HÜBRIIDOHTUDE JA KÜBERI KÄSITLUS EUROOPA LIIDU ÜHISE JULGEOLEKU- JA KAITSEPOLIITIKA TSIVIILMISSIOONIDE EKSPERTIDE KOOLITUSNÕUETE KONTEKSTIS

KOOSTANUD: INGE LINDSAAR
JAANIKA PUUSALU

Sisekaitseakadeemia
Sisejulgeoleku Instituut
2020

Sisukord

KOKKUVÕTE: EUROOPA LIIDU ÜHTSE JULGEOLEKU JA KAITSEPOLIITIKA TSIVIILMISSIOONIDE HÜBRIIDOHTUDE JA KÜBERI KOOLITUSVALDKONNA KOOLITUSNÕUETE ANALÜÜS sh KÕRGETASEMELISTE ÕPIVÄLJUNDITE VÄLJA TÖÖTAMINE

ELi küber- ja hübriidohtude poliitika

Tehnoloogia, sealhulgas info- ja kommunikatsioonitehnoloogia (IKT), kiire areng viimaste kümnendite jooksul on endaga kaasa toonud piirideta küberruumi ning tohutu hulga uusi suhtlus- ja teabevahetusvektoreid, mis muutnud nii lävimise kui ka tööpraktikaid kogu maailmas. Üksikisikud kasutavad võrguühendusega arvuteid ja seadmeid nii tööks (nt juurdepääs kaugandmebaasidele või asjakohaste dokumentide jagamine) kui ka vaba aja veetmiseks (nt ajalehtede lugemine ja suhtlus sõpradega). Riigil lihtsustab IT-tehnoloogia riigi teenuste pakkumist ning piirideta küberruum lisab võimalusi rahvusvaheliseks koostööks ja rahvusvahelistumiseks. Euroopa Liidu kontekstis soodustab küberruum riikidevahelist infovahetust ja koostööd ning annab ka ühisturu tagamiseks paremad võimalused.

Võrgustatud tehnoloogia kasvav kasutus ning üha suurem sõltumine küberruumist k.a elutähtsate teenuste tagamiseks, on kaasa toonud ka uusi ohte nii üksikisikust kasutajatele kui ka riikidele ja riikide ühendustele. Virtuaalne küberruum, näiteks, võimaldab kaugjuhtimisega küberrünnakuid, mis võivad mõjutada kogu võrku. Samuti on välja kujunenud uued kuriteovormid (sh küberkuritegevus). Lisaks rakendatakse uusi tehnoloogilisi vahendeid ka hübriidsõjas, nt veebipõhised desinformatsiooni kampaaniad, mis kasutavad piirideta ning väheste reeglitega küberruumi võimalusi informatsiooni kiireks ja laialdaseks levitamiseks. Selliste arengute ja tehnoloogiakasutuse tulemusel muutuvad inimesed vastuvõtlikuks ebasobivale ja/ või pahatahtlikule tegevusele nii tööl kui ka vabal ajal. Riikide pakutavate teenuste toimepidevus sõltub võrkude turvamise võimest ning nõuab pidevat meetmete täiendamist; desinformatsiooni kampaaniate mõju vähendamiseks ning küberkuritegevuse riskide maandamiseks on vaja elanikkonna teadlikkust tõsta.

Kuna ELi kui riikide ühenduse puhul ohustab ka pelgalt ühe riigi vastu toimunud (ühe riigi sees toimunud) küberintsident potentsiaalselt kogu liidu võrku ning ühisturu toimevõimet, on iga üksiku riigi küberturbevõime võtmetähendusega kogu ELi turvalisuse ning jätkusuutliku toimimise tagamiseks. Küberkeskkonnaga kaasnevate ning järjest lisanduvate ohtude tõttu on nii EL kui ka liikmesriigid tunnistanud vastupanuvõime suurendamise vajadust, et uusi ohte tõhusalt maandada. Oluline on tagada ühisturu toimimine ning teenuste kättesaadavus. Nende tagamiseks on Euroopa Liit alates 2000ndate algusest alates astunud konkreetseid samme näiteks nii võrgu- ja infosüsteemide turvalisuse kindlustamiseks, turvaintsidentidest teavitamiseks kui ka hübriidohtudele vastupanu suurendamiseks.

ELi ÜJKP missioonid: küber- ja hübriidohtud

Ka ELi ühise julgeoleku- ja kaitsepoliitika (ÜJKP)[1] missioonid, sealhulgas tsiviilmissioonid kolmandates riikides, tuginevad suhtlemisel ja teabevahetusel ning oluliste teenuste pakkumisel stabiilsele ja hästi toimivale küberkeskkonnale. Lisaks on tihti ka missiooniliikmete erasuhtlus veebirakendustel tuginev. ELi sees on küberturbe meetmed ühtlustatud, vajalikud institutsioonid ja agentuurid ellu kutsutud ning ka ELi ÜJKP missioonide turvalisuse tagamisele kiiresti arenevas ohukontekstis pööratakse suurendatud tähelepanu. Sellest hoolimata on ELi ÜJKP missioonid (tsiviil- ja sõjalised) haavatavas olukorras. Nimelt, kuigi tehnoloogiat ja võrke vajatakse nii tööks kui ka suhtlemiseks, ei tohi vastuvõtva riigi küberruumi ja IT-seadmete suhtes kohaldada samal tasemel julgeoleku seiret ja reguleerimist kui ELis. Samuti ei pruugi IT-taristu arendamine vastuvõtvas riigis olla nii arenenud (ja nii turvaline) kui ELis. Nii võidakse ÜJKP missiooni asukohariiki ohustada just küber- või hübriidohtude kaudu aga ka missioon ise võib nii füüsiliselt kui ka praktiliselt olla küber- või hübriidrünnakute sihtmärgiks. Just ELi ÜJKP tsiviilmissioonid on siinkohal eriti haavataval positsioonil, sest erinevalt sõjalistest missioonistes, ei vastuta vastuvõttev riik selle eest, et kommunikatsiooni- ja informatsioonisüsteemid vastaksid koostalitus- ja turvanõuetele. Samuti ei toeta ka CERT-EU[2] missioone süstemaatiliselt. Seega on tsiviilmissioonid ohustatumad ja risk puutuda kokku küber- või hübriidohtudega veelgi suurem.[3]

Süsteemsemaks ÜJKP tsiviilmissioonide küber- ja hübriidohtude ennetamiseks ning missiooni turvalisuse tagamiseks on Euroopa Välisteenistus[4] välja töötanud mitmeid viise küberjulgeoleku meetmete täiendavaks integreerimiseks ÜJKP tsiviilmissioonide kavandamisesse ja läbiviimisesse (nt 2020. aastal Kesk-Aafrika Vabariigis alustanud tsiviilmissioonil on spetsiaalselt planeeritud võimekus[5] võimalike missioonile suunatud ohtude/rünnakute ennetamiseks; Georgia missioon, sarnaselt, saab süsteemset ohuülevaadet). Samuti on kinnitamisel Euroopa Välisteenistuse poolt välja töötatud mini-kontseptsioon[6] ÜJKP tsiviiltoetuse kohta hübriidohtude vastu võitlemisel, mis käsitleb ÜJKP tsiviilmissioonide kontekstis hübriidohtude kindlakstegemise, neile reageerimise ja neile vastupanuvõime suurendamise prioriteetset valdkonda.

ELi ÜJKP missioonid: koolitusvõimalused ja kõrgetasemeliste õpiväljundite välja töötamine

ÜJKP (tsiviil)missioonide liikmete võimekuste, k.a küber- ja hübriidohtude alaste võimekuste, ühtlustamine ja tõstmine on oluline nii missioonide turvalisuse tagamiseks kui ka missiooni õnnestumiseks sh ELi ümbritsevate riikides suurema stabiilsuse ning jätkusuutliku arengu tagamiseks. Nii on missioonide turvalisuse tagamisel ning missiooni õnnestumisel Euroopa Nõukogu pööranud suurt tähelepanu lisaks missiooni üldise võimekuse tõstmisele ka

[1] Ingl k *Common Security and Defence Policy (CSDP)*
[2] Ingl k *Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU)*
[3] Allikas: *Küberjulgeoleku integreerimine ÜJKP tsiviilmissioonide kavandamisse ja läbiviimisse*. (Euroopa välisteenistuse töödokument, 16. juuni 2017, Euroopa Välisteenistus (2017) 773.
[4] Ingl k *Europan External Action Service (EEAS)*
[5] Ing k *Mission Analytic Capacity (MAC)*
[6] Mini-kontseptsiooni väljatöötamisel nõustas Euroopa Välisteenistust ka Sisekaitseakadeemia Sisejulgeoleku Instituudi nõunik ning ELi Ühise Julgeoleku- ja Kaitsepoliitikat (ÜJKP) rakendavate tsiviilmissioonide ametnike väljaõppeks vajaliku hübriidohtude ja küberi õpiväljundite väljatöötamise juht Inge Lindsaar.

missiooniliikmete individuaalsete võimekuste ning väljaõppe küsimustele k.a ootus liikmesriikide veelgi suuremale panusele tulevaste missiooni liikmete koolitamisel ning Euroopa Välisteenistuse panus tsiviilimissiooni liikmete võimekuste ühtlustamisel ja suurendamisel.

