ja seni kuni need küsimused ei ole lahendatud, takistavad need küberturvalisuse toodete ja teenuste tugeva ühtse turu väljakujundamist.

Lõpuks sõltub ELi ühtse turu väljakujundamine ka sellest, kuidas küberturvalisust võetakse arvesse kaubandust ja investeeringuid käsitlevas poliitikas. Oluline näide küberturvalisusest on välismaiste omandamiste mõju elutähtsatele tehnoloogiatele. See teema on kesksel kohal **välismaiste otseinvesteeringute eelkontrolli käsitlevas raamistikus**,[31] mille eesmärk on eelnevalt kontrollida kolmandatest riikidest pärit investeeringuid julgeoleku ja avaliku korra

---

[23] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiivi 2016/1148 (meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) reguleerimisalasse kuuluvad valdkonnad.

[24] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017

[25] Koordineeritult nõrkustest teatamine on koostöövorm, mis lihtsustab ja võimaldab turvalisuse uurijatel anda infosüsteemi omanikule või müüjale teada nõrkustest, andes organisatsioonile võimaluse diagnoosida ja parandada nõrkus korrektselt ja aegsasti, enne kui nõrkust käsitlev üksikasjalik teave avaldatakse kolmandatele isikutele või üldsusele.

[26] Näiteks *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, ENISA, 2016.

[27] *ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure*.

[28] Komisjoni eesseisev finantstehnoloogiat käsitlev töö hõlmab küberturvalisust finantssektoris.

[29] Näiteks ühendades energiasektoris omavahel väga vanad ja tipptaseme infotehnoloogiad, eelkõige seoses elektrivõrgu vajadustega reaalajas.

[30] COM(2017) 228.

[31] COM(2017) 478.

seisukohast. Küberturvalisuse nõuded ongi juba olnud ELi kaupadele ja teenustele kaubandustõketeks olulistes sektorites mitme kolmanda riigi majanduses. ELi küberturvalisuse sertifitseerimise raamistik tugevdab veelgi Euroopa rahvusvahelist positsiooni ja seda tuleks täiendada pidevate püüdlustega koostada kõrge turvalisusastmega üleilmsed standardid ja vastastikuse tunnustamise lepingud.

2.3 Rakendada täielikult võrgu- ja infosüsteemide turvalisuse direktiivi

Peamised vahendid küberturvalisuse tagamiseks on praegu riikide kätes. Seepärast on ELi tunnistanud vajadust rangemate standardite järele. Ulatuslikud küberintsidendid mõjutavad harva üksnes ühte liikmesriiki, sest kesksed valdkonnad nagu pangandus, energeetika või transport on olemuselt järjest üleilmsemad, järjest rohkem digilahendustest sõltuvad ja omavahel ühendatud.

Võrgu- ja infosüsteemide turvalisuse direktiiv (edaspidi „võrgu- ja infoturbe direktiiv“) on esimene kogu ELi hõlmav küberturvalisust käsitlev õigusakt[32]. Selle eesmärk on parandada vastupidavusvõimet riikide küberturvalisuse võimete parandamise kaudu, edendada liikmesriikide vahel paremat koostööd ning nõuda, et ettevõtjad olulistes sektorites võtaksid kasutusele tõhusad riskihaldusvõtted ja teataksid raskematest intsidentidest riiklikele ametiasutustele. Need nõuded kehtivad ka kolme tüüpi peamiste internetiteenuste pakkujate suhtes: pilvandmetöötlus, otsingumootorid ja internetipõhised kauplemiskohad. Selle eesmärk on tugevam ja süsteemsem lähenemisviis ja parem teabevahetus.

ELi kübervastupidavusvõime seisukohast on äärmiselt oluline, et kõik liikmesriigid rakendavad 2018. aasta maiks direktiivi täies ulatuses. Seda protsessi toetab liikmesriikide kollektiivne tegutsemine, mis päädib 2017. aasta sügiseks juhistega, et toetada ühtlustatumat rakendamist, eelkõige seoses oluliste teenuste operaatoritega. Komisjon avaldab ka selle küberturvalisuse paketi osana teatise,[33] et toetada liikmesriike nende püüdlustes ning pakkuda liikmesriikide parimaid tavasid, mis on seotud direktiivi rakendamisega, ja juhiseid selle kohta, kuidas direktiiv peaks praktikas toimima.

Teabevahetuse osas vajab direktiiv täiendamist. Näiteks hõlmab direktiiv üksnes olulisi strateegilisi sektoreid, kuid loogiliselt võttes oleks vaja kõigi küberründest tabatud sidusrühmade jaoks samasugust lähenemisviisi, et nõrkuseid hinnataks süstemaatiliselt ja uuritaks, mis teid pidi küberründajad sisenevad. Lisaks on avaliku ja erasektori vaheline koostöö ja teabejagamine mitmeti takistatud. Valitsused ja riigiasutused ei taha alati jagada küberturvalisuse seisukohast olulist teavet, kartes kahjustada riikliku julgeolekut või konkurentsivõimet. Eraettevõtjad ei taha jagada teavet oma kübernõrkuste ja sellest tuleneva kahju kohta, kartes avalikustada tundlikku äriteavet, riskida oma mainega või riskida andmekaitse normide rikkumisega[34]. Usaldust on vaja parandada, et avaliku ja erasektori partnerlused toetaksid laiemat koostööd ja suuremat teabejagamist rohkemate sektorite vahel. Teabe jagamise ja analüüsimise keskuste roll on eriti oluline, et luua era- ja avaliku sektori vahel teabejagamiseks vajalik usaldus. Esimesed sammud konkreetsetes elutähtsates sektorites on tehtud: näiteks lennunduses on loodud Euroopa lennunduse küberjulgeoleku

[32] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.

[33] COM(2017) 476.

[34] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017. Eraldi teema on ärisaladused. 2016. aasta juuli teatises „Euroopa kübervastupidavusvõime süsteemi tugevdamine“ nimetati, et ärisaladuste kübervargustest teatamisse suhtutakse vastumeelsusega, ja rõhutati, kui olulised on usaldusväärsed teatamiskanalid, mis tagavad konfidentsiaalsuse.

keskus[35] ja energeetikas on välja kujundatud teabe jagamise ja analüüsimise keskuseid[36]. Komisjon toetab igati seda lähenemisviisi ENISA abiga. Eelkõige tuleb tõsta kiirust sektorites, mis pakuvad võrgu- ja infoturbe direktiivis kindlaks tehtud olulisi teenuseid.

2.4 Vastupidavusvõime tänu kiirreageerimisele

Küberründe toimumise korral võib kiire ja tõhusa reageerimisega selle mõju leevendada. Nii saab ka näidata, et võimud ei ole küberrünnete ees abitud, ja see aitab parandada usaldust. Mis puudutab ELi institutsioonide enda reageerimist, siis esmalt tuleb küberaspektid integreerida olemasolevatesse ELi kriisiohjemehhanismidesse, milleks on kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord, mida koordineerib eesistujariik,[37] ja ELi üldised kiirhoiatussüsteemid[38]. Vajadus reageerida eriti raskele küberintsidendile või -ründele võib olla liikmesriigi jaoks piisav põhjus ELi solidaarsusklausli[39] kohaldamiseks.

Kiire ja tõhus reageerimine eeldab ka kiire teabevahetusmehhanismi olemasolu kõigi oluliste osalejate vahel riiklikul ja ELi tasandil, mis omakorda eeldab selgust nende vastavates rollides ja ülesannetes. Komisjon on seoses tegevuskavaga konsulteerinud institutsioonide ja liikmesriikidega, et luua tõhus protsess operatiivseks reageerimiseks liidu ja liikmesriikide tasandil ulatuslike küberintsidentide korral. Käesoleva paketi raames soovitusena esitatud **tegevuskavas**[40] selgitatakse, kuidas küberturvalisus on integreeritud olemasolevatesse ELi tasandi kriisiohjemehhanismidesse, ja kirjeldatakse liikmesriikide ning liikmesriikide ja ELi institutsioonide, asutuste ja organite[41] vahelise koostöö eesmärke ja viise ulatuslikele küberintsidentidele ja kriisidele reageerimise korral. Soovituse kohaselt peaksid liikmesriigid ja ELi institutsioonid tegevuskava rakendamiseks ühtlasi looma küberturvalisuse kriisidele reageerimise ELi raamistiku. Tegevuskava tuleks regulaarselt testida nii küberkriiside haldamise kui ka muude kriiside ohjamise õppustel[42] ja vajadusel tuleks seda ajakohastada.

