Euroopa Liidu
Nõukogu

Brüssel, 19. november 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	19. november 2018
Saaja:	Delegatsioonid
Teema:	ELi küberkaitsepoliitika raamistik (ajakohastamine 2018. aastal)

Delegatsioonidele edastatakse lisas ELi küberkaitsepoliitika raamistik (2018. aastal ajakohastatud kujul), mille nõukogu võttis vastu 19. novembril 2018 toimunud 3652. aasta istungil.

LISA

ELI KÜBERKAITSEPOLIITIKA RAAMISTIK

(2018. aastal ajakohastatud kujul)

Kohaldamisala ja eesmärgid

Muutuvatele julgeolekuprobleemidele reageerimiseks peavad EL ja tema liikmesriigid tugevdama kübervastupidavusvõimet ja looma tugeva küberjulgeoleku- ja kaitsevõime.

ELi küberkaitsepoliitika raamistik (CDPF) toetab ELi liikmesriikide küberkaitsevõime väljatöötamist ning ELi küberkaitse julgeoleku- ja infrastruktuuri tugevdamist, ilma et see piiraks liikmesriikide ja ELi õigusakte, sealhulgas küberkaitse ulatust, kui see on kindlaks määratud.

Küberruum on lisaks maale, merele, õhuruumile ja kosmosele viies tegevusvaldkond: ELi missioonide ja operatsioonide edukas rakendamine sõltub üha rohkem katkestusteta juurdepääsust turvalisele küberruumile ning seega on selle jaoks vaja tugevat ja vastupanuvõimelist küberkaitse operatiivset suutlikkust.

Ajakohastatud CDPFi eesmärk on edasi arendada ELi küberkaitsepoliitikat, võttes arvesse asjakohaseid arenguid muudel asjakohastel foorumitel ja poliitikavaldkondades ja CDPFi rakendamist alates 2014. aastast. CDPFis on kindlaks määratud küberkaitse prioriteetsed valdkonnad ning selgitatakse erinevate Euroopa osaliste rolle, austades täielikult liidu osalejate ja liikmesriikide kohustusi ja pädevusi ning ELi institutsioonilist raamistikku ja otsuste tegemise sõltumatust.

Kontekst

Euroopa Ülemkogu 2013. aasta detsembri järeldustes ÜJKP kohta ja nõukogu 2013. aasta novembri järeldustes ÜJKP kohta kutsutakse üles töötama kõrge esindaja ettepaneku alusel ning koostöös Euroopa Komisjoni ja Euroopa Kaitseagentuuriga välja ELi küberkaitsepoliitika raamistik. Nõukogu võttis 13.novembril 2014 vastu ELi küberkaitsepoliitika raamistiku[1] ja pärast seda on selle rakendamise kaudu konkreetsed väljundid aidanud suurendada märkimisväärselt liikmesriikide küberkaitsevõimet. Osana küberkaitsepoliitika raamistiku rakendamise 2017. aasta iga-aastase aruande[2] osana ja võttes arvesse ELi algatusi julgeoleku ja kaitse valdkonnas, eelkõige kaitseküsimuste iga-aastase kooskõlastatud läbivaatamist (CARD), alalist struktureeritud koostööd (PESCO), Euroopa Kaitsefondi (EDF) ja ÜJKP tsiviiltegevuse kokkulepet ning 2018. aasta võimearendusplaani (CDP) ja tsiviilvõimete arendamise kava (CCDP) läbivaatamist, kutsusid liikmesriigid kohastama ELi küberkaitsepoliitika raamistiku.

Küberjulgeolek on prioriteet Euroopa Liidu üldises välis- ja [3]julgeolekupoliitika strateegias ja ELi ambitsiooni tasemes. Üldine välis- ja julgeolekupoliitika strateegia rõhutab vajadust kaitsta ELi ja tema kodanikke ja reageerida välistele kriisidele. Üldine välis- ja julgeolekupoliitika toonitab vajadust tugevdada ELi kui julgeolekukogukonda. Seda arvestades peaks julgeoleku ja kaitse alased jõupingutused ka tugevdama ELi strateegilist rolli ja võimet vajaduse korral tegutseda iseseisvalt, tehes seda võimaluse korral koostöös partneritega. Need eesmärgid nõuavad rohkem koostööd võimete arendamise, tulemuslikkuse edendamise ja kaasneva tsiviil- ja sõjaliste võimete koostoimimisvõime osas.

---

1 Nõukogu dokument 15585/14, 18.11.2014.
2 Nõukogu dokument 15870/17, 19.12.2017.
3 Nõukogu järeldused ELi üldise strateegia rakendamise kohta julgeoleku- ja kaitsevaldkonnas, 14.11.2016.

Ühised ettepanekud ühisdeklaratsiooni kohta, mille Euroopa Ülemkogu eesistuja, Euroopa Komisjoni president ja Põhja-Atlandi Lepingu Organisatsioon (NATO) allkirjastasid 8. juulil 2016 Varssavis,[4] sisaldavad konkreetseid meetmeid laiendamaks ELi ja NATO koostööd küberturvalisuse ja -kaitse kohta, sealhulgas missioonide ja operatsioonide kontekstis, samuti seoses küberkaitsevõime arendamise, teadusuuringute ja tehnoloogia, hariduse, koolituse, õppuste ja küberi kriisiohjamisse süvalaiendamisega. Koostöö toimub nii, et täielikult austatakse avatuse, läbipaistvuse, kaasamise, vastastikkuse ja ELi otsuste tegemise sõltumatust. Veebruaris 2016 alla kirjutatud tehniline kokkulepe ELi institutsioonide ja ametite infoturbeintsidentidega tegeleva rühma (CERT-EU) ja NATO küberturbeintsidentidele reageerimise üksuse (NCIRC) vahel lihtsustab tehnilise teabe jagamist, et parandada küberintsidentide ennetamist, tuvastamist ja neile reageerimist kummaski organisatsioonis.

Tuleks meenutada, et mitmed ELi poliitikameetmed aitavad kaasa küberkaitsepoliitika eesmärkidele, mis on esitatud käesolevas dokumendis, ja selle raames võetakse arvesse ka asjaomaseid õigusakte, poliitikat ja tehnoloogia toetust tsiviilvaldkonnas. Näiteks juulis 2016 võeti vastu Euroopa Parlamendi ja nõukogu küberturvalisuse direktiiv[5] (NIS), mis suurendab liikmesriikide üldist valmisolekut ja küberohtude puhul ja suurendab kogu ELi hõlmavat koostööd. Selles direktiivis sätestatakse meetmed võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge taseme saavutamiseks liidus, parandades seeläbi siseturu toimimist. Direktiivi ülevõtmise tähtaeg on 9. mai 2018.

