SOOVITUSED

KOMISJONI SOOVITUS (EL) 2017/1584,

13. september 2017,

koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 292,

ning arvestades järgmist:

(1) Info- ja kommunikatsioonitehnoloogiate kasutamine ja sõltuvus neist on muutunud kõigi majandusvaldkondade lahutamatuks osaks, sest ettevõtjad ja kodanikud on üksteisega üha rohkem ühendatud ja sõltuvad üksteisest rohkem kui kunagi varem nii valdkondadevaheliselt kui ka piiriüleselt. Liikmesriigid ja ELi institutsioonid peavad olema hästi ette valmistatud küberturvalisuse intsidentideks, mis mõjutavad organisatsioone mitmes liikmesriigis või suisa kogu Euroopa Liidus ning võivad põhjustada tõsiseid häireid siseturul ja laiemalt võrkudes ja infosüsteemides, millest sõltuvad liidu majandus, demokraatia ja ühiskond.

(2) Küberturvalisuse intsidenti võib pidada ELi taseme kriisiks, kui intsidendi põhjustatud häired on liiga laialdased, et neist mõjutatud liikmesriik üksi suudaks nendega toime tulla, või kui intsidendil on mitmes liikmesriigis niivõrd laiaulatuslik tehniline või poliitiline mõju, et seda tuleb liidu poliitilisel tasandil õigel ajal koordineerida ja sellele reageerida.

(3) Küberturvalisuse intsidentidest võib alguse saada suurem kriis, mis mõjutab mitte ainult võrgu- ja infosüsteeme ja sidevõrke; otstarbekas reageerimine peab hõlmama nii küber- kui ka muid leevendusmeetmeid.

(4) Küberturvalisuse intsidendid ei ole ette ennustatavad; sageli leiavad need aset ja arenevad väga lühikese aja jooksul ning seetõttu peavad intsidendist mõjutatud üksused ja need, kes vastutavad intsidendile reageerimise ja selle tagajärgede leevendamise eest, oma vastumeetmeid kiiresti koordineerima. Küberturvalisuse intsidendid ei leia enamasti aset geograafiliselt piiritletud alal ning võivad samal ajal ilmneda mitmes riigis või levida mitmesse riiki.

(5) ELi tasandil küberturvalisuse intsidentidele ja kriisidele tulemuslikult reageerimine eeldab kõigi asjaomaste sidusrühmade sujuvat ja tulemuslikku koostööd ning tugineb nii üksikute liikmesriikide valmisolekule ja suutlikkusele kui ka koordineeritud ühismeetmetele, mida toetab liidu suutlikkus. See tähendab, et õigeaegseks ja tulemuslikuks intsidentidele reageerimiseks peavad olemas olema varem koostatud ja võimaluse piires ka korralikult läbi harjutatud koostöökord ja koostöömehhanismid, milles on selgelt kindlaks määratud nii riikide kui ka liidu tasandi peamiste osaliste rollid ja vastutus.

(6) Nõukogu esitas 27. mai 2011. aasta järeldustes ([1]) elutähtsate infoinfrastruktuuride kaitse kohta ELi liikmesriikidele üleskutse tõhustada liikmesriikidevahelist koostööd ning anda oma panus, „tuginedes riikide kriisijuhtimisega seotud kogemustele ja tulemustele ning koostöös ENISAga, Euroopa küberjuhtumitega seotud koostöömehhanismide arendamisse, mida testitakse järgmise Euroopa küberõppuse raames 2012. aastal".

(7) 2016. aasta teatises „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine" ([2]) kutsuti liikmesriike üles võrgu- ja infoturbedirektiivi ([3])

([1]) Nõukogu järeldused elutähtsate infoinfrastruktuuride kaitse kohta „Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas", dokument 10299/11, Brüssel, 27. mai 2011.
([2]) COM(2016) 410 final, 5. juuli 2016.
([3]) 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).

koostöömehhanisme võimalikult hästi kasutama ning tõhustama ulatuslikeks küberintsidentides valmisoleku alast piiriülest koostööd. Samas lisati, et valmisolekut suurendaks see, kui kooskõlastatud lähenemisviis küberökosüsteemi eri valdkondades tehtavale kriisiaegsele koostööle oleks sõnastatud tegevuskavas, ning et selline tegevuskava peaks ühtlasi aitama tagada koostoime ja järjepidevuse olemasolevate kriisihalduse mehhanismidega.

(8) Nõukogu järeldustes [1] nimetatud teatise kohta tegid liikmesriigid komisjonile ülesandeks esitada selline tegevuskava asutustele ja muudele asjaomastele sidusrühmadele kaalumiseks. Võrgu- ja infoturbedirektiiv ei näe paraku ette liidu koostööraamistikku ulatuslike küberturvalisuse intsidentide ja kriiside korral.

(9) Komisjon konsulteeris liikmesriikidega 5. aprillil ja 4. juulil 2017 kahel Brüsselis toimunud spetsiaalsel seminaril, millel osalesid liikmesriikide esindajad küberturbe intsidentide lahendamise üksustest (CSIRT), võrgu- ja infoturbedirektiiviga loodud koostöörühmast ja nõukogu küberküsimuste horisontaalsest töörühmast ning Euroopa välisteenistuse, ENISA, Europol/EC3 ja nõukogu peasekretariaadi esindajad.

(10) Käesoleva soovituse lisas olev tegevuskava, milles käsitletakse liidu tasandil koordineeritud reageerimist ulatuslikele küberturvalisuse intsidentidele ja kriisidele, on nimetatud konsultatsioonide tulemus ja täiendab ühtlasi teatist „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“.

(11) Tegevuskavas kirjeldatakse liikmesriikide ning ELi institutsioonide, organite, asutuste ja ametite (edaspidi „ELi institutsioonid“) vahelise koostöö eesmärke ja viise ulatuslikele küberturvalisuse intsidentidele ja kriisidele reageerimise korral ning seda, kuidas olemasolevates kriisihaldusmehhanismides täielikult ära kasutada ELi tasandil olemasolevaid küberturvalisuse üksuseid.

(12) Kui reageeritakse küberturvalisuse kriisile põhjenduses 2 kirjeldatud tähenduses, koordineeritakse liidu poliitilisel tasandil reageerimist nõukogus kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra (IPCR) [2] kohaselt; komisjonis kasutatakse kõrgetasemelist valdkondadevahelist kriisikoordineerimismenetlust ARGUS [3]. Kui kriisiga kaasneb oluline välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, siis aktiveeritakse Euroopa välisteenistuse kriisidele reageerimise mehhanism [3].

(13) Teatavates valdkondades on ELi tasandi valdkondlikes kriisihalduse mehhanismides nähtud ette ka koostöö küberturvalisuse intsidentide või kriisi korral. Näiteks Euroopa ülemaailmse satelliitnavigatsioonisüsteemi (GNSS) raames on nõukogu otsuses 2014/496/ÜVJP [4] juba kindlaks määratud nõukogu, kõrge esindaja, komisjoni, GNSSi agentuuri ja liikmesriikide rollid operatiivkohustuste ahelas, mis on loodud, et reageerida liitu, liikmesriike või GNSSi ähvardavale ohule, muu hulgas küberrünnetele. Seetõttu ei tohiks käesolev soovitus piirata selliste mehhanismide kohaldamist.

(14) Esmane vastutus reageerimise eest juhul, kui liikmesriiki mõjutab ulatuslik küberturvalisuse intsident või -kriis, lasub liikmesriigil endal. Komisjonil, kõrgel esindajal ja muudel ELi institutsioonidel või talitustel on aga samuti oluline roll, mis tuleneb liidu õigusest või asjaolust, et küberturvalisuse intsidendid ja kriisid võivad mõjutada majandustegevuse kõiki sektoreid ühtsel turul, liidu julgeolekut ja rahvusvahelisi suhteid ning institutsioone endid.

(15) Liidu tasandil on küberturvalisuse intsidentidele reageerijate hulgas peamisteks osalisteks võrgu- ja infoturbedirektiiviga värskelt loodud struktuurid ja mehhanismid, täpsemalt küberturbe intsidentide lahendamise üksuste (CSIRTide) võrgustik, aga ka asjaomased ametid ja organid, nagu Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA), Europoli juures tegutsev küberkuritegevusevastase võitluse Euroopa keskus (Europol/EC3), ELi luureandmete analüüsi keskus (INTCEN), ELi sõjalise staabi luureosakond (EUMS INT) ja vaatluskeskus (SITROOM), kes töötavad koos ühtse luureandmete analüüsivõime (SIAC) üksusena, ELi hübriidohtude ühisüksus (mis tegutseb INTCENis), ELi institutsioonide infoturbeintsidentidega tegelev rühm (CERT-EU) ja Euroopa Komisjoni hädaolukordadele reageerimise koordineerimiskeskus.

(16) Liikmesriikidevaheline koostöö küberturvalisuse intsidentidele reageerimisel toimub võrgu- ja infoturbedirektiiviga loodud CSIRTide võrgustikus. ENISA pakub võrgustikule sekretariaaditeenuseid ja toetab aktiivselt CSIRTidevahelist koostööd. Riikide CSIRTid ja CERT-EU teevad koostööd ja vahetavad teavet vabatahtlikkuse alusel, kaasa

[1] Dokument 14540/16, 15. november 2016.
[2] Lisateavet leiab ELi tasandi kriisihaldust, koostöömehhanisme ja osalejaid käsitleva liite punktist 3.1.
[3] Samas.
[4] Nõukogu 22. juuli 2014. aasta otsus 2014/496/ÜVJP Euroopa ülemaailmse satelliitnavigatsioonisüsteemi kasutuselevõtu, toimimise ja kasutamise aspektide kohta, mis mõjutavad Euroopa Liidu julgeolekut, ning millega tunnistatakse kehtetuks ühismeede 2004/552/ÜVJP (ELT L 219, 25.7.2014, lk 53).

arvatud siis, kui see on vajalik, et reageerida üht või mitut liikmesriiki mõjutavatele küberturvalisuse intsidentidele. Liikmesriigi CSIRTi esindaja taotlusel võivad nad arutada koordineeritud reageerimist sama liikmesriigi jurisdiktsioonis tuvastatud intsidendile ning võimaluse korral selle kindlaks määrata. Asjaomased menetlused määratakse kindlaks CSIRTide võrgustiku standardse töökorraga ([1]).

(17) CSIRTide võrgustiku ülesandeks on ka operatiivkoostöö täiendavate vormide üle arutlemine, nende uurimine ja nende kindlaksmääramine muu hulgas seoses riskide ja intsidentide kategooriatega, varajaste hoiatustega, vastastikuse abistamisega ning koordineerimise põhimõtete ja korraga juhtudel, kui liikmesriigid reageerivad piiriülestele riskidele ja intsidentidele.

(18) Võrgu- ja infoturbedirektiivi artikliga 11 loodud koostöörühma ülesandeks on anda strateegilisi juhiseid CSIRTide võrgustiku tegevuse jaoks, arutleda liikmesriikide suutlikkuse ja valmisoleku üle ning hinnata vabatahtlikkuse alusel riikide võrgu- ja infosüsteemide turvalisuse strateegiaid ja CSIRTide tulemuslikkust ning teha kindlaks parimad tavad.

(19) Töörühma ühe eraldi töösuuna raames valmistatakse vastavalt võrgu- ja infoturbedirektiivi artikli 14 lõikele 7 ette juhiseid intsidentidest teatamiseks olukordades, kus oluliste teenuste operaatorid peavad intsidentidest teatama vastavalt artikli 14 lõikele 3, ning sellise teatamise vormi ja korda ([2]).

(20) Aruannete, hindamiste, teadusuuringute, uurimise ja analüüsi käigus omandatud teadlikkus ja arusaamine olukorrast reaalajas, riskiseisundist ja ohtudest on põhjendatud otsuste tegemiseks hädavajalik. Selline olukorrateadlikkus kõigi asjaomaste sidusrühmade seas on tulemusliku koordineeritud reageerimise jaoks eluliselt tähtis. Olukorrateadlikkus hõlmab elemente, mis puudutavad nii intsidendi põhjuseid, mõju kui ka päritolu. Teadvustatakse, et see eeldab, et asjaomased pooled vahetavad teavet sobivas vormis, kasutades intsidendi kirjeldamiseks ühist taksonoomiat ning asjakohaselt turvalisel viisil.