Arvestades, et küberintsidendid võivad oluliselt mõjutada majanduse toimimist ja inimeste igapäevaelu, võiks uurida ka võimalust luua **küberturvalisuse kiirreageerimisfond**, võttes eeskujuks muud sellised kriisimehhanismid muudes ELi poliitikavaldkondades. See aitaks liikmesriikidel saada ELi tasandil abi olulise intsidendi käigus või pärast seda, tingimusel et liikmesriigis on enne intsidendi toimumist loodud usaldusväärne küberturvalisuse süsteem, mis hõlmab muu hulgas võrgu- ja infoturbe direktiivi täielikku rakendamist, hästi väljaarendatud riskihaldust ja riikliku tasandi järelevalveraamistikku. Sellist olemasolevaid ELi tasandi kriisiohjemehhanisme täiendavat fondi saaks kasutada kiirreageerimisvõimena solidaarsuse huvides ja konkreetsete erakorraliste reageerimismeetmete rahastamiseks, nt rikutud seadmete väljavahetamiseks või leevendamise või reageerimisvahendite

---

35 https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

36 Tegemist on liikmelisusel põhinevate mittetulundusorganisatsioonidega, mis koosnevad era- ja avaliku sektori üksustest ja mille eesmärk on jagada teavet küberohtude, -riskide, ärahoidmise, leevendamise ja reageerimise kohta. Vt nt Euroopa energiavaldkonna teabe jagamise ja analüüsimise keskused (http://www.ee-isac.eu).

37 Nii on võimalik koordineerida reageerimist valdkondadevahelistele kriisidele kõige kõrgemal poliitilisel tasandil.

38 Need süsteemid võimaldavad süsteemisiseselt teabejagamist ja koordineerimist esilekerkivate mitut sektorit hõlmavate kriiside või ettenähtavate või otseste ohtude korral, mis vajavad tegutsemist ELi tasandil.

39 Euroopa Liidu toimimise lepingu artikli 222 kohaselt.

40 C(2017) 6100.

41 Sealhulgas Europol, ENISA, ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm (CERT-EU) ja Euroopa Liidu luureandmete analüüsi keskus (INTCEN).

42 Näiteks ENISA korraldatavad õppused: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

kasutuselevõtmiseks, kasutades ära riiklikke erialateadmisi, nagu seda tehakse ELi kodanikukaitse mehhanismis.

2.5 Küberturvalisuse pädevusvõrgustik Euroopa küberturvalisuse uurimis- ja pädevuskeskusega

Küberturvalisuse tehnoloogilised vahendid on ühest küljest strateegilised vahendid, aga teisalt ka tulevase majanduskasvu võtmetehnoloogiad. Oma strateegiliste huvide kindlustamiseks tuleb ELil säilitada peamised võimed ja neid arendada, et tagada turvaline digimajandus, ühiskond ja demokraatia ning kaitsta elutähtsat riist- ja tarkvara ja pakkuda peamisi küberturbeteenuseid.

2016. aastal loodud küberturvalisust käsitlev avaliku ja erasektori partnerlus[43] oli esimene oluline samm, millega kaasneb kuni 1,8 miljardi euro ulatuses investeeringuid 2020. aastaks. Samas näitab mujal maailmas tehtavate investeeringute maht,[44] et EL peab investeeringuid suurendama ja saama üle võimete killustatusest üle ELi.

EL saab siin luua lisaväärtust, arvestades küberturvalisuse tehnoloogia keerukust, vajalikke ulatuslikke investeeringuid ja vajadust lahenduste järele, mis töötavad kõikjal ELis. Tuginedes liikmesriikide ning avaliku ja erasektori partnerluse tööle, tuleks järgmise sammuna suurendada ELi küberturvalisuse alast suutlikkust, kasutades selleks **küberturvalisuse pädevuskeskuste võrgustikku,**[45] mille keskmes on **Euroopa küberturvalisuse uurimis- ja pädevuskeskus**. See võrgustik ja keskus stimuleerivad küberturvalisuse valdkonna tehnoloogia arendamist ja kasutuselevõttu ja täiendavad selle valdkonna suutlikkuse parandamist ELi ja riiklikul tasandil. Komisjon algatab mõju hindamise, et hinnata võimalikke variante, sealhulgas ühisettevõtte loomise võimalust, et panna sellele struktuurile alus 2018. aastal.

Esimese sammuna ning tulevasele mõttevahetusele ainese andmiseks teeb komisjon ettepaneku käivitada programmi „Horisont 2020" raames katseetapp, et koondada riiklikud keskused võrgustikku ning anda küberturvalisuse pädevuse ja tehnoloogia arendamisele hoogu juurde. Sel eesmärgil teeb komisjon ettepaneku lühiajaliselt investeerida 50 miljonit eurot. See tegevus täiendab käimasoleva küberturvalisust käsitleva avaliku ja erasektori partnerluse elluviimist.

Võrgustik ja keskus keskenduksid alguses teadustöö koondamisele ja kujundamisele. Selleks et toetada tööstusliku suutlikkuse arendamist, saaks keskus toimida rahvusvaheliste projektide projektijuhina. See annaks ka lisatõuke ELi tööstuse innovatsioonile ja konkurentsivõimele maailma areenil uue põlvkonna digitehnoloogiate, sh tehisintellekti, kvantandmetöötluse, plokiahela ja turvaliste digitaalidentiteetide väljatöötamisel ning tagaks ELis asuvatele äriühingutele juurdepääsu massandmetele: need kõik on tulevikus küberturvalisuse jaoks võtmetähtsusega elemendid. Keskus tugineks ka ELi tööle, et parandada kõrgjõudlusega andmetöötluse taristut: see on suurte andmemahtude analüüsimiseks, andmete kiireks krüpteerimiseks ja dekrüpteerimiseks, identiteetide kontrollimiseks, küberrünnete simuleerimiseks ja videomaterjali analüüsimiseks äärmiselt oluline[46].

---

[43] C(2016) 4400 final.

[44] Ameerika Ühendriigid investeerivad küberturvalisusse ainuüksi 2017. aastal 19 miljardit dollarit, s.t 35 % rohkem kui 2016. aastal. Valge Maja, pressisekretäri büroo. „Fact Sheet: Cybersecurity National Action Plan", 9. veebruar 2016.

[45] Võrgustikku kuuluksid olemasolevad ja tulevased liikmesriikides loodud küberturvalisuse keskused, mille liikmeteks on reeglina riiklikud teadusorganisatsioonid ja laborid.

[46] COM(2012) 45 final ja COM(2016) 178 final.

Pädevuskeskuste võrgustikul peaks olema ka suutlikkus toetada testimise ja simulatsioonide kaudu tööstust, et tagada punktis 2.2 kirjeldatud küberturvalisuse sertifitseerimine. Võrgustiku kaasatus kõigisse ELi küberturvalisuse alastesse toimingutesse tagaks selle, et tema tegevust ajakohastatakse pidevalt vastavalt vajadustele. Keskuse eesmärgiks poleks üksnes tagada kõrged küberturbe standardid tehnoloogias ja küberturvalisuse süsteemides, vaid ka erialatöötajate jaoks kõrgetasemeliste pädevuste väljatöötamine, pakkudes riikide jaoks välja digioskuste arendamise lahendusi ja näidiseid. Sellisel kujul parandaks see küberturvalisuse suutlikkust ELi tasandil ja looks koostoime eelkõige ENISA, CERT-EU, Europoli, võimaliku tulevase küberturvalisuse kiirreageerimisfondi ja riikide CSIRTidega.

Teema, millele pädevusvõrgustik peab oma töös eriliselt keskenduma, on Euroopa suutlikkus hinnata toodete ja teenuste **krüpteerimist**, mida kasutavad kodanikud, ettevõtted ja valitsused digitaalsel ühtsel turul. Tugev krüpteerimine on turvalise digitaalse tuvastamise süsteemide alus ja sellel on tõhusa küberturvalisuse tagamisel äärmiselt oluline roll[47]. See aitab ka kindlustada inimeste intellektuaalomandi turvalisuse, kaitsta põhiõiguseid, nagu väljendusvabadus, ja isikuandmeid ning tagada turvalise e-kaubanduse[48].