---

4 Nõukogu järeldused Euroopa Ülemkogu eesistuja, Euroopa Komisjoni presidendi ja Põhja-Atlandi Lepingu Organisatsiooni peasekretäri ühisdeklaratsiooni rakendamise kohta (6. detsember 2016, 15283/16; 5. detsember 2017, 14802/17).

5 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).

2017. aasta septembri ettepanek ELi küberturvalisuse seaduse kohta sisaldab uut volitust ELi küberturvalisuse ameti (ENISA) ja kogu ELi hõlmava sertifitseerimise raamistiku loomise kohta. Kui see on loodud, peaks sertifitseerimise raamistik toetama IKT protsesside, toodete ja teenuste jaoks kõrgeid standardeid, olema konkurentsieelise allikas ja tugevdama usaldust tarbijate ja tellija poolel. Samuti võttis komisjon septembris 2017 veel ühe sammu, et valmistada EL ette ulatuslike piiriüleste küberintsidentide juhtumiteks („Blue Print“), ja teeb praegu liikmesriikide ja teiste institutsioonide, ametite ja asutustega tööd Euroopa küberturvalisuskriisikoostöö arendamise kallal, asetades oma kohale asjaomaste osalejate, protsesside ja menetluste praktilise operatsionaliseerimise ja dokumenteerimise ELi kriiside ja katastroofide ohjamise mehhanisme kontekstis, eelkõige kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra raames.

Nõukogu 2016. aasta novembri järeldustes Euroopa kübervastupidavusvõime tugevdamise kohta visandati ühist eesmärki, mis käsitleb ELi strateegilise autonoomsusesse panustamist, nagu on osutatud nõukogu 2016. aasta Euroopa Liidu üldist välis- ja julgeolekupoliitika strateegiat käsitlevates järeldustes, sealhulgas küberruumis. Euroopa Ülemkogu kinnitas seda sõnumit juunis 2018 ja ka rõhutas vajadust tugevdada võimet tegutseda EList väljastpoolt pärinevate küberohtude vastu.

2017. aastal võttis nõukogu vastu pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku („küberdiplomaatia meetmete kogum“).[6] Raamistik peaks innustama koostööle, hõlbustama ohtude leevendamist ning avaldama pikas perspektiivis mõju võimalikele rünnakute toimepanijatele. Raamistik kasutab pahatahtlikule kübertegevusele reageerimiseks ja selle ärahoidmiseks ära ÜVJP meetmeid, sealhulgas piiravaid meetmeid. Pahatahtliku kübertegevuse toimepanemises osalejad on vaja võtta oma tegude eest vastutusele ning ELi liikmesriike ergutatakse täiendavalt arendama oma võimet reageerida pahatahtlikule kübertegevusele koordineeritult kooskõlas küberdiplomaatia meetmete kogumiga. Liikmesriigid ei peaks või ei peaks teadvalt toetama info- ja kommunikatsioonitehnoloogia alast tegevust, mis on vastuolus nende rahvusvahelise õiguse kohaste kohustustega, ega peaks teadvalt võimaldama kasutada oma territooriumi rahvusvaheliste süüliste tegude tarbeks, kasutades info- ja kommunikatsioonitehnoloogiat.

Septembris 2017 esitasid komisjon ja kõrge esindaja / asepresident ühisteatise[7] kübervaldkonna kohta, et maandada uuest ohtude maastikust tulenevaid riske. See hõlmab küberkaitset kui ühte peamistest tegevusvaldkondadest, ja CDPF on üks sammas selle konkreetsest rakendamisest.[8]

Nõukogu novembri 2017 järeldustes küberruumi küsimustes tunnustati arenevaid sidemeid küberturvalisuse ja -kaitse vahel ning kutsuti üles tugevdama koostööd küberkaitse valdkonnas, sealhulgas ergutades koostööd intsidentidele reageerivate tsiviil- ja sõjaväeliste kogukondade vahel. Samuti ta rõhutas, et eriti raske küberintsident või -kriis võib liikmesriigi jaoks olla piisav põhjus ELi solidaarsusklausli ja/või vastastikuse abi klausli kohaldamiseks;

---

6 Nõukogu järeldused pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku kohta („küberdiplomaatia meetmete kogum“), 9916/17, 7. juuni 2017

7 Ühisteatis Euroopa Parlamendile ja nõukogule: „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“ (13. september 2017, JOIN (2017) 450 final)).

8 Nõukogu järeldused, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“ (20. november 2017, JOIN(14435)17)

11. detsembril 2017 käivitati alaline struktureeritud koostöö (PESCO). See ambitsioonikas, siduv ja kaasav koostööraamistik on kehtestatud 25 liikmesriigi vahel ja see sisaldab kohustust suurendada pingutusi küberkaitsekoostöö valdkonnas ja ka seotud PESCO projektide puhul. Esimene PESCOs osalevate liikmesriikide poolt 2017. aastal kindlaks tehtud PESCO projektide komplekt hõlmab kahte küberkaitsega seotud projekti: „Küberturbe kiirreageerimisrühmad ja küberturvalisuse alane vastastikune abistamine“ ja „Küberohtudele ja -intsidentidele reageerimise teabevahetuse platvorm“. Kavandatud on veel muid PESCO projekte. PESCO arendab küberkaitsevõimet ja seega tugevdab koostööd osalevate liikmesriikide vahel ning parandab koostalitlusvõimet.

Juunis 2018 Euroopa Kaitseagentuuri juhtnõukogu poolt ajakohastatud ELi võimearendusplaanis (CDP) käsitatakse küberkaitset põhielemendina, tunnistades vajadust kaitsvate küberoperatsioonide järele kõigis operatsionaalsetes kontekstides, tuginedes praegusele ja prognoosivale küberruumi olukorrateadlikkusele, sealhulgas võimele koondada suuri andmehulki ja arvukatest allikatest pärit jälitusteavet, toetades kiiret otsuste tegemist ja andmete üha automaatsema kogumise, analüüsimise ja otsuste tegemise toetamise protsessi. CDP 2018 teeb kindlaks küberkaitse prioriteedid järgmistes valdkondades: koostöö ja sünergia asjaomaste osalejatega küberkaitse ja küberturvalisuse valdkondades; küberkaitsealased teadusuuringud ja tehnoloogiauuendused; süsteemide loomise raamistikud küberoperatsioonide tarbeks; haridus, väljaõpe, õppused ja hindamine (ETEE); küberkaitse alaste probleemidega tegelemine õhus, kosmoses, merel ja maismaal.

