EUROOPA KONTROLLIKODA

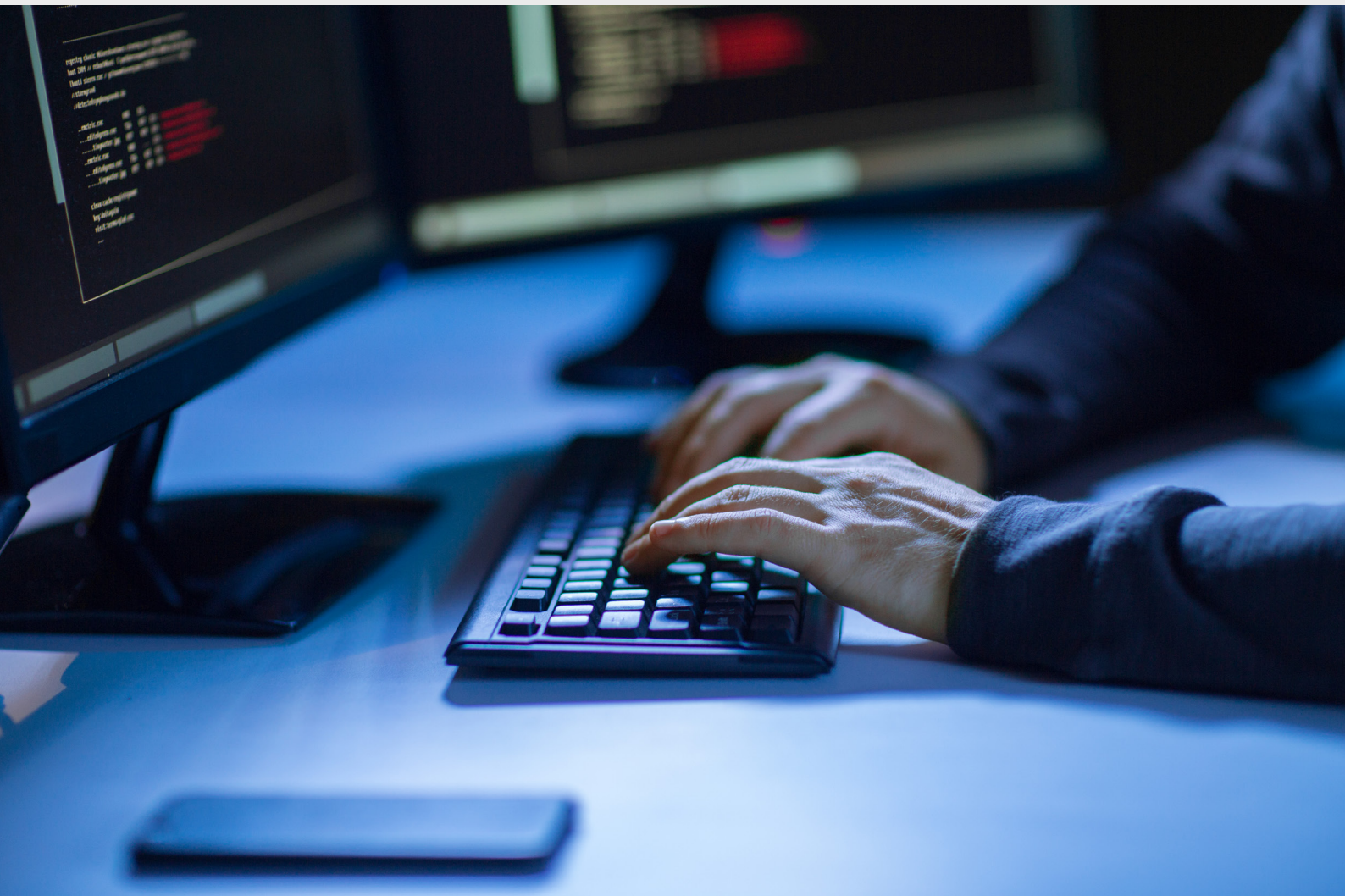
ET

2019

ELi küberturvalisuse poliitika tõhusust mõjutavad probleemid

Infodokument

Märts 2019



Lühidalt dokumendist

Käesolev infodokument ei ole auditiaruanne ning selle eesmärk on anda ülevaate ELi keerukast küberturvalisuse poliitikamaastikust ja kirjeldada selle poliitika tõhusa rakendamise ees seisvaid peamisi ülesandeid. See hõlmab võrgu- ja infoturvalisust, küberkuritegevust, küberkaitset ja väärinfot. Dokumendis esitatud teavet kasutatakse ka meie võimalike tulevaste auditi tegemisel selles valdkonnas.

Meie analüüs põhineb avalikult kättesaadaval teabel (ametlikud dokumendid, kirjalikud seisukohavõtud ja kolmandate isikute koostatud aruanded). Kohapealne töö tehti ajavahemikus aprillist septembrini 2018 ning infodokumendi koostamisel võeti arvesse kuni detsembrini 2018 toimunud sündmusi. Lisaks viidi läbi küsitlus liikmesriikide kõrgeimate kontrolliasutuste seas ning vesteldi ELi institutsioonide oluliste sidusrühmade ja erasektori esindajatega.

Jagasime leitud probleemid nelja suurde rühma: i) poliitikaraamistik; ii) rahastamine ja kulutused; iii) kübervastupidavusvõime suurendamine; iv) tõhus reageerimine küberintsidentidele. Kõige olulisem ülesanne on endiselt ELis parema küberturvalisuse saavutamine. Seetõttu esitame iga peatüki lõpus mitu ideed, mis on mõeldud poliitikakujundajate, seadusandjate ja praktikute edasiste arutelude jaoks.

Soovime tänada komisjoni talitusi, Euroopa välisteenistust, Euroopa Liidu Nõukogu, ENISAt, Europoli, Euroopa küberturvalisuse organisatsiooni ja liikmesriikide kõrgemaid kontrolliasutusi konstruktiivse tagasiside eest.

Sisukord

Kokkuvõte

I Tehnoloogia avab palju uusi võimalusi ning uued tooted ja teenused muutuvad meie igapäevaelu lahutamatuks osaks. Samas suureneb oht langeda küberkuritegevuse või küberründe ohvriks, ning selle kuriteoliigi ühiskondlik ja majanduslik mõju üha suureneb. ELi jõupingutused kiirendada küberturvalisuse parandamiseks ja liidu digitaalse autonoomia suurendamiseks võetavaid samme tehakse seega täpselt õigel ajal.

II Käesoleva infodokumendi, mis ei ole auditiaruanne ning põhineb avalikult kättesaadaval teabel, eesmärk on anda ülevaade sellest komplekssest ja ebaühtlasest poliitikavaldkonnast ja selgitada välja poliitika tõhusa rakendamise ees seisvad peamised ülesanded. Meie dokumendi ulatus hõlmab nii ELi küberturvalisuse poliitikat, küberkuritegevust ja küberkaitset kui ka väärinfo vastast võitlust. Jagasime leitud probleemid nelja suurde rühma i) poliitikaraamistik; ii) rahastamine ja kulutused; iii) kübervastupidavusvõime suurendamine; iv) tõhus reageerimine küberintsidentidele. Iga peatükk sisaldab selles esitatud probleeme käsitlevaid ideid.

Poliitika- ja õigusraamistik

III ELi küberturvalisuse strateegia üldiste eesmärkidega (st olla maailma kõige turvalisem digitaalkeskkond) seotud meetmete väljatöötamine on keeruline ülesanne, kuna puuduvad mõõdetavad eesmärgid ning on vähe usaldusväärseid andmeid. Tulemeid mõõdetakse harva ja hinnatud on vaid väheseid poliitikavaldkondi. Seetõttu on üks põhiülesanne võtta kasutusele hindamist sisaldav tulemuskultuur ning tagada selle abil **aruandekohustuse sisuline täitmine ja tulemuste hindamine**.

IV Õigusraamistik on endiselt puudulik. **Lüngad ELi õiguses ja õigusaktide ebajärjekindel ülevõtmine** võivad raskendada õigusaktide täieliku potentsiaali ärakasutamist.

Rahastamine ja kulutused

V Raske on tagada, et **investeeringute maht vastaks eesmärkidele**: see ei eelda üksnes küberturvalisusse tehtavate investeeringute (need on ELis väiksed ja killustatud) suurendamist, vaid ka suuremat mõju, mille aluseks peaks olema eelkõige teadusuuringute tulemuste parem kasutamine ning tõhusam keskendumine idufirmadele ja nende rahastamisele.

VI Selleks et teada, millised lüngad tuleb seatud eesmärkide saavutamiseks sulgeda, on oluline, et **EL ja selle liikmesriigid omaksid ELi kulutustest selget ülevaadet**. Kuna küberturvalisuse strateegia rahastamiseks ei ole konkreetset ELi eelarvet ette nähtud, puudub selge ülevaade sellesse investeeritud vahenditest.

VII Samal ajal kui turvalisust puudutavate poliitiliste prioriteetide tähtsus suureneb, ei pruugi **ELi kübervaldkonna asutustele eraldatud piiratud ressurssidest** piisata ELi eesmärkide täitmiseks. Selle probleemi lahendamiseks tuleb leida viise, kuidas andekaid töötajaid leida ja hoida.

Kübervastupidavusvõime suurendamine

VIII Küberturvalisuse juhtimises on kogu ELis ja mujal maailmas nii avalikus kui ka erasektoris arvukalt puudusi. See kahjustab kogu maailma võimet küberrünnetele reageerida ja nende mõju vähendada, ning õõnestab kogu ELi hõlmavat ühtset küberturvalisuse lähenemisviisi. Seega on oluline **tugevdada küberturvalisuse juhtimist**.

IX Küberturvalisuse alaste oskuste vähesuse tõttu kogu maailmas on oluline **arendada oskusi ja parandada teadlikkust** kõigis sektorites ja ühiskonna kõigil tasanditel. Praegu on ELis vähe kogu liitu hõlmavaid koolitus-, sertifitseerimis- ja küberriskide hindamise standardeid.

X Üldise kübervastupidavusvõime tugevdamiseks on oluline omada usaldusel põhinevat vundamenti. Isegi komisjoni hinnangul on koordineerimine üldiselt ebapiisav. Jätkuvalt on probleemiks avaliku ja erasektori vaheline puudulik **teabevahetus ja koordineerimine**.

Tõhus reageerimine küberintsidentidele

XI Digitaalsed süsteemid on muutunud nii keeruliseks, et iga rünnet ei ole võimalik vältida. Seega on oluline **kiire avastamine ja reageerimine**. Küberturvalisust ei ole aga veel täielikult integreeritud olemasolevatesse ELi tasandi kriisidele reageerimise koordineerimismehhanismidesse, mis võib piirata ELi suutlikkust reageerida ulatuslikele piiriülestele küberintsidentidele.

XII Võtmetähtsusega ülesanne on **elutähtsa taristu ja ühiskonna toimimiseks vajalike funktsioonide** kaitsmine. Oluline probleem on ka võimalik sekkumine valimisprotsessidesse ja väärinfokampaaniad.

XIII Praegu ELi ja kogu maailma ohustavatest küberohtudest tulenevad ülesanded eeldavad jätkuvat tähelepanu ja ELi põhiväärtuste kindlat järgimist.

Sissejuhatus

01 Tehnoloogia avab meile tohutult uusi võimalusi. Uued tooted ja teenused muutuvad meie igapäevaelu lahutamatuks osaks. Samas suureneb iga uuendusega ka meie sõltuvus tehnoloogiast ja küberturvalisuse tähtsus. Mida rohkem isikuandmeid me internetti paneme ja mida intensiivsemalt elektrooniliselt suhtleme, seda tõenäolisem on langeda mingit liiki küberkuritegevuse või küberründe ohvriks.

Mis on küberturvalisus?

02 Küberturvalisuse jaoks puudub standardne üldtunnustatud määratlus[1]. Üldiselt hõlmab see kõiki kaitsemeetmeid ja samme, mida võetakse selleks, et kaitsta infosüsteeme ja nende kasutajaid volitamata juurdepääsu, rünnete ja kahju eest, et tagada andmete konfidentsiaalsus, terviklus ja käideldavus.

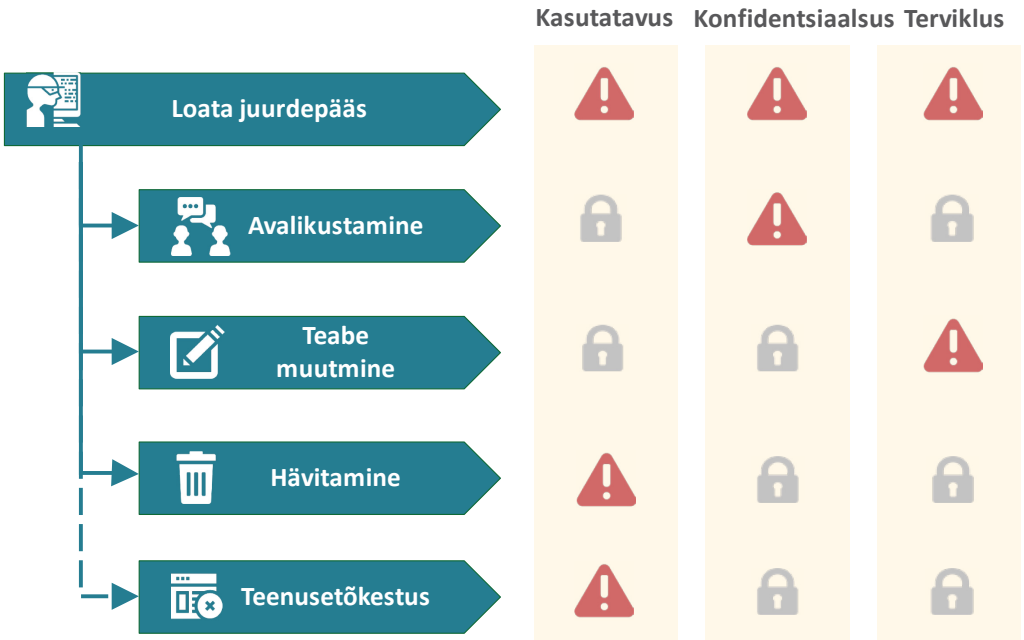
03 Küberturvalisus hõlmab küberintsidentide ennetamist, avastamist, neile reageerimist ja nende tekitatud kahju kõrvaldamist. Intsidendid võivad olla kavandatud või mitte ning need võivad ulatuda näiteks teabe juhuslikust avalikustamisest ettevõtete ja elutähtsa taristu vastu suunatud rünnete, isikuandmete varguse ja isegi demokraatlikesse protsessidesse sekkumiseni. Neil kõigil võib olla inimestele, organisatsioonidele ja kogukondadele ulatuslik kahjulik mõju.

04 ELi poliitilistes ringkondades kasutatav termin „küberturvalisus“ ei tähenda üksnes võrgu- ja infoturvet. See hõlmab igasugust ebaseaduslikku tegevust, millega kaasneb digitehnoloogia kasutamine küberruumis. See võib tähendada küberkuritegusid, nagu arvutiviiruste ründed ja mittesularahaliste maksevahenditega seotud pettused, ning hõlmata nii süsteeme kui ka sisu puudutavat tegevust ning näiteks internetis toimuvat laste seksuaalset kuritarvitamist kujutava materjali levitamist. See võib hõlmata ka internetis toimuvat arutelu ja potentsiaalselt valimisi mõjutava väärteabe levitamise kampaaniaid. Lisaks näeb Europol küberkuritegevuse ja terrorismi põimumist[2].

05 Eri osalejate – sealhulgas riikide, kuritegelike ühenduste ja nn häktivistide – tegevust mõjutavad erinevad motiivid. Nende juhtumite mõju avaldub riikide, Euroopa ja isegi ülemaailmsel tasandil. Interneti immateriaalne olemus ning kasutatavad vahendid ja taktikad raskendavad aga sageli ründe algataja leidmist (nn süüdlase kindlakstegemise probleem).

06 Küberturvalisus koosneb paljudest ohutüüpidest ning neid võib liigitada vastavalt sellele, mida nad andmetega teevad – andmete avalikustamine, muutmine, hävitamine või neile juurdepääsu keelamine – või põhiliste infoturbe põhimõtete alusel, mida nad rikuvad (vt allpool ***joonis 1***). Mõningaid näiteid rünnakutest kirjeldatakse ***1. selgituses***. Infosüsteemide ründamise kasvav keerukus vähendab meie kaitsemehhanismide tõhusust[3].

Joonis 1. Ohutüübid ja turvapõhimõtted, mida nad ohustavad



Allikas: Euroopa Kontrollikoda Euroopa Parlamendi uuringu[4] põhjal. Tabalukk = turvalisus ei ole ohus; hüüumärk = oht turvalisusele

1. selgitus

Küberründe liigid

Iga kord, kui mõni uus seade internetti või teiste seadmetega ühendatakse, suureneb nn rünnatav pind. Asjade interneti, pilvandmetöötluse, suurandmete ja tööstuse digiteerimise hüppelise kasvuga kaasneb suurem haavatavus, mis võimaldab pahatahtlikel ründajatel üha rohkem ohvreid sihikule võtta. Ründeliikide paljususe ja nende üha suureneva keerukuse tõttu on kaitsjatel ründajatega väga raske sammu pidada[5].

Pahavara on loodud seadmete või võrkude kahjustamiseks. See võib hõlmata viiruseid, Trooja hobuseid, lunavara, usse, reklaamvara ja nuhkvara. Lunavara krüpteerib andmeid, takistades kasutajatel juurdepääsu oma failidele, kuni on makstud lunaraha (tavaliselt krüptorahas) või tehtud mingi muu toiming. Europoli andmetel on lunavararünded kõikjal maailmas kõige levinumad ning lunavara liikide arv on viimastel aastatel plahvatuslikult kasvanud. **Hajus teenusetõkestusrünne**

(DDoS) on ründeliik, mis muudab teenused või ressursid kättesaamatuks, esitades neile rohkem päringuid kui need suudavad käsitleda; selle ründeliigi kasutamine on samuti suurenemas – 2017. aastal oli sellega kokku puutunud kolmandik kõigist organisatsioonidest[6].

Kasutajaid võidakse manipuleerida tahtmatult midagi tegema või konfidentsiaalset teavet avaldama. Kirjeldatud kavalat võtet võib kasutada andmevarguseks või küberspionaažiks ning seda tuntakse ka **sotsiaalse manipulatsiooni** nime all. Selle saavutamiseks on erinevaid võimalusi, kuid levinud meetod on **andmepüük** – e-posti teel esmapilgul usaldusväärsetest allikatest tulevate sõnumitega meelitatakse kasutajaid oma andmeid paljastama või klõpsama linkidele, mis nakatavad seadmed alla allalaaditud pahavaraga. Rohkem kui pooled liikmesriigid teatasid, et uurisid võrgurünnaid[7].

Kõige salakavalamat liiki ohud võivad aga olla **kinnisrünnaohud**. Need on professionaalsed ründajad, kes jälgivad oma ohvreid pikka aega, varastavad andmeid ja võivad kohati ka hävitustööd teha. Sellise ründe puhul on eesmärk võimalikult pikaks ajaks märkamatuks jääda. Kinnisrünnaohud on sageli seotud riiklike struktuuridega ja nende sihtmärkideks on eriti tundlikud sektorid, nagu tehnoloogia, kaitsevaldkond ja elutähtis taristu. Küberspionaaž moodustab hinnanguliselt vähemalt neljandiku kõigist küberintsidentidest ja enamiku nende põhjustatud kuludest[8].

Kui tõsise probleemiga on tegu?

07 Halba ettevalmistust küberrünnaks vastu on raske kvantifitseerida, sest puuduvad usaldusväärsed andmed. Küberkuritegevuse tekitatud majanduslik kahju kasvas aastatel 2013–2017 viis korda[9], tabades nii suuri kui ka väikseid valitsusi ja ettevõtteid. Nimetatud suundumust kajastab ka prognoos, mille kohaselt suurenevad kübervaldkonna kindlustuspreemiad 2018. aasta 3 miljardilt eurolt 2020. aastaks 8,9 miljardi euroni.

08 Kuigi küberrünnetest tingitud rahaline kahju üha kasvab, erineb rünnaku käivitamise maksumus kardinaalselt selle ennetamise, uurimise ja heastamise kuludest. Näiteks võib hajus teenusetõkestusrünnak (DDoS) maksta vaid 15 eurot kuus, kuid sihtmärgiks olevale ettevõttele tekitatud kahju, sealhulgas mainekahju, on oluliselt suurem[10].

09 Kuigi 80% ELi ettevõtetest puutus 2016. aastal kokku vähemalt ühe küberturvalisuse intsidendiga[11], tunnistatakse riske endiselt murettekitavalt vähe. 69%-l ELi ettevõtetest on küberohtudest vaid väga algeline arusaam või puudub see üldse[12], ning 60% neist ei ole kunagi hinnanud küberohtudest tulenevat võimalikku

finantskahju[13]. Ühe ülemaailmse uuringu kohaselt maksaks üks kolmandik organisatsioonidest pigem häkkereile lunaraha kui investeeriks infoturbesse[14].

10 2017. aastal toimunud ülemaailmsel *Wannacry* lunavarareründel ja kõvakettaid tühjendava *NotPetya* ründel oli umbes 150 riigis rohkem kui 320 000 ohvrit[15]. Need juhtumid tõid kaasa küberrünnetest tulenevat ohtu puudutava n-ö ülemaailmse ärkamise, andes uut hoogu protsessile, mis aitab küberturvalisust peavoolu poliitilisse mõtlemisse tuua. Lisaks usub 86% ELi kodanikest nüüd, et küberkuritegevuse ohvriks langemise oht suureneb[16].

ELi tegevus küberturvalisuse valdkonnas

11 2001. aastal sai EL vaatleja staatuse Euroopa Nõukogu küberkuritegevuse konventsioonis[17] (Budapesti konventsioon). Sellest ajast alates on EL kasutanud oma kübervastupidavusvõime parandamiseks nii poliitikameetmeid, õigusakte kui ka liidu finantsvahendeid. Suuremate küberrünnete ja intsidentide sagenemise tõttu on see tegevus alates 2013. aastast kiirenenud (vt ***joonis 2***). Samal ajal on liikmesriigid vastu võtnud (ja mõnel juhul ka juba ajakohastanud) oma esimesed riiklikud küberturvalisuse strateegiad.

12 Küberturvalisuse alaste ülesannetega ELi peamisi osalejaid kirjeldatakse ***I lisa 2. selgituses***.

2. selgitus

Kes on tegevusse kaasatud?

Euroopa Komisjoni eesmärk on suurendada küberturvalisuse alast suutlikkust ja koostööd, tugevdada ELi positsiooni küberturvalisuse vallas ning integreerida see teistesse ELi poliitikavaldkondadesse. Peamised küberturvalisuse poliitika eest vastutavad peadirektoraadid on sidevõrkude, sisu ja tehnoloogia peadirektoraat (**CNECT**) (küberturvalisus) ja siseasjade peadirektoraat (**HOME**) (küberkuritegevus), kes vastutavad vastavalt digitaalse ühtse turu ja julgeolekuliidu eest. Komisjoni enda süsteemide IT-turvalisuse eest vastutab informaatika peadirektoraat (**DIGIT**).