(21) Küberturvalisuse intsidentidele reageerimine võib toimuda mitmel viisil alates sellest, et määratakse kindlaks tehnilised meetmed, mis võivad tähendada seda, et kaks või enam üksust uurivad ühiselt intsidendi tehnilisi põhjuseid (nt pahavara analüüs), või määratakse kindlaks moodused, kuidas organisatsioonid saavad hinnata, kas nad on intsidendist mõjutatud (nt rikkeindikaatorid), ja lõpetades operatiivsete otsustega selliste tehniliste meetmete kohaldamise kohta ja poliitilise tasandi otsustega kasutada muid vahendeid, nagu ELi ühise diplomaatilise reageerimise raamistik kuritahtliku kübertegevuse suhtes ([3]) või ELi hübriidohutõrje operatiivprotokoll, ([4]) sõltuvalt intsidendist.

(22) Selleks, et digitaalne ühtne turg saaks olla edukas, peab Euroopa kodanikel ja ettevõtjatel olema usaldus digiteenuste vastu. See tähendab, et kriisiolukorra teabevahetusel on küberturvalisuse intsidentide ja kriiside kahjuliku mõju leevendamises eriti oluline roll. Ka ühise diplomaatilise reageerimise raamistiku puhul võib teabevahetust kasutada kui vahendit, millega mõjutada kolmandatest riikidest tegutsevate (potentsiaalsete) agressorite käitumist. Selleks et poliitiline reageerimine oleks tulemuslik, on äärmiselt oluline, et avalik teabevahetus, mis on suunatud küberturvalisuse intsidentide ja kriiside kahjuliku mõju leevendamisele, ja avalik teabevahetus, mis on suunatud agressori mõjutamisele, oleksid omavahel kooskõlas.

(23) Ulatusliku küberturvalisuse intsidendi või kriisi leevendamisel võib tulemuslikuks meetmeks olla see, kui üldsusele jagatakse teavet, kuidas kasutaja ja organisatsiooni tasandil leevendada intsidendi mõju (nt paiga installeerimine, lisameetmed ohu vältimiseks vms).

(24) Komisjon tegeleb Euroopa ühendamise rahastu küberturvalisuse digitaalteenuste taristu kaudu osalevate liikmesriikide CSIRTide vahelise tuumteenuste platvormi koostöömehhanismi (MeliCERTes) arendamisega, et parandada CSIRTide valmisoleku taset, koostööd ja esilekerkivatele küberohtudele ja intsidentidele reageerimist. Komisjon kaasrahastab Euroopa ühendamise rahastu toetuste saamiseks korraldatavate konkurentsipõhiste projektikonkursside kaudu liikmesriikide CSIRTe, et parandada nende operatiivsuutlikkust riigi tasandil.

([1]) Väljatöötamisel; eeldatavasti võetakse vastu 2017. aasta lõpuks.
([2]) Juhised peaksid valmis saama 2017. aasta lõpuks.
([3]) Nõukogu järeldused pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku kohta („küberdiplomaatia meetmete kogum"), dokument 9916/17.
([4]) Talituste ühine töödokument „ELi hübriidohutõrje operatiivprotokoll (ELi käsiraamat)", SWD(2016) 227 final, 5. juuli 2016.

(25) Liikmesriikide ja erasektori koostöö ergutamiseks ja parandamiseks on olulised ELi tasandil korraldatavad küberõppused. Selleks on ENISA alates 2010. aastast korraldanud regulaarseid üleeuroopalisi küberintsidentide õppusi („Cyber Europe“).

(26) Nõukogu järeldustes ([1]) Euroopa Ülemkogu eesistuja, Euroopa Komisjoni presidendi ja Põhja-Atlandi Lepingu Organisatsiooni peasekretäri ühisdeklaratsiooni rakendamise kohta esitati üleskutse tugevdada küberõppustealast koostööd sellega, et vastastikku avatakse oma õppused (eeskätt „Cyber Coalition“ ja „Cyber Europe“) osalemiseks teineteise töötajatele.

(27) Ohtude pidev areng ja hiljutised küberturvalisuse intsidendid annavad märku sellest, et liitu ähvardavad riskid suurenevad, ning seetõttu peaksid liikmesriigid käesoleva soovituse täitmiseks meetmeid võtma viivitamata ja igal juhul 2018. aasta lõpuks,

ON VASTU VÕTNUD KÄESOLEVA SOOVITUSE:

1) Liikmesriigid ja ELi institutsioonid peaksid looma küberturvalisuse kriisidele reageerimise ELi raamistiku, millesse tuleks integreerida tegevuskavas tutvustatud eesmärgid ja koostöökord, järgides sealjuures tegevuskavas kirjeldatud juhtpõhimõtteid.

2) Küberturvalisuse kriisidele reageerimise ELi raamistikus tuleks eeskätt kindlaks määrata kõigi tasandite – tehnilise, operatiivse, strateegilise/poliitilise tasandi – asjaomased osalised, ELi institutsioonid ja liikmesriikide ametiasutused ning töötada vajaduse korral välja standardne töökord, milles kehtestataks nende osaliste vahelise koostöö kord ELi kriisiohjemehhanismide kontekstis. Tähelepanu tuleks pöörata sellele, et teabevahetus saaks toimuda põhjendamatute viivitusteta ning ulatuslike küberturvalisuse intsidentide ja kriiside käigus koordineeritaks vastumeetmeid.

3) Liikmesriikide pädevad ametiasutused peaksid selle nimel koos tegutsema, et panna veelgi täpsemalt paika teabe jagamise ja koostöö protokollid. Koostöörühm peaks vahetama sellealaseid kogemusi kõigi asjaomaste ELi institutsioonidega.

4) Liikmesriigid peaksid tagama, et nende riiklikes kriisiohjemehhanismides käsitletakse piisavalt põhjalikult küberturvalisuse intsidentidele reageerimist ning nähakse ette ELi raamistiku kohaselt toimuva ELi tasandi koostöö kord.

5) Mis puudutab olemasolevaid ELi kriisiohjemehhanisme, peaksid liikmesriigid kooskõlas tegevuskavaga kehtestama koos komisjoni talituste ja Euroopa välisteenistusega praktilised rakendussuunised oma riiklike kriisiohje- ja küberturvalisuse üksuste integreerimiseks olemasolevatesse ELi kriisiohjemehhanismidesse, milleks on IPCR ja Euroopa välisteenistuse kriisidele reageerimise kord (EEAS CRM). Eeskätt peaksid liikmesriigid tagama, et olemas on vajalikud struktuurid, mis võimaldavad ELi kriisimehhanismide raames tõhusat teabe liikumist nende riiklike kriisiohjeasutuste ja nende ELi tasandi esindajate vahel.

6) Liikmesriigid peaksid täies ulatuses kasutama Euroopa ühendamise rahastu küberturvalisuse digitaalteenuste taristu programmi pakutavaid võimalusi ning tegema komisjoniga koostööd selle nimel, et praegu arendamisjärgus oleva tuumteenuste platvormi koostöömehhanism pakuks vajalikke funktsioone ja vastaks nende koostöövajadustele ka küberturvalisuse kriiside ajal.

7) Liikmesriigid peaksid tegema ENISA abiga ja varem selles valdkonnas tehtule toetudes koostööd, et arendada välja ja võtta kasutusele ühine taksonoomia ja vorm, mis võimaldaks olukorraaruannetes kirjeldada küberturvalisuse intsidentide tehnilisi põhjuseid ja mõju, et veelgi tõhustada liikmesriikide omavahelist tehnilist ja operatiivkoostööd kriiside ajal. Seoses sellega peaksid liikmesriigid võtma arvesse intsidentidest teavitamise juhiste vallas koostöörühmas pooleli olevat tööd ja eeskätt riikide teadete vormiga seotud aspekte.

8) Raamistikuga ette nähtud menetlusi tuleks testida ja vajaduse korral tuleks need läbi vaadata, lähtudes kogemustest, mille liikmesriigid on omandanud riiklikel, piirkondlikel ja liidu, aga ka küberdiplomaatia ja NATO küberturvalisuse õppustel osalemise käigus. Eeskätt tuleks neid testida seoses ENISA korraldatud õppustega CyberEurope. Esimese võimaluse selleks annab CyberEurope 2018.

([1]) ST 15283/16, 6. detsember 2016.

9) Liikmesriigid ja ELi institutsioonid peaksid pidevalt harjutama reageerimist ulatuslikele küberturvalisuse intsidentidele ja kriisidele nii riigi kui ka Euroopa tasandil; vajaduse korral tuleks harjutada ka poliitilist reageerimist ja kaasata erasektori üksused.

Brüssel, 13. september 2017

Komisjoni nimel

komisjoni liige

Mariya GABRIEL

LISA

Tegevuskava koordineeritud reageerimiseks ulatuslike piiriüleste küberturvalisuse intsidentide ja kriiside korral

SISSEJUHATUS

Käesolevat tegevuskava rakendatakse küberturvalisuse intsidentide (edaspidi „küberintsidendid“) suhtes, mille põhjustatud häired on liiga laialdased, et neist mõjutatud liikmesriik üksi suudaks nendega toime tulla, või millel on mitmes liikmesriigis või ELi institutsioonis niivõrd laiaulatuslik tehniline või poliitiline mõju, et need eeldavad õigeaegset poliitika koordineerimist ja reageerimist liidu poliitilisel tasandil.

Sellise ulatusega küberintsidente käsitatakse küberkriisidena.

Kübertunnustega ELi-ülese kriisi korral koordineerib liidus poliitilisel tasandil reageerimist nõukogu, kes lähtub oma tegevuses kriisidele poliitilist reageerimist käsitlevast ELi integreeritud (IPCR) korrast.

Komisjonis kasutatakse koordineerimiseks kiirhoiatussüsteemi ARGUS.

Kui kriisiga kaasneb oluline välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, siis aktiveeritakse Euroopa välisteenistuse kriisidele reageerimise mehhanism.

Tegevuskavas kirjeldatakse, kuidas need sissetöötatud kriisiohjamismehhanismid peaksid ära kasutama kõik võimalused, mida pakuvad ELi tasandi olemasolevad küberturbeüksused ja liikmesriikidevahelised koostöömehhanismid.

Tegevuskavas lähtutakse teatavatest juhtpõhimõtetest (proportsionaalsus, subsidiaarsus, täiendavus ja teabe konfidentsiaalsus) ja esitatakse koostöö põhieesmärgid (tulemuslik reageerimine, ühine olukorrateadlikkus, avalik kommunikatsioon) kolmel (strateegilisel/poliitilisel, operatiivsel ja tehnilisel) tasandil, seotud mehhanismid ja osalised ning meetmed nimetatud põhieesmärkide saavutamiseks.

Tegevuskava ei hõlma kriisihalduse kogu elutsüklit (ennetamine/leevendamine, valmisolek, reageerimine, taaste), vaid keskendub reageerimisele. Tegevuskavas käsitletakse siiski teatavaid tegevusi, eelkõige selliseid, mis aitavad saavutada ühise olukorrateadlikkuse.

Tuleb ka silmas pidada, et küberintsidendid võivad olla laiema kriisi põhjuseks või sellele kaasa aidata, mõjutades muid sektoreid. Arvestades, et enamik küberkriise mõjutab eeldatavasti füüsilist maailma, peab asjakohane reageerimine tuginema nii küberruumiga seotud kui ka muudele laiematele leevendamise meetmetele. Küberkriisidele reageerimist tuleks koordineerida muude kriisiohjemehhanismidega ELi, riiklikul või valdkondlikul tasandil.

Tegevuskava ei asenda siiski olemasolevaid sektoripõhiseid või poliitikaspetsiifilisi mehhanisme, kordasid või instrumente, nagu Euroopa ülemaailmse satelliitnavigatsioonisüsteemi programm, ([1]) ega piira nende kasutamist.

Juhtpõhimõtted

Eesmärkide püstitamisel, vajalike tegevuste kindlakstegemisel ning vastavatele osalejatele või mehhanismidele rollide ja ülesannete määramisel lähtutakse järgmistest juhtpõhimõtetest, mida tuleb järgida ka tulevikus rakendussuuniste koostamisel.