Lõpetuseks, viimase paari aasta jooksul on saanud selgeks, et rahvusvahelisel kogukonnal on vaja hoida ära konflikte, teha koostööd ja stabiliseerida küberruum. EL edendab tihedas koostöös teiste rahvusvaheliste organisatsioonidega, eriti ÜRO, OSCE, ASEANi piirkondliku foorumiga, strateegilist raamistikku konfliktide ennetamiseks ja stabiilsuseks küberruumis, mis hõlmab: i) rahvusvahelist õiguse, eriti kogu ÜRO harta kohaldamist küberruumis; ii) vastutustundliku riigi käitumise üldiselt kohaldatavate mittesiduvate normide, eeskirjade ja põhimõtete austamist; iii) piirkondlike usaldust suurendavate meetmete arendamist ja rakendamist. Seda ponnistust peaks samuti toetama ELi küberkaitsepoliitika raamistik.

Prioriteedid

Ajakohastatud küberkaitsepoliitika raamistikus on määratletud kuus prioriteeset valdkonda. Käesoleva poliitikaraamistiku tähelepanu keskmes on küberkaitsevõime arendamine ning ELi ÜJKPga seotud side- ja infovõrkude kaitse. Teised prioriteetsed valdkonnad on: väljaõpe ja õppused, teadusuuringud ja tehnoloogia, tsiviil-sõjaline koostöö ning rahvusvaheline koostöö. Väljaõppe valdkonnas seatakse rõhuasetus liikmesriikide osutatava ÜJKP käsuliini küberkaitsekoolituse ja küberteadlikkuskoolituse laiendamisele. Samuti tuleb õppustel piisavalt käsitleda kübermõõdet, et parandada ELi võimet reageerida küber- ja hübriidkriisidele, parandades strateegiliste otsuste langetamise menetlust ja teabe kättesaadavust. Küberruum on kiirelt arenev valdkond ning nii tsiviil- kui sõjalises valdkonnas tuleb toetada uusi tehnoloogilisi arenguid. Tsiviil-sõjaline koostöö kübervaldkonnas on võtmetähtsusega element, et tagada ühtne reageering küberohtudele. Lõpetuseks, kuid mitte vähem olulisena, võib rahvusvaheliste partneritega tehtava koostöö tõhustamine aidata tõhustada küberturvalisust ELis ja mujal ning edendada ELi põhimõtteid ja väärtusi.

Käesolevas raamistikus tuuakse esile ettepanekud ja võimalused koordineerimiseks asjakohaste ELi institutsioonide, organite ja asutuste vahel. Samuti kajastatakse raamistikus erasektori olulist rolli küberturvalisuse ja küberkaitse tehnoloogiate arendamisel.

Lisaks toetatakse küberkaitsepoliitika raamistikuga küberkaitse integreerimist liidu kriisiohjemehhanismidesse, mille osas võivad küberkriisi mõjude käsitlemise puhul olla kohaldatavad ELi lepingu ja ELi toimimise lepingu asjakohased sätted[9].

1. Liikmesriikide küberkaitsevõime arendamise toetamine

Küberkaitsevõime ja -tehnoloogia arendamisel tuleks käsitleda kõiki võimete arendamisega seotud aspekte, sealhulgas doktriini, juhtimist, organisatsiooni, personali, koolitust, tööstust, tehnoloogiat, taristut, logistikat ja koostalitlusvõimet. Liikmesriigid peaksid sel eesmärgil tõhustama oma jõupingutusi, et saavutada tõhus küberkaitsevõime. Euroopa välisteenistus, komisjon ja Euroopa Kaitseagentuur peaksid tegema koostööd ja neid jõupingutusi toetama.

ÜJKP missioone ja operatsioone toetava teabetaristu nõrku kohti tuleb pidevalt hinnata ning kaitse tulemuslikkusest tuleb aru saada peaaegu reaalajas. Operatiivtasandi seisukohast on üheks küberkaitse valdkonna põhiküsimuseks ÜJKP side- ja infovõrkude kättesaadavuse, terviklikkuse ja konfidentsiaalsuse säilitamine, kui operatsiooni või missiooni volitustes ei ole sätestatud teisiti. Lisaks integreerib Euroopa välisteenistus koostöös liikmesriikidega täiendavalt kübersuutlikkust ÜJKP missioonidese ja operatsioonidesse.

Pahatahtliku kübertegevuse toimepanijad tuleb nende tegude eest vastutusele võtta. On oluline, et ELi liikmesriigid, keda toetab Euroopa välisteenistus, tugevdavad vastastikust koostööd, et reageerida pahatahtlikule kübertegevusele. Sellise ühise reageeringu saavutamise aitamiseks töötatakse välja küberdiplomaatia meetmete kogum. Euroopa välisteenistus ja Euroopa Kaitseagentuur korraldavad küberdiplomaatia meetmete kogumi alusel korrapäraselt õppusi, mille käigus saavad ELi liikmesriigid seda harjutada.

[9] ELi toimimise lepingu artikkel 222 ja ELi lepingu artikli 42 lõige 7, võttes nõuetekohaselt arvesse ELi lepingu artiklit 17.

Võttes arvesse, et liikmesriikide ja ELi õigusaktides (juhul kui see üldse on määratletud) on küberkaitse kohaldamisala ulatuslik ja mitmekesine, tuleb välja töötada ühine arusaamine küberkaitse kohaldamisala kohta.

Kuna ÜJKP sõjalised operatsioonid põhinevad juhtimise, side ja infotehnoloogia (C4) taristul, mille annavad liikmesriigid, on teabetaristu küberkaitsealaste nõuete planeerimisel vaja teatud määral strateegilist lähendamist.