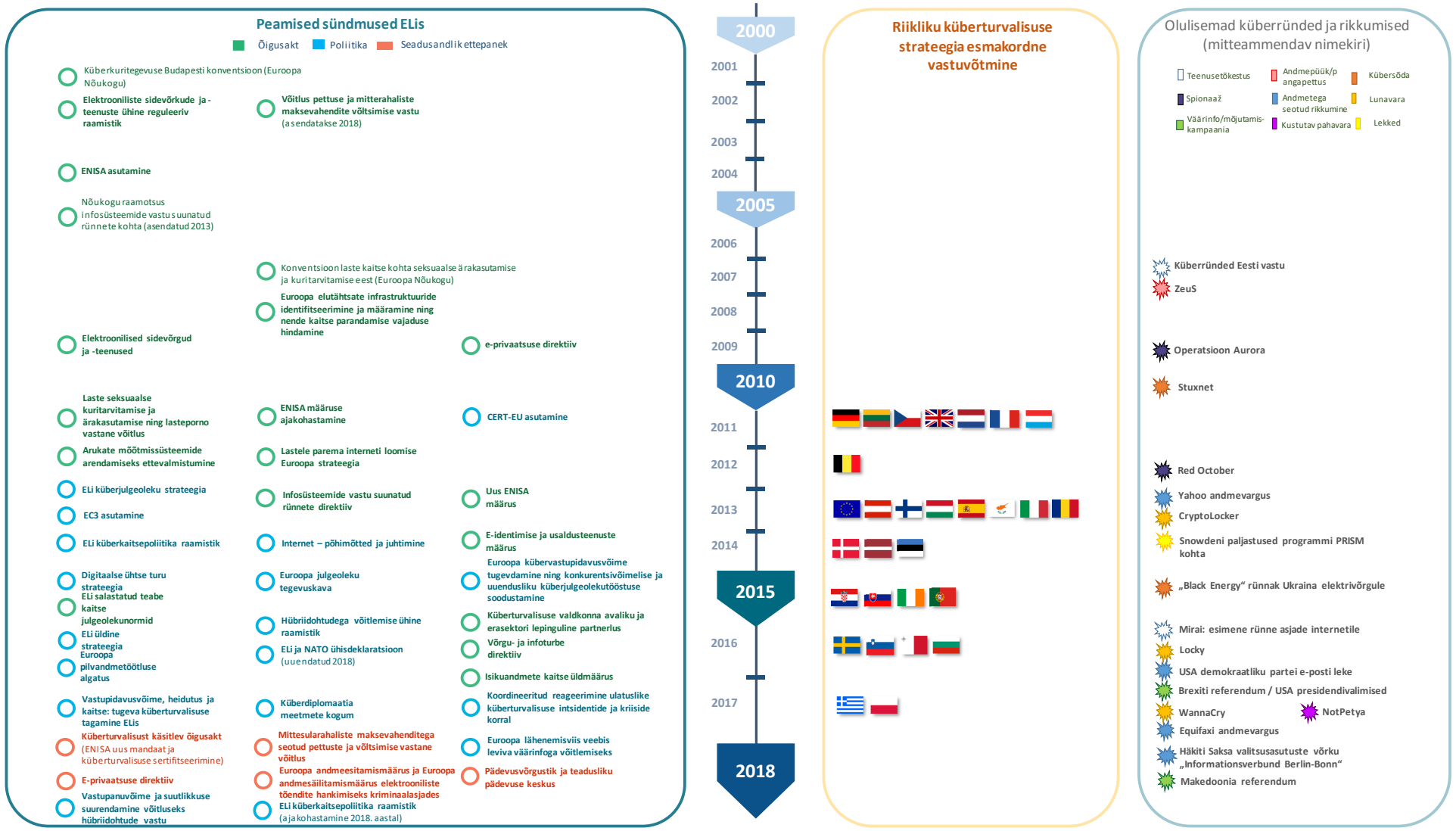
Komisjoni toetab mitu ELi asutust, eelkõige Euroopa Liidu Võrgu- ja Infoturbeamet (**ENISA**) – ELi küberturvalisusega tegelev asutus, mis on peamiselt nõuandev organ ning aitab poliitikat välja töötada, suutlikkust arendada ja teadlikkust tõsta. ELi küberkuritegevuse vastase võitluse tugevdamiseks loodi Europoli küberkuritegevuse vastase võitluse Euroopa keskus (**EC3**). Komisjoni struktuuris tegutseb ka ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm (**CERT-EU**).

Küberkaitse, küberdiplomaatia ja strateegilise teabevahetuse esirinnas on **Euroopa välisteenistus** (EEAS), mille struktuuris on teabe- ja analüüsikeskused. Küberkaitsevõimekuse arendamisega tegeleb **Euroopa Kaitseagentuur** (EDA).

Liikmesriigid vastutavad peamiselt enda küberturvalisuse eest ja tegutsevad ELi tasandil **nõukogu** kaudu, kellel on palju koordineerimis- ja teabeasutusi (nende seas ka horisontaalne küberküsimuste töörühm). **Euroopa Parlamendil** on kaasseadusandja roll.

Erasektori organisatsioonid, sealhulgas valdkonna ettevõtted, interneti haldamisega tegelevad asutused ja akadeemilised ringkonnad, panustavad nii poliitika väljatöötamisse kui ka rakendamisse, sealhulgas avaliku ja erasektori lepingulise partnerluse kaudu.

Joonis 2. Poliitika väljatöötamise ja õigusloome kiirendamine (2018. aasta 31. detsembri seisuga)



Allikas: Euroopa Kontrollikoda.

Poliitika

13 ELi kübervaldkonna ülesehitus on keeruline ja mitmekihiline ning hõlmab mitut sisepoliitika valdkonda (nt justiits- ja siseküsimused), digitaalset ühtset turgu ja teaduspoliitikat. Välispoliitikas on küberturvalisusest saanud diplomaatia osa ning see mängib ka üha enam rolli ELi kujunevas kaitsepoliitikas.

14 ELi poliitika nurgakivi on **2013. aasta küberturvalisuse strateegia**[18]. Strateegia eesmärk on muuta ELi digitaalne keskkond kõige turvalisemaks maailmas, kaitstes samal ajal põhiväärtusi ja -vabadusi. Sellel on viis järgmist põhieesmärki: i) suurendada kübervastupidavusvõimet; ii) vähendada küberkuritegevust; iii) arendada küberkaitsepoliitikat ja küberkaitsevõimet; iv) arendada tööstuslikke ja tehnoloogilisi küberturvalisuse ressursse; v) luua rahvusvaheline küberruumipoliitika, mis on kooskõlas ELi põhiväärtustega.

15 Küberjulgeoleku strateegia on seotud kolme hiljem vastu võetud strateegiaga:

— **Euroopa julgeoleku tegevuskava** (2015) eesmärk on parandada õiguskaitset ja õiguslikku reageerimist küberkuritegevusele, uuendades peamiselt olemasolevat poliitikat ja õigusakte[19]. Samuti seati selles eesmärgiks küberkuritegevust käsitlevate kriminaaluurimiste takistuste tuvastamine ja kübersuutlikkuse suurendamise tõhustamine;

— **Euroopa digitaalse ühtse turu strateegia**[20] (2015) eesmärk on luua parem juurdepääs digitaalsetele kaupadele ja teenustele, luues õiged tingimused digitaalmajanduse kasvupotentsiaali maksimeerimiseks. Selleks on oluline suurendada võrguturvalisust, usaldust ja kaasatust;

— 2016. aasta **üldine strateegia**[21], mille eesmärk on suurendada ELi rolli maailmas. Küberturvalisus on selle üks põhisammas, mille aluseks on uuendatud pühendumine küberküsimustele, koostöö peamiste partneritega ja otsus tegeleda küberprobleemidega kõigis poliitikavaldkondades, sealhulgas väärinfo ümberlükkamine strateegilise kommunikatsiooni kaudu.

16 Viimastel aastatel on küberruum muutunud üha enam militariseerituks[22] ja relvastatuks[23] ning seda on hakatud käsitlema kui sõjapidamise viiendat relvaliiki[24]. Küberkaitsega turvatakse küberruumis olevaid süsteeme, võrke ja elutähtsat taristut sõjaliste ja muude vahendite abil ründe vastu. **Küberkaitsepoliitika raamistik** võeti vastu 2014. ja ajakohastati 2018. aastal[25]. 2018. aasta ajakohastatud versioonis määratleti kuus prioriteeti, sealhulgas küberkaitsevõime arendamine ning ELi ühise

julgeoleku- ja kaitsepoliitika (ÜJKP) side- ja teabevõrkude kaitse. Küberkaitse on osa alalisest struktureeritud koostöö raamistikust (PESCO) ning ELi ja NATO koostööst.

17 ELi **hübriidohtudega võitlemise ühine raamistik** (2016) tegeleb küberohtudega nii elutähtsa taristu kui ka erasektori kasutajate jaoks, rõhutades, et küberrünnakuid on võimalik ellu viia ka sotsiaalmeedia väärinfo levitamise kampaaniate kaudu[26]. Samuti juhitakse selles tähelepanu vajadusele suurendada teadlikkust ning tõhustada ELi ja NATO koostööd, mis on sätestatud ELi ja NATO 2016. ja 2018. aasta ühisdeklaratsioonides[27].

18 2017. aastal esitas komisjon uue küberjulgeoleku paketi, mis kajastab digitaalse kaitse kasvavat kiireloomulisust. See hõlmas komisjoni uut teatist, millega ajakohastatakse 2013. aasta küberjulgeoleku strateegiat[28], tegevuskava kiire ja kooskõlastatud reageerimise kohta suurele ründele ning võrgu- ja infosüsteemide turvalisuse direktiivi (küberturvalisuse direktiivi) kiiret rakendamist[29]. Lisaks sisaldas pakett mitut seadusandlikku ettepanekut (vt punkt ***22***).

Õigusaktid

19 Alates 2002. aastast on vastu võetud õigusakte, mis puudutavad erineval määral ka küberturvalisust.

20 2013. aasta küberjulgeoleku strateegia üheks peamiseks tugisambaks on 2016. aasta **võrgu- ja infoturbe direktiiv**[30], mis on esimene kogu ELi hõlmav küberturvalisust käsitlev õigusakt. Direktiiviga, mis tuli üle võtta maiks 2018, soovitakse saavutada ühtlustatud suutlikkuse miinimumtase, kohustades liikmesriike võtma vastu riiklikud võrgu- ja infoturbestrateegiad ning looma ühtsed kontaktpunktid ja arvutiturbe intsidentide lahendamise üksused (CSIRTid)[31]. Direktiivis sätestatakse ka turva- ja teatamisnõuded oluliste teenuste operaatorite jaoks elutähtsates sektorites ja digitaalse teenuse osutajate jaoks.

21 Samal ajal jõustus 2016. aastal **isikuandmete kaitse üldmäärus**[32], mida kohaldatakse alates maist 2018. Selle eesmärk on kaitsta Euroopa kodanike isikuandmeid, kehtestades nende töötlemise ja levitamise eeskirjad. Määrusega antakse andmesubjektidele teatavad õigused ja vastutavatele töötlejatele (digitaalse teenuse osutajatele) kohustused teabe kasutamise ja edastamise kohta. Määrusega kehtestatakse ka teavitamisnõuded rikkumise korral ning mõnel juhul trahvid. ***Joonisel 3*** näitlikustatakse, kuidas võrgu- ja infoturbe direktiivi ning isikuandmete

kaitse üldmäärus täiendavad teineteise eesmärke, milleks on küberturvalisuse tugevdamine ja andmekaitse tagamine.

22 Praegu on arutlusel näiteks küberturvalisust käsitlev õigusakt (et tugevdada ENISAt ja kehtestada kogu ELi hõlmav sertifitseerimismehhanism[33]), elektroonilisi tõendeid puudutavate andmete esitamist ja säilitamist käsitleva määruse ettepanek[34] ning elektroonilisi tõendeid käsitleva direktiivi ettepanek[35]. Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse ning riiklike koordineerimiskeskuste võrgustik (edaspidi „küberturvalisuse pädevuskeskuste võrgustik ning uurimis- ja pädevuskeskus“) on osa 2017. aasta küberturvalisuse paketist[36].

23 Raske võib olla mõista küberturvalisust puudutava poliitika- ja õigusraamistiku ulatust ja seda, kuidas see mõjutab meie igapäevaelu.

24 ***Joonisel 4*** püütakse kaardistada eri õigusaktide ja muu tegevuse kokkupuuteid tavalise Euroopa kodaniku eluga.

Joonis 3. Kuidas isikuandmete kaitse üldmäärus ja võrgu- ja infoturbe direktiiv üksteist täiendavad

Allikas: Euroopa Kontrollikoda.

Joonis 4. Kuidas ELi küberjjulgeoleku strateegia haakub kodanike igapäevaeluga

Allikas: Euroopa Kontrollikoda.

Poliitika- ja õigusraamistiku rajamine

25 ELi kübervaldkonna ülesehitus on keeruline ja mitmekihiline ning hõlmab paljud sidusrühmi (vt ***I lisa***). Kõigi selle erinevate osade ühendamine on keeruline ülesanne. Alates 2013. aastast on tehtud kooskõlastatud jõupingutusi, et ELi küberturvalisuse valdkonda ühtlustada[37].

1. ülesanne: sisuline hindamis- ja järelevalvekord

26 Komisjoni sõnul on keeruline näha põhjuslikku seost 2013. aasta strateegia ja peale seda toimunud muutuste vahel. 2013. aasta strateegia eesmärgid olid sõnastatud väga üldsõnaliselt, „väljendades pigem visiooni kui mõõdetavat eesmärki“[38]. Nende üldiste eesmärkidega seotud meetmete väljatöötamine on keeruline ülesanne, kuna puuduvad mõõdetavad eesmärgid. Ajakohastatud küberkaitsepoliitika raamistiku (2018) eesmärk on töötada välja eesmärgid, millega kehtestatakse küberturvalisuse ja usalduse miinimumtase. See piirdub aga vaid küberkaitsega; ELi kui terviku vastupidavuse soovitud taseme määratlemine seisab aga alles ees.

27 Tulemeid mõõdetakse harva ja hinnatud on vaid vähe poliitikavaldkondi[39]. See on osaliselt tingitud paljude meetmete (õigusloome või muud) hiljutisest rakendamisest, mis takistab nende mõju täielikku hindamist. Keeruline on määrata kindlaks asjakohased hindamiskriteeriumid, mis aitaksid mõõta meetmete mõju. Lisaks ei ole range hindamine küberturvalisuse valdkonnas tervikuna veel juurdunud. Seetõttu on vaja võtta kasutusele tulemuskultuur koos selles sisalduva hindamise ja standarditud aruandlusega. ENISA praegune mandaat ei hõlma ELi küberturvalisuse taseme ja intsidentideks valmisoleku hindamist ja seiret.

28 Tõenditel põhinev poliitikakujundamine sõltub küllaldase hulga usaldusväärsete andmete ja statistika kättesaadavusest, mis aitavad jälgida ja analüüsida suundumusi ja vajadusi. Kohustusliku ja ühise järelevalvesüsteemi puudumise tõttu on usaldusväärseid andmeid vähe. Näitajad ei ole sageli kergesti kättesaadavad ja neid on raske määratleda[40]. Mõnes valdkonnas on siiski välja töötatud konkreetsed parameetrid (näiteks ELi poliitikatsükkel, mida kasutatakse raske ja organiseeritud kuritegevuse tõkestamise alaseks võitluseks).

29 Võrreldavust takistab see, et vähesed liikmesriigid koguvad korrapäraselt ametlikke andmeid küberküsimustega seotud teemade kohta. EL on seni andnud vähe teavet vajaduse kohta statistikat Euroopa tasandil konsolideerida[41]. ELi tasandil on ka vähe sõltumatuid analüüse, mis hõlmavad selliseid võtmeteemasid nagu[42] küberturvalisuse ökonoomika, sealhulgas käitumuslikud aspektid (stiimulite ebakõla, teabe asümmeetria); kübervaldkonna puuduste ja küberkuritegevuse mõju mõistmine; kübersuundumusi ja eeldatavaid probleeme käsitlev makrostatistika; ning parimad lahendused ohtude kõrvaldamiseks.

30 Konkreetsete eesmärkide puudumise ning usaldusväärsete andmete ja täpselt määratletud näitajate vähesuse tõttu on strateegia saavutuste hindamine olnud seni suuresti kvalitatiivne. Eduaruannetes kirjeldatakse sageli läbiviidud tegevusi või saavutatud eesmärke, ilma tulemusi põhjalikult analüüsimata. Lisaks ei ole veel kindlaks määratud lähtetasemeid, mis võimaldaksid hinnata süsteemide vastupidavusvõimet. Pealegi on küberkuritegevuse kodifitseeritud määratluse puudumise tõttu peaaegu võimatu leida asjakohaseid Euroopa näitajaid, mis toetaksid järelevalvet ja hindamist.

31 Sõltumatu järelevalve küberturvalisuse poliitika rakendamise üle on liikmesriigiti erinev. Küsitlesime liikmesriikide kõrgemaid kontrolliasutusi, et selgitada välja nende kogemus kõnealuse valdkonna auditeerimisel. Pooled vastanutest[43] ei olnud kõnealust valdkonda kunagi auditeerinud. Nende puhul, kes olid valdkonda auditeerinud, oli peamine rõhk pandud teabe haldamisele, elutähtsa taristu kaitsele, peamiste sidusrühmade vahelisele teabevahetusele ja koordineerimisele ning intsidentideks valmisolekule, neist teatamisele ja neile reageerimisele. Vähem oli käsitletud selliseid teemasid nagu teadlikkuse suurendamise meetmed ja digitaaloskuste puudus. Riikliku julgeoleku kaalutlustel nende auditite või hindamiste tulemusi alati ei avalikustata. Liikmesriikide kõrgeimate kontrolliasutuste avaldatud auditiaruannete nimekiri on esitatud ***III lisas***.

32 Kõige raskemateks ülesanneteks valitsuse meetmete auditeerimisel selles valdkonnas peeti digitaaloskuste puudust (vt ka punktid ***82-90***) ja raskusi küberturvalisuse alal tehtud edusammude hindamisel.

2. ülesanne: täita lüngad ELi õiguses ja tagada õigusaktide rakendamine

33 Uue tehnoloogia ja ohtude leviku kiirus ületab ELi õigusaktide väljatöötamise ja rakendamise tempot. Liidu menetluste väljatöötamisel ei võetud arvesse digitaalajastu nõudeid, mis tähendab uuenduslike ja paindlike menetluste väljatöötamist, et tagada eesmärgipärane poliitika ja õigusaktid[44] – prioriteet on tuleviku parem prognoosimine ja kujundamine[45].

34 Vaatamata sellele, et eesmärgiks on suurem sidusus, on küberturvalisuse õigusraamistik endiselt puudulik (mõned näited on esitatud ***tabelis 1***). Killustatus ja lüngad takistavad üldiste poliitikaeesmärkide saavutamist ning põhjustavad ebatõhusust. Komisjoni poolt strateegia hindamisel kindlaks tehtud puudujäägid hõlmasid asjade internetti, kasutajate ja digitaalsete toodete pakkujate kohustuste tasakaalu ning teatavaid aspekte, mida võrgu- ja infoturbe direktiivis ei käsitleta. Kavandatud küberturvalisust käsitlevas õigusaktis püütakse seda osaliselt käsitleda, edendades sisseprojekteeritud turvet kogu ELi hõlmava sertifitseerimissüsteemi abil. Mõned sidusrühmad on arvamusel, et õigusakti ettepanekust puuduvad endiselt selgelt määratletud kübertööstuspoliitika ja ühine lähenemisviis küberspionaažile[46].

Tabel 1. Lüngad õigusraamistikus ja ebaühtlane ülevõtmine (mitteammendav loetelu)

Poliitikavaldkond	Näited
Digitaalne ühtne turg	o Praegune tarbekaupade müügi direktiiv ei hõlma küberturvalisust. See lünk üritatakse täita kavandatavate digitaalset sisu[47] ja veebimüüki[48] käsitlevate direktiividega. o ELi liikmesriikide õiguses on vähe hoolsuskohustust puudutavaid sätteid ja need on riigiti erinevad, mis tekitab õiguslikku ebakindlust ja raskusi õiguskaitsevahendite jõustamisel[49]. o Tarkvara haavatavust puudutava teabe avalikustamise põhimõtteid töötatakse välja eri liikmesriikides erinevatel kiirustel, kuna puudub üldine ELi tasandi õigusraamistik, mis võimaldaks kooskõlastatud lähenemisviisi[50].
Võrgu- ja infoturbe parandamine	o Liikmesriikidel on vabadus käsitleda sektoreid, mis on võrgu- ja infoturbe direktiivist välja jäetud[51]. Direktiivist välja jäetud andmemajutusega tegelevad ettevõtted võivad olla väravaks muudele kuritegudele, sealhulgas inim- ja narkokaubandusele ning ebaseaduslikule sisserändele[52].
Võitlus küberkuritegevusega	o Paljud liikmesriigid ei ole elektroonilisi tõendeid oma riigisisestes õigusaktides määratlenud[53] (vt ka punkt ***22***).

Poliitikavaldkond	Näited
	o Kehtiv raamotsus mittesularahaliste maksevahenditega seotud pettuste kohta ei sisalda sõnaselgelt mittefüüsilisi maksevahendeid, nagu virtuaalvaluutad, e-raha ja mobiilraha, ega hõlma selliseid toiminguid nagu andmepüük, skimming ning maksjaga seotud teabe valdamine ja jagamine[54]. o Infosüsteemide vastu suunatud rünnete direktiivis ei käsitleta otseselt andmete ebaseaduslikku omandamist organisatsiooni sees (nt küberspionaaž), mis tekitab probleeme õiguskaitse valdkonnas[55]. o Pärast andmete säilitamise kohta tehtud Euroopa Liidu Kohtu otsust[56] on erinevused liikmesriikide õigusliku raamistiku kohaldamises takistanud õiguskaitset, mille tagajärjeks võib olla uurimise tulemusel kogutud juhtlõngade mittekasutamine ja küberkuritegevuse eest süüdistuste esitamise takistamine[57].

Allikas: Euroopa Kontrollikoda.

35 Õigusaktide teatavate aspektide kohaldamine on nii liikmesriikide ametiasutuste kui ka eraettevõtjate jaoks endiselt vabatahtlik. Näiteks koostöörühma raames on riiklike võrgu- ja infosüsteemide turvalisuse strateegiate ning CSIRTide tõhususe hindamine vabatahtlik. Ka küberturvalisust käsitlevas õigusaktis välja pakutud sertifitseerimissüsteemi kohaselt on IKT-toodete ja -teenuste sertifitseerimine vabatahtlik.

36 ELis on küberturvalisusega tegelemine liikmesriikide pädevuses. Sellele vaatamata on ELil oluline roll tingimuste loomisel, et parandada liikmesriikide suutlikkust, ning edendada nende koostööd ja usalduse loomist. Arvestades aga suuri erinevusi liikmesriikide suutlikkuses ja aktiivsuses[58], jääb riikliku julgeoleku seisukohast tundliku teabe esitamine vabatahtlikuks.