ELi tsiviil- ja kaitsevaldkonna küberturvalisuse turgude probleemid on sarnased[49] ja ka kahesuguse kasutusega tehnoloogia eeldab tihedat koostööd elutähtsates valdkondades. Seepärast võiks võrgustikku ja selle keskust teises etapis edasi arendada ja lisada küberkaitsemõõtme, järgides samal ajal aluslepingus ühise julgeoleku- ja kaitsepoliitika kohta sätestatut. Lisaks sellele tehnoloogilisele suunale aitaks kaitsemõõde parandada küberkaitse alast koostööd liikmesriikide vahel, sh teabevahetuse, olukorrateadlikkuse, teadmiste parandamise ja koordineeritud reageerimise kaudu, ja toetaks liikmesriike ühisvõimete arendamisel. See võiks toimida ka platvormina, mille kaudu liikmesriikidel on võimalik panna paika ELi küberkaitse prioriteedid, otsida ühiseid lahendusi, panustada ühiste strateegiate väljatöötamisse, hõlbustada ühiseid küberkaitse alaseid koolitusi, õppusi ja testimist Euroopa tasandil ja toetada tööd küberkaitse taksonoomiate ja standardite kallal, kus keskusel oleks toetav ja nõuandev roll. Ülalnimetatud tegevuste elluviimiseks peaks keskus tegema küberkaitse valdkonnas tihedat ja üksteist täiendavat koostööd Euroopa Kaitseagentuuriga ning kübervastupanuvõime valdkonnas ENISAga. Selles kaitsemõõtmes võetaks arvesse Euroopa kaitse tulevikku käsitlevas aruteludokumendis algatatud protsessi.

Küberkaitses nõutav kõrge vastupidavusvõime eeldab väga sihipärast teaduslikku ja tehnoloogilist tegevust. Äriühingute väljatöötatud küberkaitsealaseid projekte või tehnoloogiaid saaks nii teadus- kui ka arendustegevuse etapis rahastada Euroopa Kaitsefondist[50]. Konkreetsed valdkonnad nagu kvanttehnoloogiatel põhinevad krüpteerimise süsteemid, küberolukorrateadlikkus, juurdepääsu biomeetrilise reguleerimise süsteemid, kinnisründeohtude avastamine või andmekaeve võiksid siinkohal olla eriti asjakohased. Kõrge esindaja, Euroopa Kaitseagentuur ja komisjon toetavad liikmesriike, et selgitada välja valdkonnad, kus võiks kaaluda ühiste küberturvalisuse projektide elluviimist Euroopa Kaitsefondi toetusel.

2.6 Tugeva ELi küberoskuste baasi tagamine

[47] Komisjon paneb juba programmi „Horisont 2020“ raames välja rahalise auhinna, millega premeeritakse e-autentimismeetodite seast parimat innovatiivset lahendust 4 miljoni euroga.

[48] Cybersecurity in the European Digital Single Market, High level group of Scientific Advisors, March 2017.

[49] *Study on synergies between the civilian and the defence cybersecurity markets* (Optimity; SMART 2014-0059).

[50] Küberkaitsealased projektid on juba praegu seatud Euroopa kaitsetööstuse arenguprogrammis prioriteediks ja küberkaitse on üks 2018. aastal korraldatavate projektikonkursside teemadest.

Küberturvalisusega seondub tugevalt hariduslik mõõde. Tõhus küberturvalisus sõltub palju sellest, millised on asjaomaste isikute oskused. Prognooside kohaselt on aastaks 2022 Euroopas erasektoris puudu 350 000 küberturbepädevustega erialaspetsialisti[51]. Küberturvalisuse valdkonna haridust tuleks parandada kõigil tasanditel, alustades kübervaldkonna töötajate korrapärase koolituse, kõigi IT-spetsialistide küberturvalisuse alase täiendkoolituse ja uute spetsiifiliste küberturvalisuse õppekavadega. Tuleks luua tugevad akadeemilise pädevuse keskused, et rahuldada vajadused kiirendatud õppe ja koolituse järele, mis võiks põhineda Euroopa küberturvalisuse uurimis- ja pädevuskeskuse ja ENISA juhistel. Eesmärk on, et selliste IKT-toodete ja -süsteemide loomine, kus turvalisuse põhimõtetega arvestatakse juba algusest peale, muutuks iseenesestmõistetavaks. Küberturvalisuse alane haridus ei tohiks piirduda IT-spetsialistidega, vaid küberturvalisust tuleks arvesse võtta ka teiste valdkondade õppekavades, nagu inseneriteadustes, ärijuhtimises või õigusteaduses, ja ka konkreetsete sektorite kutseõppes. Lõpuks tuleks parandada digioskuste omandamise käigus koolis nii alg- kui ka keskkooli õpetajate ja õpilaste teadlikkust küberkuritegevusest ja -turvalisusest.

Ka EL peaks koos liikmesriikidega aitama sellele tööle kaasa, tuginedes digioskuste ja töökohtade koalitsioonile[52] ja luues näiteks VKEde jaoks küberturvalisusega seotud praktikakavu.

2.7 Küberhügieeni ja küberteadlikkuse propageerimine

Kuna 95 % küberintsidentidest on väidetavalt põhjustatud „teatavat liiki inimlikust eksimusest (kas tahtlikust või mitte)“,[53] siis on inimteguril oluline osa. Seega vastutame me kõik küberturvalisuse eest. See tähendab, et peab muutuma meie isiklik käitumine, aga ka ettevõtete ja haldusasutuste käitumine tagamaks, et kõik mõistavad ohu tõsidust ning omavad vahendeid ja oskusi, mille abil rünne kiiresti avastada ja end selle vastu aktiivselt kaitsta. Inimesed peavad välja kujundama küberhügieeniharjumused ning ettevõtted ja organisatsioonid peavad vastu võtma nõuetekohased riskipõhised küberturvalisuse programmid ja neid korrapäraselt ajakohastama, et need kajastaksid muutuvat riskikeskkonda.

Võrgu- ja infoturbe direktiivis nähakse ette liikmesriikide kohustus vahetada teavet ELi tasandil toimuvate küberrünnete kohta ning tehakse neile ülesandeks koostada põhjalik riiklik küberturbestrateegia ja võrgu- ja infosüsteemide turvalisuse raamistik. Ametiasutustel peaks nii ELi kui ka liikmesriikide tasandil ka edaspidi olema nende jõupingutuste tegemisel juhtiv roll.

Esiteks, liikmesriigid peaksid tegema küberturbevahendid ettevõtetele ja inimestele võimalikult kättesaadavaks. Eelkõige tuleks rohkem teha selleks, et ennetada küberkuritegevust ja leevendada selle mõju lõppkasutajale. Üheks näiteks on Europoli kampaania „Ei lunavarale“ (NoMoreRansom),[54] mis töötati välja õiguskaitseasutuste ja küberturbeettevõtete tihedas koostöös, et aidata kasutajal ennetada lunavaraga nakatumist ja dekrüptida andmed, kui ta on langenud ründe ohvriks. Samalaadsed projektid tuleks töötada välja ka muud liiki pahavara jaoks ja muudes valdkondades ning EL peaks looma **koondportaali, et pakkuda kõiki asjaomaseid vahendeid ühtse kontaktpunkti kaudu**, kus

[51] *Global Information Security Workforce Study 2017*. Maailma tasandil on prognoositud puudujäägiks 1,8 miljonit.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM „The Cybersecurity Intelligence Index“ 2014, viidatud väljaandes Securitymagazine.com, 19. juuni 2014.

[54] https://www.nomoreransom.org/.

antaks kasutajatele nõu selle kohta, kuidas ennetada pahavararündeid ja avastada pahavara, ja jagataks teavitusmehhanismide linke.