Tuginedes Euroopa Kaitseagentuuri küberkaitse projekti meeskonna tööle küberkaitsevõime väljatöötamisel, teevad Euroopa Kaitseagentuur ja liikmesriigid järgmist:

- kasutavad võimearendusplaani ja teisi vahendeid nagu kaitseküsimuste iga-aastane kooskõlastatud läbivaatamine, mis hõlbustavad ja toetavad liikmesriikidevahelist koostööd, et suurendada strateegilisel tasandil lähenemist liikmesriikide küberkaitsealaste nõuete planeerimisel, eelkõige jälgimise, olukorrast ülevaate saamise, ennetamise, tuvastamise ja kaitsmise, teabevahetuse, kohtuekspertiisi ja pahavara analüüsi võime, saadud kogemuste, kahju piiramise, dünaamilise taastumise võime, jagatud andmete säilitamise ja andmete varukoopiate valdkonnas;
- toetavad praegusi ja tulevasi küberkaitsega seotud võimete ühiskasutamise projekte sõjaliste operatsioonide jaoks (näiteks kohtuekspertiisi, koostalitlusvõime arendamise, standardite kehtestamise valdkonnas);
- töötavad välja eesmärkide ja nõuete standardid, milles määratakse kindlaks küberturvalisuse ja usalduse miinimumtase, mis tuleb liikmesriikidel saavutada, tuginedes olemasolevatele kogu ELis saadud kogemustele.

Euroopa välisteenistus ja Euroopa Kaitseagentuur teevad järgmist:

- hõlbustavad liikmesriikide vahelist teabevahetust riiklike küberkaitsedoktriinide kohta ning küberkaitsele suunatud töölevõtmise, tööl hoidmise ja töölt lahkumise programmide kohta.

Euroopa Kaitseagentuur teeb järgmist:

- analüüsib liikmesriikide õigusaktides ja parimates tavades küberkaitse sõjaliste vajaduste kohaldamisala erinevusi. Analüüsi põhieesmärgiks on töötada välja küberkaitsealane ettevõtte struktuur ning lisada liikmesriikide poolt valdkonnas kasutatavad kohaldamisala, funktsioonid ja vajadused siseriiklikesse ja ELi õigusaktidesse.

Liikmesriigid teevad vabatahtlikult järgmist:

- parandavad koostööd oma infoturbeintsidentidega tegelevate sõjaliste rühmade vahel, et parandada intsidentide ennetamist ja käsitlemist;
- kasutavad alalist struktureeritud koostööd, et täiendavalt suurendada koostööd küberkaitse valdkonnas, sealhulgas uute projektide osas;
- kasutavad Euroopa Kaitsefondi, et ühiselt arendada küberkaitsevõimet;
- kujundavad ühise arusaamise vastastikuse abistamise klausli kohaldamise kohta kübervaldkonnas, säilitades samas selle paindlikkuse;
- töötavad välja teabetaristu küberkaitse põhivajadused;
- kuivõrd küberkaitsevõime parandamine sõltub tsiviilotstarbelisest võrgust ja infoturbe alastest ekspertteadmistest, kasutavad ekspertteadmisi, mida omavad ENISA, võrgu- ja infoturbe koostöörühma kuuluvad liikmesriikide asutused ning teised võimalikud üksused ELi tasandil, kel on ekspertteadmisi tsiviilalase küberturvalisuse valdkonnas.

Liikmesriigid, Euroopa välisteenistus/ELi sõjaline staap, Euroopa Julgeoleku- ja Kaitsekolledž ning Euroopa Kaitseagentuur teevad järgmist:

- kaaluvad küberkaitsekoolituse edasiarendamist, pidades silmas ELi lahingugruppide sertifitseerimist.

Komisjon teeb koostöös liikmesriikidega järgmist:

- analüüsib küberkaitset Euroopa kaitsevaldkonna tööstusliku arendamise programmi ja Euroopa Kaitsefondi tööprogrammides.

2. ELi üksuste kasutatavate ÜJKP side- ja infosüsteemide kaitse tõhustamine

Piiramata ELi institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma (CERT-EU) kui kõikide liidu institutsioonide, organite ja asutuste keskse ELi küberintsidentidele reageerimise koordineerimise struktuuri rolli, ning liidu eelarvet käsitlevate asjakohaste eeskirjade raames, töötab Euroopa välisteenistus välja asjakohase ja iseseisva arusaama julgeoleku ja võrgukaitse küsimustes ning töötab välja oma IT-julgeolekualase suutlikkuse. Selle eesmärk on parandada Euroopa välisteenistuse ÜJKP võrgustike vastupanuvõimet, mille keskmes on ennetamine, tuvastamine, intsidentidele reageerimine, olukorrast ülevaate saamine, teabevahetus ja varase hoiatamise mehhanismid.

Euroopa välisteenistuse side- ja infosüsteemide kaitset ning infotehnoloogia julgeolekualase suutlikkuse arendamist korraldab Euroopa välisteenistuse eelarve ja halduse peadirektoraat. Täiendavaid sihtotstarbelisi vahendeid ja täiendavat toetust annavad Euroopa Liidu sõjaline staap (EUMS), kriisiohjamise ja planeerimise direktoraat (CMPD) ja tsiviilmissioonide plaanimise ja juhtimise teenistus (CPCC). See IT-julgeolekualane suutlikkus hõlmab salastatud ja salastamata süsteeme ning see on olemasolevate tegevusüksuste lahutamatu osa.

Samuti on vaja ühtlustada ÜJKP missioonide ja operatsioonide läbiviimisel erinevate ELi institutsionaalsete osalejate kasutatud infosüsteemide julgeolekueeskirju. Seoses sellega tuleks kaaluda ühtset käsuliini, mille eesmärk on parandada ÜJKP jaoks kasutatud võrgustike vastupanuvõimet.

2017. aastal loodi Euroopa välisteenistuse peasekretäri alluvuses Euroopa välisteenistuse sisene küberhalduse nõukogu, et parandada koordineerimist ning tõhustada ÜJKP side- ja infosüsteemide ja võrgustike kaitset ja vastupidavust.

Euroopa välisteenistus/eelarve ja halduse peadirektoraat teevad järgmist:

- tugevdavad Euroopa välisteenistuse IT-julgeolekualast suutlikkust, tuginedes olemasolevale tehnilisele võimekusele ja korrale; selle keskmes on ennetamine, tuvastamine, intsidentidele reageerimine, olukorrast ülevaate saamine, teabevahetus ja varase hoiatamise mehhanismid; tõhustavad täiendavalt koostööstrateegiat ELi infoturbeintsidentidega tegeleva rühmaga (CERT-EU) ja olemasolevaid ELi küberturvalisuse alaseid võimeid.