Proportsionaalsus. Suur osa liikmesriike mõjutavatest küberintsidentidest ei ole oma olemuselt midagi sellist, mida saaks käsitada riikliku või veel vähem Euroopa kriisina. Liikmesriikidevaheline koostöö sellistele intsidentidele reageerimisel toimub võrgu- ja infoturbedirektiiviga ([2]) loodud küberturbe intsidentide lahendamise üksuste (CSIRTide) võrgustiku raames. Riikide CSIRTid teevad kooskõlas CSIRTide võrgustiku standardse töökorraga koostööd ja vahetavad iga päev vabatahtlikult teavet, sh vajaduse korral selleks, et reageerida küberintsidentidele, mis mõjutavad ühte või mitut liikmesriiki. Seepärast peaks tegevuskava kasutama ära kõik standardses töökorras pakutavad võimalused ja töökorras tuleks võtta arvesse kõiki muid spetsiifiliselt küberintsidentidega seotud ülesandeid.

([1]) Otsus 2014/496/ÜVJP.
([2]) Direktiiv (EL) 2016/1148.

Subsidiaarsus. Subsidiaarsuse põhimõte on kesksel kohal. Esmane vastutus reageerimise eest juhul, kui liikmesriiki mõjutab ulatuslik küberintsident või -kriis, lasub liikmesriigil endal. Kuid ka komisjonil, Euroopa välisteenistusel ja muudel ELi institutsioonidel, asutustel ja organitel on oluline roll. See roll on sõnaselgelt sätestatud IPCR-korras, kuid tuleneb ka liidu õigusest või lihtsalt asjaolust, et küberintsidendid ja -kriisid võivad mõjutada majandustegevuse kõiki sektoreid ühtsel turul, liidu julgeolekut ja rahvusvahelisi suhteid ning institutsioone endid.

Täiendavus. Tegevuskavas võetakse täielikult arvesse olemasolevaid ELi tasandi kriisihalduse mehhanisme, eelkõige kriisidele poliitilist reageerimist käsitlev ELi integreeritud (IPCR) kord, ARGUS ja Euroopa välisteenistuse kriisidele reageerimise mehhanism, ning uue võrgu- ja infoturbedirektiivi struktuure ja mehhanisme, eelkõige CSIRTide võrgustik, ning asjaomaseid asutuseid ja organeid, eelkõige Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA), küberkuritegevuse vastase võitluse Euroopa keskus (Europol/EC3), Euroopa Liidu luureandmete analüüsi keskus (INTCEN), ELi sõjalise staabi luureosakond (EUMS INT) ja INTCENi vaatluskeskus (SITROOM), mis toimivad koos ühtse luureandmete analüüsivõimena (SIAC); ELi hübriidohtude ühisüksus (mis asub INTCENis) ning ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm (CERT-EU). Seda tehes tuleks tegevuskavas tagada, et nende omavahelises koostoimes ja koostöös saavutataks maksimaalne täiendavus ja et kattuvust oleks võimalikult vähe.

Teabe konfidentsiaalsus. Kogu tegevuskava raames toimuv teabevahetus peab olema kooskõlas normidega, mis kehtivad julgeoleku ([1]) ja isikukandmete kaitse suhtes ning fooritulede analoogial põhineva protokolli suhtes teabe tundlikkuse märgistamiseks ([2]). Salastatud teabe edastamiseks tuleb salastusmärkest sõltumata kasutada kättesaadavaid akrediteeritud vahendeid ([3]). Isikuandmete töötlemisel järgitakse ELi kohaldatavaid norme, eelkõige isikuandmete kaitse üldmäärust, ([4]) e-privaatsuse direktiivi ([5]) ning määrust ([6]) üksikisikute kaitse kohta isikuandmete töötlemisel liidu institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta.

Põhieesmärgid

Tegevuskava raames toimuva koostöö puhul järgitakse eespool nimetatud kolmetasandilist – poliitilist, operatiivset ja tehnilist – lähenemisviisi. Igal tasandil võib koostöö hõlmata teabevahetust ja ühistegevust. Koostöö eesmärk on saavutada järgmised põhieesmärgid.

— Võimaldada tulemuslik reageerimine. Reageerimine võib toimuda mitmel viisil, nt tehes kindlaks tehnilised meetmed, mis võivad tähendada seda, et kaks või enam üksust uurivad ühiselt intsidendi tehnilisi põhjuseid (nt pahavara analüüs), või tehes kindlaks moodused, kuidas organisatsioonid saavad hinnata, kas nad on intsidendist mõjutatud (nt rikkeindikaatorid). Lisaks võib teha operatiivseid otsuseid selliste tehniliste meetmete kohaldamiseks ja poliitilisel tasandil võidakse otsustada sõltuvalt intsidendist kasutada muid instrumente, nagu kuritahtliku kübertegevuse suhtes kohaldatav ELi ühise diplomaatilise reageerimise raamistik (küberdiplomaatia meetmed) või ELi hübriidohutõrje operatiivprotokoll.

— Ühine olukorrateadlikkus. Koordineeritud reageerimisel on äärmiselt oluline, et kõik sidusrühmad mõistaksid sündmusi ja nende arengut piisavalt hästi kõigil kolmel tasandil (tehniline, operatiivne, poliitiline). Olukorrateadlikkus võib hõlmata tehnoloogilisi elemente nii intsidendi põhjuste, mõju kui ka päritolu kohta. Küberintsidendid võivad mõjutada väga eri sektoreid (rahandus, energeetika, transport, tervishoid jne). Seepärast peab asjakohane teave jõudma sobivas vormis õigeks ajaks kõigi asjaomaste sidusrühmadeni.

([1]) Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/443 komisjoni julgeoleku kohta (ELT L 72, 17.3.2015, lk 41) ja komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta (ELT L 72, 17.3.2015, lk 53); liidu välisasjade ja julgeolekupoliitika kõrge esindaja 19. aprilli 2013. aasta otsus Euroopa välisteenistuse julgeolekueeskirjade kohta (ELT C 190, 29.6.2013, lk 1); nõukogu 23. septembri 2013. aasta otsus 2013/488/EL ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta (ELT L 274, 15.10.2013, lk 1).

([2]) https://www.first.org/tlp/

([3]) 2016. aasta juunis olid sellisteks edastuskanaliteks CIMS (salastatud teabe haldamise süsteem), ACID (krüpteerimisalgoritm), RUE (RESTREINT UE / EU RESTRICTED dokumentide loomiseks, vahetamiseks ja salvestamiseks mõeldud süsteem) ja SOLAN. Muud salastatud teabe vahetamiseks mõeldud süsteemid on PGP või S/MIME.

([4]) 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).

([5]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

([6]) Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, 12.1.2001, lk 1) – läbivaatamisel.

— Leppida kokku peamistes avaliku kommunikatsiooni sõnumites ([1]). Kriisikommunikatsioonil on oluline koht küberintsidentide ja -kriiside negatiivse mõju leevendamisel, kuid seda saab ka kasutada (võimalike) agressorite käitumise mõjutamise vahendina. Õiget sõnumit saab kasutada ka selleks, et saata selge signaal diplomaatilise reageerimise võimalikest tagajärgedest ja mõjutada agressori käitumist. Selleks et poliitiline reageerimine oleks tulemuslik, on äärmiselt oluline, et omavahel oleksid kooskõlas küberintsidentide ja -kriiside negatiivse mõju leevendamisele suunatud avalik kommunikatsioon ja agressori mõjutamisele suunatud avalik kommunikatsioon. Küberturvalisuses on eriti oluline anda täpsemaid tegevusjuhised selle kohta, mida inimesed saavad ise teha intsidendi tagajärgede leevendamiseks (nt kasutama paikamist, võtma lisameetmeid ohtude ärahoidmiseks jne).

KOOSTÖÖ LIIKMESRIIKIDE VAHEL NING LIIKMESRIIKIDE JA ELI OSALEJATE VAHEL TEHNILISEL, OPERATIIVSEL JA STRATEEGILISEL/POLIITILISEL TASANDIL

Tulemuslik reageerimine ulatuslike ELi tasandi küberintsidentide või -kriiside korral sõltub tulemuslikust tehnilisest, operatiivsest ja strateegilisest/poliitilisest koostööst.

Igal tasandil peaks osaleja täitma konkreetsed ülesanded, et saavutada kolm põhieesmärki:

— koordineeritud reageerimine

— ühine olukorrateadlikkus

— avalik kommunikatsioon

Intsidendi või kriisi käigus hoiatavad, teavitavad ja toetavad madalamad koostöötasandid kõrgemaid koostöötasandeid. Kõrgemad koostöötasandid annavad juhiseid ([2]) ja teevad madalamate tasemete suhtes otsuseid vastavalt vajadusele.

Koostöö tehnilisel tasandil

Tegevuse ulatus

— Intsidendikäsitlus ([3]) küberkriisi ajal

— Intsidentide seire ja järelevalve, sh ohtude ja riski pidev analüüs

Võimalikud osalejad

Tehnilisel tasandil on tegevuskavas keskne koostöömehhanism CSIRTide võrgustik. Selle eesistujana tegutseb eesistujariik ja sekretariaaditeenused tagab ENISA.

— Liikmesriigid:

  — Võrgu- ja infoturbedirektiivi kohased pädevad asutused ja ühtsed kontaktpunktid

  — CSIRTid

— ELi organid/asutused

  — ENISA

  — Europol/EC3

  — CERT-EU

([1]) Siinkohal on oluline märkida, et avalik kommunikatsioon hõlmab nii sellist kommunikatsiooni, mis on suunatud avalikkusele tervikuna, kui ka sellist, mis on suunatud elutähtsatele sektoritele ja/või neile, keda intsident on mõjutanud, ning mis on tehnilisem ja operatiivsem. Selleks võib olla vajalik kasutada konfidentsiaalseid edastuskanaleid ja spetsiifilisi tehnilisi vahendeid/platvorme. Iga juhul on kommunikatsioon liikmesriikides operaatorite ja laiema avalikkusega iga liikmesriigi eesõigus ja kohustus. Seepärast vastutavad kooskõlas eespool selgitatud subsidiaarsuse põhimõttega lõppastmes liikmesriigid ja riikide CSIRTid selle eest, millist teavet nad oma territooriumil ja kasutajate hulgas levitavad.

([2]) „Luba tegutsemiseks" – küberkriisi korral on kiire tegutsemine asjakohaste leevendamise meetmete võtmiseks äärmiselt oluline. Selleks et oleks võimalik kiiresti tegutsema hakata, saab üks liikmesriik anda teisele vabatahtlikult loa tegutsemiseks, mis annab liikmesriigile loa hakata viivitamata tegutsema, ilma et ta peaks konsulteerima kõrgemate tasanditega või ELi institutsioonidega ja läbima kõiki tavaliselt nõutud ametlikke kanaleid, kui see ei ole konkreetse intsidendi puhul vajalik (nt CSIRTidel ei peaks olema vaja konsulteerida kõrgemate tasanditega, selleks et edastada väärtuslikku teavet CSIRTile teises liikmesriigis).

([3]) „Intsidendikäsitlus" – intsidendi tuvastamist, analüüsimist ja ohjeldamist ning intsidendile reageerimist toetavad toimingud.

— Euroopa Komisjon

  — ERCC (DG ECHO juures asuv ööpäev läbi tegutsev operatiivne talitus) ja määratud juhttalitus (tuleb valida kas DG CNET või DG HOME, sõltuvalt konkreetse intsidendi olemusest), peasekretariaat (ARGUSe sekretariaat), DG HR (julgeoleku direktoraat), DG DIGIT (IT-turbe toimingud)

  — Muude ELi asutuste ([1]) jaoks vastav haldusala peadirektoraat komisjonis või Euroopa välisteenistus (esimene kontaktpunkt)

— Euroopa välisteenistus

  — SIAC (ühtne luureandmete analüüsivõime: EU INTCEN ja EUMS INT)

  — ELi vaatluskeskus ja määratud geograafiline või valdkonna talitus

  — ELi hübriidohtude ühisüksus (osa EU INTCENist – küberturvalisus hübriidohtude kontekstis)

Ühine olukorrateadlikkus

— ENISA peaks liidu olukorrateadlikkust toetava tehnilise tasandi korrapärase koostöö raames korrapäraselt koostama intsidentide ja ohtude kohta ELi küberturvalisuse tehnilist olukorda käsitleva aruande, mis põhineb avalikult kättesaadaval teabel, tema enda analüüsidel ja aruannetel, mida jagavad temaga (vabatahtlikkuse alusel) liikmesriikide CSIRTid või võrgu- ja infoturbedirektiivi kohased ühtsed kontaktpunktid, Europoli juures tegutsev küberkuritegevuse vastase võitluse Euroopa keskus (EC3) ja CERT-EU ja kui asjakohane, siis Euroopa Liidu luureandmete analüüsi keskus (INTCEN) Euroopa välisteenistuse juures. Aruanne tuleks teha kättesaadavaks nõukogu asjakohastele organitele, komisjonile, liidu välisasjade ja julgeolekupoliitika kõrgele esindajale ja CSIRTide võrgustikule.