37 ELi õigusaktide ebajärjekindel ülevõtmine liikmesriikides võib kaasa tuua õigusliku ja operatiivse sidususe puudumise ning takistada õigusaktide potentsiaali täielikku ärakasutamist. Näiteks tõlgendavad liikmesriigid kahesuguse kasutusega kaupade ekspordikontrolli nõudeid erinevalt[59], mistõttu võivad mõned ELis paiknevad äriühingud eksportida tehnoloogiat ja teenuseid, mida saab kasutada küberseireks ja inimõiguste rikkumiseks tsensuuri või pealtkuulamise teel. Euroopa Parlament on selles küsimuses oma muret väljendanud[60]

38 Lisaks eeldab eraelu puutumatuse ja sõnavabaduse kaitsmine paremini vajadustele vastavaid õigusakte, et leida vajalik tasakaal põhiväärtuste kaitsmise ja ELi julgeolekueesmärkide saavutamise vahel. Näiteks, kuidas tagada otspunktkrüpteerimine ning toetada samas optimaalselt õiguskaitseorganite tööd? Või kuidas täita isikuandmete kaitse üldmääruse eesmärgid, kui on teada selle mõju avalikult kättesaadavale teabele domeeninimede registreerijate ja IP-aadresside plokkide omanike kohta? Ning kuidas see võib negatiivselt mõjutada õiguskaitseasutuste uurimisi[61]?

39 Vastupidavusvõimet ei saa tagada üksnes õigusaktidega. Kuigi võrgu- ja infoturbe direktiivi eesmärk on saavutada kõrge turvalisuse tase kogu ELis, keskendutakse selles sõnaselgelt minimaalse, mitte maksimaalse ühtlustamise saavutamisele[62]. Kübermaastiku muutudes tekib ka edaspidi uusi katmata lünki.

Mõttekohad – poliitikaraamistik

- Millised kriitilise tähtsusega sammud on vajalikud, et nii poliitikakujundajad kui ka seadusandjad saaksid kiirendada küberturvalisuse valdkonnas tulemuskultuuri tekkimist, sealhulgas üldise vastupidavusvõime määratlemist?
- Kuidas saaks uurimistööga paremini kaasa aidata vajalike andmete ja statistika koostamisele, et võimaldada sisulist hindamist?
- Kuidas kohandada ELi seadusandlikke menetlusi, et need oleksid paindlikumad, ja võtta paremini arvesse tehnika ja ohtude kiiret arengut?
- Kuidas saaks ELi poliitikatsüklis välja töötatud mõõdikuid (näitajaid, eesmärke) kohandada, skaleerida ja kasutada neid kogu küberturvalisuse valdkonnas?
- Mida saavad liikmesriikide kõrgeimad kontrolliasutused õppida üksteise lähenemisviisidest küberturvalisuse valdkonna poliitika ja meetmete auditeerimisel?
- Millised vastuolud ELi õigusraamistiku ülevõtmisel ja rakendamisel õõnestavad tõhusamat võitlust küberturvalisuse valdkonna puuduste ja küberkuritegevusega, ning kuidas saaksid liikmesriigid ja ELi institutsioonid neid kõige paremini kõrvaldada?
- Kui tulemuslikud on küberkaupu ja -teenuseid käsitlevad ELi ekspordikontrollid, mille eesmärk on vältida inimõiguste rikkumisi väljaspool ELi?

Rahastamine ja kulutused

40 ELi eesmärk on saada maailma turvalisimaks internetikeskkonnaks. Selle saavutamine nõuab kõigilt sidusrühmadelt märkimisväärseid jõupingutusi, sealhulgas tugevat ja hästi hallatud rahalist panust.

3. ülesanne: tagada eesmärkide saavutamiseks vajalikud investeeringud

Investeeringute suurendamine

41 Maailmas kulutatakse küberturvalisusele kokku hinnanguliselt umbes 0,1% SKPst. Ameerika Ühendriikides[63] on see näitaja ligikaudu 0,35% (kaasa arvatud erasektor). USA föderaalvalitsuse 2019. aasta eelarves on küberturvalisusele ette nähtud ligikaudu 0,1% SKPst (*ca* 21 miljardit dollarit)[64].

42 ELis küberturvalisuse valdkonna kulutused on aga olnud väikesed, killustatud ja ei ole sageli põhinenud riiklikel programmidel. Arvnäitajaid on raske leida, kuid ELi avaliku sektori kulutused küberturvalisusele moodustavad hinnanguliselt üks kuni kaks miljardit eurot aastas[65]. Mõne liikmesriigi kulutused protsendina SKPst on vaid kümnendik USA tasemest või isegi vähem[66]. EL ja selle liikmesriigid peavad teadma kõigi kokku investeeritava summa suurust, et otsustada, millised lüngad tuleb sulgeda.

43 Selgete andmete puudumisel on raske saada põhjalikku ülevaadet: see tuleneb küberturvalisuse valdkonnaülesest olemusest ja asjaolust, et küberturvalisuse ja üldised IT-kulutused on sageli eristamatud[67]. Meie küsitlus kinnitas, et raske on saada usaldusväärset statistikat nii avaliku kui ka erasektori kulutuste kohta. Kolmveerand liikmesriikide kõrgeimatest kontrolliasutustest vastas, et neil puudub keskne ülevaade kübervaldkonnaga seotud riiklikest kulutustest, ning mitte ükski liikmesriik ei kohusta avaliku sektori asutusi esitama küberturvalisuse kulutuste kohta oma eelarvekavades eraldi aruandeid.

44 Eriti raske ülesanne on avaliku ja erasektori investeeringute suurendamine Euroopa küberturvalisuse ettevõtetes. Avaliku sektori kapital on sageli kättesaadav varajastes etappides, kuid vähem kasvu- ja laienemise etapis[68]. ELil on küll palju rahastamisalgatusi, kuid neid ei kasutata (sageli bürokraatia tõttu)[69]. Kokkuvõttes on ELi küberturbefirmad oma rahvusvaheliste konkurentidega võrreldes nõrgemad: nende kaasatavad investeeringud on keskmiselt oluliselt väiksemad[70]. ELi digitaalarengu

poliitika eesmärkide saavutamisele kaasa aitamiseks on seega oluline tagada sihipärane keskendumine idufirmadele ja nende tõhus rahastamine.

Mõju suurendamine

45 Kübervaldkonna investeeringute suurendamine vajalikule tasemele peab andma kasulikke tulemusi. Näiteks hoolimata ELi teadus- ja innovatsioonisektori tugevusest ei ole selle tulemusi piisavalt patenteeritud, turustatud ega suuremas mahus reprodutseeritud, et aidata suurendada ELi vastupidavusvõimet ja konkurentsivõimet ning digitaalset autonoomiat[71]. Eriti kehtib see võrdluses ELi üleilmsete konkurentidega. Tulemuste ebapiisav ärakasutamine tuleneb mitmest tegurist[72], mille hulka kuuluvad

- ühtse riikidevahelise strateegia puudumine lähenemisviisi jaoks, mis võtaks arvesse ELi laiemaid digitaalvajadusi konkurentsivõime ja suurema autonoomia saavutamiseks;
- väärtusahela tsükli pikkus, mis tähendab töövahendite kiiret iganemist;
- puuduv jätkusuutlikkus, kuna projektide lõppedes saadetakse projektimeeskonnad tavaliselt laiali ja lõpetatakse kasutajate toetamine, sealhulgas uuenduste väljatöötamine ja nn tarkvarapaikade avaldamaine.

46 Komisjoni ettepanek luua küberturvalisuse pädevuskeskuste võrgustik ning uurimis- ja pädevuskeskus on katse, millega püütakse ületada küberturvalisuse uuringute valdkonna killustatus ja hoogustada investeeringuid[73]. Kokku on ELis ligikaudu 665 eksperdikeskust.

4. ülesanne: selge ülevaade ELi eelarve kulutustest

47 Läbipaistvuse ja parema koordineerimise seisukohast on oluline omada keskset ülevaadet. Vastasel juhul on poliitikakujundajatel raske mõista, kas kulutused vastavad esmatähtsate eesmärkide saavutamiseks vajalikele vajadustele.

48 Küberjulgeoleku strateegia rahastamiseks puudub konkreetselt selleks mõeldud eelarve. ELi tasandil rahastatakse küberturvalisust ELi üldeelarvest ja liikmesriikide eraldatud kaasrahastamisest. Meie analüüs näitab, et ELi üldeelarves kasutatakse selleks vähemalt kümmet eri vahendit, kuid puudub selge ülevaade selle kohta, kui palju ja milleks raha kulutatakse (vt ***II lisa***).

49 Niisiis seisab ees raske ülesanne saada selge ülevaade paljusid poliitikavaldkondi puudutava küberturvalisuse kulutuste kohta. Kuluprogramme haldavad komisjoni eri talitused, millest igaühel on oma eesmärgid, eeskirjad ja ajakavad. Olukord on veelgi keerulisem, kui võtta arvesse liikmesriikide kaasrahastamist (näiteks Sisejulgeolekufondi politsei osa raames)[74].

Teadaolevad kulutused küberturvalisusele

50 Aastatel 2014–2018 kulutas komisjon strateegia rakendamiseks vähemalt 1,4 miljardit eurot[75], millest suurima osa moodustab programm „Horisont 2020“[76]. Programmi „Horisont 2020“ rahastamine toimub peamiselt turvalise ühiskonna programmi ning erieesmärgi „Juhtpositsioon progressi võimaldava ja tööstusliku tehnoloogia vallas“ projektide kaudu[77]. 2018. aasta septembri seisuga tegime kindlaks 279 küberturvalisusega seotud projektideks sõlmitud lepingut, mille ELi-poolne rahastamine oli kokku 786 miljonit eurot[78]. ***Joonisel 5*** kirjeldatakse meie analüüsil põhinevat projektide tüpoloogiat.

Joonis 5. Programm „Horisont 2020“ küberturvalisuse uuringute allkirjastatud projektid (miljonites eurodes)

Allikas: Euroopa Kontrollikoda.

51 2016. aastal loodi Euroopa küberturvalisuse valdkonna ettevõtete edendamiseks avaliku ja erasektori lepinguline partnerlus. Eesmärk oli suunata sellesse programmist „Horisont 2020“ 450 miljonit eurot ning kaasata 2020. aastaks erasektorist täiendavalt 1,8 miljardit eurot. 18 kuu jooksul kuni 31. detsembrini 2017 eraldati programmist „Horisont 2020“ partnerlusele 67,5 miljonit eurot ning erasektor investeeris miljard eurot[79].

52 Küberkuritegevuse vastast võitlust toetab ka Sisejulgeolekufondi politsei osa (ISF-P). ISF-P toetab uuringuid, ekspertide kohtumisi ja kommunikatsioonitegevust; ajavahemikul 2014–2017 tehti seda 62 miljoni euro suuruses summas. Liikmesriigid võivad jagatud eelarve täitmise raames saada ka toetust varustuse, koolituse, teadusuuringute ja andmete kogumise rahastamiseks. Neid toetusi on kasutanud 19 liikmesriiki summas 42 miljonit eurot.

53 Justiitsvaldkonna koostööd ja vastastikuse õigusabi osutamise lepinguid toetati õigusküsimuste peadirektoraadi hallatava õigusprogrammi raames 9 miljoni euroga; seejuures keskenduti eelkõige elektrooniliste andmete ja finantsteabe vahetamisele.

54 Võrgu- ja infoturbe direktiivis on sõnaselgeelt sätestatud, et CSIRTidel peavad olema oma ülesannete tulemuslikuks täitmiseks piisavad ressursid[80]. Ajavahemikul 2016–2018 eraldati Euroopa ühendamise rahastust igal aastal 13 miljonit eurot, mida liikmesriigid said kasutada direktiivi nõuete rakendamiseks. Samas ei ole uuritud, kui palju raha vajaksid CSIRTide võrgustik ja koostöörühm tegelikult selleks, et nende tegevusel oleks mõju.

55 Mitu asutust on kasutanud oma tegevuskulusid konkreetselt küberturvalisuse ja küberkuritegevusega seotud meetmeteks. Täpseid andmeid on kättesaadavatest avalikest andmetest aga raske kätte saada.

56 Väljaspool ELi tehtavate kübervaldkonna kulutuste selgroo moodustab Budapesti konventsioon (vt punkt ***11***). Aastatel 2014–2018 kulutas EL väljaspool liidu piire küberturvalisuse tugevdamiseks ligikaudu 50 miljonit eurot. Peaaegu pool sellest kasutati stabiilsuse ja rahu edendamise rahastamisvahendi raames, mille ühe peamise projekti (GLACY+, 13,5 miljonit eurot) eesmärk oli suurendada ülemaailmset suutlikkust töötada välja ja rakendada küberkuritegevust käsitlevaid õigusakte ning parandada rahvusvahelist koostööd[81]. Teiste ELi rahastamisvahendite puhul keskenduti peamiselt Lääne-Balkani riikidele[82], samuti Euroopa naabruskonna riikidele: näiteks idapartnerluse riikidega tehtava Cybercrime@EaP projekti eesmärk on parandada rahvusvahelist koostööd küberkuritegevuse ja elektrooniliste tõendite alal.

Muud kulutused küberturbele

57 Alati ei ole võimalik kindlaks teha, milline osa ELi programmide kulutustest tehti küberturbele

- programmi „Horisont 2020“ raames rahastatakse ka küberfüüsikaliste süsteemide valdkonna ühisettevõtet ECSEL (Euroopa juhtpositsiooni tugevdamine elektroonikakomponentide ja -süsteemide toel). Samas ei suutnud me kindlaks teha, milline osa aastatel 2015–2016 läbi viidud 27 projektist (summas 437 miljonit eurot) on seotud konkreetselt küberturbega;

- küberturbe ja usaldusteenuste jaoks on Euroopa struktuuri- ja investeerimisfondide raames kavandatud kuni 400 miljonit eurot. See hõlmab turvalisuse ja andmekaitsevaldkonna investeeringuid, mille eesmärk on parandada digitaaltaristu koostalitlusvõimet ja vastastikust ühenduvust, e-identimist ning eraelu puutumatust ja usaldusteenuseid.

58 Euroopa Investeerimispank teatas oma 2018. aasta tegevuskavas kavatsusest suurendada kahesuguse kasutusega tehnoloogia, küberturvalisuse ja tsiviiljulgeoleku rahastamist kuni 6 miljardi euroni kolme aasta jooksul[83].

Tulevikuväljavaated

59 Kavandatud uue digitaalse Euroopa programmi[84] (DEP) 2021.–2027. aasta 2 miljardi euro suuruse küberturvalisuse komponendi eesmärk on tugevdada ELi küberturvalisuse valdkonna ettevõtteid ja ühiskonna üldist kaitset, sealhulgas võrgu- ja infoturbe direktiivi rakendamisele kaasaaitamise abil. Kavandatud küberturvalisuse pädevuskeskuste võrgustikust ning uurimis- ja pädevuskeskusest, mille eesmärk on lähenemisviisi ühtlustada, peaks eeldatavasti saama peamine rakendusmehhanism ELi kulude jaoks DEP raames.

60 ELi eelarve kaitsekulutusi suurendati hiljuti Euroopa kaitsevaldkonna tööstusliku arendamise programmi kaudu, millest 500 miljonit eurot eraldatakse 2019. ja 2020. aastal[85]. Programm keskendub liikmesriikide kaitsekulutuste koordineerimise ja tõhususe parandamisele ühiseks arendustööks antavate stiimulite kaudu. Selle eesmärk on investeerida Euroopa Kaitsefondi kaudu kaitsevõimekuse suurendamiseks kokku 13 miljardit eurot, millest osa hõlmab küberkaitset[86].

5. ülesanne: ELi asutuste piisavad ressursid

61 ELi küberturvalisuse poliitika keskmes on kolm peamist asutust – ENISA, Europoli küberkuritegevuse vastase võitluse Euroopa keskus (EC3) ja CERT-EU (vt ***2. selgitus***), millele on eraldatud napilt ressursse ajal, mil turvalisuse temaatika on saanud üheks oluliseks poliitiliseks prioriteediks. Inim- ja finantsressursside praeguse jaotuse juures on ELi asutustel keeruline täita neile esitatud ootusi[87].

62 Asutuste taotlusi täiendavate vahendite saamiseks, et rahuldada kasvavat nõudlust, ei ole täielikult rahuldatud, mis võib seada ohtu poliitiliste eesmärkide (ajakavakohase) täitmise. Näiteks

- piiratud ressursid olid üks tegur, mis takistas ENISA-l oma eesmärke 2017. aastal täielikult saavutada[88]. 2017. aasta paketis tehti ettepanek eraldada täiendavaid vahendeid, et neist piisaks ENISA uute volituste jaoks;

- Europoli küberkuritegevuse vastase võitluse Euroopa keskuse analüütikute arv ja IKT-suutlikkusse tehtud investeeringute suurus ei vasta nõudlusele[89]. Samuti töötavad Europoli küberkuritegevuse vastase võitluse keskuse ühises küberkuritegevuse vastases rakkerühmas (J-CAT) liikmesriikide ja kolmandate riikide eksperdid, et toetada jälitusteabel põhinevaid uurimisi. Kulud kannavad aga suures osas lähetajad riigid, mis pärsib suurema hulga ekspertide kasutamist. Europoli ja ELi poliitikatsükli rahastamise raames kasutatakse ka töötajate ajutist ja juhtumipõhist lähetamist, et võimaldada rohkematel riikidel töös osaleda.

63 Mõned piirangud on ise põhjustatud. CERT-EUs ja ENISAs töötab palju lepingulisi töötajaid, kelle värbamiseks kasutatavad menetlused võtavad tavaliselt kaua aega. Mõned teised piirangud (näiteks andekate töötajate ligimeelitamine ja säilitamine) tulenevad asutuste suutmatusest konkureerida erasektori palkadest või aeglastest karjääriväljavaadetest. Seetõttu tellis ENISA suure osa oma tööst aastatel 2014–2016 väljast[90].

64 Töötajate ja vajalike vahendite puudus võib kaasa tuua märkimisväärseid riske, eelkõige seoses ohuteabe kogumisega. Avatud ja suletud allikatest pärit andmete maht kasvab jätkuvalt ning tekitab riski, et analüütikud ei ole enam võimelised nõuetekohaseid ohuanalüüse tegema. Ilma õige võimekuse ja õigete töövahenditeta, mis võimaldaksid andmeid edukalt integreerida ja omavahel siduda, ei suudeta koostada kasutusvalmis ohuteavet, mida saaks jagada ja analüüsida kogu ELis[91].

Mõttekohad – rahastamisallikad ja kulutused

- Kuidas saaks komisjon ja seadusandjad ühtlustada ELi küberturvalisusega seotud kulutusi ja viia need selgemalt kooskõlla selgelt määratletud eesmärkidega?
- Kuidas saaks terviklikult käsitleda ELi asutuste ressursside nappuse küsimust, võttes arvesse liidu vajadusi ja eesmärke?
- Milliseid meetmeid on ELi ja liikmesriikide tasandil välja töötatud selleks, et vähendada takistusi, mis ei lase VKEdel kaasata oma tegevuse laiendamiseks vajalikke investeeringuid?
- Millised konkreetseid ja jätkusuutlikke tulemusi annavad programmi „Horisont 2020“ vahendid küberturvalisuse lahenduste väljatöötamiseks?
- Kuidas suurendavad ELi suutlikkuse arendamise meetmed suutlikkust väljaspool liidu piire kooskõlas ELi väärtustega?

Küberohtudega toime tuleva ühiskonna ehitamine

65 Küberturvalisuse valdkonna juhtimine tegeleb ohtude ja riskide juhtimisega, suutlikkuse ja teadlikkuse suurendamise ning usaldusele rajatud koordineerimise ja teabejagamisega.

6. ülesanne: juhtimise ja standardite tugevdamine

Infoturbe juhtimine

66 Infoturbe juhtimine tähendab struktuuride ja põhimõtete kehtestamist, et tagada andmete konfidentsiaalsus, terviklus ja kättesaadavus. Tegu on enam kui vaid tehnilise küsimusega, mis nõuab tõhusat juhtimist, usaldusväärseid protsesse ja organisatsiooniliste eesmärkidega joondatud strateegiaid[92]. Selle üks osa on küberturvalisuse juhtimine, mis tegeleb igat liiki küberohtudega, mille hulka kuuluvad suunatud, keerukad ründed, rikkumised ja intsidendid, mida on raske avastada või hallata.

67 Küberturvalisuse juhtimismudelid erinevad liikmesriigiti ja vastutus küberturvalisuse eest on sageli jagatud paljude üksuste vahel. Need erinevused võivad takistada koostööd, mis on vajalik selleks, et reageerida suuremahulistele piiriülestele intsidentidele ja vahetada ohte käsitlevat teavet nii riikide kui ka ELi tasandil. Meie küsitlus liikmesriikide kõrgeimate kontrolliasutuste seas näitas, et kõige riskantsemaks peeti puudusi avaliku sektori asutuste juhtimiskorralduses ja riskijuhtimises.

68 Kuigi tagajärjed erasektori organisatsioonidele võivad olla tõsised, on kübervaldkonna juhtimises palju puudusi. Peaaegu üheksa organisatsiooni kümnest arvavad, et nende küberturvalisuse funktsioon ei vasta täielikult organisatsiooni vajadustele[93], ning küberturvalisusega tegelevad töötajad on hierarhias vähemalt kaks taset juhatusest allpool[94].

69 ELi äriühinguõiguse direktiivid ei sisalda konkreetseid nõudeid küberohtude avalikustamise kohta. Ameerika Ühendriikides avaldas väärtpaberi- ja börsikomisjon (SEC) hiljuti mittesiduvad suunised, et aidata börsil noteeritud ettevõtetel koostada teavet küberturvalisuse riskide ja intsidentide kohta[95]. Euroopa järelevalveasutuste ühiskomitee[96] hoiatas küberriskide suurenemise eest, innustas finantsasutusi

parandama haavatavaid IT-süsteeme ning uurima infoturvet, ühenduvust ja allhanget ohustavaid olemuslikke riske[97].

70 VKEde infoturbealase juhtimise tugevdamine on eriti raske, kuna sageli ei ole nad võimelised asjakohaseid süsteeme rakendama. VKEdel puuduvad sobivad suunised infoturbe ja eraelu puutumatuse nõuete rakendamiseks ja tehnoloogiariskide leevendamiseks[98]. Peamised probleemid on seega nende vajaduste parem mõistmine ning vajalike stiimulite ja toe pakkumine.

71 Sidusa rahvusvahelise küberturvalisuse juhtimise raamistiku puudumine kahjustab rahvusvahelise kogukonna võimet küberrünnetele reageerida ja neid piirata. Seepärast on oluline saavutada konsensus sellise juhtimisraamistiku loomiseks, mis peegeldaks kõige paremini ELi huve ja väärtusi[99]. Rahvusvaheliste küberruumi jaoks siduvate normide seadmine muutub üha ebakindlamaks, nagu näitab konsensuse puudumine ÜRO valitsusekspertide rühmas 2017. aastal selle kohta, kuidas tuleks rahvusvahelist õigust intsidentide korral kohaldada.

72 Küberruumi juhtimist käsitleva tegevuse tugevdamiseks on EL loonud ka kuus küberpartnerlust, et luua korrapärane poliitikadialoog, mis tekitaks usaldust ja looks ühiseid koostöövaldkondi[100]. Koostöö senised tulemused on ebaühtlased, kuid üldiselt ei saa ELi pidada rahvusvahelises mõõtmes globaalseks tegijaks, kuigi liit on oma positsiooni parandanud[101].

Infoturve ELi institutsioonides

73 Igal ELi institutsioonil on oma infoturbeeeskirjad. Institutsioonidevahelise kokkuleppe kohaselt abistab komisjon infoturbe alal teisi institutsioone ja asutusi. ELi institutsioonid ja organid on tunnistanud vajadust arendada sidusalt oma kübersuutlikkust ja riskijuhtimismeetodeid. Komisjon, nõukogu ja Euroopa välisteenistus esitavad 2020. aastal küberküsimusi käsitlevale horisontaalsele töörühmale aruande infoturbe juhtimise kohta ning edusammudest ELi institutsioonide ja asutuste küberturvalisuse juhtimise selgitamisel ja ühtlustamisel[102].