Ühe meetmena alustati vastavalt Euroopa Liidu Tsiviilse Koolitusgrupi (EUCTG)[7] strateegilistele juhistele[8] 2019. aastal Euroopa Välisteenustuse algatusel ja koordineerimisel ning liikmesriikide ja liikmeriikide institutsioonidega koostöös ÜJKP tsiviilväljaõppeks vajalike võimete kaardistamist ning Tsiviilse koolitusvaldkonna kõrgetasemeliste õpiväljundite välja töötamist varem tuvastatud võimeklastrite[9] alusel.

Eesti panus: hübriidohtude ja küberi tsiviilkoolitusvaldkonna kõrgetasemeliste õpiväljundite välja töötamine

2019. aasta oktoobris võttis Sisejulgeoleku Instituut (SJI) Eesti Välisministeeriumi ettepanekul kohustuse koostada ELi Ühise Julgeoleku- ja Kaitsepoliitikat (ÜJKP) rakendavate tsiviilmissioonide ametnike väljaõppeks vajaliku hübriidohtude ja küberi õpiväljundid (võimeklaster: *Hybrid threats and cyber*) .

Kõrgetasemeliste õpiväljundite välja töötamiseks moodustati SJI juhtimisel konsortsium, kuhu kuulusid Eesti ja Austria Siseministeeriumite, Tallinna Tehnikaülikooli, Euroopa Liidu vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimise agentuuri (eu-LISA), Euroopa Julgeoleku- ja Kaitsekolledži (ESDC) ja Hübriidohtude vastu võitlemise Euroopa Oivakeskuse (Hybrid CoE) esindajad.

Õpiväljundite koostamise eesmärgiks on ühtlustada ÜJKP missioonidele saadetavate esmatasandi, keskastme ja küberi ja hübriidohtude ekspertide teadmiste ja oskuste tase kõikidel ÜJKP missioonidel.[10] Samuti loovad kõrgetasemelised õpiväljundid kindla raamistiku ühtsete hübriidohtude ja küberi õppekavade välja töötamiseks ning võimaluse luua sihtgrupi

[7] *EU Civilian Training Group*

[8] Allikas: *EUCTG Stategic Guidance on CSDP Civilian Training.* (Strateegiline juhis, 6 juuni 2019, Euroopa Liidu Tsiviilne Koolitusgrupp, 9898/19).

[9] Võimeklastrid (originaalkeeles): Leadership and management; Planning (strategic and operational planning, situational awareness); Political analysis and reporting; Rule of Law ; Security Sector Reform (SSR) ; Good governance, state building, civil administration, building integrity and anti-corruption; Gender; IHL, Human Rights, Protection of Civilians; Mentoring, monitoring and advising (MMA); Mediation, negotiation and dialogue; Language skills; Communication, behavioural and cultural skills; Strategic Communication, Press and public information; Human resources and finance; Logistics, procurement, IT and CIS; Safety and security; Code of Conduct; Medical issues; Standards of behaviour; The EU Integrated Approach to external conflicts and crises applied to CSDP; Conflict prevention; Countering organised crime; Support to border management; Countering terrorism and radicalisation; Addressing irregular migration related security challenges; Support to maritime security; *Hybrid threats and cyber*; Protection of cultural heritage; Climate change. (Hiljem lisandus ka võimeklaster 'prantsuse keel võõrkeelena').

[10] ELi ÜJKP tsiviilmissioone on 2020. aasta oktoobri seisuga 11. ELi ÜJKP struktuurid juhavad 10 missiooni, mis asuvad Ukrainas (EUAM Ukraine), Georgias (EUMM Georgia), Palestiina aladel (EUBAM RAFAH), Kosovos (EULEX Kosovo), Malis (ECAP SAHEL Mali), Nigeerias (EUCAP SAHEL Niger), Liibüas (EUBAM Libya), Kesk-Aafrika Vabariigis (AUAM RCA Central Africa Republic), Somaalias (EUCAP Somalia), Iraagis (EUAM Iraq).

vajadustele vastavad koolituskavad. Nimetatud raamistik on paindlik ning võimaldab erinevate hübriidohtude ja küberi teemaliste kursuste ja koolituste korraldamist.

Õpiväljundite loomiseks koostati ülevaade ELi vastavatest poliitikadokumentidest ja analüüsiti õiguslikku raamistikku ning kaardistati ja analüüsiti missioonidele saadetavate kandidaatide ettevalmistusega seotud õppeasutuste koolitusprogramme.

2020. aasta kevad-suvel viidi läbi ka ELi ÜJKP tsiviilmissioonidel viibivate ametnike küsitlus eesmärgiga selgitada välja hübriidohtusid ja küberit puudutavad olulised ja huvipakkuvad teemad edasiste koolituste kavandamiseks. Dokument esitati ELi Välisteenistusele oktoobris 2020.

Edasised võimalused

Hübriidohtude ja küberi Koolitusnõuete Analüüsi sh kõrgetasemeliste õpiväljundite loomisega on ELi Välisteenistute poolt püstitatud ülesanne täidetud. Erinevate võimeklastrite õpiväljundid konsolideerib ELi Välisteenistus kõigu õpiväljundite valmimisel, mil peaks toimuma ka arutelu edasiste sammude osas ÜJKP missioonidele saadetavate ja missioonidel viibivate teenistujate teadmiste ja oskuste taseme ühtlustamiseks kõikidel ÜJKP missioonidel.

Välja töötaud hübriidohtude ja küberi õpiväljundite alusel on EL liikmesriikidel (k.a sobilikel liikmesriikide institutsioonidel) aga ka ELi institutsioonidel (nt European Security and Defence College või Hybrid CoE) edaspidi võimalus luua ja pakkuda koolitusi, mis tuvastatud koolitusvajadusi kataks ning kõrgetasemelistele õpiväljunditele vastaks. Koolituste välja töötamisel peaks arvesse võtma ka õpiväljundite välja töötamiseks tehtud ELi institutsioonides olemasolevate ning missiooni liikmetele kättesaadavate koolituste analüüsi ja missiooni liikmete koolitusvajadusi ja -huvisid.

Olemasolevate koolituste analüüs toob välja, et I) hetkel on EÜJP missioonidele kättesaadavatest baastaseme hüriidohtude ja küberi koolitustest vajaka; II) hetkel pole konkreetselt EÜJP tsiviilmissioonidele suunatud hüriidohtude ja küberi koolitused piisavalt organiseeritud ja hübriidohtudele ja küberile suunatud; ning III) enamus pakutavatest ning kättesaadavates koolitustest k.a spetsialistide tasemel, on küber-teemalised.

Tsiviilmissiooni liikmete koolitushuvi analüüsis selgus, et I) missiooni liikmetel on huvi ennekõike praktilist-laadi koolituste järele; II) koolituse kättesaadavuse tagamiseks eelistatakse veebi-põhist õpet; ning III) kiiresti muutuva ohumaastiku tõttu on vajadus korduva ning täiendkoolituse järele.

Loodud kõrgetasemelised õpiväljundid on üles ehitatud seitsmele kesksele hübriidohtude ja küberi teemale[11]. Koolituste sihtgruppideks on missioonidele saadetavad või enam kui 3 aastat missioonidel töötanud baas-, kesk- või eksperttaseme ametnikud.

[11] Teemad: (I) ELi vastus hübriidohtudele ja küberile; (II) Tööks vajaliku riist- ja tarkvara turvaline kasutus tööruumides; (III) Isikliku riist- ja tarkvara turvaline kasutus tööruumidest väljapool; (IV) Olukorrateadlikkus; (V) Hübriidohud; (VI) Küberohud; (VII) Füüsilised ohud riist- ja tarkvarale nt IT-süsteemidele. Teemad (originaalkeeles): (I) General EU response to hybrid threats and cyber; (II) Safe use of work-related systems and devices in mission premises; (III) Safe use of personal devices outside mission premises; (IV) Situational awareness; (V) Hybrid threats; (VI) Cyber threats; (VII) Physical threats to IT-systems etc.

ELi ÜJKP MISSIOONIDE HÜBRIIDOHTUDE JA KÜBERI TSIVIILKOOLITUSVALDKONNA KOOLITUSNÕUETE ANALÜÜS[12]

SISSEJUHATUS

2019. aasta oktoobris võttis Sisejulgeoleku Instituut (SJI) Eesti Välisministeeriumi ettepanekul kohustuse koostada ELi Ühise Julgeoleku- ja Kaitsepoliitikat (ÜJKP) rakendavate tsiviilmissioonide ametnike väljaõppeks vajaliku hübriidohtude ja küberi õpiväljundid (võimeklaster: *Hybrid threats and cyber*) .

Kõrgetasemeliste õpiväljundite välja töötamiseks moodustati SJI juhtimisel konsortsium, kuhu kuulusid Eesti ja Austria Siseministeeriumite, Tallinna Tehnikaülikooli, Euroopa Liidu vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimise agentuuri (eu-LISA), Euroopa Julgeoleku- ja Kaitsekolledži (ESDC) ja Hübriidohtude vastu võitlemise Euroopa Oivakeskuse (Hybrid CoE) esindajad.

Õpiväljundite koostamise eesmärgiks on ühtlustada ÜJKP missioonidele saadetavate esmatasandi, keskastme ja küberi ja hübriidohtude ekspertide teadmiste ja oskuste tase kõikidel ÜJKP missioonidel.[13] Samuti loovad kõrgetasemelised õpiväljundid kindla raamistiku ühtsete hübriidohtude ja küberi õppekavade välja töötamiseks ning võimaluse luua sihtgrupi vajadustele vastavad koolituskavad. Nimetatud raamistik on paindlik ning võimaldab erinevate hübriidohtude ja küberi teemaliste kursuste ja koolituste korraldamist.