Teiseks peaksid liikmesriigid kiirendama **e-halduse arendamisel küberturvalisemate vahendite kasutuselevõttu** ja kasutama täies ulatuses pädevusvõrgustiku võimalusi. Turvaliste identifitseerimisvahendite vastuvõtmist tuleks edendada, võttes aluseks e-identimise ja e-tehingute jaoks vajalike usaldusteenuste jaoks siseturul loodud ELi raamistiku, mis jõustus 2016. aastal ja millega on loodud prognoositav regulatiivne keskkond, et võimaldada turvalist ja sujuvat elektroonilist suhtlust ettevõtete, kodanike ja ametiasutuste vahel[55]. Lisaks sellele peavad eelkõige need avaliku sektori asutused, kes osutavad esmatähtsaid teenuseid, tagama, et nende töötajad on läbinud koolituse küberturvalisusega seotud valdkondades.

Kolmandaks, liikmesriigid peaksid seadma küberteadlikkuse esikohale muu hulgas koolides, ülikoolides, ettevõtetes ja teadusasutustes korraldatavates **teadlikkuse suurendamise kampaaniates**. Iga aasta oktoobris ENISA koordineerimisel korraldatav küberturvalisuse kuu ei piirdu enam ühise teavitamisega ELi ja liikmesriigi tasandil, vaid püütakse saavutada suurem ulatus. Sama tähtis on suurendada teadlikkust internetis korraldatavatest **väärteabe levitamise kampaaniatest** ja sotsiaalmeedias levivatest **libauudistest**, mille eesmärk on õõnestada demokraatlikke protsesse ja Euroopa väärtusi. Kuigi esmane vastutus muu hulgas Euroopa Parlamendi valimiste korraldamise eest jääb liikmesriikidele, on eksperditeadmiste kogumine ja kogemuste jagamine Euroopa tasandil osutunud lisaväärtuseks, võimaldades meetmeid paremini suunata[56].

Oluline roll on ka **tööstusel** laiemalt, kuid eelkõige digiteenuste osutajatel ja tootjatel. Tööstus peab toetama kasutajaid (ettevõtteid, kodanikke ja haldusasutusi) vahenditega, mis võimaldavad neil võtta vastutuse oma tegevuse eest internetis, ja tegema selgeks, et küberhügieeni eest hoolitsemine on tarbijatele pakutava teenuse lahutamatu osa[57]. Selleks et nõrkused avastada ja kõrvaldada, peab tööstus püüdma kehtestada sisemise korra nõrkuste uurimiseks, nende tähtsusjärjestusse seadmiseks ja lahendamiseks, olenemata sellest, kas potentsiaalne nõrkus tekkis väljaspool asjaomast ettevõtet või selle sees.

Peamised meetmed

- Rakendada täielikult võrgu- ja infosüsteemide turvalisuse direktiiv;
- võtta Euroopa Parlamendis ja nõukogus kiiresti vastu määrus, millega nähakse ette ENISA uued ülesanded ja kehtestatakse sertifitseerimise Euroopa raamistik[58];
- komisjoni ja tööstuse ühisalgatus eesmärgiga määratleda hoolsuskohustuse põhimõte, et vähendada toodete ja tarkvara nõrkusi ning edendada sisseprojekteeritud turvalisuse põhimõtet;
- rakendada kiiresti ulatuslikele piiriülestele küberintsidentidele reageerimise tegevuskava;
- algatada mõju hindamine, et uurida võimalust esitada 2018. aastal komisjoni ettepanek,

[55] Määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul võeti vastu 23. juulil 2014. Samuti pakub Euroopa Komisjon Euroopa ühendamise rahastu programmi kaudu e-identimise ja e-allkirja koostalitlusvõime aluselemente ja vahendeid (nt usaldusnimekirjade brauserid).

[56] Üheks näiteks on idanaabruse strateegilise kommunikatsiooni töörühm, mille 2015. aastal moodustasid liikmesriigid ning ühise välis- ja julgeolekupoliitika kõrge esindaja, et võidelda Venemaa korraldatavate väärteabe levitamise kampaaniatega. Töörühm tegeleb idapartnerluse piirkonnas ELi poliitikat selgitavate teabevahetustoodete ja -kampaaniate väljatöötamisega.

[57] Osa tootjaid on selle käsituse juba omaks võtnud: osades tooteid reguleerivates Euroopa õigusaktides (nt masinaid käsitlev direktiiv 2006/42/EÜ) nähakse ette meetmed, mis käsitlevad sisseprojekteeritud ohutust.

[58] COM(2017) 477.

mis käsitleb küberturvalisuse pädevuskeskuste võrgustiku ning Euroopa küberturvalisuse uurimis- ja pädevuskeskuse loomist, lähtudes vahetult eelnenud katseetapi kogemustest;
- toetada liikmesriike, et selgitada välja valdkonnad, kus võiks kaaluda ühiste küberturvalisuse projektide elluviimist Euroopa Kaitsefondi toetusel;
- luua küberrünnete ohvrite aitamiseks üleeuroopaline ühtne kontaktpunkt, mille kaudu antakse teavet uusimate ohtude kohta ning kuhu on koondatud praktilised nõuanded ja küberturvalisuse vahendid;
- liikmesriikide meetmed eesmärgiga koondada küberturvalisuse alane teave oskuste omandamise programmidesse, e-valitsusse ja teadlikkuse parandamise kampaaniatesse;
- tööstuse meetmed, mille eesmärk on tõhustada oma töötajatele pakutavat küberturvalisuse alast koolitust ning võtta vastu oma toodete, teenuste ja protsesside suhtes kohaldatav sisseprojekteeritud turvalisuse lähenemisviis.

3. TULEMUSLIKU ELi KÜBERHEIDUTUSE VÄLJATÖÖTAMINE

Tulemuslik heidutus tähendab, et kehtestatakse võimalike küberkurjategijate ja küberrünnete toimepanijate suhtes usutavate ja samas hoiatavate meetmete raamistik. Kuni küberrünnete toimepanijate (nii riikidega mitteseotud osalejate kui ka riikide) ainus hirm on ebaõnnestumine, puudub neil põhjus mitte proovida. Tõhusamad õiguskaitsemeetmed, mis keskenduvad küberrünnete avastamisele ja jälgitavusele ning küberkurjategijatele süüdistuse esitamisele, on tulemusliku heidutuse tagamiseks kesksel kohal. Lisaks peab EL toetama liikmesriike kahesuguse kasutusega küberturvalisuse alase suutlikkuse väljatöötamisel. Võttes meetmeid, mis suurendavad võimalust, et küberründe toimepanija tabatakse ja teda karistatakse, on võimalik vähendada küberrünnete arvu. Küberrünnete uurimine peaks toimuma kiiresti ja kuriteo toimepanija tuleks anda kohtu alla või tuleks võtta meetmed, mis võimaldavad asjakohast poliitilist või diplomaatilist tegutsemist. Kui on tegemist tõsise kriisiga, millel on oluline rahvusvaheline ja kaitsemõõde, võib ühise välis- ja julgeolekupoliitika kõrge esindaja teha nõukogule ettepanekuid asjakohase reageerimise kohta.

Samm kriminaalõiguse paremaks kohaldamiseks küberrünnete korral astuti 2013. aastal, kui võeti vastu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid[59]. Selles on sätestatud miinimumnormid, mis käsitlevad kuritegude määratlemist ja karistusi infosüsteemide vastu suunatud rünnete valdkonnas, ning nähakse ette operatiivmeetmed ametiasutustevahelise koostöö parandamiseks. Tänu direktiivile on tehtud märkimisväärseid edusamme, et kriminaliseerida küberründed võrreldaval tasemel kõikides liikmesriikides, lihtsustades nii seda liiki kuritegusid uurivate õiguskaitseasutuste piiriülest koostööd. Siiski saaks direktiivi kõiki võimalusi paremini ära kasutada, kui liikmesriigid rakendaksid kõiki selle sätteid täielikult[60]. Komisjon toetab liikmesriike ka edaspidi direktiivi rakendamisel ega pea praegu vajalikuks teha ettepanekuid selle muutmiseks.

3.1 Pahatahtlike osalejate kindlakstegemine

Selleks et suurendada võimalusi kuritegude toimepanijate kohtu alla andmiseks, peame viivitamata suurendama oma suutlikkust avastada küberrünnete toimepanijad. Küberkuritegude uurimiseks kasuliku teabe, enamasti digitaalsete jälgede leidmine on õiguskaitseasutuste jaoks keeruline ülesanne. Seetõttu peame suurendama oma tehnoloogilist

[59] Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid.