74 Komisjonis vastutab infotehnoloogia infrastruktuuri ja teenuste turvalisuse eest informaatika peadirektoraat (DIGIT) (vt ***3. selgitus***). Komisjoni digitaalse strateegia peamised IT-turbe eesmärgid hõlmavad IT-turvalisuse integreerimist juhtimisprotsessidesse, (kulu)tõhusat taristut ja vastupidavusvõimet, intsidentide avastamise ja neile reageerimise ulatuse laiendamist, ning IT ja turvalisuse juhtimise omavahelist integreerimist[103]. Komisjon tagab oma teenuseosutaja lepingu alusel, et

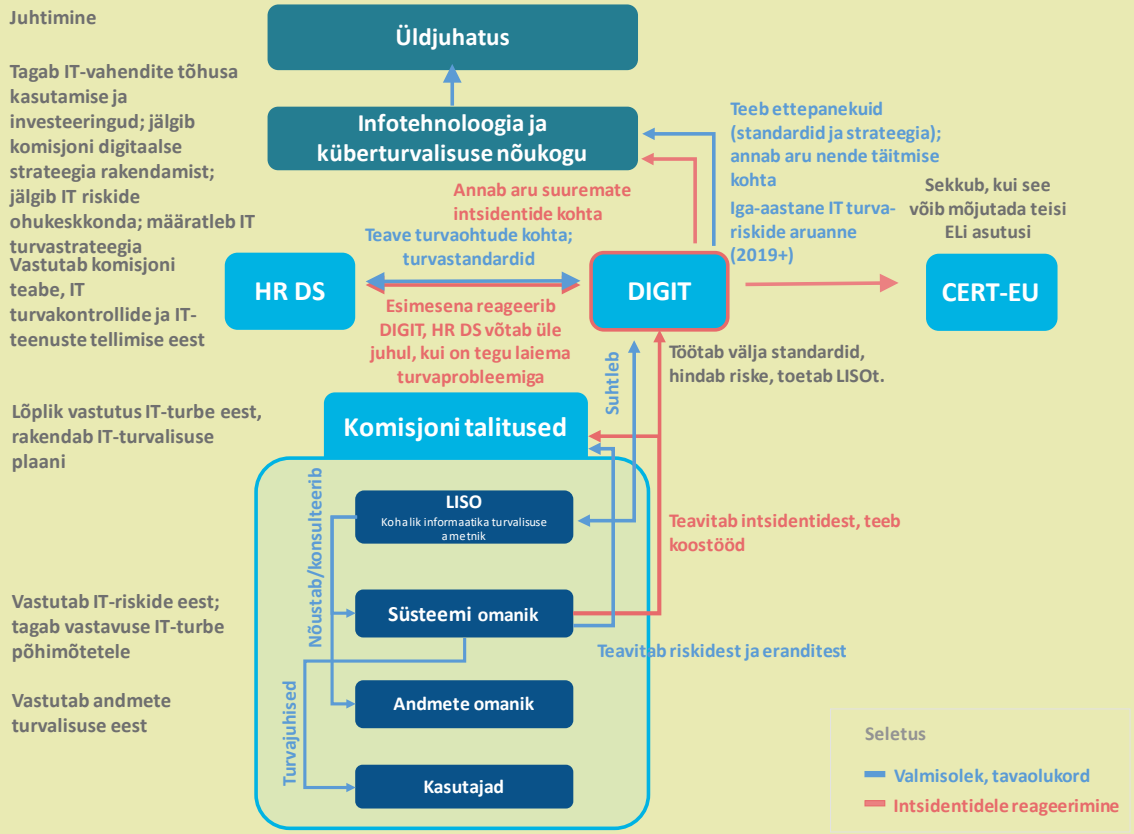
peaaegu kogu tarkvara on aktiivselt hooldatud ja et kasutatakse üksnes tarnijate toetatavat tarkvara[104].

75 Institutsioone kaitstes on oluline kaitsta ka ELi ÜJKP missioone ja struktuure kogu maailmas. ELi küberkaitse poliitilise raamistiku (2018. aasta ajakohastatud versioon) üks prioriteete on tugevdada ELi üksuste kasutatavate ÜJKP side- ja infosüsteemide kaitset. Nüüd toimib ka Euroopa välisteenistuse küberhalduse nõukogu, mis tuli esimest korda kokku juunis 2017[105].

3. selgitus

Komisjoni infosüsteemide kaitsmine

Komisjoni ligikaudu 1300 süsteemi ja 50 000 seadet ohustavad pidevalt küberründed. Vastutus IT-valdkonna eest on detsentraliseeritud, nagu on näidatud allpool esitatud joonisel. Info- ja IT-turve põhinevad informaatika peadirektoraadi ühisel IT-turvalisuse kaval. Komisjoni *de facto* infoturbejuhina toimib infotehnoloogia ja küberturvalisuse nõukogu, kes ühendab operatiivset IT-turvalisust ja komisjoni tippjuhtkonda (üldjuhatust).



Allikas: Euroopa Kontrollikoda komisjoni otsuste[106] põhjal.

Personali ja julgeoleku peadirektoraadi peamine ülesanne on kaitsta komisjoni töötajaid, teavet ja vara. Samuti uurib ta selliste intsidentide turvalisusega seotud

aspekte, millel on laiem turvamõõde kui ainult IT ning panustab seega peadirektoraadi vastuluure- ja terrorismivastasesse tegevusse.

IT-turbe eest vastutab informaatika peadirektoraat, mille ruumes asub ka CERT-EU (ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm). 2011. aastal loodud CERT-EU eelarve on ligikaudu 2,5 miljonit eurot aastas ja tal on umbes 30 töötajat. CERT-EU reageerib esimesena infoturvaintsidentide, mis puudutavad mitut institutsiooni, kuid ei tegutse ööpäevaringselt. Rühm kasutab teabevahetusplatvormi. 2018. aastal allkirjastas CERT-EU ENISA, EC3 ja Euroopa Kaitseagentuuriga mittesiduva vastastikuse mõistmise memorandumi, et tugevdada koostööd ja koordineerimist. Samuti on tal olemas tehniline kokkulepe NATO küberturbeintsidentidele reageerimise üksusega (NCIRC).

Ohu- ja riskihinnangud

76 Põhjendatud ja pidevad ohu- ja riskihinnangud on olulised töövahendid nii avaliku kui ka erasektori organisatsioonide jaoks. Samas puudub ühtne lähenemisviis küberohtude liigitamiseks ja kaardistamiseks ning riskihinnangute koostamiseks; seetõttu on hinnangute sisu on väga erinev, mis kujutab endast lahendamist vajavat ülesannet kogu ELi hõlmava sidusa küberturvalisuse lähenemisviisi jaoks[107]. Lisaks toetuvad hinnangud sageli samadele allikatele või isegi muudele ohuhinnangutele, mille tulemuseks on korduv osutamine samadele leidudele[108] ja sellega kaasnev oht pöörata ebapiisavat tähelepanu muudele ohtudele. Olukorda halvendab jätkuv vastumeelsus jagada teavet ja vahejuhtumitest teatamata jätmine.

77 Euroopa välisteenistuse struktuuris töötav hübriidohtude ühisüksus[109] loodi selleks, et parandada olukorrateadlikkust ja toetada otsuste tegemist analüüside jagamise kaudu; üksus peab aga oma teadmisi laiendama, sealhulgas küberturvalisuse valdkonnas. Samal ajal pakub CERT-EU ELi institutsioonidele, organitele ja asutustele aruandeid ja ülevaateid nende vastu suunatud küberohtude kohta.

78 ENISA on varem märkinud, et paljudel liikmesriikidel on ohtudest kvalitatiivne arusaam ja et on vaja rohkem küberohu modelleerimist[110]. Üldist arusaamist parandab strateegilise analüüsi jaoks vajalik seirevõime. Terviklikuma pildi tagamiseks võiksid ohuhinnangud aga lisaks tehnoloogilistele ohtudele hõlmata ka sotsiaalpoliitilisi ja majanduslikke ohte, samuti ohutegureid ja osaliste motiive.

Stiimulid

79 Organisatsioonidel on ikka veel liiga vähe õiguslikke ja majanduslikke stiimuleid intsidentidest teatamiseks ja nende kohta teabe jagamiseks. Mainekahju kartuses eelistavad paljud organisatsioonid ikka veel tegeleda küberrünnetega diskreetselt või maksta nende toimepanijate nõutud summad. Tulevik näitab, kui tõhusalt suurendab võrgu- ja infoturbe direktiiv intsidentidest teavitamist. Komisjon loodab, et olukord paraneb eelkõige liikmesriikide tasandil, kuid küberturvalisust käsitlev õigusakt lisab kogu ELi hõlmava perspektiivi[111].

80 Oma hangetes teatavaid standardeid kasutades saavad avaliku sektori asutused digitaalsete toodete ja teenuste ostjatena tarnijaid hangete ning teadusuuringute ja programmide rahastamise kaudu märkimisväärselt mõjutada: näiteks nõudes teatavate tehniliste standardite vastu võtmist (nt Interneti protokolli IPv6, et aidata võidelda küberkuritegevuse vastu). Praegu puudub küberturvalisuse taristu jaoks ühine hankeraamistik[112]. Komisjon saab sellega seoses palju ära teha. Järgmise mitmeaastase finantsraamistiku jaoks kavandatava DEP üks eesmärk on investeerida avaliku sektori vahendeid uusima küberturvalisuse tehnoloogia hankimiseks (seni on seda tehtud vaid piiratud määral).

81 Oma reguleerimispädevuse kaudu saab komisjon tagada, et turvalisuse suurendamiseks töötatakse välja ja võetakse laialdaselt vastu õiged standardid. Komisjon ja Europol teevad koostööd interneti haldamisega tegelevate organitega, nagu ICANN (vt punkt ***38***) ja RIPE-NCC[113], mis on väga oluline, et luua küberkuritegevuse vastu võitlemiseks õige struktuur, mis toetaks õiguskaitse- ja justiitsasutusi.

7. ülesanne: oskuste ja teadlikkuse parandamine

82 ENISA on juhtinud tähelepanu sellele, et kasutajatel on küberrünnete puhul väga oluline roll ning et oskuste, hariduse ja teadlikkuse parandamine on keskse tähtsusega, et ehitada üles küberohtudega toime tulev ühiskond[114]. Ohumärke mõistvad ja õiget tehnikat kasutavad inimesed, olgu nad tööl või kodus, võivad ründeid aeglustada või ennetada.

83 Eriti murettekitav on suurenev asümmeetria küberkuritegevuseks või küberründeks vajaliku oskusteabe ja selle eest kaitsmiseks vajalike oskuste vahel. Kuritöö kui tellitava teenuse mudel on vähendanud küberkuritegelikule turule sisenemise tõkkeid: ka robotvõrkude ehitamiseks vajalike tehniliste teadmisteta

inimesed võivad neid võrke üürida, kasutada valmis häkkimiskomplekte või lunavarapakette.

Koolitus, oskused ja suutlikkuse arendamine

84 Maailm seisab silmitsi kasvava küberturvalisuse oskuste puudujäägiga; töötajate puudus on alates 2015. aastast 20% võrra suurenenud[115]. Tavapärased värbamiskanalid (sealhulgas juhtivate ja interdistsiplinaarsete ametikohtade täitmiseks) ei vasta nõudlusele[116]. Ligi 90% maailma küberturvalisuse valdkonna töötajatest on mehed ja endiselt puuduv sooline mitmekesisus vähendab veelgi valdkonnas töötada soovivate andekate inimeste hulka[117]. Lisaks on ülikoolides kübertemaatikaga seotud ained mittetehnilistes õppekavades alaesindatud.

85 Koolitust ja haridust vajavad kõik: nii riigiametnikud, õiguskaitseametnikud, justiitsasutused, relvajõud kui ka haridustöötajad. Näiteks peavad kohtud olema võimelised tegelema küberkuritegevuse ja selle ohvrite kiiresti muutuva tehnilise eripäraga[118]; praegu puuduvad kogu ELi hõlmavad koolitus- ja sertifitseerimisstandardid[119]. ELi institutsioonidel on oluline leida töötajaid, kellel oleks kombinatsioon õigetest oskustest. Ilma selleta ei pruugi institutsioonid suuta nõuetekohaselt kindlaks määrata töö ulatust, teha kindlaks õigeid partnereid ja turvavajadusi, ning programme hallata. See võib omakorda kahjustada ELi programmide või poliitika väljatöötamise tõhusust.

86 Kuigi hariduspoliitika eest vastutavad ELis liikmesriigid, korraldatakse juba mitmeid koolitusi (vt ***tabel 2***) ja õppusi (vt ***4. selgitus***). EL saab aidata kogu ELi hõlmavate standardite lõimimisel kõigi asjaomaste valdkondade õppekavasse[120]. Näiteks digitaalkriminalistika valdkonnas on vaja ühiseid koolitusstandardeid, et hõlbustada tõendite vastuvõetavust liikmesriikides. Küberkuritegevuse piiriülese olemuse tõttu võivad juhtumid hõlmata mitut jurisdiktsiooni, mis eeldab koolitust ELi tasandil. Euroopa Liidu Õiguskaitsekoolituse Amet (CEPOL) on aga tõdenud, et enam kui kaks kolmandikku liikmesriikidest ei paku õiguskaitseametnikele korrapärast küberkoolitust[121]. Samuti võib EL leida võimalusi tsiviil- ja sõjalise valdkonna hariduse ja koolituse vaheliseks sünergiaks[122]. Sellest tulenevalt on ENISA seisukohal, et kuigi kriitilise tähtsusega sektorites on praegu palju koolitusvõimalusi, ei ole need piisavalt suunatud elutähtsa taristu vastupidavusvõime suurendamisele[123].

Tabel 2. Näited ELi kübervaldkonnaga seotud koolitusalgatustest

Euroopa Kaitseagentuuri projektid, nt erasektori toetus õppustele ja projekt *Cyber Ranges*	Euroopa Julgeoleku- ja Kaitsekolledži võrgustik (mis pakub tsiviil-sõjalist koolitust), sealhulgas küberkaitsehariduse, -koolituse ja -õppuste ning hindamisplatvorm	ENISA koolitus, mis pakub koolitusprogramme valdkondades, kus kommertsturg neid ei paku
Europoli, CEPOLi, küberkuritegevusalase hariduse ja koolituse Euroopa töörühma[124] koolitusprogrammid, sealhulgas koolituse juhtimise mudel ja pädevusraamistik (sh sertifitseerimine)	Pädevusvõrgustik ja teadusliku pädevuse keskus (kavandatud)	Julgeolekuliidu üheteistkümnendas eduaruandes välja pakutud krüpteerimist käsitlevad meetmed
ELi ja NATO koostöö küberkaitsealase koolituse ja hariduse valdkonnas	Sõjaline Erasmuse programm	Euroopa õigusalase koolituse võrgustik

Allikas: Euroopa Kontrollikoda.

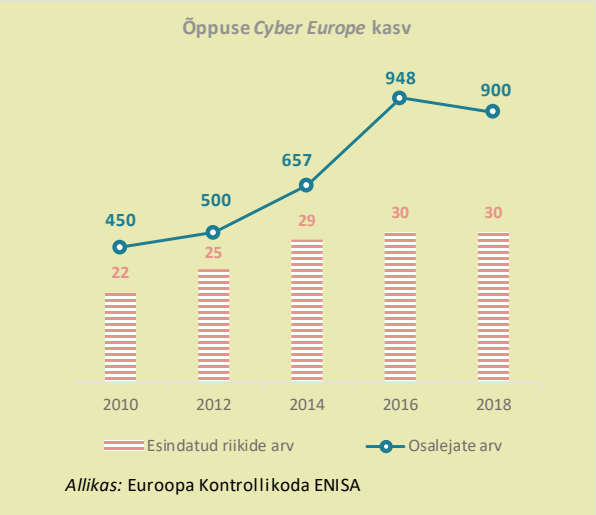
87 17 delegatsioonis töötavad ELi lähetatud terrorismivastase võitluse ja julgeolekueksperdid, et tugevdada ELi sise- ja välisjulgeoleku vahelist seost[125]. Hoolimata ressursside piiratusest võib kübervaldkonna parem oskusteave aidata alustada õigeid projekte ning teha kindlaks sünergia teiste programmide või rahastamisallikatega[126]. Samuti võiks see parandada küberturvalisuse teema nähtavust poliitilises dialoogis, kuigi see konkureeriks seal paljude teiste prioriteetidega, nagu ränne, organiseeritud kuritegevus või tagasipöörduvad välisvõitlejad.

4. selgitus

Õppused

Õppused on oluline osa küberharidusest ja -koolitusest, pakkudes head võimalust valmisoleku suurendamiseks võimekuse testimise abil, lahendusi reaalsetele stsenaariumidele ja aidates valdkonna spetsialistidel tööalaseid võrgustikke luua. Alates 2010. aastast on nende sagedus märkimisväärselt suurenenud.

Neis osaletakse kas kohapeal või kaugteel. Viiakse läbi ka järelhindamisi, et teha kindlaks saadud kogemused, kuigi need ei pruugi strateegiliste/poliitiliste, operatiiv- ja tehniliste tasandite vahel kohe täielikult haakuda[127].



Allikas: Euroopa Kontrollikoda ENISA

ELi ja NATO suurõppuste – iga kahe aasta tagant toimuv *Cyber Europe* (operatiivõppus) ja iga-aastane *Locked Shields* (tehniline õppus) – käigus tulevad kokku rohkem kui 1000 osalejat ligikaudu 30 osalevast riigist. Mõlemad õppused keskenduvad elutähtsa taristu kaitsmisele ja hooldamisele simuleeritud ründestsenaariumide käigus. Õppused on märkimisväärselt põhjalikumaks muutunud, hõlmates nüüd nii meedia, õigus- kui ka finantspoliitika elemente, et parandada praktikute olukorrateadlikkust. Paralleelse ja koordineeritud PACE-õppuse (strateegiline tasand) käigus testitatakse ELi ja NATO suhtlust hübriidkriisi korral.

Need ei ole ainsad rahvusvahelised õppused. ENISA korraldab igal aastal kübervaldkonna võistluse, kus meeskonnad konkureerivad, et lahendada turvalisusega seotud ülesandeid, mis hõlmavad näiteks veebi- ja mobiilvaldkonna turvalisust, krüpteerimist, pöördprojekteerimist, eetikat ja kriminalistikat. Esimene ministrite tasandi kohtumine, ELi CYBRID, toimus septembris 2017 ja keskendus strateegiliste otsuste tegemisele. 2018. aastal korraldati esmakordselt NATOga seotud õppus *Crossed Swords*, et arendada õppuse *Locked Shields* ründeelemente. NATO korraldab ka küberkoalitsiooni õppusi.

Üks peamine ülesanne on tagada kõigi oluliste sidusrühmade aktiivne osalemine ja kõigi õppuste koordineerimine, et vältida dubleerimist ja jagada saadud kogemusi tõhusalt.

Teadlikkus

88 Kodanikke kasutatakse sageli rünnakute läbiviimiseks ja väärinfo levitamiseks, kuna nad on odavaid ja laialt levinud seadmeid ja tarkvara lahendusi kasutades tõenäoliselt teadmatult haavatavad või langevad sotsiaalse manipulatsiooni ohvriks. Tõhusa kübervastupidavusvõime saavutamiseks on seetõttu väga oluline suurendada teadlikkust, kuid see ei ole sugugi kerge ülesanne, sest mitteekspertidel on raske mõista küberturvalisuse keerukust ja sellega seotud riske.

89 Teadlikkuse suurendamise näited on Euroopa iga-aastane küberturvalisuse teadlikkuse kuu ja turvalisema interneti päev. Küberturvalisuse teadlikkuse kuuga on nüüdseks ühinenud seitse ELi mittekuuluvat liikmesriiki[128]. Europoli kampaania „Ütle ei!“ eesmärk on vähendada ohtu, et lapsed võivad sattuda internetis seksuaalse sunduse ja väljapressimise ohvriks. Ohu vähendamine on oluline, sest praegu esitavad vaid vähesed ründeohvrid politseile kuriteoavalduse[129]. Komisjon tunnistab, et küberturvalisuse strateegia on olnud kodanike ja ettevõtjate teadlikkuse suurendamisel kõigest „osaliselt tulemuslik“[130]. See on tingitud ülesande ulatusest, piiratud vahenditest, liikmesriikide ebaühtlasest aktiivsusest ja teaduslikult põhjendatud meetodite puudumisest selle kohta, kuidas teadlikkust kõige paremini suurendada ja mõõta.

90 Komisjoni ja asjaomaste asutuste ülesanne on tagada, et teadlikkuse suurendamise meetmed oleksid hästi sihipärased ja avalikustatud, kaasavad, lähtuksid ohumaastikust, väldiksid soovimatut mõju (nt n-ö turvaväsimust)[131], ning töötada välja nende tulemuslikkuse hindamiseks vajalikud meetodid ja parameetrid. See peaks samal määral kehtima ka ELi institutsioonide kohta, kus tuleb samuti teadlikkust suurendada[132].

8. ülesanne: parem teabevahetus ja koordineerimine

91 Küberturvalisus nõuab avaliku ja erasektori koostööd, eelkõige teabe jagamisel ja parimate tavade vahetamisel. Usaldus on oluline kõigil tasandeil, et luua õige keskkond tundliku teabe piiriüleseks jagamiseks. Puudulik koordineerimine põhjustab killustumist, jõupingutuste dubleerimist ja oskusteabe kadu. Tõhus koordineerimine võib tuua käegakatsutavat edu (nt pimeveebi kauplemisplatvormide sulgemise)[133]. Hoolimata viimaste aastate edusammudest on usaldus ikka veel ebapiisav[134] – seda nii ELi tasandil kui ka mõnes liikmesriigis[135].

ELi institutsioonide ja liikmesriikide vaheline koordineerimine

92 Küberturvalisuse strateegia ning võrgu- ja infoturbe direktiiviga kasutusele võetud koostööstruktuuride üks eesmärk on suurendada sidusrühmade vahelist usaldust. Strateegia hindamisel tõdeti, et on loodud alus ELi tasandi strateegilseks ja operatiivseks koostööks[136]. Sellest hoolimata peetakse koordineerimist üldiselt ebapiisavaks[137]. Keeruline on tagada, et teabevahetus ei oleks mitte ainult mõttekas, vaid võimaldaks ka üldpildist täieliku ülevaate saada. Tunnustatud terminoloogial põhineva ühise seisukoha saavutamine on siinkohal oluline tegur (vt ***5. selgitus***).

93 ENISA hindamises märgiti siiski, et ELi lähenemisviis küberturvalisusele ei olnud piisavalt kooskõlastatud, mistõttu puudub ENISA ja teiste sidusrühmade tegevuse vaheline sünergia. Koostöömehhanismid on endiselt suhteliselt ebaküpsed[138]; küberturvalisust käsitlevas õigusaktis on kavas seda käsitleda ENISA koordineeriva rolli tugevdaamise abil. Soov tõhustada koostööd oli ka põhus vastastikuse mõistmise memorandumi sõlmimiseks, mille allkirjastasid 2018. aastal ENISA, EDA, Europoli EC3 ja CERT-EU[139]. Komisjoni lähiaastate prioriteet on poliitiliste algatuste, vajaduste ja investeerimisprogrammide asjakohane ühtlustamine, et saada üle killustatusest ja tekitada sünergiat[140].