Õpiväljundite loomiseks koostati ülevaade ELi vastavatest poliitikadokumentidest ja analüüsiti õiguslikku raamistikku ning kaardistati ja analüüsiti missioonidele saadetavate kandidaatide ettevalmistusega seotud õppeasutuste koolitusprogramme.

2020. aasta kevad-suvel viidi läbi ka ELi ÜJKP tsiviilmissioonidel viibivate ametnike küsitlus eesmärgiga selgitada välja hübriidohtusid ja küberit puudutavad olulised ja huvipakkuvad teemad edasiste koolituste kavandamiseks. Dokument esitati ELi Välisteenistusele oktoobris 2020.

Taust

Tehnoloogia, sealhulgas kommunikatsioonitehnoloogia, kiire areng on viimaste kümnendite jooksul toonud endaga kaasa tohutu hulga uusi suhtlus- ja teabevahetusvektoreid ning muutnud tööpraktikaid kogu maailmas. Võrguühendusega arvuteid ja seadmeid kasutatakse nii tööks (nt juurdepääs kaugandmebaasidele või asjakohaste dokumentide jagamine) kui ka vaba aja veetmiseks (nt ajalehtede lugemine ja suhtlus sõpradega).

[12] Tegemist on eestindatud ja kärbitud versiooniga 2020. aasta oktoobris Euroopa Välisteenistusele esitatud inglise keelsest dokumendist.

[13] ELi ÜJKP tsiviilmissioone on 2020. aasta oktoobri seisuga 11. ELi ÜJKP struktuurid juhavad 10 missiooni, mis asuvad Ukrainas (EUAM Ukraine), Georgias (EUMM Georgia), Palestiina aladel (EUBAM RAFAH), Kosovos (EULEX Kosovo), Malis (ECAP SAHEL Mali), Nigeerias (EUCAP SAHEL Niger), Liibüas (EUBAM Libya), Kesk-Aafrika Vabariigis (AUAM RCA Central Africa Republic), Somaalias (EUCAP Somalia), Iraagis (EUAM Iraq).

Võrgustatud tehnoloogia kasvav kasutamine on toonud kaasa ka uusi ohte. Virtuaalne küberruum võimaldab kaugjuhtimisega küberrünnakuid, mis võivad mõjutada kogu võrku. Samuti on välja kujunenud uued kuriteovormid (sh küberkuritegevus). Lisaks rakendatakse uusi tehnoloogilisi vahendeid ka hübriidsõjas, nt. veebipõhised desinformatsiooni kampaaniad, mis kasutavad piirideta ning väheste reeglitega küberruumi võimalusi. Selliste arengute ja kasutuse tulemusel muutuvad võrgud ja inimesed vastuvõtlikuks ebasobivale ja/ või pahatahtlikule tegevusele nii tööl kui ka vabal ajal.

EL, liikmesriigid, ELi institutsioonid ning ELi ühise julgeoleku- ja kaitsepoliitika (ÜJKP) missioonid, sealhulgas tsiviilmissioonid kolmandates riikides, tuginevad suhtlemisel ja teabevahetusel ning oluliste teenuste pakkumisel stabiilsele ja hästi toimivale küberkeskkonnale. Küberkeskkonnale tuginemisele omaste ohtude tõttu on EL tervikuna ja ka üksikud liikmesriigid eraldi tunnistanud vastupanuvõime suurendamise vajadust, et tõhusalt astuda uutele ohtudele vastu.

ELi ÜJKP missioonid (tsiviil- ja sõjalised) on eriti haavatavas olukorras, kuna nad asuvad kolmandates riikides. Ehkki nii tehnoloogiat kui ka võrke vajatakse näiteks nii tööks kui suhtlemiseks, ei tohi vastuvõtva riigi küberruumi ja IT-seadmete suhtes kohaldada samal tasemel julgeoleku seiret ja reguleerimist kui ELis. Samuti ei pruugi IT-taristu arendamine vastuvõtvas riigis olla nii arenenud (ja nii turvaline) kui ELis. Nii võidakse ÜJKP missiooni asukohariiki ohustada just küber- või hübriidohtude kaudu aga ka missioon ise võib nii füüsiliselt kui ka praktiliselt olla küber- või hübriidrünnakute sihtmärgiks.

Arvestades seda uut ja kiiresti arenevat ohumaastikku, pööratakse suuremat tähelepanu ja tunnistatakse vajadust suurendada missioonide vastupanuvõimet ja missiooni liikmete teadlikkust uutest tekkivatest ohtudest.

Eesmärk ja ulatus

Käesoleva koolitusnõuete analüüsi eesmärk on mitmetahuline. Esmalt selgitati välja tsiviilvõimeklastri „hübriidoht ja küber" jaoks vajalike koolitusteemade raamistik, seejärel kaardistati praegu missioonidega liituda soovivate ametnike jaoks saada olevad hübriidohtusid ja küberit käsitlevad koolitused ja neid pakkuvad õppeasutused ning viimaks arendati tsiviilõppeala kõrgetasemelised õpitulemused (CTALO), mis peaks olema suunavaks raamistikuks ÜJKP tsiviilmissioonide liikmete mistahes uute ja täiendkoolituste väljatöötamisel hübriidohtude ja küberi valdkonnas.

Koolitusnõuete analüüsi eesmärk on analüüsida tsiviilmissiooni liikmete ligipääsetavust hübriidohtusid ja küberit käsitletavatele koolitustele. Kõigile missiooni liikmetel mõeldud koolitused peaksid keskenduma sellele, kuidas igapäevaseid tööülesandeid missioonil viibimise ajal uusi tehnoloogiaid kasutades küberturvaliselt täita ja ka töövälisel ajal kasutada tehnoloogiaid viisil, mis ei kompromiteeriks ei missiooni ega ka missiooni turvalisust ja/või küberturvalisust.

Analüüs sisaldab soovitusi CTALO-de alusel ÜJKP missiooni liikmete täiendõppe arendamiseks, et tõsta ja ühtlustada teadlikkust seitsmest kesksest „hübriidohtude ja küberi" teemast: (I) ELi üldine reageerimine hübriidohtudele ja kübervaldkonnale; (II) tööga seotud süsteemide ja

seadmete ohutu kasutamine missiooniruumides; (III) isiklike seadmete ohutu kasutamine väljaspool missiooniruume; (IV) olukorrateadlikkus; (V) hübriidohud; (VI) küberohud; (VII) füüsilised ohud IT- ja IKT-süsteemidele jne.

Koolitusnõuete analüüsi (KNA) struktuur

KNA-l on järgmine ülesehitus:

Esimeses osas analüüsitakse hübriidohtude ja küberiga seotud poliitikadokumente pöörates seejuures erilist tähelepanu Euroopa ühisele julgeoleku- ja kaitsepoliitikale (ÜJKP) ning ELi ÜJKP tsiviilmissioonidele ja missioonide kavandamisele.

Teises osas kaardistatakse ja analüüsitakse EL-i ÜJKP tsiviilmissiooni liikmetele praegu (või lähiajal) kättesaadavad koolitused hübriidohtude ja küberi valdkonnas.

Viimases osas esitatakse tsiviilõppeala kõrgetasemelised õpitulemused (CTALO), mis on välja töötatud seitsme „hübriidohtude ja kübervaldkonna" teema järgi, mille konsortsium on ÜJKP tsiviilmissioonide liikmete jaoks asjakohaseks tunnistanud.

I POLIITIKADOKUMENTIDE ANALÜÜS

Vastavalt Euroopa Liidu Tsiviilse Koolitusgrupi (EUCTG) [14] strateegilistele juhistele ÜJKP tsiviilväljaõppe kohta viidi läbi põhjalik uuring ELi poliitikast ja raamdokumentidest, et teha kindlaks ÜJKP missioonide tulemuslikkuse seisukohast olulised poliitikavaldkonnad, eriti seoses võimekusklastriga „Hübriidohud ja küber".

Selles peatükis esitatakse esmalt kokkuvõte (siiani)[15] kõige asjakohasematest ELi dokumentidest, mis käsitlevad hübriidohtusid ja küberit. Teiseks esitatakse ühised teemad ja kolmandaks antakse soovitused või juhitakse tähelepanu aspektidele, mille rakendamisele tuleks ÜJKP tsiviilmissioonidel erilist tähelepanu pöörata.

Poliitikadokumentide kokkuvõte jaguneb omakorda kaheks. Alapeatükk 1.1. võtab kokku põhilised küberruumi ja selle haldamist käsitlevad ELi dokumendid, mis on seotud tsiviilvõimeklastriga „Hübriidohud ja küber". Need dokumendid tutvustavad ja määratlevad kogu ELi hõlmava lähenemisviisi küberruumile ja küberruumi juhtimisele, samuti esitatakse lähenemisviisid ja koostöö hübriidohtude osas. Lisaks määravad need dokumendid kindlaks küber- ja hübriidjuhtumitele reageerimise ning vastutuse, mida iga liikmesriik peab endale võtma. Alapeatükk 1.2. võtab kokku ELi dokumendid (sealhulgas aruanded), mis hõlmavad hübriidohtusid ja küberteemasid seoses ÜJKP missioonidega (sealhulgas ettepanekud lähetuseelse koolituse parandamiseks ning küber- ja hübriidohu võimekuse suurendamiseks missioonil). Mõlemas osas võetakse dokumendid kokku, esitades kesksed teemad, mis on olulised ÜJKP missioonide jaoks.