[60] COM(2017) 474.

suutlikkust kuritegusid tulemuslikult uurida, sealhulgas tugevdades Europoli küberkuritegevuse osakonda küberekspertidega. Europol on omandanud olulise rolli mitut jurisdiktsiooni hõlmavat uurimist läbiviivate liikmesriikide toetamisel. Temast peaks saama internetiuurimiste ja küberkriminalistika alaste teadmiste keskus liikmesriikide õiguskaitseasutuste jaoks.

Levinud praktika, mille kohaselt paljudel, mõnikord isegi tuhandetel, kasutajatel on üks IP-aadress, muudab pahatahtliku internetikäitumise uurimise tehniliselt väga keerukaks. Samuti osutub seetõttu mõnikord, näiteks selliste raskete kuritegude nagu lapse seksuaalse kuritarvitamise korral, vajalikuks paljude kasutajate uurimine, et tuvastada üks pahatahtlik kasutaja. EL kutsub seetõttu üles võtma kasutusele uue protokolli (IPv6), sest see võimaldab eraldada igale kasutajale IP-aadressi ning toob nii otsest kasu õiguskaitses ja küberturvalisusega seotud uurimistes. Selleks et soodustada üleminekut, kavatseb komisjon esimese sammuna lisada oma tegevuspõhimõtetesse nõude minna üle IPv6-le, seda muu hulgas avalike hangete ning projektide ja teadustegevuse rahastamise nõuetes, ning ühtlasi toetada vajalike koolitusmaterjalide koostamist. Lisaks peaksid liikmesriigid kaaluma vabatahtlikke kokkuleppeid internetiteenuste pakkujatega, et edendada IPv6 kasutuselevõtmist.

Belgia on IPv6 kasutuselevõtu ulatuselt maailmas[61] *esirinnas, muu hulgas tänu avaliku ja erasektori koostööle: asjaomased sidusrühmad on kaalunud osana vabatahtlikust isereguleerivast meetmest ühe IP-aadressi kasutamise piiramist maksimaalselt 16 kasutajaga, soodustades nii üleminekut IPv6-le*[62].

Üldisemalt tuleks edendada võrguvastutust. See tähendab selliste meetmete edendamist, millega ennetatakse domeeninimede väärkasutust soovimatute teadete levitamiseks või andmepüügiks. Komisjon kavatseb tegutseda selle nimel, et parandada teabe toimimist ning kättesaadavust ja täpsust domeeninime ja IP-WHOIS[63] süsteemides kooskõlas interneti nimede ja numbrite määramise korporatsiooni[64] jõupingutustega.

3.2 Tõhusamad õiguskaitsemeetmed

Küberruumi kasutades toime pandud kuritegude tulemuslik **uurimine** ja nende eest **süüdistuse esitamine** on peamine mõjutusvahend küberrünnete vastu. Praegune menetlusraamistik tuleb siiski paremini kohandada internetiajastu vajadustele[65]. Küberrünnete toimumise kiirus võib praeguste menetluste juures põhjustada ülekoormust ja samuti tekib viivitamatu piiriülese koostöö vajadus. Nagu Euroopa julgeoleku tegevuskavas välja kuulutatud, esitab komisjon selle probleemi lahendamiseks 2018. aasta alguses ettepanekud, milles käsitletakse **elektroonilistele tõenditele piiriülese juurdepääsu lihtsustamist**. Samal ajal rakendab komisjon praktilisi meetmeid, millega parandatakse kriminaaluurimises

[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[62] http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

[63] Päringute ja vastuste protokoll, mida kasutatakse laialdaselt päringute saatmiseks andmebaasidesse, kus salvestatakse internetiallikate registreeritud kasutajaid või kliente.

[64] Interneti nimede ja numbrite määramise korporatsioon (ICANN) on mittetulundusühendus, kes vastutab mitme interneti nimeruumidega seotud andmebaasi hoolduse ja töö koordineerimise eest.

[65] Toome ainult ühe näite: Avalanche'i robotivõrgu (virtuaalne) keskne juhtserver muutis füüsiliste serverite ja domeenide asukohta iga viie minuti järel.

piiriülest juurdepääsu elektroonilistele tõenditele, sealhulgas rahastab ta piiriülese koostöö koolitusi, ELis teabevahetuseks kasutatava elektroonilise platvormi arendamist ning liikmesriikidevaheliste õigusalase koostöö vormide standardimist.

Tulemuslikku süüdistuse esitamist takistab ka see, et küberkuritegude uurimise käigus elektrooniliste tõendite kogumiseks kasutatavad kohtumenetlused on liikmesriigiti erinevad. Seda olukorda on võimalik parandada, kui kehtestatakse ühised kohtuekspertiisistandardid. Lisaks jälgitavusele ja vastutuse väljaselgitamisele tuleb tugevdada kohtuekspertiisi suutlikkust. Üks võimalusi oleks Europoli kohtuekspertiisisuutlikkuse edasiarendamine nii, et Europoli küberkuritegevuse vastase võitluse Euroopa keskuse praegused eelarvevahendid ja inimressursid vastaksid kasvavale vajadusele operatiivtoe järele piiriüleste küberkuritegude uurimisel. Samuti võiks kasutada ära eespool kirjeldatud tehnoloogilist keskendumist krüpteerimisele, uurides seda, kuidas selle kasutamine kurjategijate poolt tekitab suuri probleeme võitluses raskete kuritegudega, sealhulgas terrorismi ja küberkuritegevusega. Oktoobriks 2017[66] esitab komisjon dokumendi praegu **krüpteerimise rolli üle kriminaaluurimises**[67] toimuva arutelu tulemustega.

Arvestades interneti piirideta olemust, pakub Euroopa Nõukogu **Budapesti küberkuritegevuse konventsiooniga**[68] loodud rahvusvahelise koostöö raamistik väga erinevate riikide rühmale võimaluse kasutada erinevate küberkuritegevust käsitlevate riiklike õigusnormide korral optimaalset õiguslikku standardit. Praegu uuritakse võimalust lisada konventsioonile protokoll;[69] sellega võiks kaasneda hea võimalus tegeleda piiriülese juurdepääsuga elektroonilistele tõenditele rahvusvahelistes olukordades. Selle asemel et koostada uusi rahvusvahelisi õiguslikke vahendeid, mis käsitlevad küberkuritegevust, kutsub EL kõiki riike üles koostama asjakohaseid siseriiklikke õigusakte ja edendama koostööd olemasolevas rahvusvahelises raamistikus.

Andmete anonüümseks muutmise vahendite ulatuslik kättesaadavus muudab kurjategijate jaoks enda varjamise lihtsamaks. **Pimevõrk**[70] on loonud kurjategijatele uued võimalused juurdepääsuks lapspornole, narkootikumidele ja tulirelvadele ning sageli on oht vahele jääda väike[71]. Samuti on sellest saanud küberkuritegude toimepanemiseks kasutatavate vahendite, nagu pahavara ja häkkimisvahendite peamine allikas. Koos asjaomaste sidusrühmadega kavatseb komisjon analüüsida liikmesriikide lähenemisviise, et töötada välja uusi lahendusi. Europol peaks lihtsustama ja toetama pimevõrku käsitlevaid uurimisi, hindama ohte ning

---

66 Kaheksas eduaruanne tulemusliku ja tegeliku julgeolekuliidu suunas liikumise kohta, 29. juuni 2017 (COM(2017) 354 final).

67 Eesistujariik, justiits- ja siseküsimuste nõukogu 8. ja 9. detsembri 2016. aasta istungi tulemused, dokument nr 15391/16.

68 Konventsioon on esimene rahvusvaheline kokkulepe, mis käsitleb interneti ja muude arvutivõrkude kaudu toime pandud kuritegusid, tegeledes eelkõige autoriõiguse rikkumise, arvutitega seotud pettuste, lapsporno ja võrguturbe rikkumisega. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 2017. aastal olid Euroopa Nõukogu küberkuritegevuse konventsiooni ratifitseerinud või sellega ühinenud 55 valitsust.

69 Pädevus valmistada ette Budapesti küberkuritegevuse konventsiooni teise lisaprotokolli eelnõu, T-CY (2017)3.

70 Pimevõrk koosneb sisust pealisvõrkudes, mis kasutavad internetti, kuid millele juurdepääsuks on vaja teatavat tarkvara, konfiguratsiooni või luba. Pimevõrk moodustab väikese osa süvaveebist – veebi sellest osast, mida otsingumootorid ei indekseeri.