94 Koordineerimisfunktsioonid on jagatud mitme institutsiooni vahel. Julgeolekuliidu rakkerühm loodi selleks, et täita keskset rolli komisjoni eri peadirektoraatide töö koordineerimisel, et toetada julgeolekuliidu tegevuskava[141]. Sidevõrkude, sisu ja tehnoloogia peadirektoraat (CNECT) juhatab rakkerühma küberturvalisuse valdkonnaga tegelevat allrühma.

95 Nõukogus tegeleb küberturvalisusega horisontaalne küberküsimuste töörühm, kes koordineerib strateegilisi ja horisontaalseid küberküsimusi ning aitab ette valmistada õppusi ja hinnata nende tulemusi. Töörühm teeb tihedat koostööd poliitika- ja julgeolekukomiteega, millel on keskne otsustusroll mis tahes kübervaldkonnaga seotud diplomaatiliste meetmete puhul (vt järgmise peatüki ***6. selgitus***). Kuna küberturvalisus on valdkonnaülene teema, ei ole kõigi asjaomaste huvide kooskõlastamine lihtne: hiljuti on küberteemadega seotud küsimusi käsitlenud mitte vähem kui 24 töörühma ja ettevalmistavat organit[142].

96 Kaks viimast seadusandlikku ettepanekut ENISA tugevdamise kohta (2017) ja küberturvalisuse pädevuskeskuste võrgustiku ning uurimis- ja pädevuskeskuse loomise kohta (2018) on välja töötatud spetsiaalselt selleks, et vähendada killustatust ja topelttööd. Küberturvalisuse kompetentsikeskuste võrgustiku ning uurimis- ja

pädevuskeskuse loomise ajendav tegur on olnud vajadus täita lünk, mida võrgu- ja infoturbe direktiivi koostööstruktuurid ei täida, sest need ei ole mõeldud toetama tipptasemel lahenduste väljatöötamist.

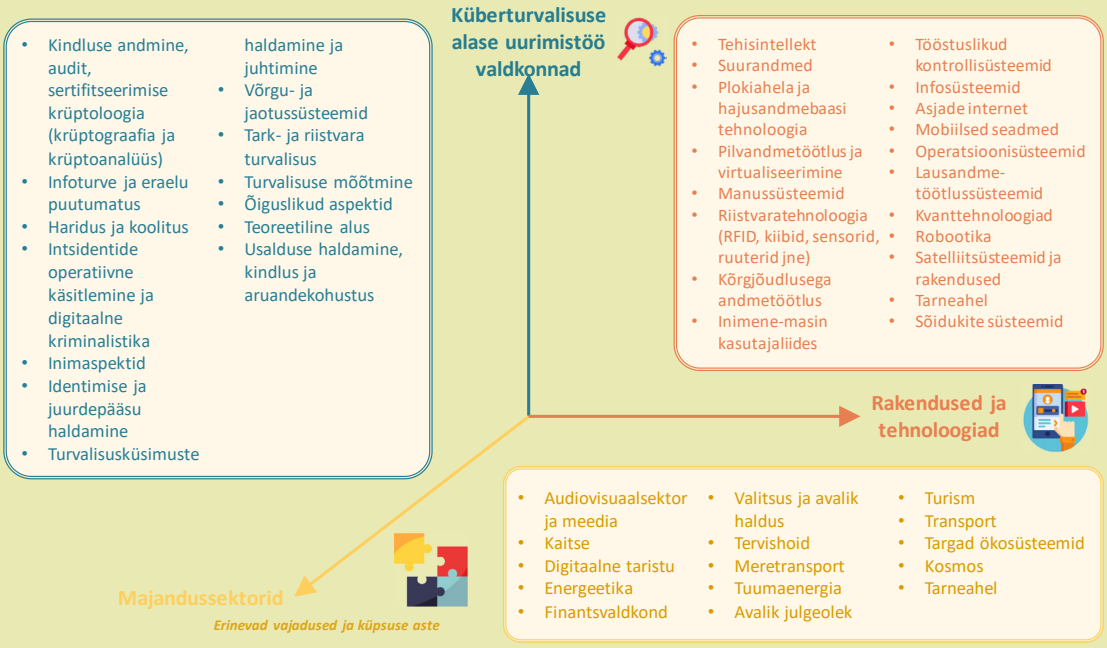
5. selgitus

Katse rääkida sama küberkeelt: *tehnoloogiline sidusus*

Terminoloogiline selgus parandab olukorrateadlikkust ja koordineerimist[143] ning aitab täpselt kindlaks teha ohud ja riskid.

Komisjoni Teadusuuringute Ühiskeskus koostas hiljuti ajakohastatud uurimistaksonoomia, mille aluseks on erinevad rahvusvahelised standardid[144]. Selle eesmärk on saada loendiks, mida kasutaksid kogu Euroopa uurimisüksused.

Küberturvalisuse taksonoomia



Allikas: Euroopa Kontrollikoda Euroopa Komisjoni edastatud andmeid kohandades.

Kuni viimase ajani puudusid ELi institutsioonidel ja asutustel ühised määratlused. See on muutumas. Tõhusa piiriülese koostöö hõlbustamiseks töötas koostöörühm tegevuskava raames välja intsidentide taksonoomia.

Koostöö ja teabevahetus erasektoriga

97 Avaliku sektori asutuste ja erasektori koostöö on küberturvalisuse üldise taseme tugevdamiseks hädavajalik. Vaatamata sellele leidis komisjon oma 2017. aasta küberjulgeoleku strateegia hindamisel, et erasektori sidusrühmade ning avaliku ja erasektori vaheline teabevahetus ei ole „veel optimaalne“, kuna puuduvad usaldusväärsed aruandlusmehhanismid ja teabe jagamise stiimulid[145], mis takistab strateegiliste eesmärkide saavutamist. Komisjon on ka märkinud, et puudub tõhus koostöömehhanism, mille raames liikmesriigid teeksid koostööd, et strateegiliselt suurendada majandusharu kestvat tööstuslikku suutlikkust[146].

98 Teabe jagamise ja analüüsimise keskused on organisatsioonid, mis on loodud selleks, et pakkuda platvorme ja vahendeid teabe jagamiseks avaliku ja erasektori vahel ning koguda teavet küberohtude kohta. Nende eesmärk on luua usaldust, jagades kogemusi, teadmisi ja analüüse, eriti algpõhjuste, intsidentide ja ohtude kohta. Riiklikud ja valdkondlikud teabe jagamise ja analüüsimise keskused on juba olemas paljudes liikmesriikides, kuid Euroopa tasandil on neid endiselt suhteliselt vähe[147]. Samas on nad silmitsi mitme probleemiga (ressursside nappus, raskused nende edu hindamisel, õigete struktuuride tagamine nii avaliku kui ka erasektori kaasamiseks, õiguskaitseasutuste kaasamine), mis tuleb ületada, et aidata kaasa võrgu- ja infoturbe direktiivi rakendamisele ja üleeuroopalise tasandi turvavõimekuse suurendamisele[148].

99 Tihe koostöö erasektoriga on eriti oluline võitluses keeruka küberkuritegevuse vastu, kuid selle tõhusus on liikmesriigiti ebaühtlane ja sõltub usalduse tasemest[149]. Europoli EC3 on siiski loonud mitu nõuanderühma, kus osalevad erasektori ettevõtjad, ELi institutsioonid ja asutused ning muud rahvusvahelised organisatsioonid, ja mille eesmärk on parandada võrgustikus osalemise, luureandmete jagamise ja koostöö kaudu sidusrühmade ühist tegutsemist. Nende töö aluseks olevad plaanid on kooskõlas ELi poliitikatsükli eesmärkidega[150]. Krüpteerimise kuritarvitamine kuritegelikul eesmärgil on veel üks valdkond, mille lahendamist vajavad probleemid nõuavad suuremat koostööd erasektoriga. Europoli EC3 uurib praegu võimalusi erasektorist ja teadusasutustest pärit ekspertide lühiajaliseks juhtumipõhiseks lähetamiseks küberkuritegevuse vastase rakkerühma (J-CAT) juurde (vt punkt ***62***).

100 Tõhusate koostöömehhanismide puudumine kahjustab nii avaliku kui ka erasektori tsiviil- ja kaitseringkondi. Ühised ülesanded hõlmavad krüptograafiat, turvalisi manussüsteeme, pahavara avastamist, simulatsioonimeetodeid, võrgu- ja süsteemikaitse- ning autentimistehnoloogiaid. Tsiviil-sõjalise koostöö edendamine ning teadusuuringute ja tehnoloogia toetamine (eelkõige VKEde toetamise kaudu) on

ajakohastatud ELi küberkaitsepoliitika raamistiku kaks prioriteeti (2018. aasta ajakohastatud versioon).

Mõttekohad – vastupidavusvõime parandamine

- Kuidas saavutada ELi tasandil asjakohane tasakaal vajaduse vahel peavoolustada küberturvalisuse poliitika ning tagada tõhus koordineerimine erinevate osaliste vahel ja vastutuse jagamine?
- Kui hästi on ELi institutsioonid ja asutused ette valmistatud järgmise otse nende pihta suunatud suure ründe korral?
- Kuidas muuta ELi kübervaldkonnaga tegelevad asutused andekate inimeste jaoks atraktiivsemaks?
- Milliseid täiendavaid meetmeid on vaja ELi institutsioonide ja asutuste piisava suutlikkuse tagamiseks, et võimaldada luua sidus riski- ja ohuhindamisraamistik?
- Kuidas aitavad Euroopa järelevalveasutused (Euroopa Pangandusjärelevalve, Euroopa Väärtpaberiturujärelevalve ning Euroopa Kindlustus- ja Tööandjapensionide Järelevalve) vähendada finantssektori haavatavust küberohtude vastu ja mida saavad muud sektorid sellest õppida?
- Arvestades valdkonna teadmiste üldist ebapiisavust, kuidas saaks maksimeerida avaliku sektori asutustele antava ELi tehnilise abi kogumõju kübervastupidavusvõime parandamisele?
- Kuidas saavad EL ja liikmesriigid tagada sisuka kohaloleku rahvusvahelistes aruteludes, et kujundada küberruumi juhtimist ja standardeid ning tutvustada ELi väärtusi?
- Millised ELi ja liikmesriikide tasandi teadlikkuse suurendamise meetmed (sealhulgas ennetustegevus) avaldavad tõesti mõju ja mida saab EL teha nende mahu suurendamiseks?
- Milline on ELi roll soolise mitmekesisuse toetamisel küberturvalisuse valdkonnas?
- Kuidas saavad EL ja liikmesriigid suurendada tsiviil- ja kaitsevaldkonna vahelist sünergiat kooskõlas küberkaitsepoliitika raamistikuga (2018. aasta ajakohastatud versioon)?

Tõhus reageerimine küberintsidentidele

101 Tõhus reageerimine küberrünnetele on väga oluline, et lõpetada need nii vara kui võimalik. Eriti oluline on, et kriitilise tähtsusega sektorid, liikmesriigid ja ELi institutsioonid suudaksid reageerida kiiresti ja kooskõlastatult. Selleks on väga oluline rünnete varajane avastamine.

9. ülesanne: tõhus avastamine ja reageerimine

Avastamine ja teavitamine

102 Ühised avastamisvahendid aitavad igapäevaselt enamiku ründeid tõrjuda[151]. Digitaalsed süsteemid on aga muutunud nii keeruliseks, et iga rünnet ei ole võimalik vältida. Nende keerukus tähendab, et ründeid ei pruugita pika aja jooksul avastada. Seetõttu peab ekspertide sõnul keskenduma rünnete kiirele avastamisele ja kaitsele[152]. Mõningaid tuvastamisvahendeid, nagu automatiseerimine, masinõpe ja käitumisanalüüs, mille eesmärk on vähendada riske ning analüüsida ja õppida süsteemi käitumisest, kasutatakse ettevõtetes aga vähe[153]. See on osaliselt tingitud valepositiivsetest juhtumitest, mille puhul peetakse ohtu mittesisaldavat tegevust ekslikult kuritahtlikuks.

103 Kui turvarikkumine on tuvastatud ja seda on analüüsitud, tuleb sellest kiiresti teatada ja aru anda, et muud avalik-õiguslikud ja eraõiguslikud üksused saaksid võtta ennetavaid meetmeid ning asjaomased ametiasutused saaksid ründest mõjutatud isikuid toetada. Paljud organisatsioonid tunnistavad küberintsidente ja annavad nende kohta teavet üksnes vastumeelselt[154]. Väga oluline on ka õiguskaitseasutuste varajane kaasamine, et kahtlustatavate küberkuritegude korral reageerida, ja proaktiivne teabevahetus CSIRTidega.

104 Võrgu- ja infoturbe direktiivi abil püüti parandada seda, et varem puudusid ELi ühtsed nõuded intsidentidest teatamise kohta, mis ohustas rikkumistest teatamist ja võis takistada neile reageerimist (vt punkt ***20***). Pärast 2017. aasta *Wannacry* ründeid järeldas komisjon, et CSIRTide võrgustik „ei olnud veel täielikult töökorras“[155]. Kuna direktiivi rakendamine jätkub, ei ole veel selge, kas koostöörühma välja töötatud suunised osutuvad tõhusaks, et ületada tõrksus intsidentidest teatamisel[156].

105 Teatavates sektorites tegutsevatel oluliste teenuste operaatoritel on kehtivate ELi õigusaktide kohaselt mitu teavitamiskohustust (sealhulgas tarbijate ees), mis võib protsessi tõhusust kahjustada. Näiteks finants- ja pangandussektori operaatorite suhtes kehtivad erinevad teatamiskriteeriumid, standardid, künnised ja tähtajad, mis tulenevad isikuandmete kaitse üldmäärusest, võrgu- ja infoturbe direktiivist, makseteenuste direktiivist, EKP/SSMi nõuetest, Target 2 süsteemist ja eIDASe määrusest[157]. Seetõttu on oluline neid kohustusi ühtlustada, sest lisaks mittevajalikule halduskoormusele võib selline paljusus kaasa tuua aruandluse killustatuse.

Koordineeritud reageerimine

106 Euroopa küberkriisialase koostööraamistiku loomine on veel pooleli. Seda käsitlevat tegevuskava[158] (vt punkt ***18***) kasutati selleks, et ELi integreeritud kord poliitiliseks reageerimiseks kriisidele sisaldaks rohkem n-ö küberperspektiivi, ning selleks, et parandada olukorrateadlikkust ja tagada parem integreeritus muude ELi kriisiohjemehhanismidega[159]. Tegevuskava hõlmab ELi institutsioone, asutusi ja liikmesriike. Kõigi nende kriisidele reageerimise mehhanismide sujuv integreerimine on keeruline[160]. Praegu on oluline puudus ka ELi institutsioonides kasutatava ühise turvalise sidevõrgu puudumine[161].

107 ELi suutlikkus reageerida ulatuslikele piiriülestele küberrünnetele operatiivsel ja poliitilisel tasandil korral on piiratud – osaliselt seetõttu, et küberturvalisus ei ole veel integreeritud olemasolevatesse ELi tasandi kriisidele reageerimise koordineerimismehhanismidesse[162]. Võrgu- ja infoturbe direktiivis seda teemat ei käsitletud.

108 Liikmesriigid ei toetanud ENISA hiljuti välja pakutud reformi, millega oleks ametile antud suurem roll suuremahuliste küberturvalisuse intsidentide käsitlemisel; liikmesriikide eelistuse kohaselt peaks ameti roll toetama ja täiendama nende endi operatiivmeetmeid[163]. Liikmesriikide tasandil on juba palju CERTe/CSIRTe, kuid nende suutlikkus on väga erinev. See takistab tõhusat piiriülest koostööd, mida on vaja laiaulatuslikele intsidentidele reageerimiseks[164].

109 Proovisime kaardistada tegevuskavas osalejatele määratud eri rollid, kuid selles oli lünki, mis tuleb täita rakendamise edenedes. Üks algselt alakäsitletud valdkond oli õiguskaitse, kuigi detsembris 2018 jõustus ELi hädaolukordadele reageerimise protokoll õiguskaitsealaseks reageerimiseks[165]. Edu eelduseks on tagada, et tegevuskava oleks praktiline ja et kõik pooled teaksid, mida teha; selleks vajatakse järgnevatel aastatel ulatuslikku testimist.

110 Tõhus reageerimine tähendab enamat kui kahju piiramist; määrava tähtsusega on ka rünnakute eest vastutajate tuvastamine. Kurjategijate jälitamine ja tuvastamine, eelkõige hübriidrünnaku korral, võib olla väga keeruline, sest üha enam kuritarvitatakse anonüümseks muutmise vahendeid, krüptoraha ja krüpteerimist. Seda nimetatakse süüdlase kindlakstegemise probleemiks. Probleemi lahendamine ei ole üksnes tehniline küsimus, vaid on keeruline ka õigusmõistmise seisukohast. Riikidevahelised õiguslikud ja menetluslikud erinevused võivad takistada kriminaalasja eeluurimist ja kahtlusalustele süüdistuste esitamist. Süüdlase kindlakstegemise probleemi lahendamiseks on vaja formaliseeritumat operatiivteabe vahetamist, mis põhineks selgematel menetlustel (näiteks Europoli või Eurojusti Euroopa küberkuritegevuse vastase õigusalase koostöö võrgustiku kaudu).

111 Poliitilisel tasandil on välja töötatud küberdiplomaatia meetmete kogum (vt ***6. selgitus***), et toetada rahvusvaheliste vaidluste lahendamist küberruumis rahumeelsete vahenditega. Küberturbe kiirreageerimisrühmade loomine ja küberturturvalisuse alase vastastikuse abistamise algatus on kaks projekti, mis edendavad tõhustatud teabejagamist, mida arendatakse PESCO raames[166].

6. selgitus

Küberdiplomaatia meetmete kogum

ELi ühine diplomaatiline reageerimine pahatahtlikule kübertegevusele[167] ehk „küberdiplomaatia meetmete kogum“ kasvas välja nõukogu 2015. aasta järeldustest küberdiplomaatia kohta[168]. Küberdiplomaatia eesmärk on töötada välja ja rakendada küberruumi jaoks ühine ja terviklik lähenemisviis, mis põhineb ELi väärtustel, õigusriigi põhimõttel, suutlikkuse arendamisel ja partnerlusel, paljusid sidusrühmi hõlmava interneti haldamise mudeli edendamisel ning küberturvalisuse ohtude leevendamisel ja rahvusvaheliste suhete stabiilsuse parandamisel.

Meetmete kogum võimaldab ELil ja selle liikmesriikidel ühiselt diplomaatiliselt reageerida pahatahtlikule kübertegevusele, kasutades täielikult ära ühise välis- ja julgeolekupoliitika meetmeid. Need võivad olla ennetavad (nt teadlikkuse suurendamine, suutlikkuse arendamine), koostööd ja stabiilsust arendavad või piiravad (nt reisikeelud, relvaembargod, rahaliste vahendite külmutamine) või toetada liikmesriikide meetmeid[169]. Mõte on selles, et edasine koostöö ohtude leevendamiseks ja selge signaal selle kohta, milliseid võimalikke tagajärgi võib tuua ELi ühine reaktsioon, võib ära hoida (potentsiaalselt) agressiivset käitumist.

ELi reageerimine pahatahtlikule kübertegevusele oleks proportsionaalne kübertegevuse ulatuse, mahu, kestuse, intensiivsuse, keerukuse ja mõjuga.

Meetmete kogumi edu sõltub nende heast seotusest tegevuskava ja IPCRiga (vt punkt ***106***), kiirel ja pideval teabejagamisel põhinevast olukorrateadlikkusest (sealhulgas süüdlase kindlakstegemise elementidest)[170] ning tõhusast koostööst. Meetmete kogumi eduka kasutuse edu võti on ka tõhus ja kooskõlastatud teabevahetus. Seni on meetmete kogumit kasutatud kaks korda: Ameerika Ühendriikidega dialoogi alustamisel peale *Wannacry* rünnnet[171] ning nõukogu järelduste väljatöötamisel, mis käsitlesid IKT pahatahtliku kasutamise taunimist[172]. Meetmete kogumi kasutuselevõtt käib ning tulevik näitab, kui tõhusaks see oma eesmärkide saavutamisel osutub.

10. ülesanne: elutähtis taristu ja ühiskonna toimimiseks vajalike funktsioonide kaitsmine

Taristu kaitsmine

112 Suurt osa ELi elutähtsast taristust käitatakse tööstuslike juhtimissüsteemide abil[173]. Paljud neist töötati välja eraldiseisvate süsteemidena, millel on välismaailmaga piiratud ühendus. Kuna tööstuslike juhtimissüsteemide komponendid on ühendatud internetiga, on need muutunud välissekkumise suhtes haavatavamaks. Olemasolevate süsteemide käitamist ja parandamist ei pruugi enam olla võimalik jätkata, kuid neid ei saa ka kiiresti või odavalt ajakohastada. Elutähtsa taristu turvalisuse suurendamiseks tehtavad jõupingutused peavad seetõttu hõlmama tööstuslike juhtimissüsteemide ajakohastamist.

113 Kuna tööstuse digiteerimine jätkub (üldtuntud kui „Tööstus 4.0“), võib ühes tööstussektoris toimunud laiaulatusliku intsidendi mõju mõjutada kaudselt ka teisi valdkondi. ENISA on märkinud, kui oluline on kaardistada elutähtsate sektorite vastastikuste sõltuvuste mõju[174]. See on oluline, et mõista intsidendi võimalikku levikut ja toetada hästi kooskõlastatud reageerimist.

114 Võrgu- ja infoturbe direktiivi eesmärk on suurendada elutähtsa taristu eest vastutavate võtmesektorite valmisolekut. See ei hõlma aga kõiki sektoreid (vt ***tabel 1***)[175], mis vähendab strateegia tulemuslikkust[176]: selles kontekstis tekitab erilist muret valimiste demokraatliku tervikluse kaitsmine valimiste taristu manipuleerimise ja väärinfo vastu (vt ***7. selgitus***). Lisaks kehtivate õigusaktide läbivaatamisele on seetõttu peamine ülesanne kindlaks teha, kuidas saaks pakkuda neile sektoreile suurte intsidentide korral tõhusaid lahendusi.

115 Elutähtsa taristu nõrgad kohad ei lõppe Euroopa piiridel. Komisjoni jaoks on eriti oluline julgustada kandidaatriike võtma kasutusele samad standardid nagu liikmesriigid, näiteks sellistes valdkondades nagu kübervaldkonnaga seotud õigusaktid või elutähtsa taristu kaitse.

7. selgitus

Ühiskonna toimimiseks vajalike funktsioonide kaitse: *võitlus valimistesse sekkumise vastu*

Mais 2019 valivad 400 miljonit valijat Euroopa Parlamenti; esimest korda toimub see isikuandmete kaitse üldmääruse alusel. Valimistele on eelnenud skandaalid, mis olid seotud isikuandmete kuritarvitamisega poliitiliste sõnumite täppissuunamiseks ja pretsedenditute koordineeritud väärinfokampaaniatega (*fake news*). Komisjon on hoiatanud tõenäoliste kübersekkumiste eest Euroopa Parlamendi valimistesse[177]; nende vastu võitlemine nõuab kogu valitsemissektorit ja ühiskonda hõlmavat lähenemisviisi.