— Oluliste intsidentide korral koostab CSIRTide võrgustiku eesistuja ENISA abil ELi küberturvalisuse olukorda käsitleva aruande ([2]). Roteeruva eesistujariigi CSIRT esitab selle eesistujariigile, komisjonile ja liidu välisasjade ja julgeolekupoliitika kõrgele esindajale.

— *Kõik muud ELi asutused* annavad aru oma haldusala peadirektoraatidele, kes omakorda annavad aru komisjoni juhttalitusele.

— *CERT-EU* esitab tehnilised aruanded CSIRTide võrgustikule, ELi institutsioonidele ja asutustele (vastavalt vajadusele) ja ARGUSele, kui see on aktiveeritud.

— *Europol/EC3* ([3]) *ja CERT-EU* esitavad tehniliste moonutuste kriminalistika-eksperdianalüüsi ja muu tehnilise teabe CSIRTide võrgustikule.

— EEAS SIAC: ELi hübriidohtude ühisüksus annab INTCENi nimel aru asjaomastele Euroopa välisteenistuse osakondadele.

Reageerimine

— *CSIRTide võrgustik* vahetab intsidenti käsitlevaid tehnilisi andmeid ja analüüse, nagu IP-aadress, rikkeindikaatorid ([4]) jne. Selline teave tuleks ENISA-le esitada ilma põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul pärast intsidendi avastamist.

— Kooskõlas CSIRTide võrgustiku standardse töökorraga teevad võrgustiku liikmed kättesaadavate tehniliste moonutuste ja muude intsidendiga seotud tehniliste andmete analüüsimisel koostööd, et selgitada välja põhjus ja võimalikud tehnilised leevendamise meetmed.

— ENISA abistab CSIRTisid nende tehnilises tegevuses, tuginedes oma eksperditeadmistele ja kooskõlas oma volitustega ([5]).

([1]) Sõltuvalt intsidendi olemusest ja mõjust eri tegevusvaldkondadele (rahandus, transport, energeetika, tervishoid jne) osalevad eri ELi asutused või organid.

([2]) ELi küberturvalisuse olukorda käsitlev aruanne on kokkuvõte riikide CSIRTide olukorraaruannetest. Aruande vormi tuleks kirjeldada CSIRTide võrgustiku standardses töökorras.

([3]) Kooskõlas EC3 õigusliku raamistiku ja selles sätestatud tingimuste ja menetlustega.

([4]) Rikkeindikaator – arvutikriminalistikas võrgus või operatsioonisüsteemis täheldatud moonutus, mis viitab sellele, et suure tõenäosusega on arvutisse sisse tungitud. Tüüpilised rikkeindikaatorid on viiruse signatuurid ja IP-aadressid, pahavara failide MD5 räsid või URLid või robotvõrgu juhtserverite domeeninimed.

([5]) Ettepanek: määrus, mis käsitleb Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA) ning millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („Küberturvalisust käsitlev õigusakt“), 13. september 2017.

— Liikmesriikide CSIRTid koordineerivad oma tehnilisi vastumeetmeid ENISA ja komisjoni abiga.

— EEAS SIAC: ELi hübriidohtude ühisüksus käivitab INTCENi nimel kogumisprotsessi esialgsete tõendite kogumiseks.

Avalik kommunikatsioon

— CSIRTid koostavad tehnilisi nõuandeid ([1]) ja hoiatusi nõrkuste kohta ([2]) ning jagavad neid kasutajate ja avalikkusega vastavalt konkreetse juhtumi suhtes kohaldatavale volituste andmise korrale.

— ENISA lihtsustab CSIRTide võrgustiku ühiste teavituste koostamist ja levitamist.

— ENISA koordineerib oma avaliku kommunikatsiooni meetmeid CSIRTide võrgustikuga ja komisjoni pressiesindaja talitusega.

— ENISA ja EC3 koordineerivad oma avalikku kommunikatsiooni liikmesriikide kokku lepitud ühisest olukorrateadlikkusest lähtudes. Mõlemad koordineerivad oma avaliku kommunikatsiooni meetmeid komisjoni pressiesindaja talitusega.

— Kui kriisiga kaasneb välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, tuleks avalik kommunikatsioon koordineerida Euroopa välisteenistuse ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja pressiesindaja talitusega.

Koostöö tehnilisel tasandil

Tegevuse ulatus

— Valmistada ette otsus poliitilisel tasandil

— Koordineerida küberkriisi haldamist (kui vaja)

— Hinnata tagajärgi ja mõju ELi tasandil ja pakkuda välja võimalikke leevendamise meetmeid

Võimalikud osalejad

— Liikmesriigid:

  — Võrgu- ja infoturbedirektiivi kohaselt loodud pädevad asutused ja ühtsed kontaktpunktid

  — CSIRTid, küberturvalisuse asutused

  — Muud riiklikud valdkondlikud asutused (mitut valdkonda hõlmava intsidendi või kriisi korral)

— ELi organid/asutused

  — ENISA

  — Europol/EC3

  — CERT-EU

— Euroopa Komisjon

  — Peasekretariaat, (ase)peasekretär (ARGUS-süsteem)

  — DG CNECT/HOME

  — Komisjoni julgeolekuasutus

  — Muud peadirektoraadid (mitut valdkonda hõlmava intsidendi või kriisi korral)

([1]) Tehniline nõuanne intsidendi põhjuste ja võimalike leevendamise meetmete kohta.
([2]) Teave tehniliste nõrkuste kohta, mida kasutatakse ära IT-süsteemide negatiivseks mõjutamiseks.

— Euroopa välisteenistus

  — Kriisile reageerimise ja SIAC eest vastutav (ase)peasekretär (EU INTCEN ja EUMS INT)

  — ELi hübriidohtude ühisüksus

— Nõukogu

  — Eesistuja (küberküsimustega tegelev horisontaalne töörühm või COREPERi eesistuja), ([1]) keda toetab nõukogu peasekretariaat või poliitika- ja julgeolekukomitee, ([2]) kui see aktiveeritakse – IPCRi korra toel

Olukorrateadlikkus

— Toetatakse poliitilist/strateegilist olukorda käsitlevate aruannete koostamist (nt integreeritud olukorrateadlikkus ja analüüs IPCRi aktiveerimise korral).

— *Nõukogu horisontaalne küberküsimuste töörühm* valmistab vastavalt vajadusele ette COREPERi või poliitika- ja julgeolekukomitee kohtumise

— IPCRi aktiveerimise korral

  — Eesistujariik võib kutsuda COREPERi või poliitika- ja julgeolekukomiteede jaoks tehtava ettevalmistuse toetamiseks kokku ümarlauakohtumise, kaasates asjaomased sidusrühmad liikmesriikides, institutsioonid, asutused ja kolmandad isikud, nagu ELi mittekuuluvad riigid ja rahvusvahelised organisatsioonid. Tegemist on kriisikohtumistega, mille käigus tehakse kindlaks kitsaskohad ja tehakse ettepanekud tegutsemiseks valdkondadeülestes küsimustes.

  — *Komisjoni juhttalitus või Euroopa välisteenistus* koostab integreeritud olukorrateadlikkuse ja analüüsi juhttalitusena integreeritud olukorrateadlikkuse ja analüüsi aruande, kuhu panustavad ENISA, CSIRTide võrgustik, Europol/EC3, EUMS INT, INTCEN ja kõik muud asjaomased osalejad. Integreeritud olukorrateadlikkuse ja analüüsi aruandes esitatakse tehniliste intsidentide ja kriisi hindamise korrelatsioonil põhinev ELi-ülene hinnang (ohuanalüüs, riskihindamine, mitte-tehnilised tagajärjed ja mõju, intsidendi või kriisi muud kui küberruumiga seotud tahud), mida on kohandatud vastavalt operatiivse ja poliitilise tasandi vajadustele.

— ARGUS-süsteemi aktiveerimise korral

  — CERT-EU ja EC3 ([3]) osalevad komisjonisiseses teabevahetuses otse.

— Euroopa välisteenistuse kriisidele reageerimise mehhanismi aktiveerimise korral

  — SIAC intensiivistab teabekogumist ja koondab kõikidest allikatest saadud teabe ning koostab intsidendi analüüsi ja hinnangu.

Reageerimine (kui seda taotletakse poliitiliselt tasandilt)

— Piiriülene koostöö ühtse kontaktpunkti ja riiklike pädevate asutustega (võrgu- ja infoturbedirektiiv), et leevendada tagajärgi ja mõju.

— Aktiveeritakse kõik tehnilised leevendamise meetmed ja koordineeritakse tehnilisi võimeid, mis on vajalikud infosüsteemide vastu suunatud ründe mõju peatamiseks või vähendamiseks.

— Koostöö ja asjaomase otsuse tegemise korral tehniliste võimekuste koordineerimine ühise või koostööl põhineva reageerimise kujundamiseks kooskõlas ***CSIRTide võrgustiku standardse töökorraga***.

— Hinnatakse koostöövajadust asjaomaste kolmandate isikutega.

— Otsuse tegemine ARGUS-süsteemis (kui see aktiveeritakse).

— Otsuste ettevalmistamine ja koordineerimine IPCRi-korra alusel (kui see aktiveeritakse).

— Euroopa välisteenistuse kriisidele reageerimise mehhanismi kaudu (kui see aktiveeritakse) Euroopa välisteenistuse otsuse tegemise toetamine, sh kontaktid kolmandate riikidega ja rahvusvaheliste organisatsioonidega, ja kõik meetmed, mis on suunatud ÜJKP sõjaliste missioonide ja operatsioonide ning ELi delegatsioonide kaitsmiseks.

([1]) Alaliste esindajate komitee ehk COREPER (Euroopa Liidu toimimise lepingu artikkel 240) vastutab Euroopa Liidu Nõukogu töö ettevalmistamise eest.

([2]) Euroopa Liidu lepingu artiklis 38 nimetatud poliitika- ja julgeolekukomitee on Euroopa Liidu Nõukogu komitee, mis tegeleb ühise välis- ja julgeolekupoliitikaga.

([3]) Kooskõlas EC3 õigusliku raamistiku ja selles sätestatud tingimuste ja menetlustega.

Avalik kommunikatsioon

— Leppida kokku intsidenti puudutavas avalikus kommunikatsioonis.

— Kui kriisiga kaasneb välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, tuleks avalik kommunikatsioon koordineerida Euroopa välisteenistuse ja liidu välisasjade ja julgeolekupoliitika kõrge esindaja pressiesindaja talitusega.

Koostöö strateegilisel/poliitilisel tasandil

Võimalikud osalejad

— Liikmesriikides küberturvalisuse eest vastutavad ministrid

— Euroopa Ülemkogus eesistuja

— Nõukogus rotatsiooni korras vahetuv eesistujariik

— Küberdiplomaatia meetmete raames võetud meetmete korral poliitika- ja julgeolekukomitee ja horisontaalne töörühm

— Euroopa Komisjonis president või delegeeritud asepresident/volinik

— Liidu välisasjade ja julgeolekupoliitikaga seotud küsimuste puhul liidu kõrge esindaja/komisjoni asepresident.

Tegevuse ulatus. Kriisi kübertahkude ja muude tahkude strateegiline ja poliitiline haldamine, sealhulgas pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku kohase reageerimise meetmed.

Ühine olukorrateadlikkus

— Selgitatakse välja kriisist tingitud häirete mõju liidu toimimisele.

Reageerimine

— Aktiveeritakse kriisihaldusmehhanismid ja -vahendid olenevalt intsidendi laadist ja mõjust, näiteks kodanikukaitse mehhanism.

— Võetakse pahatahtlikule kübertegevusele reageerimise ELi ühise diplomaatilise raamistiku kohaseid meetmeid.

— Tehakse kriisi tõttu kannatavatele liikmesriikidele kättesaadavaks erakorraline toetus, näiteks võttes kasutusele küberturvalisuse kiirreageerimisfondi, ([1]) kui see on loodud.