71 Oluline erand on kahe suurima kuritegeliku pimeveebi turu (AlphaBay ja Hansa) hiljutine sulgemine: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

aitama kindlaks määrata jurisdiktsiooni ja tegelema eelkõige kõrge riskiga juhtumitega, samas võib EL mängida juhirolli rahvusvaheliste meetmete koordineerimisel[72].

Küberkuritegevus elavneb sellises valdkonnas nagu krediitkaartide või muude elektrooniliste maksevahendite andmete kasutamine pettuse eesmärgil. Internetis tegutsevate jaemüüjate või muude seaduslike äriühingute vastu suunatud küberrünnete kaudu saadud makseandmeid müüakse internetis ja kurjategijad saavad neid kasutada pettuste toimepanemiseks[73]. Komisjon teeb ettepaneku kasutada heidutuse tõhustamiseks uut **direktiivi, mis käsitleb mittesularahaliste maksevahenditega seotud pettuste ja võltsimise vastast võitlust**[74]. Selle eesmärk on ajakohastada valdkonnas kehtivad õigusnormid ja suurendada õiguskaitseasutuste suutlikkust selle kuriteoliigiga võidelda.

Liikmesriikide õiguskaitseasutuste küberkuritegude uurimise suutlikkust tuleb suurendada, samuti tuleb parandada arusaama küberruumi kasutades toime pandud kuritegudest ning prokuröride ja kohtunike uurimisvõimalusi. Eurojust ja Europol toetavad seda eesmärki ja paremat koordineerimist, tehes tihedat koostööd spetsiaalsete nõuanderühmadega Europoli küberkuritegevuse vastase võitluse keskuses ning küberkuritegevuse üksuste juhtide ja küberkuritegevusele spetsialiseerunud prokuröride võrgustikuga. Komisjon eraldab küberkuritegevuse vastaseks võitluseks 10,5 miljonit eurot, eelkõige **politseikoostöö, kuritegevuse tõkestamise ja selle vastu võitlemise ning kriisiohje rahastamisvahendi programmi** raames. Koolituste korraldamine on oluline ning küberkuritegevusalase hariduse ja koolituse Euroopa töörühm on koostanud hulga kasulikke õppematerjale. Neid tuleks õiguskaitseasutuste töötajate hulgas laialt levitada, kasutades selleks Euroopa Liidu Õiguskaitsekoolituse Ameti (CEPOL) abi.

3.3 Avaliku ja erasektori koostöö küberkuritegevusevastases võitluses

Traditsiooniliste õiguskatsevahendite tulemuslikkus digitaalmaailmas on küsitav, sest digitaalne keskkond koosneb enamasti eraomandis olevast taristust ja paljudest erinevatest osalejatest, kes tegutsevad mitmes jurisdiktsioonis. Seetõttu on tulemuslikuks võitluseks kuritegevusega hädasti vaja ametiasutuste koostööd erasektoriga, sealhulgas tööstuse ja kodanikuühiskonnaga. Samuti on tähtis roll finantssektoril, kellega tuleks koostööd tõhustada. Näiteks tuleks suurendada rahapesu andmebüroode[75] tähtsust küberkuritegevusevastases võitluses.

Osa liikmesriike on juba astunud olulisi samme. Madalmaades teevad finantsasutused ja õiguskaitseasutused elektroonilise kuritegevuse töörühmas tihedat koostööd, et võidelda internetipettuste ja küberkuritegevusega. Saksamaa küberkuritegevusevastane pädevuskeskus on liikmete jaoks operatiivkeskus, kus vahetatakse teavet tihedas koostöös Saksamaa Föderaalpolitseiga ja töötatakse välja meetmeid, mille eesmärk on tagada kaitse küberkuritegevuse vastu. 16 liikmesriiki[76] on loonud küberkuritegevuse tippkeskused, et lihtsustada õiguskaitseasutuste, akadeemiliste ringkondade ja erasektori koostööd, mille

[72] Europolil juba on selles valdkonnas oluline roll. Vt hiljutist näidet aadressil: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] Pettusest saadud tulu on organiseeritud kuritegevuse oluline tuluallikas ja soodustab muid kuritegevuse liike, nagu terrorism, ebaseaduslik uimastikaubandus ja inimkaubandus.

[74] COM(2017) 489.

[75] Rahapesu andmebürood on riiklikud keskused, kes võtavad vastu ja analüüsivad teateid kahtlaste tehingute kohta ja muud teavet rahapesu, sellega seotud eelkuritegude ja terrorismi rahastamise kohta ning levitavad analüüsi tulemusi.

[76] Austria, Belgia, Bulgaaria, Eesti, Hispaania, Iirimaa, Kreeka, Küpros, Leedu, Poola, Prantsusmaa, Rumeenia, Saksamaa, Sloveenia, Tšehhi Vabariik ja Ühendkuningriik.

eesmärk on parimate tavade väljatöötamine ja vahetamine, koolitused ja suutlikkuse arendamine.
Komisjon toetab avaliku ja erasektori partnerluste ja koostöömehhanismide loomist selliste sihtotstarbeliste projektide kaudu nagu internetipettuste küberkeskus ja ekspertide võrgustik,[77] *kes rakendab teabevahetuse mudelit ja standardit eesmärgiga analüüsida elektrooniliste kuritegude ohtu ja internetipettusi ning vähendada nende arvu.*

Eraettevõtted peavad saama vahetada õiguskaitseasutustega teavet (sealhulgas isikuandmeid) konkreetsete küberkuritegevuse intsidentide kohta, järgides seejuures täielikult andmekaitse norme. ELi andmekaitsereform, mida hakatakse kohaldama 2018. aasta mais, sätestab ühised eeskirjad, millega nähakse õiguskaitseasutuste ja erasektori asutuste koostöö tingimused. Euroopa Komisjon kavatseb teha Euroopa Andmekaitsenõukogu ja asjaomaste sidusrühmadega koostööd, et selgitada välja parim tava selles valdkonnas ning anda vajaduse korral suuniseid.

3.4 Tugevam poliitiline reaktsioon

Hiljuti vastuvõetud **pahatahtlikule kübertegevusele reageerimise ELi ühises diplomaatilises raamistikus**[78] („küberdiplomaatia meetmete kogum“) sätestatakse ühise välis- ja julgeolekupoliitika meetmed, sealhulgas piiravad meetmed, mida on võimalik kasutada, et tugevdada ELi reaktsiooni tegevusele, mis kahjustab tema poliitilisi, julgeoleku- ja majanduslikke huve. Raamistik on oluline samm, et edendada teavitamis- ja reageerimissuutlikkust nii ELi kui ka liikmesriikide tasandil. See suurendab meie suutlikkust teha kindlaks, kes vastutab pahatahtliku kübertegevuse eest. Eesmärk on mõjutada potentsiaalsete agressorite käitumist, võttes arvesse vajadust tagada proportsionaalsed vastumeetmed. Kas vastutab riik või mitteriiklik üksus, jääb iga riigi sõltumatuks poliitiliseks otsuseks, mis põhineb kõikidest allikatest saadud luureteabel. Liikmesriigid tegelevad praegu raamistiku rakendamisega ning see peaks toimuma tihedas kooskõlas tegevuskavaga, milles käsitletakse reageerimist ulatuslikele küberintsidentidele[79]. Raamistiku kohaselt meetmete võtmiseks vajalikku olukorrateadlikkust peaks koondama, analüüsima ja jagama INTCEN[80] tihedas koostöös liikmesriikide ja ELi institutsioonidega.

3.5 Küberturvalisusega seotud heidutuse tagamine liikmesriikide kaitsevõime kaudu

Liikmesriigid juba tegelevad küberkaitsevõime arendamisega. Arvestades piiride hägustumist küberkaitse ja küberturvalisuse ning kübervahendite ja -tehnoloogiate kahesuguse kasutuse vahel, aga ka suuri erinevusi liikmesriikide lähenemisviisides, on ELil head eeldused aidata edendada tsiviil- ja militaarkoostöö sünergiaid[81].