Euroopa välisteenistus/eelarve ja halduse peadirektoraat teevad koostöös Euroopa Liidu sõjalise staabi, sõjaliste missioonide plaanimise ja juhtimise teenistuse, kriisiohjamise ja planeerimise direktoraadi ning tsiviilmissioonide plaanimise ja juhtimise teenistusega järgmist:

- töötavad välja sidusa IT-julgeoleku poliitika ja juhised, võttes arvesse ka küberkaitse tehnilised nõuded ÜJKP kontekstis, struktuuride, missioonide ja operatsioonide jaoks, võttes arvesse olemasolevaid koostöö raamistikke ja poliitikaid ELis, et saavutada eeskirjade, poliitika ja korralduse ühtlustamine.

Euroopa välisteenistus/ühtne luureandmete analüüsivõime (SIAC) teevad järgmist:

- tugevdavad olemasolevatele struktuuridele tuginedes oma küberohu hinnangu ja luurevõimet, et määrata kindlaks uued küberriskid ja esitada regulaarseid ohuhinnanguid, mis põhinevad strateegilisel ohuhinnangul ja peaaegu reaalajas saadaval teabel intsidentide kohta, mida koordineeritakse asjaomaste ELi struktuuride vahel ja mis tehakse juurdepääsetavaks erinevatel salastatuse tasemetel.

Euroopa välisteenistus/SIAC ning CERT-EU teevad järgmist:

- edendavad reaalajas küberohte käsitleva teabe vahetamist liikmesriikide ja asjaomaste ELi asutuste vahel. Sellel eesmärgil töötatakse olemasoleval koostööl põhineva vabatahtliku lähenemisviisi raames välja teabe vahetamise mehhanismid ja usaldust suurendavad meetmed asjaomaste riiklike ja Euroopa asutuste vahel.

Euroopa välisteenistus/Euroopa Liidu sõjaline staap ning sõjaliste missioonide plaanimise ja juhtimise teenistus teevad järgmist:

- töötavad täiendavalt välja ja lisavad strateegilise tasandi planeerimisele küberkaitse kontseptsiooni ÜJKP sõjaliste missioonide ja operatsioonide jaoks;
- töötavad koostöös operatsioonide peakorteriga välja üldise operatiivtasandi kübervaldkonna standardse operatiivmenetluse.

Euroopa välisteenistus/tsiviilmissioonide plaanimise ja juhtimise teenistus ning kriisiohjamise ja planeerimise direktoraat teevad järgmist:

- töötavad välja ja lisavad strateegilise tasandi planeerimisele küberkaitse kontseptsiooni ÜJKP tsiviilmissioonide jaoks;
- tugevdavad ÜJKP tsiviilmissioonide küberkaitsevõimet, tuginedes olemasolevale taristule ning edendades ÜJKP missioonides ja operatsioonides kasutatavate tehnoloogiate standardimist ja ühtlustamist, kasutades (kui see on asjakohane) CERT-EU, ENISA ja Euroopa Kaitseagentuuri ekspertteadmisi;
- analüüsivad ÜJKP tsiviilaspektide tugevdamise käigus täiendavalt ÜJKP tsiviilmissioonide poolt küberturvalisuse alase toetuse võimalikku osutamist vastuvõtvatele riikidele.

Euroopa välisteenistus teeb järgmist:

- töötab täiendavalt välja ÜJKP sõjaliste- ja tsiviilmissioonide ning operatsioonide ühiseid nõudeid;
- tõhustab küberkaitse koordineerimist, et rakendada eesmärke, mis on seotud ÜJKPd toetavate ELi institutsionaalsete osalejate kasutatud võrgustike kaitsega, tuginedes kogu ELis saadud kogemustele;
- vaatab korrapäraselt läbi ressursinõuded ja teised asjaomased poliitikaotsused, mis põhinevad muutuval ohukeskkonnal, konsulteerides liikmesriikide ja teiste ELi institutsioonidega.

3. Tsiviil-sõjalise koostöö edendamine

Küberruum on kiirelt arenev valdkond: tehnoloogilisi arenguid tuleb nii tsiviil- kui sõjalises valdkonnas tugevdada julgeolekusüsteemidega. Võimalikult suurel määral tuleks ette näha koordineerimist tsiviil- ja sõjalise valdkonna vahel, seda juhtudel, kui sarnased tehnoloogilised arengud annavad lahendusi tsiviil- ja sõjaliste rakenduste jaoks. Teistel juhtudel on sõjalised võimed ja relvasüsteemid nii spetsiifilised, et tsiviiltehnoloogiatega jagamine ei ole võimalik. Kübervaldkonnas tehtavat tsiviil- ja sõjandusvaldkonna koostööd võib muu hulgas kaaluda parimate tavade vahetamise, teabevahetuse, varajase hoiatamise mehhanismide, turvaintsidentidele reageerimise, riskihinnangute ja teadlikkuse suurendamise ning väljaõppe ja õppuste eesmärgil; seejuures ei piirata liikmesriikide siseriiklikku korraldust ja seadusandlust.

Tsiviilvaldkonna küberturvalisuse suurendamine on oluline faktor, mis toetab üldist võrgu- ja infoturbe vastupanuvõimet. Võrgu- ja infoturbe direktiiv suurendab valmisolekut siseriiklikul tasandil ning suurendab liidu tasandil liikmesriikide vahelist koostööd nii strateegilisel kui operatiivtasandil. See koostöö hõlmab riiklikke ametiasutusi, kes teostavad järelevalvet küberturvalisuspoliitika üle, ning siseriiklikke infoturbeintsidentidega tegelevaid rühmasid (CERT) ja ELi tasandi infoturbeintsidentidega tegelevat rühma. Tugevdada tuleks koostööd tsiviil- ja sõjaliste infoturbeintsidentidega tegelevate rühmade vahel, võttes nõuetekohaselt arvesse kõnealuseid arenguid. Euroopa küberturvalisust käsitleva uue õigusakti eesmärk on parandada Euroopa vastupanuvõimet küberrünnakutele ning kehtestada toodete ja teenuste küberturvalisuse sertifitseerimisraamistik, suurendades seeläbi usaldust tsiviilvaldkonna digitaalkeskonna vastu.