— Vajaduse korral tehakse koostööd ja koordineeritakse tegevust selliste rahvusvaheliste organisatsioonidega nagu Ühinenud Rahvaste Organisatsioon (ÜRO), Euroopa Julgeoleku- ja Koostööorganisatsioon (OSCE) ja eelkõige NATO.

— Analüüsitakse mõju riigi julgeolekule ja riigikaitsele.

Avalik kommunikatsioon

Ühise otsusega määratakse kindlaks avaliku kommunikatsiooni strateegia.

IPCRI KOHANE ELI KOORDINEERITUD REAGEERIMINE KOOSTÖÖS LIIKMESRIIKIDEGA

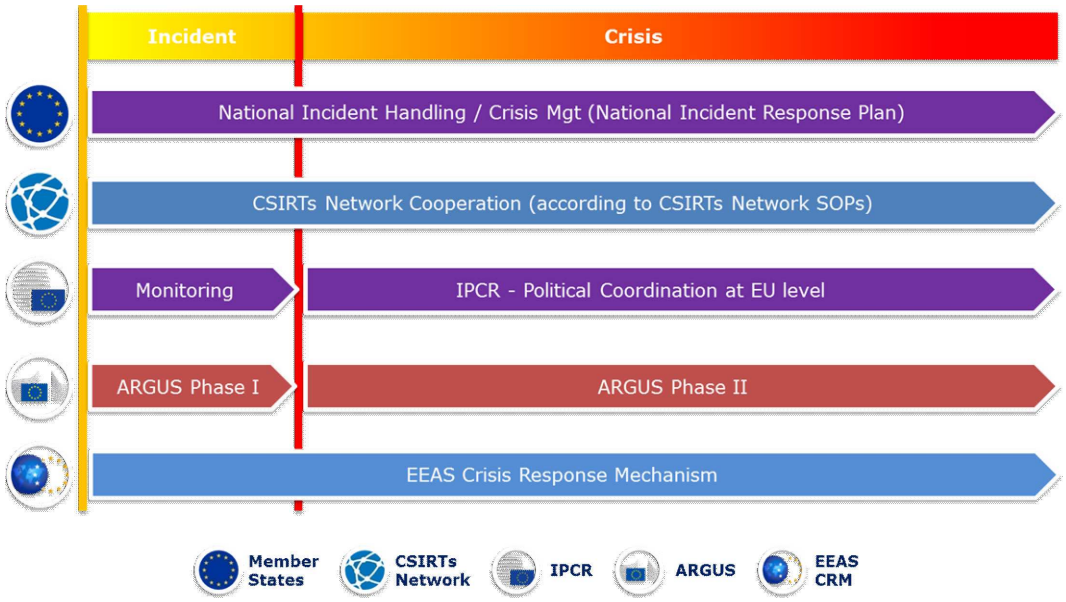
Käesolevas jaos on käsitletud eelkõige liikmesriikide ametiasutuste, CSIRTide võrgustiku, ENISA, CERT-EU, Europoli küberkuritegevuse vastase võitluse Euroopa keskuse (Europol/EC3), Euroopa Liidu luureandmete analüüsi keskuse (INTCEN), ELi hübriidohtude ühisüksuse ja nõukogu horisontaalse küberküsimuste töörühma peaeesmärke, ülesandeid ja tegevust IPCR raames. Seejuures on lähtutud ELi tasandil vastastikuse täiendavuse põhimõttest. Eeldatakse, et osalejad tegutsevad vastavalt ELi või riigi tasandil kehtestatud korrale.

On oluline märkida, et nagu on kujutatud joonisel 1, toimub riiklikul tasandil tegevus ning koostöö CSIRTide võrgustiku raames (kui vaja) kogu intsidendi/kriisi vältel vastavalt subsidiaarsuse ja proportsionaalsuse põhimõttele ega sõltu ELi kriisihaldusmehhanismi rakendamisest.

([1]) Ettepanek luua küberturvalisuse kiirreageerimisfond on esitatud ühisteatises „Vastupidavusvõime, heidutus ja kaitse – tugeva küberturvalisuse tagamine ELis“ (JOIN(2017) 450/1).

Joonis 1

Küberintsidendile või -kriisile reageerimine ELi tasandil



Kogu allpool kirjeldatud tegevus toimub vastavalt standardsele töökorrale ja asjakohaste koostöömehhanismide raames kehtivatele eeskirjadele ning kooskõlas iga osaleja ja institutsiooni volituste ja pädevusega. Nimetatud töökorda ja eeskirju võib vajaduse korral täiendada ja muuta, et tagada parim võimalik koostöö ja tõhus reageerimine suurte küberintsidentide ja -kriiside ajal.

Konkreetse intsidendi lahendamiseks ei tarvitse tingimata vaja minna kõiki allpool nimetatud osalejaid, kuid käesolevas tegevuskavas ja koostöömehhanismide standardses töökorras tuleks arvestada sellega, et neist igaüks võidakse kaasata.

Võttes arvesse, et küberintsidentide mõju ühiskonnale võib olla eri suurusega, tuleb valdkondlike osalejate igal tasandil kaasamise ja mis tahes reageerimise puhul arvestada suure paindlikkusega, mis põhineb nii küber- kui ka muudel leevendusmeetmetel.

Küberkriisi haldamine – küberturvalisuse nõuete arvessevõtmine kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra (IPCR) raames

IPCRi standardses töökorras ([1]) kirjeldatud IPCR sisaldab järgmisi samme (kuid osa samme tehakse vaid juhul, kui olukord seda nõuab).

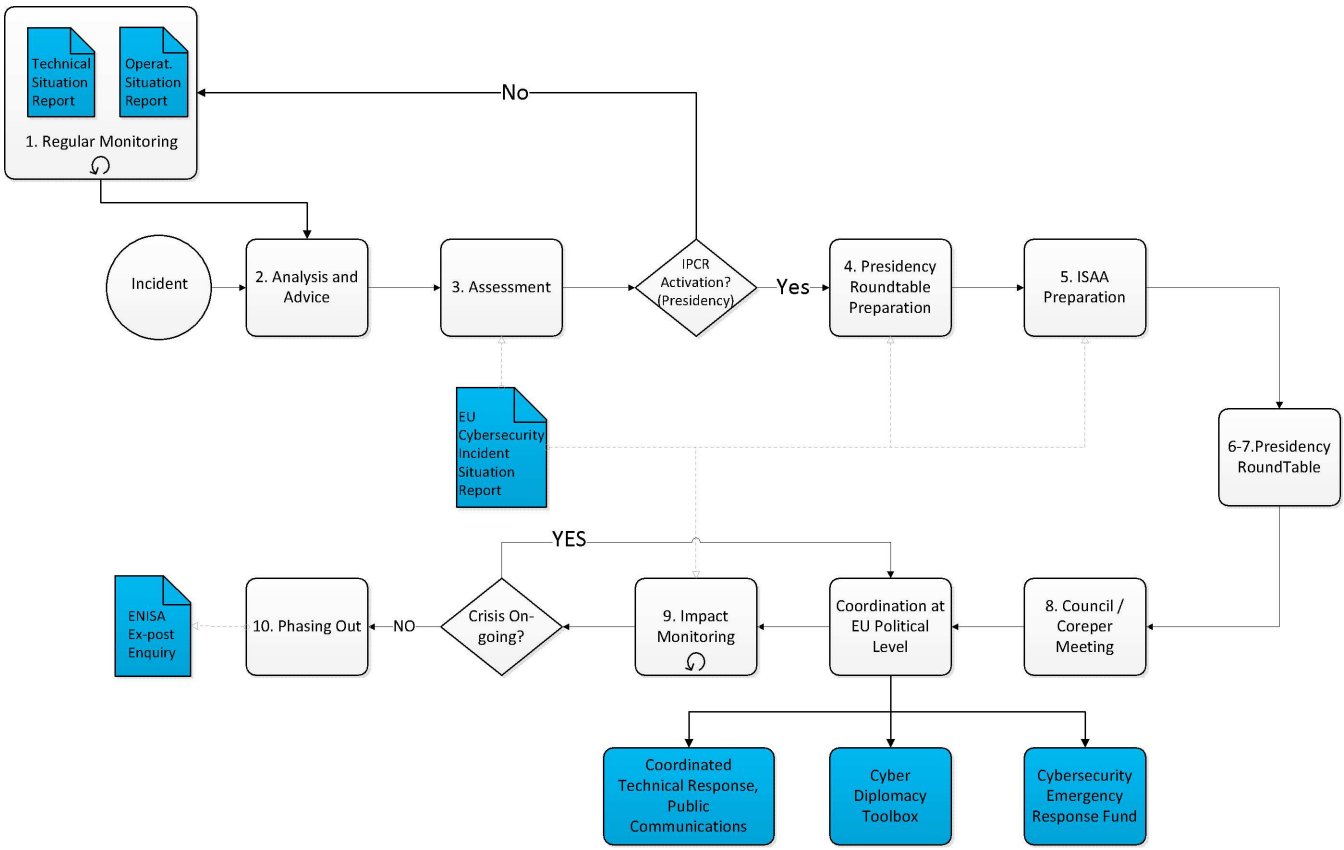
Iga sammu puhul on esitatud küberturvalisuse meetmed ja osalejad. Loetavuse huvides on iga sammu kohta esitatud IPCRi standardse töökorra tekst ja selle järel käesoleva tegevuskava kohane tegevus. Selline järkjärguline lähenemisviis võimaldab välja selgitada ka **lüngad** vajalikus võimekuses ja tegevuskorras, mis takistavad küberkriisile tõhusat reageerimist.

Joonisel 2 ([2]) on esitatud IPCRi toimimise diagramm. Sellel on uued elemendid esitatud sinisel taustal.

([1]) Vastavalt eesistujariigi sõprade rühmas heaks kiidetud dokumendile 12607/15 „IPCRi standardne töökord“, mis esitati COREPERile 2015. aasta oktoobris.
([2]) Lisas on sama joonis esitatud suuremana.

Joonis 2

Küberturvalisuse elemendid IPRCs



Märkus. Kuna kübervaldkonna hübriidohtude laad on selline, et nad on kavandatud jääma alla kriisiks tunnistamise künnist, peab EL rakendama ennetus- ja valmisolekut parandavaid meetmeid. ELi hübriidohtude ühisüksuse ülesanne on selliseid intsidente kiiresti analüüsida ning teavitada asjakohaseid koordineerimisstruktuure. Hübriidohtude ühisüksus esitab korrapäraselt aruandeid, mida saab kasutada valmisoleku parandamiseks valdkondliku poliitika raames.

— **1. samm: pidev jälgimine ja hoiatamine valdkonniti**: juba praegu esitatakse olukorra kohta korrapäraselt aruandeid ja hoiatusi, millest nõukogu eesistujariik võib järeldada kriisi tekkimist ja võimalikku kulgemist.

— **Väljaselgitatud lünk**: praegu ei esitata ELi tasandil korrapäraselt ja koordineeritult aruandeid küberturvalisuse olukorra kohta ega hoiatusi küberintsidentide ja -ohtude kohta.

— **Tegevuskava: ELi küberturvalisuse olukorra seire ja aruandlus**

— ENISA koostab küberintsidentide ja -ohtude kohta korrapäraselt **ELi küberjulgeoleku olukorra tehnilise aruande**. Ta tugineb avalikult kättesaadavale teabele, oma analüüsi tulemustele ja aruannetele, mille on kättesaadavaks teinud liikmesriikide CSIRTid (vabatahtlikkuse alusel), ELi võrgu- ja infoturbedirektiivi alusel loodud ühtsed kontaktpunktid, Europoli küberkuritegevuse vastase võitluse Euroopa keskus (EC3), CERT-EU ja Euroopa välisteenistuse (EEAS) juures asuv Euroopa Liidu luureandmete analüüsi keskus (INTCEN). Aruanne peaks olema kättesaadav nõukogu asjakohastele organitele, komisjonile ja CSIRTide võrgustikule.

— ELi hübriidohtude ühisüksuse ülesanne oleks SIACi nimel koostada **ELi küberjulgeoleku olukorra operatiivaruanne**. Aruannet kasutataks ka pahatahtlikule kübertegevusele reageerimise ELi ühise diplomaatilise reageerimise raamistikus.