Esimene dokumendikomplekt (punkt 1.1.) on oluline, kuivõrd see väljendab ÜJKP missioonidele kolmandates riikides laienevaid ELi põhiväärtusi küberruumi kohta. Samuti määratletakse dokumentides vastuste ja teabevahetusprotokollide standardiseerimine, seatakse koolituse prioriteedid, määratakse kindlaks küberintsidendi toimumisel vastutavad ELi institutsioonid, sätestatakse koostöövajadused teiste rahvusvaheliste organisatsioonide ja kolmandate riikidega jne. Neid punkte arvestades on kõigi ÜJKP ja sellega seotud missioonidega seotud töötajate jaoks oluline olla teadlik nendest dokumentidest ja nendes käsitletavatest kesksetest teemadest.

Teine dokumendikomplekt (punkt 1.2.) Sisaldab üksikasjalikku teavet ÜJKP missioonide hübriidohtude vastupanu ning küberettevalmistuse kohta. Kuigi nendes dokumenteeritud ÜJKP missioonidega seotud lepingud ja arengud on asjakohased ka kõigi missiooni liikmete jaoks, on ÜJKP missioonide olukorra ja edasiarendamise üksikasjad missiooni kõrgema juhtkonna ja asjakohaste (hübriidohtude ja küber) ekspertide jaoks eriti olulised.

[14] *EU Civilian Training Group*
[15] Oktoober 2020.

1. DOKUMENTIDE KOKKUVÕTE

1.1. HÜBRIIDIOHTUDE JA KÜBERI KÄSITLEMINE

Selles alapeatuks olevad dokumendid pärinevad alates aastast 2010 ja kirjeldavad järgmist ELi poliitikat: küberruum; ühtne turg, mida küberruum võimaldab; hübriidohtude ja küberkuritegevuse kasvavad riskid ning ELi kui terviku ja liikmesriikide individuaalne vastutus vastupanuvõime suurendamise ja koolitamise eest; kasvav vajadus ühtlustada liikmesriikide teabekeskuste ja/ või küberjulgeolekule ja hübriidohtudele spetsialiseerunud asutuste tegevusi; ELi lepingud NATOga koostöö suurendamiseks; ja kuidas hübriidohtude ja küberi temaatika peaks olema osa ELi välispoliitikast ja ka osa ELi välimissioonidest. Selles kokkuvõttes esitatakse ELi hübriidohtude ja küberpoliitika põhiteemad.

ÜJKP tsiviilmissioonide jaoks erilise tähtsusega dokumendid on:

Nõukogu järeldused Euroopa digitaalse tegevuskava kohta
3017. Transpordi, Telekommunikatsiooni ja energeetika nõukogu istung Brüssel, 31. mai 2010

Leitav aadressil:
https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/114710.pdf)

Nõukogu järelduses tunnistatakse Euroopa digitaalse tegevuskava olulisust ning tunnustatakse, et uute tehnoloogiate laialdasem kasutamine ning tõhusam rakendamine parandab Euroopa elanikkonna elu tervikuna ning suurendab sotsiaalset ja majanduslikku ühtekuuluvust, pakkudes samaaegselt võrdsemaid võimalusi. Seega peaks Euroopa tegema digitaalse ühtse turu loomiseks ühiseid jõupingutusi.

Nõukogu tunnistab siiski, et digitaalse tegevuskava[16] vastuvõtmiseks on nii ELi kui ka liikmesriikide tasandil vaja pühenduda kooskõlastatud tegevusele, et parandada IT-lahenduste koostalitlusvõimet ja edendada standartiseerimist. Lisaks peavad kõik riigid tegema koostööd võrkude turvalisuse, usaldusväärsuse ja küberruumi turvalisuse tagamise osas.

Ühine Teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus-ja Sotsiaalkomiteele ning Regioonide Komiteele: Euroopa Liidu küberturvalisuse strateegia: avatud, turvaline ja turvaline küberruum 8. veebruar 2013, 6225/13

Leitav aadressil:
http://register.consilium.europa.eu/doc/srv?l=ET&f=ST%206225%202013%20INIT

Strateegias selgitatakse ELi ja rahvusvahelise küberjulgeoleku poliitika põhimõtteid, nagu kasvav haavatavus, mida avatud ja vaba küberruum liikmesriikidele, kogukondadele ja kodanikele tekistab, ning vajadus kaitsta küberruumi juhtumite, pahatahtlike tegevuste ja

[16] *Digital Agenda*

veebipõhise väärkasutuse eest. Pettuste ohvrite arv suureneb. Strateegia hõlmab mitut ÜJKP missioonide jaoks olulist küsimust, näiteks küberkaitsepoliitika ja ühise julgeoleku- ja kaitsepoliitika (ÜJKP) raamistikuga seotud võimete arendamine. Põhitegevus on ELi küberkaitsepoliitika raamistiku väljatöötamine, et kaitsta ÜJKP missioonide ja operatsioonide võrke, sealhulgas dünaamiline riskijuhtimine, täiustatud ohuanalüüs ja teabe jagamine. Tsiviil- ja sõjaliste osalejate ning rahvusvaheliste partnerite vahel on ette nähtud dialoog ja kooskõlastamine dubleerimise vältimiseks. Rõhku tuleks panna heade tavade ja teabe vahetamisele, varajasele hoiatamisele, juhtumite reageerimisele, riskihindamisele, teadlikkuse tõstmisele ja koolitusele. Vastavalt tuleks järgida protseduure ning teatada juhtumitest, mis võivad olla seotud küberkuritegevuse, küberspionaaži või teiste riikide poolt toetatud küberrünnakutega.

Ühine Teatis Euroopa Parlamendile ja Nõukogule: ELi terviklik lähenemine väliskonfliktidele ja kriisidele 11.12.2013

Leitav aadressil: https://eur-lex.europa.eu/legal/content/EN/TXT/PDF/?uri=CELEX:52013JC0030&from=en

Ühises teatises käsitletakse ja pakutakse meetmeid, et veelgi paremini rakendada ELi terviklikku lähenemisviisi väliskonfliktidele ja kriisidele.

Pärast Lissaboni lepingu jõustumist ja selle loodud uut institutsioonilist konteksti on ELil nii suurenenud potentsiaal kui ka ambitsioon muuta oma välistegevus järjepidevamaks, tõhusamaks ja strateegilisemaks. Ehkki kõikehõlmavat lähenemisviisi reguleerivad ideed ja põhimõtted pole uued, peavad need olema süsteemsed juhtpõhimõtted ELi välistegevuseks kõigis valdkondades, eriti seoses konfliktide ennetamise ja kriisi lahendamisega. Ühisteatises esitatakse kõrge esindaja ja komisjonide arusaam ELi terviklikust lähenemisviisist väliskonfliktidele ja kriisidele - konflikti või muude väliskriiside kõikidele etappidele - ning pühendutakse täielikult selle ühisele rakendamisele ELi välispoliitikas ja -meetmetes.

Tervikliku lähenemisviisi peamine põhimõte on turvalisuse ja arengu seos nagu ka kontekstipõhise reageerimise põhimõtted. Ette nähakse kõigi ELi osalejate ühine reageerimine Brüsselis, liikmesriikides ja kohapeal kolmandates riikides.

ELi välispoliitika ning konflikti- ja kriisiolukorras tegutsemise sidususe ja tõhususe täiendavaks suurendamiseks sisaldasid sammud volitust, mis võimaldasid ühise analüüsi välja töötamist. Analüüs sisaldab meetmeid nagu olukorrateadlikkuse ja analüüsivõime parandamine, ühendades selleks paremini ELi institutsioonide ja talituste spetsiaalsed üksused, mis võimaldavad juurdepääsu ka ELi institutsioonide ja liikmesriikide teabele ja luureteabele. Teiseks nähakse ette teabe jagamise tõhustamist Brüsseli peakorteris ja kohapeal (sealhulgas ÜJKP missioonidel ja operatsioonidel). Kolmandaks nähakse vajadust ühise metoodika välja töötamiseks konflikti- ja kriisianalüüsi jaoks ning vastava analüüsi kasutamist edasise arutelu alusena asjakohases nõukogu koosseisus.

Rakendada tuleb ELi erinevaid tugevusi ja võimekust. Selleks kasutusele võetud meetmed peavad hõlmama kinnitust, et kõik asjaomased ELi osalejad on konflikti ja kriisiolukorra

analüüsimisse ja hindamisse kaasatud; samuti nähakse vajadust operatiivkoostöö tugevdamiseks ELis eri hädaolukordadele reageerimise korral ning vajadust tagada ELi ja liikmesriikide tegevuse sidusus.

Teatises rõhutatakse ka tervikliku lähenemisviisi pikaajalist perspektiivi. See nõuab tihedat koostööd sise- ja välispoliitika vahel, lisaks peaksid ELi delegatsioonid kolmandates riikides mängima keskset rolli ELi dialoogi, meetmete ja toetuse pakkumisel.