Valimiste taristu

Valimiste korraldamine on keeruline ning nende kaitse ja terviklus on liikmesriikide ülesanne. Sekkumine valimistesse ja valimiste taristusse võib mõjutada valijate eelistusi, valimisaktiivsust või valimisprotsessi, sealhulgas tegelikku hääletamist, häältelugemist ja teabevahetust. Euroopa Parlamendi valimistel on eriti keeruline tagada nn viimase miili kaitse (tulemuste teatamine liikmesriikide pealinnadest Brüsselisse), kuna puudub ühine turvalisust puudutav lähenemisviis või seda ei ole veel valimiste kontekstis katsetatud[178].

Komisjoni hiljutine valimispakett sisaldas valimiste küberturvalisuse tugevdamise meetmeid, näiteks riiklike kontaktpunktide määramist, kelle ülesandeks on enne valimisi teavet koordineerida ja vahetada. Eriti oluline on jagada parimaid tavasid ja saadud õppetunde[179].

Valimissüsteeme ei peeta elutähtsa taristu osaks[180]; neid ei käsitleta ka võrgu- ja infoturbe direktiivis. Sellele vaatamata on koostöörühm riigiasutuste toetamiseks välja töötanud praktilised suunised, milles käsitletakse valimistehnoloogia turvalisust. Riiklikud kontaktpunktid peaksid eeldatavasti kokku tulema 2019. aasta alguses[181]. Liikmesriike julgustatakse ka tegema riskihindamisi nende valimisprotsessi ohustavate küberohtude kohta.

Väärinfo

Väärinfo on üha olulisem osa hübriidrünnetest, mis hõlmavad küberründeid ja võrkude häkkimist. Neid saab kasutada ühiskonna lõhestamiseks, usaldamatuse külvamiseks ja usalduse õõnestamiseks demokraatlike protsesside vastu või muudes küsimustes (näiteks vaktsineerimine või kliimamuutused). Väärinfo kasutamise maht, kiirus ja ulatus on kasvanud ning see kujutab endast ELi jaoks tõelist julgeolekuohtu.

EL on võtnud selle probleemiga tegelemiseks mitmeid meetmeid. Alates 2015. aastast loodi Euroopa välisteenistuse raames idanaabruse strateegilise kommunikatsiooni töörühm, mille ülesanne on Venemaa väärinfokampaaniate vastu võitlemine[182]. Eksperdid on kiitnud rühma tööd ELi poliitika edendamisel, sõltumatu meedia toetamisel naaberriikides ning väärinfo prognoosimisel, jälgimisel ja tõkestamisel[183]. Väärinfo levitamise kampaaniate ulatuse ja keerukusega võrreldes on töörühma ressursid aga piiratud[184]. Vaja on süsteemsemat koostööd olemasolevate ELi struktuuridega ja paremat strateegilist teabevahetust[185]. Euroopa Ülemkogu kiitis detsembris 2018 heaks uue tegevuskava[186].

Komisjon töötas oma aprilli 2018. aasta teatise (internetis leviva väärinfoga võitlemise kohta)[187] põhjal äsja välja vabatahtliku eneseregulatsiooni koodeksi[188], mis põhineb olemasolevatel poliitikavahenditel, ning millega on liitunud veebiplatvormid ja reklaamitootjad[189]. See hõlmab meetmeid, mis aitavad suurendada sisu usaldatavust ja toetada pingutusi meedia ja uudiste lugemise oskuse parandamiseks. Samuti on käivitatud sõltumatu Euroopa faktikontrollijate võrgustik.

Komisjoni sõnul võidakse vastu võtta täiendavaid reguleerivaid meetmeid, kui tegevusjuhist ei järgita. Väga oluline on meetmete tõhususe kindlaksmääramine, eelkõige selleks, et otsustada, kuidas mõõta usalduse, läbipaistvuse ja aruandekohustuse kvaliteedi paranemist.

Veel üks keeruline ülesanne on leida viise väärinfo avastamise, analüüsi ja avaliku paljastamise parandamiseks[190]. Samuti on vaja avatud andmeallikate aktiivset ja strateegilist seiret ja analüüsi[191]. Ohuolukorra paremaks mõistmiseks tehtavad jõupingutused peaksid hõlmama ka uusi suundumusi, nagu süvavõltsinguid (võltsvideod, mille tegemiseks on kasutatud tehisintellekti ja süvamasinõpet) ja nende avastamiseks vajalikke vahendeid.

Autonoomia suurendamine

116 EL on küberturvalisuse toodete ja teenuste netoimportija, mis suurendab ka riski sattuda ELi välistest ettevõtjatest tehnoloogilisse sõltuvusse ja nende tegevuse suhtes haavatav olla[192]. See kahjustab eelkõige ELi elutähtsa taristu turvalisust, mida toetub samuti keerukatele ülemaailmsetele tarneahelatele. Nimetatud oht suureneb veelgi siis, kui kolmandate riikide ettevõtjad omandavad Euroopa küberturvalisuse

ettevõtteid. Välismaiste otseinvesteeringute taustauuringute eest vastutavad liikmesriigid ning praegu puudub kogu ELi hõlmav taustauuringute mehhanism[193].

117 Suurem strateegiline autonoomia on eesmärgina välja toodud nii ELi üldises strateegias kui ka 2017. aasta teatises „Vastupidavusvõime, heidutus ja kaitse“[194]. Käesolevas aruandes loetletud arvukate ülesannetega tegelemine aitab seda soovitud autonoomiat suurendada. Ükski meede üksi ei suuda seda saavutada.

Mõttekohad – tõhus reageerimine

- Kuidas on võrgu- ja infoturbe direktiiv parandanud küberintsidentidest teavitamist nii kriitilise tähtsusega kui ka muudes sektorites?
- Kui hästi on ELi institutsioonid omandanud suure küberintsidendi korral kriisile reageerimise koordineerimise?
- Kuidas saab küberdiplomaatia etendada olulisemat rolli ELi välistegevuses?
- Kas ELi praegused struktuurid ja meetmed väärinfo vastu võitlemiseks on proportsionaalsed probleemi ulatuse ja keerukusega?

Lõppmärkused

118 Kübervastupidavusvõime parandamise eesmärgil on küberturvalisuse tähtsus ELis ja selle liikmesriikides viimastel aastatel suurenenud. ELi küberturvalisuse suurendamine on aga endiselt väga keeruline ülesanne. Püüdsime käesolevas infodokumendis välja tuua mõned peamised ülesanded, mis on seotud ELi sooviga muutuda maailma kõige turvalisemaks digitaalkeskkonnaks.

119 Meie ülevaade näitab, et mõtestatud **aruandekohustuse ja hindamise** tagamiseks on vaja võtta kasutusele tulemuskultuur koos selles sisalduva hindamiskorraga. **Õigusaktides on endiselt mõningaid lünki ning liikmesriigid ei ole olemasolevaid õigusakte järjekindlalt üle võtnud**. See võib raskendada õigusaktide täieliku potentsiaali ärakasutamist. Raske on tagada, et **investeeringute maht vastaks strateegilistele eesmärkidele**, mis eeldab investeeringute ja nende mõju suurendamist. See on veelgi keerulisem, kui ELil ja liikmesriikidel puudub **selge ülevaade ELi küberturvalisusse tehtavatest kulutustest**. Samuti on teada, et **ELi kübervaldkonna asutustel on raskusi piisavate ressursside tagamisel**, sealhulgas andekate töötajate ligimeelitamisel ja hoidmisel.

120 Kättesaadavad uuringud näitavad, et **küberturvalisuse juhtimist saab tugevdada**, et suurendada rahvusvahelise kogukonna võimet reageerida küberrünnetele ja intsidentidele. Samas on võimatu kõiki rünnakuid vältida. Seepärast on peamised lahendamist vajavad ülesanded **intsidentide kiire avastamine ja neile reageerimine** ning **elutähtsa taristu ja ühiskonna toimimiseks vajalike funktsioonide kaitse** koos avaliku ja erasektori vahelise parema **teabevahetuse ja koordineerimisega**. Lisaks tähendab küberturvalisuse alaste oskuste vähesus seda, et esmatähtis on **arendada oskusi ja suurendada teadlikkust** kõigis sektorites ja ühiskonna kõigil tasanditel.

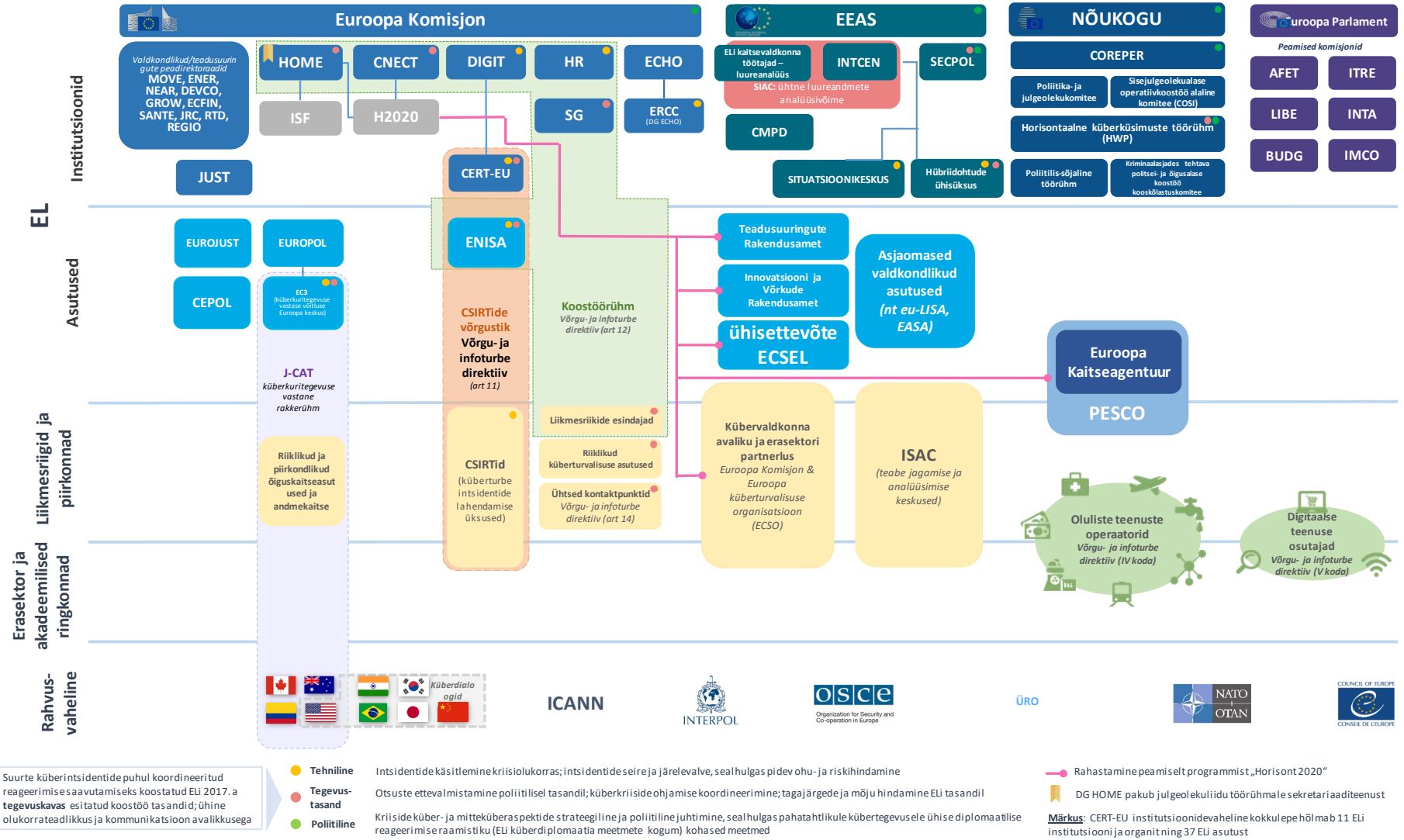
121 ELi ja kogu maailma ohustavatest küberohtudest tulenevad ülesanded eeldavad jätkuvat tähelepanu ja ELi põhiväärtuste kindlat järgimist.

III auditikoda võttis käesoleva infodokumendi vastu 14. veebruari 2019. aasta koosolekul.

Kontrollikoja nimel

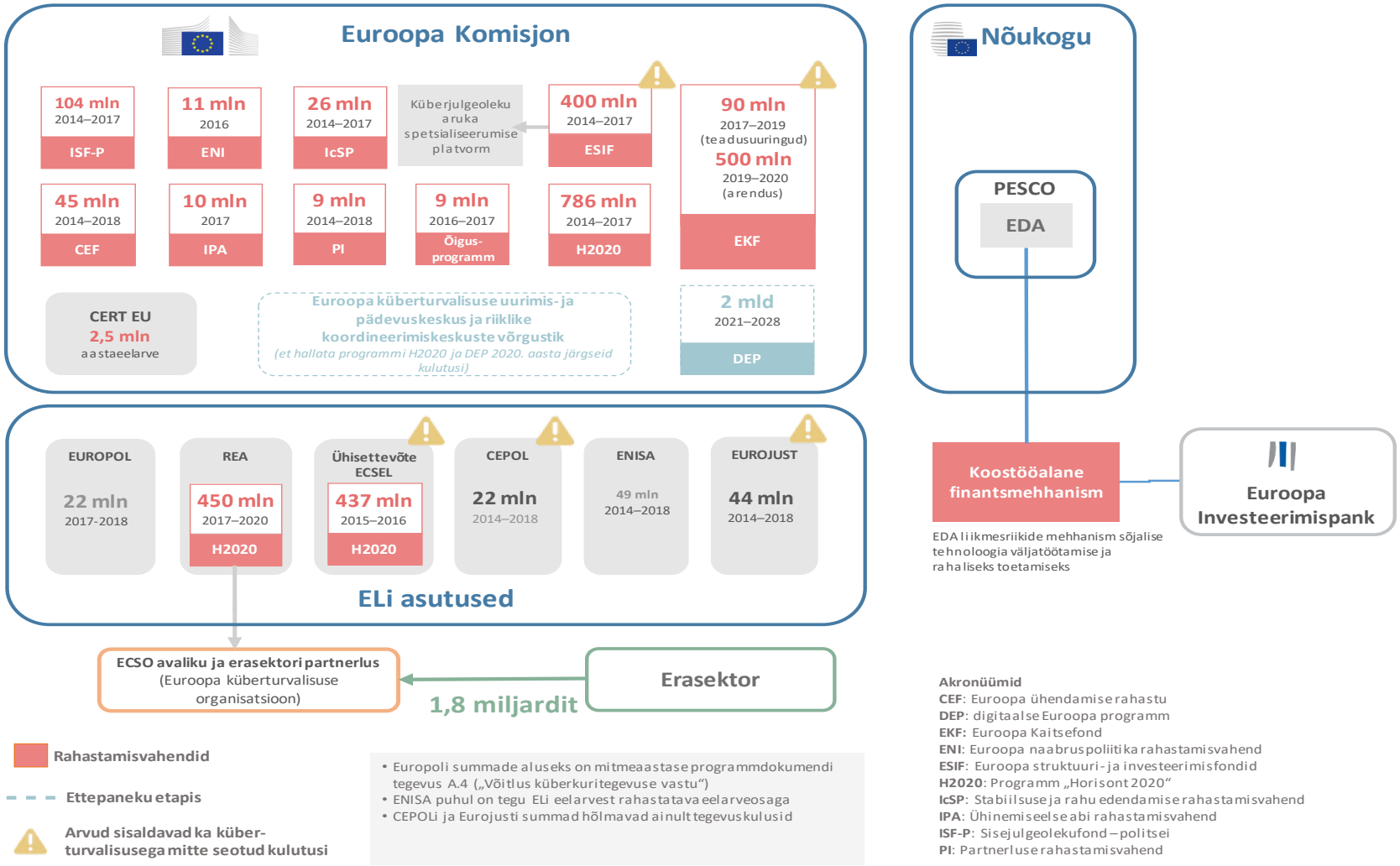
president
Klaus-Heiner Lehne

I lisa. Paljude osalejatega keeruline ja mitmekihiline keskkond



Allikas: Euroopa Kontrollikoda.

II lisa. ELi kulutused küberturvalisusele alates 2014. aastast



Allikas: Euroopa Komisjoni ja ELi asutuste dokumentidel põhinevad Euroopa Kontrollikoja andmed.

III lisa. ELi liikmesriikide kõrgeimate kontrolliasutuste aruanded

Liik	Pealkiri (hüperlingiga)	Aasta	LR
Vastavusauditid	Sisekontrolli hindamisteatis	2014	FR
	Sertifitseerimisaruanne üldise sotsiaalkindlustuskava raamatupidamise aastaaruande kohta (kaitse, välissuhted)	2016	FR
	Riigi raamatupidamise aastaaruande kinnitamine	2016	FR
	Eesti kriitilise tähtsusega riiklike andmebaaside turvalisus	Lõpetatud 2018 / veel avaldamata	EE
	Sisekontrollisüsteemide toimimine isikuandmete kaitsel riiklikes andmekogudes	2008	EE
Tulemus-/kulutõhususe auditid (*value-for money*)	Aruanne küberrünnete leevendamise kohta	2013	DK
	RIR 2014:23. Infoturve avaliku halduse asutustes	2014	SE
	Aruanne selle kohta, kuidas valitsus töötleb isikute ja äriühingute konfidentsiaalseid andmeid	2014	DK
	Riiklik küberturvalisuse programm	2014	UK
	Saksamaa Liitvabariigi parlamendi eelarvekomiteele esitatud aruanne vastavalt riigi eelarveseaduse paragrahvi 88 lõikele 2 – föderaalvalitsuse IT konsolideerimine	2015	DE
	Aruanne juurdepääsu kohta IT-süsteemidele, mis toetavad Taani ühiskonnale oluliste teenuste osutamist	2015	DK
	Plaine de France'i avaliku sektori planeerimisamet	2015	FR
	„Leedu küberturvalisuse keskkond" leedukeelne tekst ingliskeelne kokkuvõte	2015	LT
	Avaliku sektori asutuste küberturvalisuse ülesannete täitmine Poolas (poola keeles)	2015	PL
	RIR 2015:21. Küberkuritegevus – politsei ja prokurörid võivad olla tõhusamad.	2015	SE
	Digitaaloskuste puudus valitsuses (uuring)	2015	UK
	Ettekanne föderaalvalitsusele: föderaalvalitsuse rahandus: pärandimaksu kogumine	2016	BE
	Aruanne IT-turbe juhtimise kohta välistelt tarnijatelt sisse ostetud süsteemides	2016	DK
	Auditiaruanne ametliku krediidiasutuse 2016. aasta laenutegevuse kohta	2016	ES
	Valitsuse turvavõrgu juhtimine	2016	FI
	Avalike ülesannete täitmiseks kasutatavate IT-süsteemide turvalisuse tagamine	2016	PL
	Laste ja noorte küberkiusamise ennetamine ja selle vastu võitlemine	2016	PL
	Infoturvalisuse alase töö kohta üheksas asutuses - Teine infoturbe audit riigis. RiR 2016:8	2016	SE
	Valitsuse teabe kaitsmine	2016	UK
	Aruanne IT-süsteemide ja terviseandmete kaitse kohta kolmes Taani piirkonnas	2017	DK

Liik	Pealkiri (hüperlingiga)	Aasta	LR
	Märgukiri rahvusvahelise paralleelauditi „Isikuandmete kaitse riiklikes andmekogudes“ tulemuste kohta.	2017	EE
	Küberkaitsekorraldus	2017	FI
	Elektrooniliste teenuste töökindluse haldamine	2017	FI
	Põllumajanduskodade võrk (kokkuvõte)	2017	FR
	Vaucluse’i kaubandus- ja tööstuskoda (koostaja: piirkondlik auditiasutus)	2017	FR
	Eesti kriitilise tähtsusega riiklike andmebaaside turvalisus	Lõpetatud 2018 / veel avaldamata	EE
	„Riikliku elektroonilise side taristu arendamine“ leedukeelne tekst ingliskeelne kokkuvõte	2017	LT
	Infotehnoloogia audit:valitsusüksuste küberturvalisus	2017	MT
	Riiklike registrite süsteem: turvalisus, toimivus ja kasutatavus	2017	PL
	WannaCry intsident	2017	UK
	Veebipõhine pettus	2017	UK
	Aruanne lunavararünnakute vastase kaitse kohta	2018	DK
	Arpajoni haigla (koostaja: Île-de-France’i piirkondlik auditiasutus)	2018	FR
	„Riigi kriitilise tähtsusega teabeallikate haldamine“	2018	LT
	„Elektroonilised kuriteod“	2019	LT
	Infoturve Poolas	2019	PL
Muud väljaanded	Ametiasutuste andmebaas	-	BE
	Küsimustik turvalisuse- ja riskianalüüsi poliitika kohta (töös)		BE

Akronüümid ja lühendid

CERT: - EU: infoturbeintsidentidega tegelev meeskond

CSIRT: küberturbe intsidentide lahendamise üksus

DDoS: hajus teenusetõkestusrünne

DEP: digitaalse Euroopa programm

DG CONNECT: sdevõrkude, sisu ja tehnoloogia peadirektoraat

DG HOME: rände ja siseasjade peadirektoraat

DG JUST: õigus- ja tarbijaküsimuste peadirektoraat

DIGIT: informaatika peadirektoraat

EC3: Europoli küberkuritegevuse vastase võitluse Euroopa keskus

ECSEL: Euroopa juhtpositsiooni tugevdamine elektroonikakomponentide ja -süsteemide toel

ECSO: Euroopa küberturvalisuse organisatsioon

EDA: Euroopa Kaitseagentuur

EEAS: Euroopa välisteenistus

EL: Euroopa Liit

ENISA: Euroopa Võrgu- ja Infoturbeamet

ESA: Euroopa järelevalveasutus

ESIF: Euroopa struktuuri- ja investeerimisfondid

HWPCI: horisontaalne küberküsimuste töörühm

NCIRC: NATO küberturbeintsidentidele reageerimise üksus

PESCO: alaline struktureeritud koostööraamistik

VKEd: väikesed ja keskmise suurusega ettevõtjad

ÜJKP: ühine julgeoleku- ja kaitsepoliitika

Mõisted

Andmepüük: e-kirjade saatmine, milles püütakse jätta pettuse abil mulje, et need on pärit usaldusväärsest allikast, et veenda saajaid klõpsama pahatahtlikel linkidel või jagama isikuandmeid.

Asjade internet: elektroonika, tarkvara ja sensoritega varustatud igapäevaste esemete võrk, mis võimaldab neil internetis suhelda ja andmeid vahetada.

Digitaalne sisu: kõik digitaalses formaadis salvestatud andmed (nt tekst, heli, pildid ja video).

Elutähtis taristu: füüsilised ressursid, teenused ja rajatised, mille häirimine või hävimine mõjutaks oluliselt majanduse ja ühiskonna toimimist.

Haavatavustegurite haldamine: arvuti- ja võrguturvalisuse lahutamatu osa, et proaktiivselt vähendada või ennetada süsteemi ja tarkvara turvaaukude kasutamist nende identifitseerimise, liigitamise ja parandamise kaudu.

Hajus teenusetõkestusrünne: küberrünne, mis takistab volitatud kasutajate juurdepääsu internetipõhistele teenustele või -ressurssidele, saates süsteemile rohkem päringuid kui see suudab käidelda.

Häkkimiskomplekt: töövahendite komplekt, mida küberkurjategijad kasutavad võrgu- ja infosüsteemide turvaaukude ründamiseks, et levitada pahavara või teha midagi muud pahatahtlikku.

Häktivistid: infosüsteemidesse või -võrkudesse loata sisenevad inimesed või rühmitused, kelle eesmärk on juhtida tähelepanu teatavatele sotsiaalsetele või poliitilistele küsimustele.