— Mõlemad aruanded edastatakse ELi ja liikmesriikide sidusrühmadele, kes saavad neid kasutada oma riigi olukorrateadlikkuse parandamiseks ja otsuste tegemiseks, samuti piirkondlikus piiriüleses koostöös.

Pärast intsidendi avastamist

— **2. samm: analüüs ja nõuanded**: olemasoleva seire- ja hoiatusteabe alusel hoiavad komisjoni talitused, Euroopa välisteenistus ja nõukogu peasekretariaat üksteist sündmustega kursis, et olla valmis teavitama eesistujariiki vajadusest aktiveerida IPCR kas täis- või teabevahetusrežiimis.

  — **Tegevuskava**

    — Komisjoni puhul sidevõrkude, sisu ja tehnoloogia peadirektoraat, rände ja siseasjade peadirektoraat ja informaatika peadirektoraat; neid toetavad ENISA, EC3 ja CERT-EU.

    — Euroopa välisteenistus. Tuginedes ELi vaatluskeskuse (SITROOM) ja luureallikate tööle, tagab ELi hübriidohtude ühisüksus olukorrateadlikkuse ELi ja tema partnereid ähvardavatest või ähvardada võivatest hübriidohtudest, sealhulgas küberohtudest. Seega kui ELi hübriidohtude ühisüksuse analüüs ja hinnangud näitavad, et mõnda liikmesriiki, partnerriiki või organisatsiooni võib ähvardada küberoht, teavitab INTCEN neid kehtestatud korra kohaselt esmalt operatiivtasandil. Seejärel töötatakse operatiivtasandil välja soovitused poliitilise/strateegilise tasandi jaoks. Soovitustes käsitletakse muu hulgas kriisihalduskava aktiveerimist seirerežiimis (näiteks Euroopa välisteenistuse kriisidele reageerimise mehhanismi rakendamine või IPCRi seireotstarbelise veebilehe loomine).

    — CSIRTde võrgustiku eesistuja koostab ENISA abil ELi küberturvalisuse olukorda käsitleva aruande ([1]). Roteeruva eesistujariigi CSIRT esitab selle eesistujariigile, komisjonile ning liidu välisasjade ja julgeolekupoliitika kõrgele esindajale.

— **3. samm: IPRC aktiveerimise analüüs/otsus IPCR aktiveerimise kohta**: eesistujariik hindab, kas poliitiline koordineerimine, teabevahetus ja otsuste tegemine peaks toimuma ELi tasandil. Sel eesmärgil võib eesistujariik kutsuda kokku mitteametliku ümarlauakohtumise. Eesistujariik määrab esialgu kindlaks valdkonnad, kuhu tuleb kaasata COREPER või nõukogu. Sellest lähtutakse integreeritud olukorrateadlikkuse ja analüüsi aruannete koostamise suuniste väljatöötamisel. Võttes arvesse kriisi laadi, selle võimalikke tagajärgi ja sellest tulenevaid poliitilisi vajadusi, otsustab eesistujariik, kas tuleks kokku kutsuda asjaomaste nõukogu töörühmade ja/või COREPERi ja/või poliitika- ja julgeolekukomitee koosolek.

  — **Tegevuskava**

    — Ümarlaual osalejad:

      — komisjoni talitused ja Euroopa välisteenistus nõustavad eesistujariiki oma pädevusvaldkondadesse kuuluvates küsimustes.

      — Liikmesriikide esindajad horisontaalses küberküsimuste töörühmas, keda abistavad riikide eksperdid (CSIRTid, pädevad küberjulgeolekuasutused, muud).

      — Integreeritud olukorrateadlikkuse ja analüüsi aruanded poliitiliste ja strateegiliste suuniste koostamiseks põhinevad ELi küberturvalisuse olukorda käsitleval aruandel ja ümarlaual osalejate esitataval lisateabel.

      — Asjaomased töörühmad ja komiteed:

        — horisontaalne küberküsimuste töörühm.

  Komisjon, Euroopa välisteenistus ja nõukogu peasekretariaat võivad omavahelisel täielikul kokkuleppel ja koostöös eesistujariigiga ka otsustada aktiveerida IPCR teabevahetusrežiimis, luues kriisi veebilehe. Sellega valmistatakse ette IPCRi rakendamist täisrežiimis, kui seda peaks vaja olema.

— **4. samm: IPCRi aktiveerimine / teabe kogumine ja vahetamine**: kui IPCR aktiveeritakse (kas täis- või teabevahetusrežiimis), luuakse IPCRi veebiplatvormil kriisi veebileht, mille kaudu vahetatakse teavet eelkõige küsimustes, mis vastavad integreeritud olukorrateadlikkuse ja analüüsi eesmärkidele ning aitavad ette valmistada arutelu poliitilisel tasandil. See, milline talitus vastutab integreeritud olukorrateadlikkuse ja analüüsi eest (mõni komisjoni talitus või Euroopa välisteenistus), sõltub juhtumi asjaoludest.

— **5. samm: integreeritud olukorrateadlikkuse ja analüüsi aruande koostamine**: alustatakse integreeritud olukorrateadlikkuse ja analüüsi aruande koostamist. Komisjon / Euroopa välisteenistus esitab integreeritud olukorrateadlikkuse

([1]) ELi küberturvalisuse olukorda käsitlev aruanne on kokkuvõte liikmesriikide CSIRTide olukorraaruannetest. Aruande ülesehitus tuleks ette näha CSIRTide võrgustiku standardse töökorraga.

ja analüüsi standardses töökorras kirjeldatud integreeritud olukorrateadlikkuse ja analüüsi aruanded ja võib algatada teabevahetuse IPCRi veebiplatvormi kaudu või taotleda konkreetse teabe esitamist. Integreeritud olukorrateadlikkuse ja analüüsi aruanded koostatakse vastavalt eesistujariigi suunistele ja tema määratud konkreetse poliitilise tasandi (COREPERi või nõukogu) vajadustele. Eesmärk on saada olukorrast strateegiline ülevaade ja rajada eesistujariigi poolt kindlaks määratud päevakorrapunktides toimuv arutelu konkreetsele teabele. Olenevalt küberkriisi laadist otsustatakse integreeritud olukorrateadlikkuse ja analüüsi standardse töökorra kohaselt, kas integreeritud olukorrateadlikkuse ja analüüsi aruande koostab mõni komisjoni talitus (sidevõrkude, sisu ja tehnoloogia peadirektoraat või rände ja siseasjade peadirektoraat) või Euroopa välisteenistus.

Kui IPCR aktiveeritakse, määrab eesistujariik kindlaks konkreetsed valdkonnad, millele integreeritud olukorrateadlikkuse ja analüüsi aruandes keskendutakse, et toetada poliitilist koordineerimist ja otsustusprotsessi nõukogus. Pärast konsulteerimist komisjoni talituste või Euroopa välisteenistusega määrab eesistujariik kindlaks ka aruande esitamise tähtaja.

— **Tegevuskava:**

— integreeritud olukorrateadlikkuse ja analüüsi aruande koostamisel võetakse arvesse tööd, mida on teinud asjaomased talitused, sealhulgas:

— CSIRTide võrgustik (ELi küberturvalisuse olukorda käsitlev aruanne);

— EC3, SITROOM, ELi hübriidohtude ühisüksus, CERT-EU. ELi hübriidohtude ühisüksus annab vastavalt vajadusele abi ja esitab kaastööd integreeritud olukorrateadlikkuse ja analüüsi juhttalitusele ja IPCRi ümarlauale;

— ELi valdkondlikud ametid ja organid sõltuvalt sektorist, kus oht on tekkinud;

— liikmesriikide ametiasutused (v.a CSIRTid);

— andmete kogumine integreeritud olukorrateadlikkuse ja analüüsi aruande jaoks ([1]):

— komisjon ja ELi ametid: integreeritud olukorrateadlikkuse ja analüüsi sisemine tuumvõrk on IT-süsteem ARGUS. ELi ametid saadavad oma kaastöö oma vastutavatele peadirektoraatidele, kes sisestavad asjakohased andmed ARGUSesse. Komisjoni talitused ja ametid koguvad teavet olemasolevatest, koos liikmesriikide ja rahvusvaheliste organisatsioonidega loodud valdkondlikest võrgustikest ja muudest asjakohastest allikatest;

— Euroopa välisteenistus: integreeritud olukorrateadlikkuse ja analüüsi sisemine tuumvõrk ja ühtne kontaktpunkt on ELi vaatluskeskus, keda toetavad muud asjaomased Euroopa välisteenistuse osakonnad. Euroopa välisteenistus kogub teavet kolmandatest riikidest ja asjaomastest rahvusvahelistest organisatsioonidest.

— **6. samm: eesistujariigi mitteametliku ümarlaua kohtumise ettevalmistamine**: eesistujariigi mitteametliku ümarlaua kohtumise aja, päevakorra, osalejad ja oodatavad eesmärgid (tulemused) määrab kindlaks eesistujariik, keda abistab nõukogu peasekretariaat. Nõukogu peasekretariaat edastab eesistujariigi nimel asjakohase teabe IPCRi veebiplatvormile ja teavitab kohtumise toimumisest.

— **7. samm: eesistujariigi ümarlaud / ELi poliitilise koordineerimise/otsustamise ettevalmistavad meetmed**: eesistujariik kutsub kokku mitteametliku ümarlaua, kus analüüsitakse olukorda ning koostatakse ja vaadatakse läbi COREPERile või nõukogule esitatavad päevakorrapunktid. Eesistujariigi mitteametlik ümarlaud on ühtlasi foorum, kus töötatakse välja ning vaadatakse ja arutatakse läbi COREPERile või nõukogule esitatavad meetmete ettepanekud.

— **Tegevuskava:**

— horisontaalne küberküsimuste töörühm valmistab ette poliitika- ja julgeolekukomitee või COREPERi koosoleku.

— **8. samm: poliitiline kooskõlastamine ja otsuste tegemine COREPERis või nõukogus**: COREPERi või nõukogu istungite tulemuseks on vastumeetmete koordineerimine kõikidel tasanditel, otsused erakorraliste meetmete kohta, poliitilised deklaratsioonid jms. Need otsused kujutavad endast ka ajakohaseid poliitilisi ja strateegilisi suuniseid, millest lähtutakse integreeritud olukorrateadlikkuse ja analüüsi aruannete koostamisel.

— **Tegevuskava:**

— poliitilist otsust koordineerida reageerimist küberkriisile rakendavad avaliku sektori osalejad, kes rakendavad 1. jaos pealkirja „Koostöö strateegilisel/poliitilisel, operatiiv- ja tehnilisel tasandil“ all kirjeldatud **reageerimise** ja **avaliku kommunikatsiooni** meetmeid;

— **olukorrateadlikkuse** küsimuses jätkub integreeritud olukorrateadlikkuse ja analüüsi aruannete koostamisel koostöö tehnilisel, operatiiv- ja poliitilisel/strateegilisel tasandil, nagu on kirjeldatud 1. jaos.

([1]) Integreeritud olukorrateadlikkuse ja analüüsi standardsed töökorrad.

— **9. samm: mõju seire**: integreeritud olukorrateadlikkuse ja analüüsi eest vastutav talitus koos muude integreeritud olukorrateadlikkuse ja analüüsiga tegelejatega annab teavet kriisi kulgemise ning tehtud poliitiliste otsuste mõju kohta. Tegemist on pideva tagasiside tsükliga, mida võetakse arvesse vastavalt kriisi kulgemisele ja mida eesistujariik arvestab otsuse tegemisel selle kohta, kas ELi poliitilise tasandi osalemine peaks jätkuma või võib IPCRi rakendamist hakata järk-järgult lõpetama.

— **10. samm: järkjärguline lõpetamine**: eesistujariik võib IPCRi rakendamise järkjärguliseks lõpetamiseks kokku kutsuda mitteametliku ümarlauakohtumise, et analüüsida, kas selle korra rakendamist tuleks jätkata või mitte. Ümarlauakohtumine kutsutakse kokku sama korra kohaselt kui ümarlauakohtumine korra rakendamise otsustamiseks. Eesistujariik võib otsustada korra rakendamist piirata või see täielikult lõpetada.

— **Tegevuskava:**

— ENISAt võib paluda intsidendi lõppemise järel koostada selle tehniline analüüs või osaleda analüüsi läbiviimisel vastavalt oma volitustele.