Komisjoni Teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus-ja Sotsiaalkomiteele ning Regioonide Komiteele: Interneti-poliitika ja juhtimine. Euroopa roll Interneti-juhtimise tuleviku kujundamisel (EMPs kohaldatav tekst) (12. veebruar 2014)

Leitav aadressil: https://eur-lex.europa.eu/legal content/ET/TXT/PDF/?uri=CELEX:52014DC0072

Teatises pakutakse välja alus Euroopa ühisele nägemusele Interneti haldamise kohta, et kaitsta ja edendada demokraatlikke õigusi ja selget mitme sidusrühmaga juhtimisstruktuuri.

Teatises öeldakse, et kuigi EL on 15 aasta jooksul aidanud säilitada ja arendada Internetti kui digitaalse ühtse turu põhisammast, on viimasel ajal Interneti tuleviku osas vastuolulisi visioone ja kasvab usaldamatus Interneti suhtes nii hirmust küberkuritegevuse kui ka ulatuslike seireprogrammide paljastamise tõttu. Seega tugineb teatis mitme sidusrühma tugevdamisele, keskendudes Interneti keeruka ökosüsteemi seisukohast olulistele poliitikavaldkondadele. Samuti on komisjon pühendunud usalduse suurendamisele Internetis, sealhulgas püüdlustes küberkuritegevust drastiliselt vähendada. Usalduse taastamiseks teeb komisjon koos nõukogu ja parlamendiga peamiste õigusaktide kiire vastuvõtmise ja rakendamise, sealhulgas andmekaitseraamistiku ning võrgu- ja infoturvet käsitleva direktiivi reformi. Euroopa Komisjon alustab rahvusvaheliste kollisiooni kohtade ülevaatusega ja hindab, kuidas selliseid konflikte lahendada. Samuti kaalutakse hoolikalt täiendavate juhiste väljatöötamist.

Internet peaks jääma avatuks ja kaasavaks, inimõigusi austavaks ja demokraatiat kaitsvaks. Siiski peaksid Interneti suhtes kehtima samad seadused nagu teistele igapäevase elu valdkondadele. Süsteemi usalduse tagamiseks peab võrgul olema vastupidav ja läbipaistev arhitektuur. Komisjon kutsub nõukogu ja parlamenti, asjaomaseid komiteesid ja liikmesriike kokku leppima teatises rõhutatud ühises visioonis ja seda ühiselt kaitsma.

Nõukogu järeldused küberdiplomaatia kohta (6122/15) 11. veebruar 2015

Leitav aadressil: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/et/pdf

Nõukogu järelduses esitatakse ELi ühtne ja terviklik lähenemisviis küberdiplomaatiale ülemaailmsel tasandil.

Küberdiplomaatia terviklik lähenemisviis on edendada ja kaitsta ELi demokraatia, õigusriigi ja inimõiguste väärtusi ning tagada, et Interneti-käitumine neid väärtusi ei kahjustaks. Samuti tuleb tagada Euroopa majanduskasv ja konkurentsivõime, tugevdades küberturvalisust ja parandades koostööd küberkuritegevuse vastu võitlemisel. Lõpuks peaks diplomaatilistele ja õiguslikele vahenditele tuginev ELi lähenemisviis aitama kaasa küberjulgeolekuohtude leevendamisele, konfliktide ennetamisele ja rahvusvaheliste suhete suurema stabiilsuse saavutamisele. ÜJKP missioonide seisukohalt on oluline, et antud lähenemine rõhutab kübervõimekuse suurendamise olulisust kolmandates riikides, mis omakorda toetab ELi jõudpingutusi põhiväärtuste edastamisel ning lubab kogu info- ja

kommunikatsioonitehnoloogia sotsiaalse ja majandusliku potentsiaali avaldumist samaaegselt paindlike süsteemide arendamise ning ELi küberriskide maandamisega.

Selle eesmärgi saavutamiseks julgustatakse ELi ja liikmesriike muutma kübervõimekuse suurendamine osaks laiemast globaalsest lähenemisviisist kõigis küberruumi valdkondades, sealhulgas tihedas koostöös asjaomaste ELi ametitega (nt ENISA).[17] See hõlmab koostööd rahvusvaheliste sidusrühmadega (ka koolituse pakkumisel ja teadlikkuse tõstmisel) ning olemasolevate finantsinstrumentide ja programmide kasutamist.

Ühine teatis Euroopa Parlamendile ja nõukogule: Hübriidohtude vastu võitlemise ühine raamistik. Euroopa Liidu reageerimine 6. aprill 2016, JOIN (201) 18 final

Leitav aadressil: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

Ühisteatises käsitletakse muutusi ELi ja naaberriikide julgeolekukeskkonnas ning rõhutatakse vajadust mobiliseerida ELi vahendeid hübriidohtude vastu ja küberkaitse eest võitlemiseks.

Kriisijuhtimise terviklikus lähenemisviisis kaalutakse ÜJKP vahendite ja missioonide kasutamist, et aidata kolmandate riikide partneritel suurendada nende suutlikkust strateegilise kommunikatsiooni valdkonnas hübriidohtude vastu võitlemisel. Lähenemisviis näeb ette, et partnerid leiavad sünergiat ÜJKP vahendite ja julgeoleku vahel (EUROPOL, FRONTEX, CEPOL, EUROJUST, INTERPOL jne) vastavalt oma volitustele, viies läbi erimeetmeid, näiteks naabrusalade hübriidne uuring.

Teatises käsitletakse ÜJKP ettepanekuid tsiviil- ja sõjalise väljaõppe vahel; mentorlust ja nõustamismissioone; situatsiooniplaane hübriidohtude signaalide ja varajase hoiatamise võimekuse kindlakstegemiseks; ja tuge keemia-, bioloogilise-, radioloogilise- ning radioaktiivse riski[18] maandamisel.

Koostöö suurendamine kolmandate riikidega nõuab meetmeid küberkindluse ja partnerite võimekuse suurendamiseks, et tagada võime avastada küberrünnakuid ja küberkuritegevuse juhtumeid ning neile reageerida ning võidelda hübriidohtude vastu kolmandates riikides.

Ühise raamdokumendi keskmes on teadlikkuse suurendamine. Rõhutatakse vajadust parandada vastupanuvõimet sellistes valdkondades nagu küberturvalisus, esmatähtis infrastruktuur ning vägivaldse äärmusluse ja radikaliseerumise vastased jõupingutused. Lisaks võiks hübriidohtude ennetamist, neile reageerimist ja nendest taastumist tõsise hübriidrünnaku korral toetada ühine operatiivprotokoll (COP).

[17] ENISA – ingl k *European Union Agency for Cybersecurity*; e k *Euroopa Liidu võrgu- ja infoturbe agentuur*
[18] Ingl k *CBRN - Chemical Biological Radiological and Nuclear Risk*

Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning regioonide komiteele: Euroopa küberturvalisuse süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberturvalisuse edendamine. 5. juuli 2016, COM (2016) 410 final

Leitav aadressil: https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

Teatises esitatakse meetmed, mille eesmärk on tugevdada ELi kübervastupidavust ja edendada konkurentsivõimelist ja uuendusmeelset küberturvalisust Euroopas.

Hoolimata ELi jõupingutustest vähendada ELi ühtsele turule tekkivaid küberturvalisuse riske, esineb juhtumeid iga päev ja see õõnestab usaldust digitaalse ühiskonna vastu. Komisjon otsib meetmeid, et veelgi parandada ELi küberturvalisuse vastupanuvõimet ja juhtumitele reageerimist tagamaks sellega ühtse turu eesmärkide nagu majanduskasv ja suurenenud tööhõive, saavutamist.

Eesmärgi saavutamiseks on vaja täiendavalt pühenduda ühtse turu ees seisvate küberturvalisuse probleemide lahendamisele, sealhulgas koostöös küberintsidentidele reageerimisel, samuti küberturvalisuse tööstusvõimekuse toetamisel. Võrgu- ja infoturbe direktiiv suunab tegevusi ELi-sisese koostöö poole liikmesriikide vahel ja aitab valmistuda suuremahulisteks küberkriisideks. Asjakohased teadmised ELi tasandil on praegu laiali, mistõttu tuleb luua edasise koostöö kavand ja koondada asjatundlikkus teabekeskustesse. Samamoodi tuleks moodustada nõuandekogu ja hinnata ENISA volitusi koos võimalusega neid täiendada.

Praegu on ENISA-l, ECTEG-l[19], Europoli küberkuritegevuse keskustel ja CEPOLil oluline roll suutlikkuse suurendamise toetamisel. Siiski on vaja edasi arendada tsiviil-sõjalist koostööd ja sünergiat liikmesriikide, Euroopa välisteenistuse, ENISA ja muude asjaomaste ELi asutuste vahelises väljaõppes ja koolitustel, et suurendada ELi vastupanuvõimet ja juhtumitele reageerimise võimet. Samamoodi peaksid tsiviil- ja militaarvaldkondade sünergiad olema suunatud küberkaitse tootearendusele.

Lisaks sellele peavad ELi kübervastupanuvõime suurendamiseks olema tehtud järgmised sammud: kogu ELis peab olema ühtne sertifikaat, et tagada asjakohaste toodete rakendamine kõikides liikmesriikides; turvakujunduse lähenemise edendamine; ning avaliku ja erasektori lepingulise partnerluse (cPPP) loomine, et koguda ressursse teaduse ja innovatsiooni tipptaseme saavutamiseks.