Euroopa Kaitseagentuuri, Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA), küberkuritegevuse vastase võitluse Euroopa keskust (EC3) ja ELi infoturbeintsidentidega tegelevat rühma (CERT-EU) (ning samuti liikmesriike) innustatakse koos teiste asjakohaste ELi organite ja asutustega oma volituste piires ja liikmesriikide pädevusi dubleerimata täiendavalt tõhustama oma koostööd järgmistes valdkondades:

- küberturvalisuse ja -kaitse ühiste pädevusprofiilide väljatöötamine, tuginedes rahvusvahelistele parimatele tavadele ja ELi institutsioonide, organite ja asutuste kasutatavale sertifitseerimisele, võttes samas arvesse erasektori kasutatavaid sertifitseerimisstandardeid;
- avaliku sektori küberturvalisuse ja -kaitse valdkonna organisatsiooniliste ja tehniliste standardite edasiarendamise ja kohandamise toetamine kasutamiseks kaitse- ja julgeolekusektoris. Vajaduse korral tuginetakse ENISA ja Euroopa Kaitseagentuuri tehtavale tööle;
- töömehhanismide ja korra kehtestamine või täiendav väljatöötamine, mille abil vahetatakse parimaid tavasid eelkõige seoses hariduse, väljaõppe ja õppustega ning teadusuuringute ja tehnoloogiaga ja teiste valdkondadega, mis võimaldavad tsiviil-sõjalist koostoimet;
- küberkuritegevuse ennetamise, uurimise ja kohtuekspertiisi osas ELis olemasolevatele kogemustele tuginemine ning nende ulatuslikum kasutamine küberkaitsevõimete arendamisel.

Liikmesriigid teevad vabatahtlikult järgmist:

- tugevdavad koostööd liikmesriikide tsiviil- ja sõjaliste infoturbeintsidentidega tegelevate rühmade vahel.

Euroopa välisteenistus, komisjon ja liikmesriigid teevad järgmist:

- lisavad küberkaitse ELi kriiside ja katastroofide ohjamise mehhanismidesse (näidiskava protsessi kaudu).

4. Teadusuuringud ja tehnoloogia

Taristuettevõtjad ning tsiviil- ja kaitsealaseid IKT teenuseid pakkuvad ettevõtjad seisavad silmitsi sarnaste küberturvalisuse probleemidega, mille põhjuseks on tehnoloogia ja tegevusvõimekuse osas kehtestatud ühised nõuded. Ühised teadusuuringute ja tehnoloogia alased vajadused ja süsteemidele esitatavad ühised nõuded peaksid pikema aja jooksul parandama süsteemide koostoimivust ning vähendama lahenduste väljatöötamise kulusid. Mastaabisäästu saavutamine on vajalik, et reageerida üha arvukamatele ohtudele ja haavatavustele. See peaks omakorda soodustama konkurentsivõimelise küberkaitse tööstuse säilimist ja kasvu Euroopas.

Küberkaitsevõime arendamisel on oluline teadusuuringute ja tehnoloogia mõõde. Euroopa Kaitseagentuur on küberkaitse teadusuuringute tegevuskava raames loonud tugeva aluse tulevaste teadusuuringute ja tehnoloogia valdkonna rahastamise prioriteetide kehtestamiseks valitsustevahelises raamistikus. Euroopa Kaitseagentuuri asjakohases ajutises töörühmas väljatöötatud strateegilises teadusuuringute kavas esitatakse teadmispõhiselt sõjaliselt vajalike kübervaldkonna tehnoloogiate prioriteedid ning määratletakse võimalused kahesuguse kasutuse alaste jõupingutuste ja investeeringute tegemiseks, olgu siis tegemist riikide poolt, riikidevaheliselt või ELi poolt rahastatud kontekstiga.

On väga oluline, et Euroopas arendataks tehnoloogilised võimed, mille abil leevendatakse ohte ja haavatavusi. Tööstus jääb ka edaspidi peamiseks küberkaitse valdkonna tehnoloogia ja innovatsiooni arendajaks. Käsitlemist vajavad sellised valdkonnad nagu krüptograafia, turvalised manussüsteemid, pahavara tuvastamine, simulatsioonide ja visualiseerimise tehnikad, võrgu- ja infosüsteemide kaitsmine ning identimis- ja autentimistehnoloogia. Samuti on tähtis tugevdada Euroopa küberjulgeoleku tööstuse konkurentsivõimelist tarneahelat, toetades väikeste ja keskmise suurusega ettevõtjate (VKEd) kaasamist.

Tagamaks, et Euroopa suudab kübertehnoloogia võimete valdkonnas konkureerida rahvusvaheliste konkurentidega, sõltub ka meie suutlikkusest suurendada läbimurdelist innovatsiooni, kasutades selleks nii riiklikke kui ELi vahendeid, näiteks Euroopa innovatsiooninõukogu.

Lihtsustada tsiviil- ja sõjandusvaldkonna koostööd küberkaitsevõime arendamisel, tugevdada Euroopa kaitsesektori tehnoloogilist ja tööstuslikku baasi[10] ning toetada ELi strateegilist sõltumatust küberruumis, tehes seda vajaduse korral ning võimaluse korral koostöös partneritega,

Euroopa Kaitseagentuur, komisjon ja liikmesriigid teevad järgmist:

- püüavad saavutada sõjalises sektoris tehtavate teadusuuringute ja tehnoloogiaalaste jõupingutuste koostoimet tsiviilsektori teadus- ja arendustegevuse programmidega, eelkõige läbimurdelise innovatsiooniga seotud programmidega, ning võtavad kaitsevaldkonna teadusuuringute ettevalmistava meetme rakendamisel arvesse küberturvalisuse ja -kaitse mõõdet;
- jagavad omavahel küberturvalisuse teadusuuringute tegevuskavasid (nt Euroopa Kaitseagentuuri küberturvalisuse strateegiline teadusuuringute kava) ning nende tulemusel koostatud teekaarte ja tegevuskavasid; sel eesmärgil töötatakse välja valdkondadevaheline küberkaitse teadusuuringute tegevuskava, tehes seda tihedas koostöös komisjoni ja liikmesriikidega;
- toetavad küberturvalisuse ja -kaitse mõõtmete lisamise parandamist programmidesse, millel on kahesuguse kasutusega julgeoleku- ja kaitsealane mõõde, nt ühtse Euroopa taeva Euroopa lennuliikluse uue põlvkonna juhtimissüsteemi (SESAR) programm.

[10] Teatis „Konkurentsivõimelisem ja tõhusam kaitse- ja julgeolekusektor“, COM (2013) 542.

Komisjon teeb järgmist:

- analüüsib Euroopa küberturvalisuse tööstuse, tehnoloogia ja teadusuuringute pädevuskeskuse loomist koos riiklike koordinatsioonikeskuste võrgustikuga, et toetada küberturvalisuse tehnoloogilisi ja tööstuslikke võimeid ning suurendada liidu küberturvalisuse tööstuse konkurentsivõimet, tagades vastastikuse täiendavuse ja vältides dubleerimist küberturvalisuse pädevuskeskuste võrgustikus ja muude ELi ametitega. Keskus peaks muu hulgas tõhustama koostööd tsiviil- ja sõjaliste tehnoloogiate ja rakenduste vahel, tehes küberkaitse valdkonnas tihedat ja vastastikku täiendavat koostööd Euroopa Kaitseagentuuriga;
- toetab kogu julgeolekualast väärtusahelat hõlmavate tööstussektori ökosüsteemide ja innovatsiooniklastrite arendamist, tuginedes akadeemilistele teadmistele, VKEde innovatsioonile ja tööstuslikule tootmisele.