LIIDE

1. KRIISIHALDUS, KOOSTÖÖMEHHANISMID JA ELI TASANDI OSALEJAD

Kriisihaldusmehhanismid

Kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord (IPCR): 25. juunil 2013 kiitis nõukogu heaks kriisidele poliitilise reageerimise integreeritud korra, ([1]) mille eesmärk on tagada suure kriisi korral õigeaegne koordineerimine ja reageerimine ELi poliitilisel tasandil. IPCR võimaldab ka koordineerimist poliitilisel tasandil, kui võetakse kasutusele solidaarsusklausel (ELi toimimise lepingu artikkel 222), nagu on kindlaks määratud nõukogu 24. juuni 2014. aasta otsuses 2014/415/EL solidaarsusklausli liidupoolse rakendamise korra kohta. Aktiveerimise kord ja järgnev tegevus on sätestatud ICPRi standardsetes töökordades ([2]).

ARGUS: Euroopa Komisjoni poolt 2005. aastal loodud kriisidele reageerimise koordineerimise süsteem, mille raames on ette nähtud konkreetne tegevuse koordineerimise kord valdkondadeülese kriisi korral. Seda toetab samanimeline IT-vahend – üldine kiirhoiatussüsteem. ARGUS on kaheetapiline, kusjuures II etapi (suur valdkondadeülene kriis) puhul kutsutakse kokku kriisikoordineerimiskomitee, kes tegutseb komisjoni presidendi või selleks volitatud voliniku alluvuses. Kriisikoordineerimiskomitee ülesanne on juhtida ja koordineerida komisjoni reageerimist kriisile ning sellesse kuuluvad komisjoni asjaomaste peadirektoraatide, kabinettide ja muude ELi teenistuste esindajad. Kriisikoordineerimiskomiteed juhatab asepeasekretär. Komitee analüüsib olukorda, kaalub eri reageerimisvõimalusi, teeb täitmisele kuuluvaid otsuseid komisjoni nimel ELi vahendite ja instrumentide kasutuselevõtuks ning tagab otsuste elluviimise ([3]) ([4]).

Euroopa välisteenistuse kriisidele reageerimise mehhanism: Euroopa välisteenistuse kriisidele reageerimise mehhanism on Euroopa välisteenistuse struktureeritud süsteem reageerimiseks välis- või olulise välismõõtmega kriisidele ja hädaolukordadele, sealhulgas hübriidohtudele, mis mõjutavad või võivad mõjutada ELi või mõne liikmesriigi huve. Kuna kriisidele reageerimise mehhanismi kohtumistel osalevad komisjoni ja nõukogu sekretariaadi asjaomased ametnikud, soodustab mehhanism diplomaatiliste, julgeoleku- ja kaitsealaste jõupingutuste vahelist sünergiat komisjoni hallatavate finants-, kaubandus- ja koostööinstrumentidega. Kriisi ajal võidakse kasutada ka kriisiüksust.

Koostöömehhanismid

CSIRTide võrgustik: küberintsidentide lahendamise üksuste võrgustikku (CSIRTide võrgustik) kuuluvad kõikide liikmesriikide ja valitsusasutuste CSIRTide ja CERT-EU esindajad. Võrgustiku eesmärk on võimaldada ja tõhustada CSIRTide-vahelist teabevahetust ohtude ja küberintsidentide kohta ning teha koostööd küberintsidentidele ja -kriisidele reageerimisel.

Horisontaalne küberküsimuste töörühm: töörühm loodi nõukogus kübervaldkonna strateegiliseks ja horisontaalseks koordineerimiseks ja seda võib kaasata nii seadusandlikku kui ka muusse tegevusse.

Osalejad

ENISA: Euroopa Liidu Võrgu- ja Infoturbeamet loodi 2004. aastal. Amet teeb tihedat koostööd liikmesriikide ja erasektoriga, pakkudes nõuandeid ja lahendusi näiteks üleeuroopaliste küberjulgeolekuõppuste, riikliku küberjulgeoleku strateegia väljatöötamise, CSIRTide koostöö ja suutlikkuse suurendamise küsimustes. ENISA teeb vahetut koostööd kogu ELi CSIRTidega ja on ka CSIRTide võrgustiku sekretariaadi liige.

ERCC: hädaolukordadele reageerimise koordineerimiskeskus (mis on Euroopa kodanikukaitse ja humanitaarabioperatsioonide peadirektoraadi (ECHO) alluvuses) toetab ja koordineerib mitmesuguseid ennetus-, valmisoleku- ja reageerimismeetmeid iga päev ööpäev läbi. See alustas tegevust 2013. aastal ja kujutab endast komisjoni kriisidele reageerimise keskust suhtlemisel ELi kriisitalitustega. Lisaks on ta IPCRi keskne kontaktpunkt, mis toimib iga päev ööpäev läbi.

([1]) 10708/13 „Kriiside koordineerimise korra läbivaatamise lõpuleviimine: kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord“ (nõukogus heaks kiidetud 24. juunil 2013).
([2]) 12607/15 „IPCRi standardne töökord“ (heaks kiidetud eesistujariigi sõprade rühmas ja esitatud COREPERile 2015. aasta oktoobris).
([3]) Komisjoni sätted üldise kiirhoiatussüsteemi ARGUS kohta, KOM(2005) 662 (lõplik), 23. detsember 2005.
([4]) Komisjoni 23. detsembri 2005. aasta otsus 2006/25/EÜ, Euratom, millega muudetakse komisjoni töökorda (ELT L 19, 24.1.2006, lk 20), millega luuakse üldine kiirhoiatussüsteem ARGUS.

Europol/EC3: 2013. aastal loodi Europolis küberkuritegevuse vastase võitluse Euroopa keskus (EC3), mis aitab õiguskaitseasutustel võidelda küberkuritegevusega ELis. EC3 pakub operatiiv- ja analüütilist tuge uurimiste läbiviimiseks liikmesriikides. See on kuritegusid puudutava ja luureteabe keskus, mis pakub liikmesriikidele operatsioonide ja uurimiste läbiviimiseks operatiivanalüüsi, koordineerimist ja eksperditeadmisi ning ülimalt spetsiifilist tehnilist ja digitaalset kohtueksperti tasemel abi.

CERT-EU: selle ELi institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma ülesanne on parandada ELi institutsioonide, organite ja ametite kaitset küberohtude eest. Ta on CSIRTide võrgustiku liige. CERT-EU-l on küberohte käsitleva teabe vahetamiseks tehnilised kokkulepped NATO CIRCi, teatavate kolmandate riikide ja oluliste küberjulgeoleku valdkonna ettevõtetega.

Ühtse luureandmete analüüsivõime (SIAC) lepingu kohaselt kuuluvad ELi luureasutuste ühendusse ELi luureandmete analüüsi keskus (**INTCEN**) ja ELi sõjalise staabi luureosakond (EUMS INT). SIACi ülesanne on pakkuda Euroopa Liidu välisasjade ja julgeolekupoliitika kõrgele esindajale ja Euroopa välisteenistusele luureandmete analüüse, varajasi hoiatusi ja olukorrateadlikkust. SIAC pakub oma teenuseid ka ühise välis- ja julgeolekupoliitika (ÜVJP), ühise julgeoleku- ja kaitsepoliitika (ÜJKP) ja terrorismivastase võitluse valdkonnas otsuseid tegevatele ELi asutustele ning liikmesriikidele. EU INTCEN ja EUMS INT ei ole operatiivasutused ega tegele andmete kogumisega. Luureandmete kogumisteks tehtav operatiivtöö kuulub liikmesriikide pädevusse. SIAC tegeleb ainult strateegilise analüüsiga.

ELi hübriidohtude ühisüksus: 2016. aasta aprilli ühisteatisega hübriidohtudega võitlemise kohta nimetati ELi hübriidohtude ühisüksus ELi hübriidohte käsitlevate algandmete analüüsi keskuseks. Komisjon kiitis selle volitused heaks 2016. aasta detsembris talitustevahelise konsulteerimise teel. ELi hübriidohtude ühisüksus tegutseb INTCENi juures ja kuulub SIACi. Seega toimib ta koos EUMS INTiga ja selle koosseisu on määratud alaline sõjaväeline liige. Hübriidoht on oht, mille puhul teadlikult kasutatakse riiklike ja mitteriiklike osalejate ning mitmesuguste varjatud ja avalike ning sõjaväeliste ja tsiviilvaldkonna vahendite kombinatsiooni – küberrünnakuid, desinformatsiooni kampaaniaid, spionaaži, majanduslikku survet, kolmandate osapoolte jõude ja muud õõnestustegevust. ELi hübriidohtude ühisüksusel on komisjonis ja liikmesriikides ulatuslik kontaktpunktide võrk, mis võimaldab tal pakkuda integreeritud reageerimist ja kogu valitsemissektorit hõlmavat lähenemisviisi, et võidelda mitmetahuliste probleemidega.

ELi vaatluskeskus (SITROOM): ELi vaatluskeskus tegutseb ELi luureandmete analüüsi keskuse (EU INTCEN) koosseisus ning annab Euroopa välisteenistusele operatiivsuutlikkuse kriisidele kiire ja tõhusa reageerimise tagamiseks. See on alaline tsiviil-sõjaline organ, mis pakub üleilmset seiret ja olukorrateadlikkust iga päev ööpäev läbi.

Asjakohased vahendid

Pahatahtlikule kübertegevusele reageerimise ELi ühine diplomaatiline raamistik: see 2017. aasta juunis heaks kiidetud raamistik kuulub ELi küberdiplomaatia lähenemisviisi, mis aitab kaasa konfliktide ennetamisele, küberohtude leevendamisele ja rahvusvahelistes suhetes stabiilsuse suurendamisele. Raamistikus on ette nähtud kõigi välis- ja julgeolekupoliitika meetmete, sealhulgas vajaduse korral piiravate meetmete kasutamine. Raamistiku meetmete eesmärk on edendada koostööd, hõlbustada vahetute ja pikaajaliste ohtude leevendamist ning avaldada kuriteo ja võimalikele rünnaku toimepanijatele mõju pikas perspektiivis.

2. KÜBERJULGEOLEKU KRIISIDE KOORDINEERIMINE IPCRI RAAMES – HORISONTAALNE KOORDINATSIOONITASAND JA POLIITILISE REAKTSIOONI SÜVENDAMINE

IPCRi on kasutatud ja kasutatakse tehniliste ja operatiivprobleemide lahendamiseks, kuid ainult lähtudes poliitilisest/strateegilisest vaatenurgast.

Kui kriis laieneb, võib IPCRi seirerežiimilt üle minna teabevahetusrežiimile (mis on IPCRi aktiveerimise esimene tase) ja IPCRi täisrežiimile.

Täisrežiimis aktiveerimise kohta teeb otsuse ELi nõukogu rotatsiooni korras vahetuv eesistujariik. Komisjon, Euroopa välisteenistus ja nõukogu peasekretariaat võivad aktiveerida IPCRi teabevahetusrežiimis. Seire- ja teabevahetusrežiimis

võetakse kasutusele erinevad teabevahetuse tasandid, kusjuures teabevahetusrežiimis tekib vajadus integreeritud olukorra-teadlikkuse ja analüüsi aruannete järele. Kui IPCR aktiveeritakse täisrežiimis, võetakse kasutusele veel üks vahend – ümarlauakohtumised, millel osaleb ka eesistujariik (tavaliselt COREPER II eesistuja või teema asjatundja alalise esinduse nõuniku tasemel, kuid erandkorras on ümarlaudu peetud ka ministrite tasandil).

Osalejad

Juhataja – rotatsiooni korras vahetuv eesistujariik (tavaliselt COREPERi eesistuja)

Euroopa Ülemkogu poolt eesistuja kabinet

Euroopa Komisjoni poolt asepeasekretäri/peadirektoraadi tasand ja/või teemaeksperdid

Euroopa välisteenistuse poolt asepeasekretäri/tegevdirektori tasand ja/või teemaeksperdid

Nõukogu peasekretariaadi puhul peasekretäri kabinet, IPCRi üksus ja vastutavad peadirektoraadid.

Tegevuse ulatus: kõigil kolmel tasandil luuakse ühine terviklik ülevaade olukorrast ning suurendatakse teadlikkust kitsaskohtadest ja puudustest, et need lahendada poliitilisel tasandil, tehes ümarlauas need otsused, mis kuuluvad osalejate pädevusse, või esitades ettepanekud nende meetmete kohta, mida saavad võtta teised – COREPER II-st kuni nõukoguni.