Euroopa Parlamendi ja Nõukogu Direktiiv (EL) 2016/1148, 6. juuli 2016, võrgu- ja infosüsteemide ühise kõrge turvalisustaseme tagamise meetmete kohta kogu liidus.

Leitav aadressil: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=ET

[19] ECTEG ehk European Cybercrime Training and Education Group

ELi direktiivi eesmärk on saavutada liidu võrgu- ja infosüsteemide kõrgetasemeline turvalisus. Direktiiviga määratakse liikmesriikide kohustused tagada kogu ELi hõlmavate võrkude turvalisus ja vastupanu põhiteenustega seotud küberintsidentidele. Samuti määratakse selles kindlaks asjaomaste ELi institutsioonide rollid ning rõhutatakse edasise rahvusvahelise koostöö vajadust oluliste teenuste jätkusuutlikkuse tagamiseks.

Direktiivis korratakse võrgu- ja infosüsteemide ülitähtsat rolli kogu ELis, sealhulgas nende tähtsust kaubanduse jaoks, mistõttu nende võrkude toimimine on ülioluline. Praegu on liikmesriikidel valmisoleku tase väga erinev ning see kujutab endast turvariski kõigile. Olukorra parandamiseks peaks koostöögrupp (sealhulgas ENISA) hõlbustama head poliitikatava ning strateegilist koostööd liikmesriikide vahel võrgu- ja infosüsteemide turvalisuse valdkonnas. Lisaks on nõudlus turvanõuete standardiseerimise järele.

Liikmesriigid peavad vastu võtma riiklikud strateegiad, mis näevad kehtestatud ja proportsionaalseid meetmeid. See hõlmab liikmesriikide vajadust määratleda oma põhiteenused, kus põhiteenuste tagamise eest vastutavad (digitaalsete) teenuse pakkujad; luua institutsioon ja/ või teabekeskus koostöögrupiga suhtlemiseks; esitama ELile ja teistele liikmesriikidele piisavat ja ajakohast teavet, sealhulgas juhtumite aruandeid; ning tagada, et pädevatel asutustel on vajalikud volitused tuvastatud puuduste kõrvaldamiseks ning siduvate juhiste hindamiseks ja väljaandmiseks.

ELi ja NATO ühisdeklaratsioon 2016, 8. juuli 2016

Leitav aadressil: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

Ühisdeklaratsioonis esitatakse uued koostöövõimalused ELi ja NATO vahel. Kuna need kaks riikide liitu seisavad silmitsi ühiste väljakutsetega, kinnitab see vajadust täiendavate ühiste jõupingutuste ja koostöö ambitsioonide järele naabrite ja partnerite stabiilsuse suurendamiseks. Stabiilsuse suurendamine hõlmab naabrite suveräänsuse, territoriaalse terviklikkuse, sõltumatuse ja reformipüüdluste toetamist.

Selle eesmärgi saavutamiseks on vaja kiirendada hübriidohtude vastu võitlemise võimet, sealhulgas teha koostööd töötajate vahel teabe jagamisel. ÜJKP missioonide jaoks on oluline ka eesmärk laiendada kooskõlastamist küberjulgeoleku ja -kaitse valdkonnas, sealhulgas ELi ja NATO missioonide, operatsioonide, õppuste ning hariduse ja koolituse kontekstis. Selleks tuleks püüda hübriidohtude vastu võitlemise osas kavandatud harjutused ja õppused rohkem kooskõlastada. Koostööd küber- ja hübriidohtude valdkonnas peetakse strateegiliseks prioriteediks ja eriti oluliseks kiire rakendamise võtmes.

Nõukogu järelduste eelnõu ELi ühise diplomaatilise reageerimise raamistiku kohta pahatahtlikule küberettevõttele (küberdiplomaatia tööriistakast) - vastuvõtmine (7. juuni 2017)

Leitav aadressil: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/et/pdf

Nõukogu järelduste eelnõus teatatakse diplomaatiliste vastuste raamistiku vastuvõtmisest ja väljatöötamisest pahatahtlike kübertegevuste suhtes.

EL tunnistab, et vaatamata oma pakutavatele võimalustele esitab küberruum üha suurema väljakutse nii ELi välispoliitikale kui ka ELile ja selle liikmesriikidele. Seega on ELi käimasolevad küberdiplomaatiaga seonduvad tegevused ja ELi küberdialoogi sidusus vastupanuvõime suurendamise seisukohast väga olulised nii ELis kui ka kolmandates riikides. Selleks kutsub EL liikmesriike, Euroopa välisteenistust ja komisjoni üles täielikult rakendama raamistiku väljatöötamist ELi ühisele diplomaatilisele reageerimisele pahatahtlikule küberettevõttele ja kinnitama sellega seoses oma pühendumust jätkata tööd selle raamistiku nimel koostöös komisjoni, Euroopa välisteenistuse ja muude asjaomaste osapooltega, rakendades suuniseid, sealhulgas ettevalmistavaid tavasid ja teabevahetusprotseduure ning katsetades neid asjakohaste õppuste abil.

Aastaaruanne küberkaitsepoliitika raamistiku rakendamise kohta 19. detsember 2017, 15870/17

Leitav aadressil: https://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/et/pdf

Aastaaruanne annab ülevaate ELi küberkaitsepoliitika raamistiku (CDPF)[20] rakendamisest ajavahemikul november 2016 - detsember 2017.

Aruandes viidatakse nõukogu tuvastatud vajadusele 2014. aasta küberkaitsepoliitika raamistik uuesti ellu viia ja seda ajakohastada, et integreerida küberjulgeolek ja -kaitse veelgi ühisesse julgeoleku- ja kaitsepoliitikasse (ÜJKP) ning laiemasse julgeoleku- ja kaitseprogrammi. Lisaks on vaja piisavat kübervõimekuse arendamiseks Euroopas jätkata koostööd ja arendada küberalgatusi. ÜJKP missioonide puhul juhitakse tähelepanu sellele, et küberjulgeoleku integreerimise kontseptsioon ÜJKP tsiviilmissioonide kavandamisel ja läbiviimisel valmis lõplikult 2017. aasta juunis.

Euroopa Komisjoni 13.9.2018. Aasta soovitus kooskõlastatud reageerimise kohta suuremahulistele küberturvalisuse juhtumitele ja kriisidele, C (2017) 6100 final

Leitav aadressil: https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF

Soovitused juhivad tähelepanu 2016. aasta teatises „Euroopa küberturvalisuse süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberturvalisuse edendamine" tehtud ettepanekule küberökosüsteemi erinevate elementide koostöövalmiduse suurendamiseks. Plaanis on kirjas, et juhul kui kriisiga kaasneb oluline välis- või ühise julgeoleku- ja kaitsepoliitika (ÜJKP) mõõde, aktiveeritakse Euroopa välisteenistuse kriisidele reageerimise mehhanism (CRM)[21].

ELi küberkaitsepoliitika raamistik (2018. aasta värskendus) 19. november 2018, 14413/18

Leitav aadressil: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/et/pdf

Uuendatud CDPF-i eesmärk on arendada edasi ELi küberkaitsepoliitikat, võttes arvesse foorumite ja poliitikavaldkondade asjakohaseid arenguid alates CSPF-i esialgsest rakendamisest (2014. aastal). Selles määratakse kindlaks küberkaitse prioriteetsed valdkonnad ning selgitatakse erinevate asjaosaliste vastutust ja pädevust.

Küberjulgeolek on ELi ülemaailmse strateegia prioriteet, mistõttu rõhutatakse vajadust kaitsta seda kriiside eest tugevdades EL-i kui julgeolekukogukonda, mis suudab end iseseisvalt ja ka partnerluse kaudu rakendada. Need eesmärgid nõuavad suutlikkuse arendamisel edasist

[20] EU Cyber Defence Policy Framework
[21] Crisis Response Mechanism

koostööd, sealhulgas tulemuseks oleva tsiviil- ja sõjalise võimekuse tõhususe ja koostalitlusvõime edendamist.

Uuendatud CDPF keskendub esmajoones küberkaitse võimekuse arendamisele ELi ÜJKP side- ja teabevõrgus, mis tähendab ÜJKP missiooni infrastruktuuride nõrkade kohtade edasist hindamist ja asjakohase kaitse loomist. Selleks peaks Euroopa välisteenistus koos liikmesriikidega täiendavalt integreerima kübervõimalused ÜJKP missioonidesse ja operatsioonidesse. Edasised tegevused hõlmavad järgmist: Euroopa välisteenistuse ühtsete infoturbealaste ja poliitiliste suuniste väljatöötamine, ÜJKP sõjaliste ja tsiviilmissioonide ühiste küberkaitsenõuete täitmine; ohuteabe jagamise edendamine asjaomastele ELi institutsioonidele.

CSPF-i edasised prioriteedid hõlmavad koolitust ja harjutusi ning kodaniku- ja rahvusvahelist koostööd; see nõuab eelkõige ühtse reageerimise tagamiseks ÜJKP käsuliini küberkaitsealase koolituse ajakohastamist liikmesriikides ja kübervaldkonna piisavat käsitlemist õppustel ning tsiviil-sõjalist koostööd kübervaldkonnas.