Hübriidoht: vaenulik tahteavaldus, mille raames kombineeritakse oma eesmärkide saavutamiseks konventsionaalseid ja mittekonventsionaalseid tehnikaid (st sõjalised, poliitilised, majanduslikud ja tehnoloogilised meetodid).

Infoturve: protsesside ja vahendite kogum, mis kaitseb füüsilisi ja digitaalseid andmeid loata juurdepääsu, kasutamise, avalikustamise, häirimise, muutmise, salvestamise või hävitamise eest.

Isikuandmed: konkreetse isikuga seotud teave.

IT-vahenditest sõltuv kuritegu: kuritegu, mida saab toime panna üksnes IT-vahendite abil.

Juurdepääsuandmed: kasutaja sisse- ja väljalogimisandmed (näiteks kellaaeg, kuupäev ja IP-aadress).

Konfidentsiaalsus: teabe ja andmete kaitse loata juurdepääsu või avaldamise eest.

Krüpteerimine: loetava teabe loetamatuks muutmine selle kaitsmise eesmärgil. Teabe lugemiseks peab kasutajal olema salajane võti või parool.

Krüptoraha: digitaalne vara, mida emiteeritakse ja vahetatakse krüpteerimistehnikate abil; see on keskpangast sõltumatu. Virtuaalkogukond tunnustab krüptoraha maksevahendina.

Kuritöö kui tellitava teenus mudel: kuritegelik ärimudel, mis toimib digitaalses varimajanduses; selle raames pakutakse laia valikut kommertsteenuseid ja vahendeid, mis võimaldavad oskusteta küberkurjategijatel küberkuritegevusega tegelda.

Kustutav pahavara: pahavara liik, mille eesmärk on tühjendada nakatatud arvuti kõvaketas.

Käideldavus: tagab teabe õigeaegse ja usaldusväärse kättesaadavuse ja selle kasutamise.

Küberintsident: sündmus, mis otseselt või kaudselt kahjustab või ohustab IT-süsteemi vastupidavust ja turvalisust ning andmeid, mida see töötleb, salvestab või edastab.

Küberkaitse: küberturvalisuse alajaotus, mille eesmärk on sõjaliste ja muude asjakohaste vahendite abil kaitsta küberruumi, et saavutada sõjalis-strateegilised eesmärgid.

Küberkuritegu: kriminaalne tegevus, mis hõlmab nii arvuteid kui ka IT-süsteeme (kas esmase töövahendi või esmase sihtmärgina). Küberkuritegevus hõlmab traditsioonilisi kuritegusid (nt pettus, võltsimine ja identiteedivargus); infosisuga seotud kuritegusid (nt lapsporno levitamine internetis või rassiviha õhutamine); ning ainult arvutite ja infosüsteemidega seotud kuritegusid (nt infosüsteemide vastu suunatud ründed, teenusetõkestused ja pahavara).

Küberruum: mittemateriaalne üleilmne keskkond, kus inimeste, tarkvara ja teenuste vaheline suhtlus toimub arvutivõrgu ja tehnoloogiliste seadmete kaudu.

Küberruumi kasutades toime pandud kuritegu: tavaline kuritegu, mis on toime pandud suuremas mahus ja IT-süsteemide abil.

Küberrünne: katse kahjustada küberruumi kaudu andme- või arvutisüsteemi konfidentsiaalsust, terviklust ja kättesaadavust, või seda hävitada.

Küberturvalisus: kõik kaitsemeetmed ja meetmed, mis võetakse selleks, et kaitsta IT-süsteeme ja nende andmeid volitamata juurdepääsu, rünnete ja kahju eest, et tagada nende käideldavus, konfidentsiaalsus ja terviklus.

Küberturvalisuse ökosüsteem: omavahel seotud seadmete, andmete, võrkude, inimeste, protsesside ja organisatsioonide keerukas kooslus ning nende koostoimet mõjutav ja toetav protsesside keskkond.

Kübervastupidavusvõime: võime ennetada küberründeid ja intsidente, nendeks valmistuda, nendega toime tulla ja neist taastuda.

Lunavara: pahavara, mis blokeerib ohvritele juurdepääsu arvutisüsteemile või muudab failid loetamatuks (reeglina krüpteerimise teel). Tavaliselt pressib ründaja ohvrilt raha välja, lubades juurdepääsu taastada alles pärast lunaraha maksmist.

Pahavara: arvutiprogramm, mis on loodud arvuti, serveri või võrgu kahjustamiseks.

Paikamine: meetmed tarkvara muutmiseks, ajakohastamiseks, parandamiseks või täiustamiseks, sealhulgas turvaaukude sulgemine.

Pilvandmetöötlus: hostitavatelt serveritelt interneti teel pakutavad IT-ressursid (salvestus, andmetöötlusvõimsus või andmejagamine).

Pärandsüsteem: vananenud arvutisüsteem, rakendus või programmeerimiskeel, mis on endiselt kasutusel, kuid mille jaoks võivad puududa nii uuendused kui ka müüja tugi (sealhulgas turvatugi).

Reklaamvara: reklaami või hüpikaknaid kuvav pahavara, mis sisaldab ohvrite veebikäitumise jälgimiseks mõeldud tarkvarakoodi.

Robotivõrk: pahavaraga nakatatud arvutitest koosnev ja kaugelt juhitav võrk, mida omaniku teadmata kasutatakse rämpsposti levitamiseks, teabe varastamiseks või küberrünnete korraldamiseks.

Skimming: krediit- või deebetkaardiandmete vargus veebis.

Sotsiaalne manipulatsioon: infoturbe tähenduses on tegu psühholoogilise manipuleerimisega, et veenda inimesi pettuse abil midagi tegema või konfidentsiaalset teavet avaldama.

Teksti vektoriseerimine: sõnade, lausete või tervikdokumentide numbrilisteks vektoriteks muutmine, et neid saaks masinõppealgoritmidega töödelda.

Terviklus: kaitse teabe ebaõige muutmise või hävitamise eest ning teabe autentsuse tagamine.

Usaldusteenused: teenused, mis parandavad e-tehingute (nt e-allkirjade, e-templite, e-ajatemplite, registreeritud e-andmevahetusteenuste ja veebisaitide autentimise) õiguslikku kehtivust.

Valimiste taristu: sisaldab kampaania IT-süsteeme ja andmebaase, tundlikku teavet kandidaatide kohta, valijate registreerimise ja haldamise süsteeme.

Võrguturve: küberturvalisuse alaliik, mille eesmärk on kaitsta samas võrgus olevate seadmete kaudu saadetud andmeid; võrguturbe eesmärk on tagada, et teavet ei saaks salaja jälgida ega muuta.

Väärinfo: vale või eksitav teave, mida luuakse, esitatakse ja levitatakse majandusliku kasu teenimise või üldsuse tahtliku petmise eesmärgil, ja mis võib põhjustada avalikku kahju.

[1] ELi küberturvalisust käsitleva õigusakti eelnõus on see määratletud kui „kõik tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid küberohtude eest“; eeldatavasti võtavad Euroopa Parlament ja nõukogu õigusakti vastu 2019. aasta alguses.

[2] Europol, *Internet Organised Crime Threat Assessment 2017* (Europoli 2017. aasta ELi organiseeritud kuritegevuse ohtude hindamine).

[3] Euroopa küberturvalisuse organisatsioon (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* (Euroopa küberturvalisuse tööstuse ettepanek avaliku ja erasektori lepingulise partnerluse kohta), juuni 2016.

[4] Euroopa Parlament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* (Küberturvalisus Euroopa Liidus ja sellest väljaspool: ohtude ja poliitikameetmete uurimine), kodanikuvabaduste, justiits- ja siseasjade komisjonile koostatud uuring, september 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017* (ENISA ohtude kaardistamise aruanne 2017), 18. jaanuar 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018* (Europoli 2017. aasta ELi organiseeritud kuritegevuse ohtude hindamine).

[7] Europol, *ibid.*, 2018.

[8] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (Kas küberspionaaž võib kahjustada Euroopat ülemaailmses konkurentsis tööstuse konkurentsivõime nimel?), üldtoimetis, nr 2/18, veebruar 2018.

[9] Euroopa Komisjoni presidendi kõne – Euroopa Liidu olukord 2017.

[10] Europol, *World’s Biggest Marketplace selling internet paralysing DDoS attacks taken down* (Võrgust eemaldati maailma suurim portaal, kus müüdi internetti paralüseerivaid DDoS ründeid), pressiteade, 25. aprill 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017* (Europoli 2017. aasta ELi organiseeritud kuritegevuse ohtude hindamine).

[12] Euroopa Komisjoni küberturvalisuse teabeleht, september 2017.

[13] Kulud võivad hõlmata järgmist: saamatajäänud tulu, kahjustatud süsteemide parandamise kulud, varastatud varast või teabest tulenevad võimalikud kohustused, klientide säilitamiseks vajalikud kulud, suuremad kindlustuspreemiad, suuremad kaitsekulud (uued süsteemid, töötajad, koolitus), võimalikud nõuete täitmise ja kohtuvaidluste kulud.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] *Wannacry* lunavara kasutas Microsofti Windowsi protokolli haavatavust, mis võimaldas kontrolli mis tahes arvuti üle kaugpöördusega üle võttta. Microsoft avaldas peale turvaaugu avastamist hädaparanduse. Sadadele tuhandetele arvutitele ei olnud aga tarkvaraparandust

veel installeeritud ja paljud neist ka hiljem nakatati. *Allikas*: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19. detsember 2017.

[16] Euroopa Komisjon, „Eurooplaste suhtumine küberturvalisusesse“, Eurobaromeetri eriuuring nr 464a, september 2017. Järeluuring avaldatakse kavakohaselt 2019. aasta alguses.

[17] Budapesti konventsioon on riikide jaoks mõeldud siduv rahvusvaheline juhis küberkuritegevuse vastaste õigusaktide koostamiseks. See on riikidevahelise rahvusvahelise koostöö raamistik. ELi esindavad praegu komisjon, Euroopa Liidu Nõukogu, Europol, ENISA ja Eurojust.

[18] Euroopa Komisjon, *Euroopa Liidu küberjulgeoleku strateegia:avatud, ohutu ja turvaline küberruum* (JOIN (2013) 1 final), 7. veebruar 2013.

[19] Euroopa Komisjon, *Euroopa julgeoleku tegevuskava*, COM (2015) 185 final, 28. aprill 2015.

[20] Euroopa Komisjon, *Euroopa digitaalse ühtse turu strateegia*, COM (2015) 192 final, 6. mai 2015.

[21] Euroopa välisteenistus, *Ühtne visioon, ühine tegevus:tugevam Euroopa.Euroopa Liidu üldine välis- ja julgeolekupoliitika strateegia*, juuni 2016.

[22] Euroopa Poliitikauuringute Keskus, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, november 2018.

[23] Wannacry lunavara, millega sooritatud ründe algatajaks peeti Ameerika Ühendriikide, Ühendkuningriigi ja Austraalia hinnangul Põhja-Koread, töötas algselt välja ja säilitas USA Riikliku Julgeolekuagentuur, et kasutada ära Windowsi operatsioonisüsteemi nõrkusi. *Allikas*: A. Greenberg, ibid., WIRED, 19. detsember 2017. Pärast rünnakuid mõistis Microsoft hukka selle, et valitsused koguvad tarkvara haavatavust puudutavat teavet ning kordas oma nõudmist, et vaja on Genfi digitaalkonventsiooni.

[24] Lisaks maa-, mere-, õhu- ja kosmoseväele.

[25] ELi küberkaitsepoliitika raamistik (ajakohastamine 2018. aastal), 14413/18, 19. november 2018.

[26] Euroopa Komisjon/Euroopa välisteenistus, *Hübriidohtudega võitlemise ühine raamistik: Euroopa Liidu lahendus“*, JOIN (2016) 18 final, 6. aprill 2016.

[27] Euroopa Ülemkogu eesistuja, Euroopa Komisjoni presidendi ja Põhja-Atlandi Lepingu Organisatsiooni peasekretäri ühisavaldus,8. juuli 2016 ja 10. juuli 2018.

[28] Euroopa Komisjon / Euroopa välisteenistus, *„Vastupidavusvõime, heidutus ja kaitse:tugeva küberturvalisuse tagamine ELis“*, JOIN (2017) 450 final, 13, september 2017.

[29] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

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

[31] Need on integreeritud direktiiviga loodud koostööstruktuuridesse, milleks on CSIRTide võrgustik (võrgustik, mis koosneb ELi liikmesriikide määratud CSIRTidest ja CERT-EUst; sekretaariaadi teenust pakub ENISA) ja koostöörühm (toetab ja hõlbustab strateegilist koostööd ja teabevahetust nende liikmesriikide vahel, kelle jaoks komisjon sekretariaadi teenust pakub)

[32] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

[33] Euroopa Komisjon, *ettepanek: Euroopa parlamendi ja nõukogu määrus, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist* („küberturvalisust käsitlev õigusakt“), COM (2017) 477 final, 13. september 2017.

[34] Euroopa Komisjon, *ettepanek: Euroopa parlamendi ja nõukogu määrus, mis käsitleb Euroopa andmeesitamismäärust ja Euroopa andmesäilitamismäärust elektrooniliste tõendite hankimiseks kriminaalasjades*, COM (2018) 225 final, 17. aprill 2018.

[35] Euroopa Komisjon, *ettepanek: Euroopa parlamendi ja nõukogu direktiiv, millega kehtestatakse ühtlustatud normid kriminaalmenetluses tõendite kogumise eesmärgil esindajate määramise kohta*. COM (2018) 226 final, 17. aprill 2018.

[36] Euroopa Komisjon, *ettepanek: Euroopa parlamendi ja nõukogu määrus, millega luuakse Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus ning riiklike koordineerimiskeskuste võrgustik*, COM (2018) 630 final, 12. september 2018.

[37] H. Carrapico ja A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, *Journal of Common Market Studies*, kd 55, nr 6, 2017.

[38] Euroopa Komisjon, *ibid*., SWD (2017) 295 final, 13. september 2017.

[39] Euroopa Parlamendi uuringuteenistus, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects* (Atlandiülene küberturvalisus ja küberkuritegevus. Majanduslik mõju ja tulevikuväljavaated), PE 603.948, detsember 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies* (küberturvalisuse strateegiate hindamisraamistik), 27. november 2014.

[41] Erandiks on Euroopa Parlamendi ja Nõukogu 12. augusti 2013. aasta direktiivi 2013/40/EL (milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK) artikkel 14 („Järelevalve ja statistika“).

[42] Euroopa Majandus- ja Sotsiaalkomitee, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, märts 2018. CEPS-ECRI rakkerühm, *Cybersecurity in Finance: Getting the policy mix right!*, juuni 2018.

[43] Küsimustikule vastas 24 liikmesriigi kõrgeimat kontrolliasutust 28-st.

[44] See tähendab, et põhimõtetel põhinemist ja võimalikult suurt tehnoloogianeutraalsust.

[45] Euroopa Komisjoni teadusnõustamise mehhanismTeaduslik arvamus nr 2/2017, 24. märts 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach* (Võimalik läghenemisviis ELi digitaalsele autonoomiale), *Digma Zeitschrift für Datenrecht und Informationssicherheit*, september 2018. European Centre for Political Economy, *ibid*., üldtoimetis, nr 2/18, veebruar 2018.

[47] Euroopa Komisjon, *ettepanek: Euroopa Parlamendi ja nõukogu direktiiv digitaalse sisu üleandmise lepingutega seonduvate teatavate aspektide kohta (COM(2015) 634 final*, 9. detsember 2015.

[48] Euroopa Komisjon, *ettepanek: Euroopa Parlamendi ja nõukogu direktiiv kaupade internetimüügi ja muu kaugmüügi lepingutega seonduvate teatavate aspektide kohta (COM(2017) 635 final*, 9. detsember 2015.

[49] Madalmaadde küberturvalisuse nõukogu, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Euroopa Poliitikauuringute Keskus, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* (Tarkvara haavatavuse rääkimine Euroopas: tehnoloogiad, põhimõtted ja õiguslikud küsimused – CEPSi rakkerühma aruanne), juuni 2018.

[51] Euroopa Komisjon, *Parimate tulemuste saavutamine võrgu- ja infoturbe direktiivi rakendamisel – jõupingutused direktiivi (EL) 2016/1148 (meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) tulemuslikuks rakendamiseks*, COM(2017) 476 final/2, 4. oktoober 2017.

[52] Europol, *ibid*., 2017.

[53] Euroopa Liidu Nõukogu, *Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime"* (vastastikuse hindamise seitsmenda vooru lõpparuanne teemal „Euroopa poliitika praktiline rakendamine ja toimimine küberkuritegevuse ennetamise ja tõkestamise valdkonnas"), 12711/1/17 REV 1, 9. oktoober 2017.

[54] Euroopa Komisjon, mõjuhindamine, mis on lisatud dokumendile „Ettepanek: direktiiv, mis käsitleb mittesularahaliste maksevahenditega seotud pettusi ja võltsimist", SWD/2017/0298 final, 13. september 2017. Poliitiline kokkulepe uue õigusakti kohta saavutati detsembris 2018 ja see võetakse eeldatavasti vastu 2019. aasta alguses.

[55] Europol, *ibid*., 2017.

[56] C-362/14: C-362/14: Maximillian Schrems *vs*. andmekaitsevolinik (Iirimaa), 6. oktoober 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime* (Ühised probleemid võitluses küberkuritegevusega), 7021/17, 13. märts 2017.

[58] Euoopa Komisjon, *Assessment of the EU 2013 Cybersecurity Strategy* (ELi 2013. aasta küberjulgeoleku strateegia hindamine), SWD (2017) 295 final, 13. september 2017.

[59] Euroopa Parlamendi uuringuteenistus, *Briefing: EU Legislation in Progress – Review of dual-use export controls* (Uued ELi õigusaktid – kahesuguse kasutusega kaupade ekspordikontrolli läbivaatamine), PE589.832.

[60] Euroopa Parlamendi resolutsioon *inimõiguste ja tehnoloogia ning sekkumis- ja jälgimissüsteemide mõju kohta inimõigustele kolmandates riikides*, (2014/2232(INI)), 8. september 2015. Kahesuguse kasutusega kaupu ja teenuseid, mis hõlmavad tarkvara ja tehnoloogiat, võib kasutada nii tsiviil- kui ka sõjalisel otstarbel.

[61] Avalikult kättesaadavat teavet säilitatakse ICANNi (interneti nimede ja numbrite määramise korporatsioon) hallatavas andmebaasis WHOIS. ICANN haldab domeeninimede süsteemi. Domeeninimede väärkasutamine lihtsustab küberkuritegevust.

[62] Võrgu- ja infoturbe direktiivi artikkel 3, *ibid*.

[63] Atlandi Nõukogu, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*(Küberohud. Kübertuleviku stsenaariumide majanduslik kasu ja hind), 10. september 2015.

[64] Valge Maja, *Cybersecurity spending fiscal year 2019* (Kulutused küberturvalisusele eelarveaastal 2019).

[65] Euroopa Komisjoni *talituste töödokument: mõjuhinnang, mis on lisatud dokumendile „Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse ajavahemikuks 2021–2027 digitaalse Euroopa programm“*, SWD(2018) 305 final, 6. juuni 2018.

[66] Haagi strateegiauuringute keskus, *Dutch investments in ICT and cybersecurity: putting it in perspective* (Madalmaade investeeringud IKTsse ja küberturvalisusesse), detsember 2016.

[67] Euroopa Komisjon, *ibid*., COM (2018) 630 final, 12. september 2018.

[68] Euroopa Parlamendi uuringuteenistuse teaduslike tuleviku-uuringute üksus, *Achieving a sovereign and trustworthy ICT industry in the EU* (Euroopa suveräänse ja usaldusväärse IKT-sektori saavutamine), detsember 2017.

[69] Digivaldkonna VKEde Euroopa ühendus, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* (Seisukoht Euroopa küberturvalisuse strateegia kohta: VKEde ökosüsteemi tugevdamine), 31. juuli 2017.

[70] Euroopa Parlamendi uuringuteenistuse teaduslike tuleviku-uuringute üksus, *ibid*., detsember 2017.

[71] *Ibid*.

[72] Euroopa Komisjon, *Impact assessment on the proposed research competence centre and network of national coordination centres* (Mõjuhinnang kavandatud teadusliku pädevuse keskuse ning riiklike koordineerimiskeskuste võrgustiku kohta, SWD(2018) 403 final (osa1/4), 12. september 2018.

[73] Euroopa Komisjon, *ibid*., COM (2018) 630 final, 12. september 2018.

[74] Kontrollikoja eriaruanne nr 13/2018: „Terrorismi põhjustava radikaliseerumise vastane võitlus“.

[75] Dokumendi käesolevas osas esitatud arvandmed pärinevad avalikult kättesaadavatest komisjoni dokumentidest, välja arvatud punktis ***51*** toodud 42 miljonit eurot, mille komisjon esitas meile otse.

[76] Programm „Horisont 2020“ on ELi 80 miljardi euro suurune teadusuuringute ja innovatsiooni programm, millega toetatakse juhtalgatust „Innovatiivne liit“, mille eesmärk on tagada ELi ülemaailmne konkurentsivõime.

[77] Programmi „Horisont 2020“ ühiskondlik väljakutse nr7: „Turvaline ja innovatiivne ühiskond: Euroopa ja selle kodanike vabaduse ja turvalisuse kaitsmine“.

[78] Analüüsisime CORDISe andmekogumi sisaluvaid programmi „Horisont 2020“ projekte. Vektoriseerisime iga projekti kirjelduse, kasutades Teadusuuringute Ühiskeskuse küberturvalisuse taksonoomiat (vt järgmise peatüki ***5. selgitus***), et teha kindlaks projektid, mis on tõenäoliselt seotud küberturvalisusega. Seejärel kontrollisime ja analüüsime tulemusi käsitsi.

[79] Euroopa küberturvalisuse organisatsioon, *ECS cPPP Progress Monitoring Report 2016-2017* (Avaliku ja erasektori lepingulise partnerluse eduaruanne 2016–2017), 29. oktoober 2018.

[80] Võrgu- ja infoturbe direktiivi artikli 9 lõige 2, *ibid*.

[81] GLACY+ (*Global Action against Cybercrime*+) on ühisprojekt Euroopa Nõukoguga. Projekt toetab 12 Aafrika, Aasia ja Vaikse ookeani ning Ladina-Ameerika ja Kariibi mere piirkonna riiki, kes võivad omakorda olla sõlmpunktid, et jagada oma kogemusi vastavates piirkondades.

[82] Euroopa Poliitilise Strateegia Keskus (EPSC), mis on komisjoni mõttekoda, on kommenteerinud nn digitaalse pimeala riski, mis tekib siis, kui lõhe ELi ja tema Lääne-Balkani naaberriikide vahel jätkuvalt suureneb. Näiteks Hiina ja Venemaa investeerivad piirkonda märkimisväärseid summasid, millega kaasneb oht, et ELi kui piirkonna kübervaldkonna osaleja roll piirkonnas marginaliseerub. *Allikas*: EPSC, *Engaging with the Western Balkans: an investment in Europe's security* (Lääne-Balkani riikide kaasamine: investeering Euroopa julgeolekusse), 17. mai 2018.

[83] Euroopa Investeerimispank, *The EIB Group Operating Framework and Operational Plan 2018*(EIP grupi tegevusraamistik ja tegevuskava 2018), 12. detsember 2017.

[84] Euroopa Komisjon, *Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse ajavahemikuks 2021–2027 digitaalse Euroopa programm“*, COM(2018) 434 final, 6. juuni 2018.