Komisjon teeb koostöös liikmesriikidega järgmist:

- võtab küberkaitse küsimusi arvesse kaitsevaldkonna teadusuuringute ettevalmistava meetme projektikonkursi käigus;
- võtab küberkaitse küsimusi arvesse Euroopa Kaitsefondi projektikonkursi valdkondades;
- toetab ELi poliitika sidusust, tagamaks et ELi küberkaitse poliitilised ja tehnilised aspektid on tehnoloogiainnovatsioonis jätkuvalt esikohal ning et neid ühtlustatakse kogu ELis (küberohu analüüsi- ja hindamisvõimekus, „lõimitud julgeoleku“ algatused, tehnoloogiale ligipääsust sõltumise haldamine jne).

5. Haridus-, koolitus- ja õppuste võimaluste parandamine

Selleks, et suurendada küberohtude käsitlemise valmisolekut ja töötada kogu ELis välja ühine küberkaitsekultuur, mis annab kasu ka ELi missioonidele ja operatsioonidele, tuleb parandada ja laiendada küberkaitsealaseid koolitusvõimalusi. On väga oluline, et haridus- ja koolituseelarveid kasutatakse tõhusalt, tagades samas parima võimaliku kvaliteedi. Võtmetähtsusega on küberkaitse valdkonna hariduse ja koolituse panustamine ja jagamine Euroopa tasandil.

Euroopa Julgeoleku- ja Kaitsekolledž, Euroopa välisteenistus, Euroopa Kaitseagentuur, komisjon ja liikmesriigid teevad järgmist:

- loovad Euroopa Kaitseagentuuri küberkaitse koolitusvajaduste analüüsile ning Euroopa Julgeoleku- ja Kaitsekolledži küberjulgeoleku koolituse käigus saadud kogemustele tuginedes ÜJKP koolitus- ja hariduskavad erinevatele sihtgruppidele, mille hulka kuuluvad Euroopa välisteenistus, ÜJKP missioonide ja operatsioonide personal ning liikmesriikide ametnikud; nende kavadega käsitletakse ka kvalifitseeritud töötajate hoidmise küsimusi lühikeses, keskmises ja pikas perspektiivis;
- teevad ettepaneku käivitada küberkaitsealane dialoog, mis käsitleb koolitusstandardeid ja sertifitseerimist ning mida peetakse liikmesriikide, ELi institutsioonide, kolmandate riikide ja teiste rahvusvaheliste organisatsioonide ning erasektoriga;
- teevad koostööd Euroopa erasektori koolitajatega ning akadeemiliste institutsioonidega, et parandada ÜJKP missioonide ja operatsioonide personali pädevust ja oskusi.

Euroopa Julgeoleku- ja Kaitsekolledž teeb järgmist:

- arendab edasi enda struktuuris loodud küberhariduse, -koolituse, -hindamise ja -õppuste platvormi (küberplatvorm);
- loob koostoime teiste sidusrühmade koolitusprogrammidega (ENISA, Europol, Euroopa politseikolledž) ning NATO kooperatiivse küberkaitse kompetentsikeskusega;
- analüüsib võimalusi luua Euroopa Julgeoleku- ja Kaitsekolledži ja NATO Kaitsekolledži ühiseid küberkaitse koolitusprogramme, mis on avatud kõigile ELi liikmesriikidele, et tugevdada ühist küberkaitsealast kultuuri.

Komisjon teeb järgmist:

- hindab võimalusi küberplatvormi määratletud koolitus- ja haridusvõimaluste laiendamiseks liikmesriikides.

Euroopa Kaitseagentuur teeb järgmist:

- arendab koostöös Euroopa Julgeoleku- ja Kaitsekolledžiga edasi oma kursusi, et täita liikmesriikide küberkaitse hariduse, koolituse ja õppuste alaseid nõudeid;
- toetab küberplatvormi, muu hulgas järkjärguliselt integreerides sinna Euroopa Kaitseagentuuri raames väljatöötatud küberhariduse, -koolituse, -hindamise ja -õppuse moodulid.

Euroopa välisteenistus ja liikmesriigid teevad järgmist:

- järgivad Euroopa Julgeoleku- ja Kaitsekolledži kehtestatud koolitusprogrammide sertifitseerimismehhanisme, tehes seda tihedas koostöös ELi institutsioonide, organite ja asutuste asjakohaste talitustega ning tuginedes olemasolevatele standarditele ja teadmistele. Analüüsivad võimalusi luua sõjalise Erasmuse algatuse raames kübervaldkonda käsitlevaid koolitusmooduleid.

Parandada tuleb küberkaitseõppuste läbiviimise võimalusi ÜJKP sõjaliste ja tsiviilvaldkonna osapoolte jaoks. Ühisõppused aitavad arendada ühiseid teadmisi ja ühist arusaamist küberkaitse kohta. See võimaldab siseriiklikel osalejatel tõhustada oma valmisolekut tegutseda rahvusvahelises keskkonnas. Ühiste küberkaitseõppuste läbiviimine suurendab ka koostalitlusvõimet ja usaldust.

Euroopa välisteenistus, Euroopa Kaitseagentuur, ELi infoturbeintsidentidega tegelev rühm ja liikmesriigid keskenduvad küberkaitse elementide edendamisele ÜJKP ja teiste õppuste raames ning:

- lisavad küberkaitse mõõtme õppuste *MILEX* ja *MULTILAYER* olemasolevatesse stsenaariumitesse;
- korraldavad korrapäraselt strateegilisi/poliitilisi õppusi nagu *CYBRID 2017*, koordineerides seejuures ELi juhitud paralleelse ja koordineeritud õppusega (PACE) ning tehnilis-operatiivsete õppustega nagu *DEFNET*;
- töötavad vajaduse korral välja ELi ÜJKP küberkaitseõppuse ning analüüsivad võimalusi tegevuse koordineerimiseks üleeuroopaliste küberõppustega nagu näiteks ENISA korraldatud *CyberEurope*;
- osalevad jätkuvalt teistes mitmepoolsetes küberkaitseõppustes nagu *Locked Shields*;
- kutsuvad asjakohaseid rahvusvahelisi partnereid (nagu NATO) osalema õppustel kooskõlas ELi õppuste poliitilise raamistikuga;
- korraldavad korrapäraselt õppusi, võttes aluseks küberdiplomaatia meetmete kogumi, mille käigus saavad ELi liikmesriigid harjutada reageerimist pahatahtlikule kübertegevusele.