Nõukogu otsus Liitu või selle liikmesriike ähvardavate küberrünnakute vastu suunatud piiravate meetmete kohta 14. mai 2019, 7299/19

Leitav aadressil: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/et/pdf

14. mail 2019 kehtestas nõukogu raamistiku, mis võimaldab ELil kehtestada suunatud piiravad meetmed küberrünnakute, mis kujutavad endast välist ohtu ELile või selle liikmesriikidele, ärahoidmiseks ja neile reageerimiseks. See hõlmab küberrünnakuid kolmandate riikide või rahvusvaheliste organisatsioonide vastu, kui ühise välis- ja julgeolekupoliitika (ÜVJP) eesmärkide saavutamiseks peetakse vajalikuks piiratud meetmeid.

Selle uue sanktsioonirežiimi reguleerimisalasse kuuluvad küberrünnakud, millel on märkimisväärne mõju ja mis:

- pärinevad või viiakse läbi väljastpoolt ELi või
- kasutavad infrastruktuuri väljaspool ELi või
- teostatakse väljaspool ELi asutatud või tegutsevate isikute poolt või on üksused või
- teostatakse väljaspool ELi tegutsevate isikute või üksuste toel.

See raamistik võimaldab ELil esmakordselt rakendada sanktsioone isikutele või üksustele või asutustele, kes vastutavad või on seotud küberrünnakute või küberrünnakute katsetega, kes pakuvad selliste rünnakute jaoks rahalist, tehnilist või materiaalset tuge või on seotud rünnakutega muudel viisidel.

Nõukogu järeldused: täiendavad jõupingutused vastupanuvõime suurendamiseks ja hübriidohtude vastu võitlemiseks 10. detsember 2019, 14972/19

Leitav aadressil: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/et/pdf

Järeldustes määratakse prioriteedid ja suunised ELi koostööks hübriidohtude vastu võitlemisel ja nendele ohtudele vastupidavuse suurendamisel, tuginedes viimastel aastatel tehtud edusammudele.

Järeldustes kutsutakse hübriidohtude vastu võitlemiseks kasutama terviklikku lähenemisviisi julgeolekule, töötades kõigis asjakohastes poliitikavaldkondades strateegilisemalt, koordineeritumalt ja sidusamalt. Selles rõhutatakse vajadust jätkata koostöö arendamist rahvusvaheliste organisatsioonide ja partnerriikidega vastupanuvõime suurendamiseks ja hübriidohtude vastu võitlemiseks, eriti ELi ja NATO koostöö ning koostöö ELi naabruses asuvate riikidega. Samuti rõhutab nõukogu riiklike ametiasutuste, samuti ELi institutsioonide, asutuste ja ametite vahelise koostöö pideva parandamise tähtsust kogu sise- ja välisjulgeoleku vahel.

Desinformatsiooni tõkestamise osas tuletab nõukogu meelde desinformatsiooni vastu võitlemise tegevuskava jätkuva rakendamise tähtsust. Selles rõhutatakse vajadust piisavate ressursside järele Euroopa välisteenistuse kolme Stratcomi rakkerühma (Ida, Lääne-Balkani riigid, Lõuna) jaoks ning kutsutakse Euroopa välisteenistust üles hindama strateegilise kommunikatsioonitöö tugevdamise vajadusi ja võimalusi teistes geograafilistes piirkondades, näiteks Sahara-tagune Aafrika. Samuti kutsutakse komisjoni ja Euroopa välisteenistust üles arendama kiirreageerimissüsteem koos liikmesriikidega edasi terviklikuks liikmesriikide ja ELi institutsioonide platvormiks koostöö, kooskõlastamise ja teabevahetuse jaoks. Sotsiaalmeedia platvormide osas kutsutakse komisjoni üles kaaluma võimalusi desinformatsiooni käsitleva tegevusjuhendi, sealhulgas võimalike jõustamismehhanismide, rakendamise tõhustamiseks.

ELi teabe- ja sidevõrkude ning otsustusprotsesside turvalisuse suurendamiseks kutsutakse ELi institutsioone ja asutusi välja töötama ja rakendama terviklikke meetmeid hübriidohtude ja muu pahatahtliku tegevuse vastu võitlemiseks.

Nõukogu otsus (ÜVJP) 2020/1127, 30. juuli 2020, millega muudetakse otsust (ÜVJP) 2019/797, mis käsitleb liitu või selle liikmesriike ohustavate küberrünnakute vastaseid piiravaid meetmeid

Leitav aadressil: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32020D1127&from=ET

Nõukogu muudab eelmist otsust, kirjeldades küberrünnakute, millel on märkimisväärne mõju ja mis kujutavad endast välist ohtu oma liikmesriikide liidule, vastaseid sihipäraseid piiravaid meetmeid. Need meetmed on olulised vahendid rünnakutele reageerimisel ja nende ärahoidmisel ning need meetmed on lisatud küberdiplomaatia tööriistakasti. Neid meetmeid

saab rakendada ka tõsise rünnaku korral kolmandate riikide või rahvusvaheliste organisatsioonide vastu.

Sellega seoses tuleks küberruumis toimuva pahatahtliku käitumise tõkestamise ja ennetamise meetmena lisada kuus füüsilist isikut ja kolm üksust või asutust nende füüsiliste ja juriidiliste isikute nimekirja, kelle suhtes kohaldatakse piiravaid meetmeid. Need isikud ja üksused või asutused vastutavad küberrünnakute eest, pakuvad neile tuge, osalesid, hõlbustasid või katsetasid küberrünnakut, sealhulgas küberrünnaku katse OPCW vastu ja küberrünnakud, mis on avalikult tuntud kui WannaCry, NotPetya ja 'Operation Cloud Hopper'.

1.2. ÜJKP TSIVIILMISSIOONI ÜLESANNETEGA SEOTUD HÜBRIIDIOHTUSID JA KÜBERIT KÄSITLEVAD DOKUMENDID

Selles alapeatuükis olevad dokumendid annavad ülevaate ELi ja Euroopa välisteenistuse lähenemisviisist hübriidohtudele ja küberküsimustele, eriti seoses ÜJKP tsiviilmissioonidega. See alapeatükk hõlmab ka uuringuid ja aruandeid, mis dokumenteerivad hübriidohu ja kübervastupanuvõime meetmete edasise rakendamise vajadust missiooni planeerimisel/ kogu missioonistruktuuris ning näitavad selle protsessi esialgseid tulemusi.

ÜJKP tsiviilmissioonide hübriidohtude ja küberkoolituse planeerimise jaoks on eriti olulises järgmised dokumendid:

Euroopa Liidu võrgu- ja infoturbeagentuuri (ENISA) uuring:
Küberturvalisus ELi ühises julgeoleku- ja kaitsepoliitikas (ÜJKP): väljakutsed ja riskid ELile (uuring EPRS / STOA / SER / 16 / 214N) (mai 2017)

Leitav aadressil: http://publications.europa.eu/resource/cellar/2e35913c-1d03-11e8-ac73-01aa75ed71a1.0001.01/DOC_1

See on Euroopa Liidu võrgu- ja infoturbe agentuuri (ENISA) Euroopa Parlamendi teaduse ja tehnoloogia võimaluste hindamise (STOA) paneeli uuring, mille eesmärk on tuvastada küberkaitse riske, väljakutseid ja võimalusi ELi kontekstis ÜJKP raamistikus.

Uuring keskendub kolmele temaatilisele valdkonnale: poliitikale, suutlikkuse suurendamisele ja küberintegratsioonile ÜJKP missioonidel. Uuringu eesmärk on pakkuda ettepanekuid, mida saaks ÜJKP jaoks küberturvalisuses suurendamiseks rakendada kesk-pikas ja pikas perspektiivis. Arvestades liikmesriikide erinevat küberaktiivsust, erinevat ohutaset, erinevaid prioriteete ja võimekust, keskendutakse uuringus sidususe suurendamisele.

Uuringus esitatakse loetelu tegevuskohtadest, mis on eriti olulised ÜJKP missioonide jaoks: i) ÜJKP hankeseadmetes tuleks vastu võtta kavandatava turvalisuse põhimõte, käsitledes ka vastutust ja tarneahela terviklikkuse sätteid; ii) ÜJKP kontekstis tuleks küberturvalisuse suutlikkuse arendamisel ja jälgimisel kaaluda suutlikkuse küpsuse mudelit, näiteks CMM (küberjulgeoleku võimekuse mudel). iii) EL peaks tagama sobivad vahendid küberjulgeoleku suutlikkuse suurendamiseks ja jätkama investeerimist küberjulgeolekusse, toetades samal ajal haridust, koolitust ja karjääritee arengut; iv) teabe edastamine ELi tasandi mehhanismidele,

nagu näiteks EU INTCEN[22] ja ÜJKP peakorterid, edasi arendamine ÜJKP missioonide turvalisema töökeskkonna tagamise jaoks; v) küberoskusi ja võimekust operatiivkihil tuleks veelgi parandada, kuna need on ÜJKP missioonide küberohtude hindamiseks hädavajalikud.

Aruandes soovitatakse lisaks, et ÜJKP missioonid peaksid välja töötama vajaliku kübervõimekuse taseme mis tahes missiooni jaoks missiooni kavandamise etapis ning edasised leevendusmeetmed ÜJKP missioonide operatiivtasandil. Lõpuks puudub küberjulgeoleku osas õiguslikus aspektis rahvusvaheline koostöö ning juhitakse tähelepanu sellele, et ÜJKP missioonid on selles osas eriti haavatavas olukorras, arvestades, et missioonid toimuvad väljaspool ELi.