Ühine olukorrateadlikkus:

(kui IPCRi ei ole aktiveeritud): võib luua IPCRi seirelehed, mille kaudu jälgitakse olukorda, mis võib muutuda ELi mõjutavaks kriisiks;

(IPCRi teabevahetusrežiim): integreeritud olukorrateadlikkuse ja analüüsi juhttalitus koostab integreeritud olukorra-teadlikkuse ja analüüsi aruandeid komisjoni talitustelt, Euroopa välisteenistuselt ja liikmesriikidelt saadud teabe alusel. Teavet saadakse IPCRi küsimustike kaudu;

(IPCRi täisrežiim): koostatakse integreeritud olukorrateadlikkuse ja analüüsi aruandeid ning lisaks korraldatakse puuduste ja kitsaskohtade arutamiseks mitteametlikke IPCRi ümarlaudu, kus osalevad liikmesriikide asjakohased talitused, komisjon, Euroopa välisteenistus, asjaomaste ametid jt.

Koostöö ja reageerimine:

olenevalt intsidendi laadist ja mõjust aktiveeritakse/ühtlustatakse täiendavad kriisihaldusmehhanismid ja -vahendid, näiteks kodanikukaitse mehhanism, pahatahtlikule kübertegevusele reageerimise ELi ühine diplomaatiline raamistik või hübriidohtudega võitlemise ühine raamistik.

Kriisiolukorras teavitamine:

pärast konsulteerimist komisjoni asjaomaste talituste, nõukogu peasekretariaadi ja Euroopa välisteenistusega võib eesistujariik aktiveerida IPCRi kriisiteavitusvõrgustiku eesmärgiga toetada ühiste sõnumite koostamist. Ta võib ka teha ettepanekuid kõige tulemuslikumate kommunikatsioonivahendite kasutamiseks.

3. KÜBERKRIISI HALDAMINE ARGUSE KAUDU – EUROOPA KOMISJONI SISENE TEABEVAHETUS

Pärast Euroopa tasandil meetmete võtmist nõudvaid ootamatuid kriise, nagu terrorirünnakud Madridis 2004. aasta märtsis, Kagu-Aasia tsunami 2004. aasta detsembris ja terrorirünnakud Londonis 2005. aasta juulis, lõi komisjon 2005. aastal koordineerimissüsteemi ARGUS koos samanimelise üldise kiirhoiatussüsteemiga [1] [2]. Selle eesmärk on tagada konkreetse **kriisi koordineerimine** mitut valdkonda hõlmava ulatusliku kriisi korral, et võimaldada reaalajas vahetada kriisiga seotud teavet ja teha kiiresti otsuseid.

ARGUSe süsteemi raames eristatakse juhtumi raskusastmest olenevalt kahte etappi.

I etapp: teabevahetus väikse kriisi puhul

[1] Euroopa Komisjoni 23. detsembri 2005. aasta teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele: „Komisjoni sätted üldise kiirhoiatussüsteemi ARGUS kohta“, KOM(2005) 662 (lõplik).

[2] Otsus 2006/25/EÜ, Euratom.

Hiljutiste I etapis teatavaks tehtud sündmuste hulka kuuluvad näiteks metsatulekahjud Portugalis ja Iisraelis, 2016. aasta terrorirünnak Berliinis, üleujutused Albaanias, orkaan Matthew Haitil ja põud Boliivias. I etapi sündmuse saab avada iga peadirektoraat, kui ta leiab, et olukord tema pädevusvaldkonda kuuluvates küsimustes on piisavalt tõsine, et selle kohta teavet vahetada. Nii näiteks võivad I etapi sündmuse avada sidevõrkude, sisu ja tehnoloogia peadirektoraat ning rände ja siseasjade peadirektoraat, kui nad leiavad, et olukord nende pädevusvaldkonda kuuluvates küsimustes on piisavalt tõsine, et selle kohta teavet vahetada.

II etapp: käivitatakse suure, mitut valdkonda hõlmava kriisi ja liitu ähvardava ennustatava või vahetu ohu puhul.

II etapis käivitatakse konkreetne koordineerimisprotsess asjaomase pädevusvaldkonna kõrgeimal tasandil ja koostöös teiste institutsioonidega, et komisjon saaks vastu võtta otsused ning korraldada kiire, koordineeritud ja järjekindla reageerimise. II etapp võetakse kasutusele mitut valdkonda hõlmava suure kriisi või ennustatava või vahetu suure kriisi tekkimise ohu puhul. Tegelikult toimunud II etapi sündmused on näiteks 2015. aastal alanud ja seni kestev rände- ja pagulaskriis, Fukushima kolmikkatastroof 2011. aastal ja Islandi Eyjafjallajökulli vulkaani purse 2010. aastal.

II etapi aktiveerib president omal algatusel või komisjoni liikme taotlusel. President võib määrata komisjoni reageerimise eest poliitiliseks vastutajaks kriisiga enim seotud valdkonda juhtiva voliniku või otsustada, et vastutab ise.

Ette on nähtud kriisikoordineerimiskomitee erakorraliste koosolekute korraldamine. Need kutsutakse kokku presidendi või selle komisjoni liikme alluvuses, kelle pädevusse see juhtum on antud. Koosolekud kutsub kokku peasekretariaat IT-vahendi ARGUS kaudu. Kriisikoordineerimiskomitee on spetsiaalne kriiside reguleerimise toimimisstruktuur, mis on loodud selleks, et juhtida ja kooskõlastada kriisile reageerimist ning ühendada asjaomaste komisjoni peadirektoraatide, kabinettide ja talituste esindajaid. Kriisikoordineerimiskomiteed juhatab asepeasekretär. **Komitee analüüsib olukorda, kaalub eri reageerimisvõimalusi ning tagab otsuste elluviimise** ja selle, et reageerimine on sidus ja järjekindel. Kriisikoordineerimiskomitee tegevust toetab peasekretariaat.

4. EUROOPA VÄLISTEENISTUSE KRIISIDELE REAGEERIMISE MEHHANISM

Euroopa välisteenistuse kriisidele reageerimise mehhanism aktiveeritakse sellise raske juhtumi või hädaolukorra puhul, mis mõjutab mingil viisil ELi välismõõdet. Asepeasekretär aktiveerib kriisidele reageerimise mehhanismi pärast konsulteerimist liidu välisasjade ja julgeolekupoliitika kõrge esindaja või peasekretäriga. Kriisidele reageerimise mehhanismi käivitamist võivad kriisidele reageerimise eest vastutavalt asepeasekretärilt taotleda ka liidu välisasjade ja julgeolekupoliitika kõrge esindaja, peasekretär või mõni muu asepeasekretär ja tegevdirektor.

Kriisidele reageerimise mehhanism aitab kaasa sellele, et julgeolekustrateegia kohane ELi reageerimine kriisidele on sidus. Kriisidele reageerimise mehhanism soodustab diplomaatiliste, julgeoleku- ja kaitsealaste jõupingutuste vahelist sünergiat komisjoni hallatavate finants-, kaubandus- ja koostööinstrumentidega.

Kriisidele reageerimise mehhanism on seotud komisjoni üldise hädaolukordadele reageerimise süsteemiga ARGUS ja IPCRiga, mille samaaegne aktiveerimine võimaldab saavutada sünergiat. Euroopa välisteenistuse vaatluskeskus toimib välisteenistuse ning nõukogu ja komisjoni hädaolukordadele reageerimise süsteemide vahelise teabevahetuskeskusena.

Tavaliselt algab kriisidele reageerimise mehhanismi rakendamine Euroopa välisteenistuse, komisjoni ja nõukogu kriisiga seotud tippjuhtide **kriisikoosoleku** kokkukutsumisega. Kriisikoosolekul analüüsitakse kriisi lühiajalist mõju ja võidakse otsustada kiireloomuliste meetmete võtmine, kriisiüksuse kasutamine või kriisiplatvormi kokkukutsumine. Seda võib teha mis tahes järjekorras.

Kriisiüksus on väikesearvuline operatiivüksus, kuhu kuuluvad Euroopa välisteenistuse, komisjoni ja nõukogu kriisile reageerimisega seotud talitused. Kriisiüksus jälgib pidevalt olukorda, toetades Euroopa välisteenistuse peakorteri otsusetegijaid. Oma tegutsemise ajal toimib kriisirühm iga päev ööpäev läbi.

Kriisiplatvorm ühendab Euroopa välisteenistuse, komisjoni ja nõukogu asjaomaseid teenistusi, kes analüüsivad kriiside keskpikka ja pikaajalist mõju ning lepivad kokku, milliseid meetmeid võetakse. Kriisiplatvormi juhib liidu välisasjade ja julgeolekupoliitika kõrge esindaja, peasekretär või kriisidele reageerimise eest vastutav asepeasekretär. Kriisiplatvorm analüüsib ELi meetmete mõju kriisist mõjutatud riigile või piirkonnale, langetab otsuseid lisameetmete võtmise kohta ja arutab nõukogu meetmete kohta esitatud ettepanekuid. Kriisiplatvorm toimib *ad hoc* koosolekutena ega tegutse pidevalt.

Töökond koosneb reageerimisega seotud talituste esindajatest ja seda võib kasutada ELi reageerimise jälgimiseks ja reageerimisele kaasaaitamiseks. Töökond analüüsib ELi meetmete mõju, valmistab ette poliitika- ja reageerimisvõimalusi käsitlevaid dokumente, aitab ette valmistada kriisiga tegelemise poliitilist raamistikku, osaleb teavitamise strateegia väljatöötamises ning teeb muid ELi reageerimist soodustavaid korraldusi.

5. KASUTATUD DOKUMENDID

Allpool on esitatud loetelu dokumentidest, mida on kasutatud tegevuskava ettevalmistamisel.

— The European Cyber Crises Cooperation Framework, Version 1 (17. oktoober 2012)

— Report on Cyber Crisis Cooperation and Management (ENISA, 2014)

— Actionable Information for Security Incident Response (ENISA, 2014)

— Common practices of EU-level crisis management and applicability to cyber crises (ENISA, 2015)

— Strategies for Incident Response and Cyber Crisis Cooperation (ENISA, 2016)

— EU Cyber Standard Operating Procedures (ENISA, 2016)

— A good practice guide of using taxonomies in incident prevention and detection (ENISA, 2017)

— Teatis „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“ (COM(2016) 410 final, 5. juuli 2016)

— Nõukogu järeldused Euroopa kübervastupidavusvõime süsteemi tugevdamise ning konkurentsivõimelise ja uuendusliku küberjulgeolekusektori toetamise kohta (15. november 2016, 14540/16)

— Nõukogu 24. juuni 2014. aasta otsus 2014/415/EL solidaarsusklausli liidupoolse rakendamise korra kohta (ELT L 192, 1.7.2014, lk 53)

— Kriiside koordineerimise korra läbivaatamise lõpuleviimine: ELi integreeritud poliitiline kriisidele reageerimise kord (IPCR) (10708/13, 7. juuni 2013)

— Integrated Situational Awareness and Analysis (ISAA) – Standard Operating Procedures (DS 1570/15, 22. oktoober 2015)

— Komisjoni sätted üldise kiirhoiatussüsteemi ARGUS kohta (KOM(2005) 662 (lõplik), 23. detsember 2005)

— Komisjoni 23. detsembri 2005. aasta otsus 2006/25/EÜ,Euratom, millega muudetakse komisjoni töökorda (ELT L 19, 24.1.2006, lk 20)

— ARGUS Modus Operandi (Euroopa Komisjon, 23. oktoober 2013)

— Nõukogu järeldused pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku kohta („küberdiplomaatia meetmete kogum“), dokument 9916/17

— EU operational protocol for countering hybrid threats 'EU Playbook' (SWD(2016) 227)

— EEAS Crisis Response Mechanism (8. november 2016, Ares(2017)880661). Talituste ühine töödokument „EU operational protocol for countering hybrid threats, 'EU Playbook'“ (SWD(2016) 227 final, 5. juuli 2016)

— Ühisteatis Euroopa Parlamendile ja nõukogule: „Hübriidohtudega võitlemise ühine raamistik – Euroopa Liidu lahendus“ (JOIN/2016/18 final, 6. aprill 2016)

— EEAS(2016) 1674 – Working Document of the European External Action Service – EU Hybrid Fusion Cell – Terms of Reference

6. KÜBERTURVALISUSE ELEMENDID IPCRIS