Liikmesriigid, kellel on suurem küberturvalisuse alane suutlikkus ja kes soovivad teha koostööd, võiksid kaaluda kõrge esindaja, komisjoni ja Euroopa Kaitseagentuuri toetusel küberkaitse kaasamist alalise struktureeritud koostöö (PESCO) raamistikku. Seda võiks

[77] Algatuse EU-OF2CEN eesmärk on võimaldada kogu ELis süstemaatiliselt vahetada pankade ja õiguskaitseasutuste vahel teavet internetipettuste kohta, et ennetada petturitele ja rahamuuladele maksete tegemist ning tegeleda kuritegude uurimisega ja nende toimepanijatele süüdistuste esitamisega. Seda kaasrahastab EL (politseikoostöö, kuritegevuse tõkestamise ja selle vastu võitlemise ning kriisiohje rahastamisvahendi programm).

[78] http://www.consilium.europa.eu/et/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

[79] C(2017) 6100.

[80] JOIN(2016) 018 final.

[81] ELi jaoks on küberruum sama moodi tegevusruum nagu maa, õhk ja vesi. Küberkaitsealased jõupingutused sisaldavad kosmosevarade ja asjaomase maapealse taristu kaitsmist ja vastupidavusvõime tagamist.

toetada eespool kirjeldatud tegevus, et suurendada ELi tööstuslikku suutlikkust ja strateegilist sõltumatust. EL saab edendada koostalitlusvõimet, kui ta hõlbustab suutlikkuse arendamist, koolituste ja hariduse koordineerimist ning kahesuguse kasutusega kaupade standardimist.

Täielikult tuleks ära kasutada hübriidohtudega (millega sageli kaasnevad küberründed) võitlemise ühise raamistiku pakutavad võimalused. Seda peaksid tegema eelkõige ELi hübriidohtude ühiskeskus ja hiljuti Helsingis asutatud Euroopa Hübriidohutõrje Oivakeskus, kelle ülesanne on kutsuda üles pidama strateegilist dialoogi ning tegema teadusuuringuid ja analüüse.

EL kavatseb pöörata suuremat tähelepanu 2014. aastal vastu võetud ELi küberkaitsepoliitika raamistikule,[82] mille eesmärk on küberturvalisuse ja -kaitse kaasamine ühisesse julgeoleku- ja kaitsepoliitikasse. Kesksel kohal on ühise julgeoleku- ja kaitsepoliitika missioonide ja operatsioonide kübervastupidavusvõime. Kavas on välja arendada standardmenetlused ja tehniline suutlikkus, mida saab kasutada nii tsiviil- ja militaarmissioonidel ja -operatsioonidel kui ka nende plaanimise ja juhtimise üksustes ning Euroopa välisteenistuse infotehnoloogia talituses. Selleks et edendada liikmesriikide koostööd ja paremini suunata ELi jõupingutusi selles valdkonnas, hõlbustavad Euroopa Kaitseagentuur ja Euroopa välisteenistus koostöös komisjoni talitustega liikmesriikide küberkaitse poliitika kujundajate osalemist strateegilisel tasandil. EL toetab ka Euroopa kaitsesektori tehnoloogilise ja tööstusliku baasi arendamiseks tehtava töö raames Euroopa küberturvalisuse lahenduste väljatöötamist. Siia kuulub ka küberturvalisuse ja -kaitse piirkondlike teaduspõhiste tipptaseme klastrite edendamine.

Komisjoni talitused, kes teevad tihedat koostööd Euroopa välisteenistuse, liikmesriikide ja muude asjaomaste ELi asutustega, loovad 2018. aastaks **küberkaitsealase koolituse ja hariduse platvormi**, et parandada praegu puudulikke küberkaitsealaseid oskusi. Nii täiendatakse Euroopa Kaitseagentuuri tööd selles valdkonnas, aidates vähendada praegusi puudujääke küberturvalisuse ja küberkaitse valdkonnas.

Peamised meetmed

- Komisjoni algatus, milles käsitletakse piiriülest juurdepääsu elektroonilistele tõenditele (2018. aasta algus);
- mitterahaliste maksevahenditega seotud pettuste ja võltsimise vastast võitlust käsitleva direktiivi ettepaneku kiire vastuvõtmine Euroopa Parlamendis ja nõukogus;
- IPv6 nõuete kehtestamine ELi avalikes hangetes, teadustegevuse ja projektide rahastamises; liikmesriikide ja internetiteenuste pakkujate vahelised vabatahtlikud lepingud, mis käsitlevad IPv6 kasutuselevõtmise edendamist;
- Europoli uuendatud/ulatuslikum keskendumine küberkriminalistikale ja pimevõrgu seirele;
- ELi ühist diplomaatilist reageerimist pahatahtlikule kübertegevusele käsitleva raamistiku rakendamine;
- suurem rahaline toetus riiklikele ja riikidevahelistele projektidele, millega parandatakse küberruumi käsitlevat kriminaalõigussüsteemi;
- küberturvalisust käsitlev haridusplatvorm, et vähendada 2018. aastal praegusi puudujääke küberturvalisuse ja küberkaitse valdkonnas.

4. RAHVUSVAHELISE KOOSTÖÖ TUGEVDAMINE KÜBERTURVALISUSE VALDKONNAS

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

Lähtudes ELi põhiväärtustest ja põhiõigustest, nagu sõnavabadus ning õigus privaatsusele ja isikuandmete kaitsele, ning avatud, vaba ja turvalise küberruumi edendamisest, on ELi rahvusvaheline küberturvalisuse poliitika loodud küberstabiilsuse pidevalt muutuva teemaga tegelemiseks, samuti panuse andmiseks Euroopa strateegilisele sõltumatusele küberruumis.

4.1 Küberturvalisus välissuhetes

Tõendite kohaselt peavad inimesed kõikjal maailmas teiste riikide küberründeid üheks suurimaks ohuks riigi julgeolekule[83]. Arvestades ohu üleilmset iseloomu, on rahvusvahelist stabiilsust ja julgeolekut üha enam mõjutavate küberrünnete ennetamises ja heidutuses kesksel kohal kolmandate riikidega püsivate liitude ja partnerluste loomine ja säilitamine. EL peab oma kahepoolsetes, piirkondlikes, mitut sidusrühma hõlmavates ja mitmepoolsetes kohustustes prioriteediks küberruumis konfliktide ennetamise ja stabiilsuse tagamise strateegilise raamistiku loomist.

EL on kindlalt seisukohal, et küberruumis tuleb kohaldada rahvusvahelist õigust, eelkõige ÜRO hartat. Lisaks siduvatele rahvusvahelise õiguse normidele toetab EL vabatahtlikke mittesiduvaid norme, eeskirju ja põhimõtteid, mis käsitlevad riikide vastutustundlikku käitumist ja mille on sõnastanud ÜRO valitsusekspertide töörühm[84]. Samuti kutsub ta üles töötama välja ja rakendama piirkondlikke usaldust suurendavaid meetmeid nii Euroopa Julgeoleku- ja Koostööorganisatsioonis kui ka muudes piirkondades.

Kahepoolsel tasandil arendatakse edasi küberdialooge[85] ja täiendatakse neid jõupingutustega, mille eesmärk on lihtsustada koostööd kolmandate riikidega, et tugevdada hoolsuskohustuse ja riigi vastutuse põhimõtet küberruumis. EL seab oma rahvusvahelistes kohustustes esikohale rahvusvahelise turvalisuse küsimused küberruumis, kinnitades samas, et küberturvalisust ei kasutata turukaitse kehtestamise ning põhiõiguste ja -vabaduste, sealhulgas sõnavabaduse ja teabele juurdepääsu piiramise ettekäändena. Terviklik lähenemisviis küberturvalisusele eeldab inimõiguste austamist ja EL edendab ka edaspidi kogu maailmas oma põhiväärtusi, lähtudes ELi inimõigustealastest suunistest sõnavabaduse kohta internetis[86]. Sellega seoses rõhutab EL, et oluline on kõikide sidusrühmade kaasatus interneti haldamisse.

Komisjon on teinud ettepaneku[87] ajakohastada ELi ekspordikontrolli, sealhulgas võtta kasutusele sellise küberseiretehnoloogia ekspordi kontroll, mille kasutamine võib rikkuda inimõigusi või mida on võimalik kasutada ELi enda julgeoleku ohustamiseks, ning ta kavatseb tõhustada dialooge kolmandate riikidega, et edendada selles valdkonnas üleilmset lähenemist ja vastutustundlikku käitumist.