[85] Euroopa Komisjon, *Euroopa Parlamendi ja nõukogu 18. juuli 2018. aasta määrus (EL) 2018/1092, millega kehtestatakse Euroopa kaitsevaldkonna tööstusliku arendamise programm eesmärgiga toetada liidu kaitsetööstuse konkurentsi- ja uuendusvõimet* (ELT L 200, 7.8.2018, lk 30). Lisaks loodi 2017. aastal kaitsealaseid teadusuuringuid ettevalmistav meede kogusummas 90 miljonit eurot (2017–2019), mida rahastatakse programmist „Horisont 2020“. Ei ole selge, kas see hõlmab ka kübervaldkonnaga seotud kulutusi.

[86] Kontrollikoda plaanib 2019. aastal avaldada ELi kaitset käsitleva eraldi infodokumendi.

[87] Europoli küberkuritegevuse vastase võitluse Euroopa keskusel, ENISA-l, Euroopa välisteenistusel, Euroopa Kaitseagentuuril ja CERT-EU-l on kokku 159 töötajat. Nimetatud arv ei hõlma Euroopa Komisjoni ja liikmesriikide kübertemaatikaga tegelevaid töötajad. *Allikas*: Euroopa Poliitikauuringute Keskus, *ibid*., november 2018.

[88] *ENISA evaluation*(ENISA hindamine), 2017.

[89] Europol taotles oma 2018.–2020. aasta mitmeaastases kavas iga-aastase ajutiste teenistujate arvu suurendamist 70 inimese võrra, kuid 2018. aastal kiideti heaks ainult 26 lisatöötaja palkamine. Järgmise mitmeaastase kava (2019–2021) eelnõus lähtus Europol tagasihoidlikust kasvust, „eeldades, et nõudlust ressurside järele suuremas osas ei täideta“. *Allikas*: Parlamentaarse ühiskontrolli töörühmale esitatud 2019.–2021. aasta mitmeaastase kava arutelu, A 000834, 1. veebruar 2018.

[90] *ENISA evaluation*(ENISA hindamine), 2017. 2014.–2016. aastal kasutati umbes 80% ENISA tegevuseelarvest uuringute hankimiseks.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms* (Praeguste ohtuteabe kogumise platvormide võimaluste ja piirangute uurimine), detsember 2017.

[92] ISACA (varem tuntud nime all *Information Systems Audit and Control Association*), *Information Security Governance: Guidance for Boards of Directors and Executive Management*(Suunised nõukogudele ja tegevjuhtkonnale), 2. väljaanne, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* (Küberturvalisuse taassaavutamine: valmistumine küberrünneteks. Ülemaailmse infoturbe 20. uuring, 2017), lk 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs* (Tabamus või müüt? Küberjulgeoleku programmide tegelike kulude ja mõju mõistmine), juuli 2017.

[95] Väärtpaberi- ja börsikomisjon, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (Avaliku sektori küberturvalisuse alase teabe avalikustamine ja sellealane tõlgendav juhend), 21. veebruar 2018.

[96] Euroopa Pangandusjärelevalve, Euroopa Väärtpaberiturujärelevalve ning Euroopa Kindlustus- ja Tööandjapensionide Järelevalve koostööfoorum.

[97] Euroopa Väärtpaberiturujärelevalve, *Joint Committee report on risks and vulnerabilities in the EU financial system* (Ühiskomitee aruanne ELi finantssüsteemi riskide ja haavatavuse kohta), aprill 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*(Infoturbe ja eraelu puutumatuse standardid VKEdele: soovitused, et parandada infoturbe ja eraelu puutumatuse standardite vastuvõtmist VKEdes), detsember 2015.

[99] Komisjoni teadusnõustamise mehhanism märkis ELi liikmesriikidele viidates, et ollakse ühel nõul aluspõhimõtete ja -väärtuste ning ühise strateegilise huvi suhtes, mille ümber saab ehitada tõhusa ELi küberturvalisuse juhtimise. *Allikas*: Teaduslik arvamus nr 2/2017, 24. märts 2017.

[100] Ameerika Ühendriigid, Hiina, Jaapan, Lõuna-Korea, India ja Brasiilia.

[101] Euroopa Julgeoleku- ja Kaitsekolledž (T. Renard ja A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence* (Küberjulgeoleku käsiraamat, peatükk 3.4: EL kui partner küberdiplomaatia ja -kaitse valdkonnas), 23. november 2018.

[102] Euroopa Liidu Nõukogu, *Action Plan for implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (ühisteatise „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“ käsitlevate nõukogu järelduste rakendamise tegevuskava, 15748/17, 12. detsember 2017.

[103] Euroopa Komisjon, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission* Euroopa Komisjoni digistrateegia: digitaalselt ümberkorraldatud, kasutajakeskne ja andmepõhine komisjon), C (2018) 7118 final, 21. november 2018.

[104] Volinik Gabrieli vastus parlamendi kirjalikule küsimusele (E-004294-17), 28. juuni 2017.

[105] Euroopa Liidu Nõukogu küberkaitsepoliitika raamistiku rakendamise iga-aastane aruanne (*Annual Report on the Implementation of the Cyber Defence Policy Framework*), 15870/17, 19. detsember 2017.

[106] Otsused 2015/443, 2015/444 ja 2017/46 reguleerivad komisjoni side- ja infosüsteemide turvalisust. Komisjoni 21. novembri 2018. aasta otsusega C (2018) 7706 loodi infotehnoloogia ja küberturvalisuse nõukogu, mis ühendab endist IT-nõukogu ja infosüsteemide turvalisuse juhtnõukogu.

[107] Euroopa Majandus- ja Sotsiaalkomitee, *ibid*., märts 2018.

[108] Euroopa Parlament, *ibid*., september 2015.

[109] Hübriidohtude ühisüksus loodi 2016. aastal ELi luure- ja situatsioonikeskuse raames. Üksus võtab vastu ja analüüsib eri sidusrühmadelt hübriidohtude kohta saadavaid salastatud ja avatud lähteandmeid.

[110] ENISA, *National-level Risk Assessments: An Analysis Report* (Liikmesriikide tasandi riskihinnangud: analüüsiaruanne), november 2013.

[111] Euroopa Komisjon, *Impact assessment on the proposed research competence centre and network of national coordination centres* (Mõjuhinnang Euroopa Liidu Küberturvalisuse Ameti ja küberturvalisust käsitleva õigusakti kohta), SWD(2017) 500 final (osa 1/6), 13. september 2018.

[112] Euroopa Komisjon, *ibid*., COM (2018) 403 final, 12. september 2018.

[113] *Résaux IP Européens Network Coordination Centre* (Euroopa piirkondlik internetiregister), mis teostab järelevalvet interneti numbriressursside jaotamise ja registreerimise üle.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* (EISAS suuremahuline katseprojekt ELi kodanike teadlikkuse suurendamiseks), november 2012).

[115] The Centre for Cyber Safety and Education, koostöös Booz Allen Hamiltoni, Alta Associatesi ja Frost & Sullivaniga, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* (2017. aasta ülemaailmse infoturbe valdkonna tööjõu-uuring – tööjõud ja reaktsioon küberriskidele).

[116] Euroopa Majandus- ja Sotsiaalkomitee, *ibid*., märts 2018.

[117] Ühendkuningriigi Parlamendi Ülemkoda, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19* (Ühendkuningriigi Parlamendi Ülemkoja ühiskomisjon – riikliku julgeolekustrateegia, küberturvalisuse alased oskused ja Ühendkuningriigi esmatähtis taristu, 2017.–2019. aasta istungjärgu teine aruanne), 16. juuli 2018.

[118] Europol/Eurojust, *Common challenges in combating cybercrime* (Ühised probleemid võitluses küberkuritegevusega), 7021/17, 13. märts 2017.

[119] Europol/Eurojust, *ibid*., 7021/17, 13. märts 2017.

[120] Euroopa Komisjon, *ibid*., COM (2018) 403 final, 12. september 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022* (Juhatuse otsus 33/2018/MB CEPOLi ühtse programmdokumendi kohta aastateks 2020–2022), 20. novembril 2018.

[122] Näiteks Euroopa välisteenistuse, liikmesriikide, ametite ja asutuste (nt CEPOL, küberkuritegevusalase hariduse ja koolituse Euroopa töörühm ning Euroopa Julgeoleku- ja Kaitsekolledž) vaheline koostöö.

[123] ENISA, *Stock-taking of information security training needs in critical sectors* (Infoturbe koolitusvajaduste jaotus kriitilise tähtsusega sektorites), detsember 2017.

[124] Küberkuritegevusalase hariduse ja koolituse Euroopa töörühm.

[125] Euroopa Komisjon, Kolmeteistkümnes eduaruanne tulemusliku ja tegeliku julgeolekuliidu suunas liikumise kohta, COM (2018) 46 final, 24. jaanuar 2018.

[126] Eriaruande nr 14/2018 tähelepanekute põhjal, *ibid*.

[127] Euroopa Parlamendi 13. juuni 2018. aasta resolutsioon küberkaitse kohta (2018/2004(INI)) (2018/2004(INI)). Euroopa Liidu Nõukogu, *ibid*., 15870/17, 19. detsember 2017.

[128] Šveits, endine Jugoslaavia Makedoonia vabariik, Ukraina, Bosnia ja Hertsegoviina ning Kosovo (nimetus ei piira Kosovo staatust käsitlevaid seisukohti ning on kooskõlas ÜRO Julgeolekunõukogu resolutsiooniga 1244 ja Rahvusvahelise Kohtu arvamusega Kosovo iseseisvusdeklaratsiooni kohta), Türgi ja Ameerika Ühendriigid.

[129] Europol, *Internet Organised Crime Threat Assessment 2018* (Europoli 2017. aasta ELi organiseeritud kuritegevuse ohtude hindamine).

[130] Euroopa Komisjon, *ibid*., SWD (2017) 295 final, 13. september 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman ja S. Furman, *Security Fatigue* (Turvaväsimus), „IT Professional“ kd 18, nr 5, 2016, lk 26–32. Vt ka NIST.

[132] Euroopa Komisjon/Euroopa välisteenistus, *Increasing resilience and bolstering capabilities to address hybrid threats* (Vastupidavusvõime tugevdamine ja suutlikkuse suurendamine võitluseks hübriidohtudega), JOIN(2018) 16 final, 13. juuni 2018.

[133] Näiteks AlphaBay ja Hansa sulgemine FBI ja Madalmaade politsei ühisoperatsioonides, mida toetas Europol. Need kaks suurimat platvormi, kus kaubeldakse ebaseaduslike toodete, nagu uimastite, tulirelvade ja küberkuritegevuseka vajalike vahenditega (näiteks pahavaraga). *Allikas*: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*(Ainus vahend on õiguskaitseorganiste töö koordineerimine), pressiteade, 29. mai 2018.

[134] Euroopa Komisjon, *ibid*., COM (2018) 403 final, 12. september 2018.

[135] Euroopa Liidu Nõukogu, *ibid*., 12711/1/17 REV 1, 9. oktoober 2017.

[136] Euroopa Komisjon, *ibid*., SWD (2017) 295 final, 13. september 2017.

[137] Euroopa Komisjon/Euroopa välisteenistus, *ibid*., JOIN(2018) 16, 13. juuni 2018.

[138] Euroopa Komisjon, SWD (2017) 500 final, 13. september 2017.

[139] *Vastastikuse mõistmise memorandum – ENISA, EDA, Europoli EC3,CERT-EU*; 23. mai 2018.

[140] Euroopa Komisjoni hange: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap* (Küberturvalisuse pädevusvõrgustiku katseprojekti loomine, et töötada välja ja rakendada ühine küberturvalisuse teadusuuringute tegevuskava), 27. oktoober 2017.

[141] Jean-Claude Juncker, julgeolekuliidu voliniku missioonikiri, 2. august 2016. Rakkerühma ülesannete hulka ei kuulu kaitseküsimused.

[142] Euroopa Liidu Nõukogu, *EU cybersecurity roadmap* (ELi küberturvalisuse tegevuskava), 8901/17, 11. mai 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues*(Julgeolekudebatt: ühispanustamine lahendused maailma julgeolekuküsimustele, 5. trükk, november 2017.

[144] Teadusuuringute Ühiskeskuse tehnilised aruanded, Euroopa küberturvalisuse eksperdikeskused: *mõisted ja taksonoomia. Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres* (Mõjuhinnang kavandatud teadusliku pädevuse keskuse ning riiklike koordineerimiskeskuste võrgustiku kohta), SWD(2018) 403 final, 12. september 2018.

[145] Euroopa Komisjon, *ibid*., SWD (2017) 295 final, 13. september 2017.

[146] Euroopa Komisjon, *ibid*., COM (2018) 403 final, 12. september 2018.

[147] Näiteks Euroopa finantseerimisasutuste teabe jagamise ja analüüsimise keskusse kuuluvad finantssektori esindajad, riikide CERTid, õiguskaitseasutused, ENISA, Europol, Euroopa Keskpank, Euroopa Maksenõukogu ja Euroopa Komisjon.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models* (Teabe jagamise ja analüüsimise keskuste koostöömudelid), 14. veebruar 2018.

[149] Euroopa Liidu Nõukogu, *ibid*., 12711/1/17 REV 1, 9. oktoober 2017.

[150] https://www.europol.europa.eu/empact.

[151] 2018. aastal konsultatsioonieettevõtte Accenture poolt 15 riigis tehtud uuringus leiti, et 87% suunatud küberrünnakutest suudeti ära hoida: *2018 State of Cyber Resilience* (Kübervastupidavusvõime olukord 2018. aastal), 10. aprill 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* (Küberturvalisus sunnib meid strateegilise autonoomia küsimuses ümber mõtlema), Oxford University Politics Bolog, 14. september 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective* (Kolm põhjust, miks küberohtude tuvastamine on endiselt ebatõhus), IT Pro, 14. juuli 2017.

[154] Euroopa Majandus- ja Sotsiaalkomitee, *ibid.*, märts 2018.

[155] Euroopa Komisjon, *Kaheksas eduaruanne tulemusliku ja tegeliku julgeolekuliidu suunas liikumise kohta*, COM (2017) 354 final, 29. juuni 2018.

[156] St võrgu- ja infoturbe koostöörühma erinevad väljaanded.

[157] PSD2: makseteenuste direktiiv, EKP/SSM: Euroopa Keskpank / ühtne järelevalvemehhanism; Target 2: üleeuroopaline automatiseeritud reaalajaline brutoarvelduste kiirülekandesüsteem (2. põlvkond), määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul. *Allikas*: CEPS-ECRI rakkerühm, *ibid*., juuni 2018.

[158] Euroopa Komisjon, *ELi Soovitus koordineeritud reageerimise kohta ulatuslike küberintsidentide ja kriiside korral*, C(2017) 6100 final, 13. september 2017.

[159] Euroopa Komisjon, *ibid*., SWD (2017) 295 final, 13. september 2017. On olemas mitu kriisiohjemehhanismi, sealhulgas ELi integreeritud kord poliitiliseks reageerimiseks kriisidele (IPCR), Argus (komisjoni kriisidele reageerimise mehhanism), Euroopa välisteenistuse kriisidele reageerimise mehhanism, liidu kodanikukaitse mehhanism ja ELi hädaolukordadele reageerimise protokoll õiguskaitsealaseks reageerimiseks.

[160] Lisaks võib see tuua kaasa Euroopa Liidu lepingu artikli 42 lõike 7 (vastastikuse abi klausel) või Euroopa Liidu toimimise lepingu artikli 222 (solidaarsusklausel) kohaldamise.

[161] Euroopa Komisjon/Euroopa välisteenistus, *ibid*., JOIN(2018) 16, 13. juuni 2018. 2018. aasta detsembris kajastati meedias Euroopa välisteenistuse diplomaatilise kommunikatsioonivõrgu (COREU) väidetavat häkkimist (allikas: *New York Times, Hacked*

European Cables Reveal a World of Anxiety About Trump, Russia and Iran; 18. detsember 2018). Seda juhtumit praegu uuritakse.

[162] Ka varajase hoiatamise ja vastastikuse abi valdkonna koostöö vajab edasiarendamist: *Nõukogu järeldused koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral*, 10085/18, 26. juuni 2018.

[163] Euroopa Parlamendi uuringuteenistus, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*(ENISA ja uus küberturvalisust käsitlev õigusakt), PE 614.643, september 2018.

[164] Euroopa Majandus- ja Sotsiaalkomitee, *ibid*., märts 2018.

[165] Euroopa Liidu Nõukogu, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks* (ELi hädaolukordadele reageerimise protokoll õiguskaitsealaseks reageerimiseks suurte piiriüleste küberrünnete korral), 14893/18, detsember 2018.

[166] Küberturbe kiirreageerimisrühmad, küberturvalisuse alane vastastikune abistamine, küberohtudele ja -intsidentidele reageerimise teabevahetuse platvorm. *Allikas*: Euroopa Liidu Nõukogu, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*(Alalise struktureeritud koostöö (PESCO) projektide ajakohastatud nimekiri (ülevaade)), 19. november 2018.

[167] Euroopa Liidu Nõukogu, Järeldused pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku kohta („küberdiplomaatia meetmete kogum“), 9916/17, 7. juuni 2017.

[168] Euroopa Liidu Nõukogu, *Nõukogu järeldused küberdiplomaatia kohta*, 6122/55, 11. veebruar 2015.

[169] Euroopa Liidu Nõukogu, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities* (Ettepanek: rakendamissuunised pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku jaoks) , 13007/17.

[170] Intsidendi süüdlase kindlakstegemine on endiselt liikmesriikide suveräänne poliitiline otsus ja mitte kõik meetmete kogumi osad ei nõua süüdlase kindlakstegemist.

[171] Meetmete kogumi abil ei suudetud kokku leppida ühismeetmeid; mõned liikmeseriigid võtsid üle USA seisukohad.

[172] Euroopa Liidu Nõukogu, *Nõukogu järeldused pahatahtliku kübertegevuse kohta*, 7925/18, 16. aprill 2018.

[173] Erinevates tööstusharudes (nt kommunaalteenused, keemia- ja töötlev tööstus, toiduainetööstus, transpordisüsteemid ja -sõlmed ning logistikateenused) protsesside juhtimiseks kasutatavad arvutisüsteemid.

[174] ENISA, *ibid*., detsember 2017.

[175] Näiteks avalik haldus, keemia- ja tuumatööstus, töötlev tööstus, toiduainetööstus, turism, logistika ja kodanikukaitse.

[176] Euroopa Komisjon, *ibid*., SWD (2017) 295 final, 13. september 2017.

[177] Volinik Věra Jourová sõnavõtt Euroopa Parlamendi 14. novembri 2018. aasta täiskogu istungil teemal *ELi vastupidavuse suurendamine välisosalejate mõju suhtes tulevaste Euroopa Parlamendi valimiskampaania käigus*.

[178] Carnegie Rahvusvahelise Rahu Sihtasutus, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Euroopa reaktsioon võltsuudistele ja küberrünnetele), 23. mai 2018.

[179] Euroopa Poliitilise Strateegia Keskus (L. Past), Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses, in: „Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts", 2018.

[180] Vastavalt nõukogu direktiivile 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta.

[181] Euroopa Komisjon, soovitus valimiskoostöö võrgustike, veebisisu läbipaistvuse, küberintsidentide eest kaitsmise ning väärinfo levitamise kampaaniate vastu võitlemise kohta Euroopa Parlamendi valimiste raames, C(2018) 5949 final, 12. september 2018.

[182] Euroopa Ülemkogu järeldused, EUCO 11/15, 20. märts 2015. Hiljem on lisatud kaks täiendavat rakkerühma – Lääne-Balkani riikide ja lõunapoolsete naaberriikide jaoks.

[183] Atlandi ookeani Nõukogu aruandes kutsuti ELi üles nõudma, et kõik liikmesriigid saadaksid oma eksperdid rakkerühmas osalema. Vt D. Fried ja A. Polyakova, *Democratic Defense Against Disinformation*, 5. märts 2018.

[184] Töörühmal puudus esialgu eraldi eelarve, 2018. aastal eraldas Euroopa Parlamendi rühmale „StratCom Plus" ettevalmistava meetme jaoks 1,1 miljonit eurot.

[185] Carnegie Rahvusvahelise Rahu Sihtasutus (E. Brattberg, T. Maurer), *ibid*., 23. mai 2018.

[186] Euroopa Komisjoni, liidu välisasjade ja julgeolekupoliitika kõrge esindaja, *Väärinfovastane tegevuskava*, JOIN(2018) 36 final. Kavas keskendutakse järgmisele: ELi institutsioonide suutlikkuse parandamine väärinfo avastamisel, analüüsimisel ja paljastamisel; koordineeritud ja ühiste meetmete tugevdamine; erasektori kaasamine; teadlikkuse suurendamine ja ühiskonna vastupidavuse parandamine.

[187] Euroopa Komisjon, *Euroopa lähenemisviis veebis leviva väärinfoga võitlemiseks*, COM(2018) 236 final, 26. aprill 2018.

[188] Seda ei tohi segi ajada tegevusjuhendiga, mis käsitleb võitlust internetis leviva vihakõne vastu.

[189] Teadusuuringute Ühiskeskus, *The digital transformation of news media and the rise of disinformation and fake news* (Uudistemeedia digitaalne ümberkujundamine ning väärinfo ja libauudiste sagenemine), Teadusuuringute Ühiskeskuse tehnilised aruanded, *JRC Digital Economy Working Paper* 2018-02, aprill 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* (Võrgu- ja infoturvalisuse tugevdamine ning kaitse veebis levitatava väärinfo vastu), aprill 2018.

[191] Euroopa poliitika- ja strateegiakeskus (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* (Valimisorganisatsioonide toetamine küberohtude prognoosimisel ja nende vastu võitlemisel),*ibid.*, 2018.

[192] Euroopa Komisjon, *ibid*., COM (2018) 403 final, 12. september 2018.

[193] Ettepanek määruseks, millega luuakse Euroopa Liitu tehtavate välismaiste otseinvesteeringute taustauuringute raamistik (COM(2017) 487 final, 13. september 2018) on praegu õigusloomeprotsessis. See hõlmab konkreetselt elutähtsat tehnoloogiat, mis tähendab tehisintellekti, küberturvalisust ja kahese kasutusega rakendusi.

[194] Euroopa Komisjon/Euroopa välisteenistus, *ibid*., JOIN(2017) 450 final, 13. september 2018.

Infodokumendi koostajad

Infodokumendi „ELi küberturvalisuse poliitika tõhusust mõjutavad probleemid“ koostas välistegevuse, turvalisuse ja õiguse kuluvaldkondade auditeerimise eest vastutav III auditikoda, mille eesistuja on kontrollikoja liige Bettina Jakobsen. Dokumendi koostamist juhtis kontrollikoja liige Baudilio Tomé Muguruza; teda toetasid kabinetiülem Daniel Costa de Magalhães ja kabineti atašee Ignacio García de Parada, valdkonnajuht Alejandro Ballester-Gallardo, ülesande juht Michiel Sweerts, audiitorid Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha ja praktikant Johannes Bolkart. Keelealast abi osutas Hannah Critoph.

Vasakult paremale: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes

EUROOPA
KONTROLLIKODA

Väljaannete talitus

EUROOPA KONTROLLIKODA
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel +352 4398-1

Päringud: eca.europa.eu/et/Pages/ContactForm.aspx
Veebisait: eca.europa.eu
Twitter: @EUAuditors