6. Koostöö tõhustamine asjakohaste rahvusvaheliste partneritega

Rahvusvahelise koostöö raames tuleb tagada dialoog rahvusvaheliste partneritega, eelkõige NATO ja teiste rahvusvaheliste organisatsioonidega, et toetada tulemuslike küberkaitsevõime arendamist. Tuleks püüda suurendada osalemist töös, mida tehakse Euroopa Julgeoleku- ja Koostööorganisatsiooni (OSCE) ja Ühinenud Rahvaste Organisatsiooni (ÜRO) raames, et aidata luua küberruumis konfliktide ennetamist, koostööd ja stabiilsust käsitlev strateegiline raamistik.

ELis on olemas poliitiline tahe teha küberkaitse küsimustes täiendavat koostööd NATOga ning luua tugev ja vastupidav küberkaitsevõime, nagu nähti ette Euroopa Ülemkogu eesistuja, Euroopa Komisjoni presidendi ja Põhja-Atlandi Lepingu Organisatsiooni peasekretäri ühisdeklaratsioonis, mis võeti vastu Varssavis 8. juulil 2016. Korrapärased ametnikevahelised konsultatsioonid, vastastikused teavitamised ning poliitilis-sõjalise töörühma ja NATO asjakohaste komiteede võimalikud kohtumised aitavad ära hoida mittevajalikku töö dubleerimist ning tagada jõupingutuste sidusus ja vastastikune täiendavus, mis on kooskõlas eelnimetatud raamistikuga.

Euroopa välisteenistus ja Euroopa Kaitseagentuur arendavad koos liikmesriikidega küberkaitse valdkonnas täiendavat koostööd ELi ja NATO vahel, võttes nõuetekohaselt arvesse institutsioonilist raamistikku ja kõnealuste organisatsioonide sõltumatust otsuste tegemisel ning:

- tõhustavad käimasolevaid tegevusi Euroopa Ülemkogu eesistuja, Euroopa Komisjoni presidendi ja Põhja-Atlandi Lepingu Organisatsiooni peasekretäri ühisdeklaratsiooni rakendamise raames;
- vahetavad parimaid tavasid kriisiohjamise küsimustes ning sõjaliste- ja tsiviilmissioonide ja operatsioonide küberkaitse küsimustes;
- tagavad küberkaitsevõime nõuete arendamisel tulemuste sidususe, kui need nõuded kattuvad, eelkõige küberkaitse pikaajaliste võime arendamise puhul;
- kasutavad täiendavalt Euroopa Kaitseagentuuri ja NATO kooperatiivse küberkaitse kompetentsikeskuse vahelist koostööraamistikku, mis toimib esialgse platvormina tõhustatud koostöö tegemiseks rahvusvaheliste küberkaitse projektide raames, tuginedes asjakohastele hindamistele.

Euroopa Julgeoleku- ja Kaitsekolledž, Euroopa välisteenistus ja Euroopa Kaitseagentuur teevad järgmist:

- tõhustavad koostööd küberkaitse valdkonna koolituse ja hariduse ning õppuste kontseptsioonide osas;
- tagavad töötajate vastastikkuse osalemise õppustes kooskõlas heakskiidetud raamistikuga.

ELi infoturbeintsidentidega tegelev rühm teeb järgmist:

- kasutab täiendavalt tehnilist kokkulepet, mis on sõlmitud ELi infoturbeintsidentidega tegeleva rühma ning NCIRC (NATO küberturbeintsidentidega tegelev organ) vahel, et parandada olukorrast ülevaate saamist, teabevahetust ja varase hoiatamise mehhanisme ning tuvastada ohte, mis võivad mõlemat organisatsiooni mõjutada.

Teiste rahvusvaheliste organisatsioonide ja ELi asjakohaste rahvusvaheliste partnerite osas teevad Euroopa välisteenistus ja liikmesriigid vajadusel järgmist:

- jälgivad strateegilisi arenguid ja peavad rahvusvaheliste partneritega (rahvusvahelised organisatsioonid ja kolmandad riigid) konsultatsioone küberkaitse küsimustes;
- analüüsivad koostöövõimalusi küberkaitse küsimustes, sealhulgas kolmandate riikidega, kes osalevad ÜJKP missioonides ja operatsioonides;
- edendavad asjakohastes rahvusvahelistes organisatsioonides, eelkõige ÜROs, OSCEs ja ASEANi piirkondlikus foorumis kehtiva rahvusvahelise õiguse (eelkõige ÜRO põhikirja) kohaldamist küberruumis, riikide vastutustundliku küberruumis käitumise üldiste mittesiduvate normide väljaarendamist ja rakendamist ning piirkondlikke usalduse suurendamise meetmeid riikide vahel, et suurendada läbipaistvust ning vähendada riigi käitumise vääritimõistmise ohtu.

Komisjon ja Euroopa välisteenistus teevad järgmist:

- toetavad vajadusel ELi partnerite kübersuutlikkuse suurendamist, kasutades selleks muudetud stabiilsuse ja rahu edendamise rahastamisvahendit.

Järelmeetmed

Euroopa välisteenistus koordineerib küberkaitsepoliitika raamistiku rakendamist ning Euroopa välisteenistus, Euroopa Kaitseagentuur ja komisjon peaksid igal aastal esitama poliitilis-sõjalisele töörühmale (horisontaalse küberküsimuste töörühma liikmete osalusel) ning poliitika- ja julgeolekukomitee eduaruande, mis hõlmab ülaltoodud kuut valdkonda, et hinnata küberkaitsepoliitika raamistiku rakendamist. Iga kuue kuu järel tehakse ka suuline ettekanne.

Väga oluline on, et küberohu arenemisega üheaegselt tehakse kindlaks uued küberkaitse nõuded, mis seejärel lisatakse küberkaitsepoliitika raamistikku. Küberkaitsepoliitika raamistiku järgmine läbivaatamine peaks toimuma hiljemalt 2022. aasta keskpaigaks ning toimuma liikmesriikidega tihedalt konsulteerides.