4.2 Küberturvalisuse alase suutlikkuse arendamine

Üleilmse küberstabiilsuse aluseks on kõikide riikide nii kohaliku kui ka riikliku tasandi suutlikkus ennetada küberintsidente ja neile reageerida ning uurida küberkuritegusid ja esitada nende eest süüdistusi. Jõupingutused riikliku vastupidavusvõime loomiseks kolmandates riikides tõstavad üleilmset küberturvalisuse taset ja neil on positiivne mõju ELile. Võitlus kiiresti arenevate küberohtudega toob kaasa vajaduse koolituse ning poliitika ja õigusaktide väljatöötamise järele, samuti tuleb luua kõikides riikides tõhusalt toimivad infoturbeintsidentidega tegelevad rühmad ja küberkuritegevuse üksused.

---

83 Kevad 2017, üleilmsete hoiakute uuring, Pew Research Centre.
84 A/68/98 ja A/70/174.
85 2017. aasta septembris pidas EL küberdialooge USA, Hiina, Jaapani, Lõuna-Korea ja Indiaga.
86 ELi inimõiguste alased suunised sõnavabaduse kohta internetis ja mujal.
87 COM(2016) 616

Alates 2013. aastast on ELil olnud juhtiv roll rahvusvahelises küberturvalisuse suutlikkuse arendamises ja nende jõupingutuste süstemaatilises kaasamises oma arengukoostöösse. EL jätkab õigustel põhineva suutlikkuse arendamise mudeli edendamist kooskõlas lähenemisviisiga „Digitaalsus arengu heaks“ (Digital4Development)[88]. Suutlikkuse arendamise prioriteedid on ELi naabruses asuvad riigid ja arengumaad, kus interneti kasutamine kiiresti kasvab, kuid kiiresti arenevad ka ohud. ELi jõupingutused täiendavad ELi arengukava, olles seotud kestliku arengu tegevuskavaga aastani 2030 ja üldiste jõupingutustega institutsioonilise suutlikkuse arendamiseks.

Selleks et parandada ELi võimet kasutada oma kollektiivseid teadmisi suutlikkuse suurendamise toetamiseks, tuleks luua spetsiaalne ELi kübersuutlikkuse suurendamise võrgustik, mis koondaks Euroopa Komisjoni, Euroopa välisteenistuse, liikmesriikide kübervaldkonna ametiasutused, ELi ametid, teadusringkonnad ja kodanikuühiskonna. Paremaks poliitiliseks suunamiseks ning ELi poolt kolmandate riikide abistamisele suunatud tegevuse prioriseerimiseks koostatakse ELi kübersuutlikkuse suurendamise suunised.

EL teeb samuti koostööd teiste selle valdkonna rahastajatega, et vältida dubleerimist ja soodustada sihipärasemat suutlikkuse suurendamist eri piirkondades.

4.3 ELi ja NATO koostöö

Võttes aluseks juba tehtud olulised edusammud, kavatseb EL süvendada ELi ja NATO koostööd küberturvalisuse, hübriidohtude ja kaitse alal, nagu ette nähtud 8. juuli 2016. aasta ühisdeklaratsioonis[89]. Prioriteetideks on muu hulgas koostalitlusvõime edendamine ühtsete küberkaitsenõuete ja -standardite kaudu, koolituste ja õppuste alal tehtava koostöö tugevdamine ning koolitusnõuete ühtlustamine.

Samuti kavatsevad EL ja NATO edendada koostööd küberkaitsealaste teadusuuringute ja innovatsiooni alal ning arendada edasi praegust tehnilist kokkulepet küberturvalisuse alase teabe vahetamiseks oma küberturvalisuse organite vahel[90]. Hiljutisi ühiseid jõupingutusi võitluses hübriidohtudega, eelkõige ELi hübriidohtude ühiskeskuse ja NATO hübriidohtude analüüsi osakonna koostööd, tuleks edendada, et tugevdada vastupidavusvõimet ja tõhustada küberkriisidele reageerimist. ELi ja NATO edasist koostööd edendatakse küberkaitseõppuste kaudu, kuhu on kaasatud Euroopa välisteenistus ja muud ELi üksused ning asjakohased NATO osalejad, sealhulgas NATO Küberkaitsekoostöö Keskus Tallinnas. NATO ja EL korraldavad esimest korda paralleelsed ja koordineeritud õppused, harjutades reageerimist hübriidohu olukorrale. 2017. aastal juhib õppuste korraldamist NATO, 2018. aastal aga EL. 2017. aasta detsembris esitavad EL ja NATO kumbki oma nõukogule järgmise aruande, mis käsitleb ELi ja NATO koostööd. See loob võimaluse kaaluda koostöö süvendamist, eeskätt võttes kõikide osalevate institutsioonide, sealhulgas ENISA vahelises suhtluses kasutusele ühised, turvalised ja kindlad sidevahendid.

Peamised meetmed

- Täiustada strateegilist raamistikku konfliktide ennetamiseks ja stabiilsuse tagamiseks küberruumis;
- töötada välja uus suutlikkuse arendamise võrgustik, et toetada kolmandate riikide suutlikkust küberohtudega toime tulla, ja ELi küberturvalisuse suutlikkuse arendamise suunised, et ELi jõupingutusi paremini prioriseerida;

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/et/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] CERT-EU ja NATO küberturbeintsidentidele reageerimise üksus (NCIRC).

- ELi ja NATO edasine koostöö, sealhulgas osalemine paralleelsetel ja koordineeritud õppustel, ning küberturvalisuse standardite suurem koostalitlusvõime.

5. KOKKUVÕTE

ELi kübervalmisolek on kesksel kohal nii digitaalse ühtse turu kui ka julgeoleku- ja kaitsekoostöö liidu jaoks. Euroopa küberturvalisuse parandamine ning võitlus tsiviil- ja militaarsihtmärkidele suunatud ohtudega on hädavajalik.

Lähenev digitaalteemaline tippkohtumine, mille korraldab eesistujariik Eesti 29. septembril 2017, pakub võimaluse näidata ühist tahet seada küberturvalisus ELi kui digitaalse ühiskonna huvide keskmesse. Osana sellest ühisest kohustusest kutsub komisjon liikmesriike üles andma teada, kuidas nad kavatsevad tegutseda valdkondades, kus neil on esmane vastutus. Selle raames tuleks küberturvalisuse tugevdamiseks kasutada järgmisi võimalusi:

- tagada võrgu- ja infoturbe direktiivi täielik ja tõhus rakendamine 9. maiks 2018 ning eraldada küberturvalisuse tagamise eest vastutavatele ametiasutustele ülesannete tulemuslikuks täitmiseks vajalikud vahendid;
- kohaldada haldusasutuste suhtes samu eeskirju, kuna neil on ühiskonnas ja majanduses oluline roll;
- korraldada haldusasutustes küberturvalisuse alaseid koolitusi;
- seada küberteadlikkus teavituskampaaniates esikohale ning kaasata küberturvalisus akadeemilistesse ja kutseõppe õppekavadesse;
- kasutada alalist struktureeritud koostööd (PESCO) ja Euroopa Kaitsefondi küberkaitseprojektide arendamise toetamiseks.

Ühisteatises on kirjeldatud probleemi ulatust ja meetmeid, mida EL saab võtta. Vajame vastupanuvõimelist Euroopat, kes suudab oma kodanikke tõhusalt kaitsta, ennetades võimalikke küberintsidente, luues oma struktuurides ja käitumises kindla kaitse, toibudes küberrünnetest kiiresti ning heidutades nende eest vastutavaid isikuid. Selles teatises tutvustatakse meetmeid, mis on suunatud ELi küberturvalisuse struktuuride ja suutlikkuse koordineeritud tugevdamisele liikmesriikide ja ELi asutuste täielikus koostöös ning oma pädevuse ja kohustuste kohaselt. Teatise rakendamine näitab, et EL ja liikmesriigid teevad koostööd, et kehtestada küberturvalisuse standard, mis vastab pidevalt suurenevatele probleemidele, millega Euroopa peab tegelema.