ÜJKP üldiste tsiviilülesannete ja -nõuete loetelu mustand. Euroopa välisteenistus, 9. veebruar 2017, 6616/17

Leitav aadressil: https://data.consilium.europa.eu/doc/document/ST-6166-2017-INIT/et/pdf

2016. aasta novembris võtsid ELi välis- ja kaitseministrid vastu nõukogu järeldused, otsustades uue ambitsioonitaseme ning julgeoleku- ja kaitsevaldkonna peamised sammud globaalse strateegia eesmärkide saavutamiseks. Need järeldused põhinesid kõrge esindaja/ asepresident Mogherini julgeoleku ja kaitse rakenduskaval. Täpsemalt tehti Euroopa välisteenistuse nõuete loendis ülesandeks jätkata vajalike võimete kindlakstegemisega lähtudes ÜJKP tsiviilülesannete üldiste ülesannete loetelus tehtud töödest ja tsiviilvõimekuse arengukava (CCDP)[23] läbivaatamisest.

Tsiviilvaldkonna võimete nõuete loetelu väljatöötamine algas juba 2008. aasta tsiviilvaldkonna peaeesmärgi vastuvõtmisel. Sel ajal viis see õppus siiski ametijuhendite loendini, mitte ei hõlmanud selliseid võimevaldkondi nagu varustus, planeerimine, logistika, missioonide tugi ning juhtimine ja kontroll: kõik tõhusa tsiviil-ÜJKP olulised alad.

Kavandatava nimekirja eelnõus määratakse kindlaks iga ülesande nõuded ja hinnatakse nende nõuete täitmise võimet.

Loendis tehti kindlaks vajadus kommunikatsiooni- ja infosüsteemide[24] arendamise järele, nii praktiline (nt tehnoloogilisemad lahendused) kui ka teoreetiline (nt selgitatud juhised ja määrused).

Küberjulgeoleku integreerimine ÜJKP tsiviilmissioonide kavandamisse ja läbiviimisse (Euroopa välisteenistuse töödokument, 16. juuni 2017, Euroopa välisteenistus (2017) 773[25]

Kontseptsioonidokumendis öeldakse, et kübervaldkonnast tulenevaid ÜJKP tsiviilmissioonide ohte peetakse sama tõsisteks, kuna need võivad ohustada ka personali turvalisust ja õõnestada kogu operatsiooni. Kiiresti on vaja tõhusaid kaitsemeetmeid, ka osana ELi laiematest jõupingutustest hübriidohtude vastu võitlemiseks. Küberohtude vastu tuleb

[22] EU Intelligence and Situation Centre
[23] Civilian Capabilities Development Plan
[24] CIS ehk *Communication and Information systems*
[25] *Integrating cyber security in the planning and conduct of civilian CSDP missions (12 June 2017, EEAS (2017) 773).* Dokumendil on AK märge.

rakendada turvameetmeid, et tagada personali turvalisus, sageli tundlike andmete ja infovarade kaitse ning missioonide mandaatide täitmine. Eesmärk on, et ÜJKP missioonil oleks võime end kaitsta küberohtude eest.

Erinevalt ELi sõjalistest missioonidest, ei vastuta tsiviilmissiooni vastuvõttev riik selle eest, et kommunikatsiooni- ja informatsioonisüsteemid vastaksid koostalitus – ja turvanõuetele. Samuti ei toeta ka CERT-EU[26] missioone süstemaatiliselt. Seega on tsiviilmissioonid haavatavamad ja puutuvad kokku küberohtudega. Missioonide olemus tähendab, et tuleb tagada koostalitlusvõime/ ühendatud vahendid. Koostalitlusvõime ohustab siiski turvariske, kuna süsteemi tugevus sõltub kõigi süsteemi külge kinnitatud objektide turvalisusest.

Plaani eesmärk on integreerida küberjulgeolek, sealhulgas küberluure aruanded ÜJKP tsiviilmissioonide kavandamisse ja läbiviimisse, seada ÜJKP tsiviilmissioonidel suurema küberturvalisuse parameetrid ja edendada küberprobleemide suuremat rõhutamist kogu tööea jooksul. Selleks peaksid strateegiline planeerija, operatiivplaneerijad ja missioonide juhid suutma tuvastada võimalike küberrünnakute piirkonnad, suhelda riskide vältimise ja leevendamisega seotud ekspertidega ning astuda samme rünnakule reageerimise võimekuse tagamiseks.

Ajakohane koolitus on põhiline element küberturvalisuse intsidentide riskide maandamisel, mida võimaldavad inimlikud eksimused ja manipuleerimisründed.[27] Lisaks peaksid küberohtudele reageerimiseks olema ette nähtud spetsiaalsed õppused kõigile ÜJKP struktuuridele. ÜJKP missioonide väga erineva iseloomu tõttu tuleks kaaluda ka missiooni personali jaoks eraldi väljaõppe arendamist.

Tsiviilvõimekuste arengukava, Euroopa välisteenistus (2018) 906, 4. september 2018

Leitav aadressil: https://data.consilium.europa.eu/doc/document/ST-11807-2018-INIT/et/pdf

See tsiviilvõimekuse arengukava (CCDP) on teine samm tsiviil-ÜJKP tugevdamise protsessis. Eesmärk on muuta ÜJKP tsiviilmissioonid paindlikumaks, võimaldades ühtlasi missioonidel toetada julgeolekuohtudega võitlemist jne. Kuigi esialgsed võimete prioriteedid (politsei, õigusriik, tsiviilhaldus ja julgeolekusektori reform (SSR)[28]) on endiselt täielikult kehtivad ja asjakohased, kaasaegse ohumaastiku muutuse tõttu tuleb ajakohastada ka põhikategooriaid.

Kava põhirõhk sisaldab järgmist: (i) liikmesriigid soovivad selgelt integreerida nendesse prioriteetidesse (sealhulgas hübriidohud, küberturvalisus jne) uutest julgeolekuohtudest ja väljakutsetest tulenevad vajadused; (ii) tsiviilvõimekuse arendamine nii riiklike kui ka kokkulepitud ELi vajaduste rahuldamiseks on riiklik vastutus; iii) tuleks välja töötada süstemaatilisemad seosed nõutavate oskuste, koolituse kättesaadavuse (nii liikmesriikide kui ka ELi tasandil, sealhulgas CEPOL ja muud ELi asutused) ning koolituse õppekavade koostalitusvõime vahel; iv) Uute seatud turvalisuse prioriteetide jaoks, mis on hõlmatud minikontseptsioonidega, tuleks ÜJKP missioonidel koostöös asjaomaste ametite ja

[26] Computer Emergency Response Team for the EU Institutions, bodies and agencies ehk CERT-EU
[27] Ingl k *social engineering*
[28] Security Sector Reform

teenistustega, sealhulgas kodanikuühiskonna koostööga, luua katseprojektid; v) kõikides ÜJKP tsiviilmissioonide piirkondades tuleks luua missioonipõhine olukorrateadlikkuse platvorm (MSAP) ning see peaks konsolideerima juba olemasolevad koordineerimis- ja teabevahetusstruktuurid; vi) üks ÜJKP missiooni ülesanne on pakkuda (spetsialisti tasandil) tuge hübriidohtude vastu võitlemiseks ning aidata kaasa küberjulgeolekule ja strateegilisele kommunikatsioonile.

Nõukogu ja nõukogus kokku tulnud liikmesriikide valitsuste esindajate järeldused ÜJKP tsiviillepingu sõlmimise kohta. Nõukogu peasekretariaat, 19. november 2018, 14305/18

Leitav aadressil: https://www.consilium.europa.eu/media/37027/st14305-en18.pdf

Kokkuvõttes antakse ülevaade ELi ja liikmesriikide poliitilisest kokkuleppest ÜJKP tsiviilkokkulepe,[29] mis sisaldab strateegilisi suuniseid tsiviil-ÜJKP tõhusamaks ja ühendamiseks ning tegevuste ettepanekuid nende eesmärkide saavutamiseks. Kokkulepe tuleks ellu viia võimalikult kiiresti, hiljemalt 2023. aasta suve alguseks.

Järelduses tunnistatakse, et ELi strateegilise keskkonna halvenemine nõuab jätkuvalt vajadust tugevdada ELi rolli ja suutlikkust tegutseda ÜJKP kaudu julgeoleku pakkujana, kasutades nii tsiviil- kui ka sõjalisi missioone. EL on otsustanud teha tsiviil-ÜJKPs nii kvalitatiivset kui ka kvantitatiivset arenguhüpet. Kuid kuna operatiivne suutlikkus tuleneb liikmesriikidest, nõuab ÜJKP tsiviilüksuse tugevdamine liikmesriikidelt vajalike võimete kasutamist.

Mis puutub võimekusklastri „hübriidohud ja küber“, peaks ELi tugevdatud suutlikkus tsiviilkriiside ohjamise missioonide lähetamisel aitama kaasa ka kogu ELis reageerimisele julgeolekuprobleemide lahendamisel hõlmates ka hübriidohtusid ja küberjulgeolekut, ning aidata oluliselt kaasa vastupanuvõime ja julgeoleku tagamisele. Jätkusuutlikud tulemused peaksid olema partnerriikides tunnetatavad. Selleks hõlmab ELi ja liikmesriikide kokkulepe kohustust nii enne kui ka missiooni ajal ÜJKP koolituspoliitika alusel eksperte koolitada. Samuti tõhustatakse koostööd ELi tasemel koolitusel, eriti konkreetsete koolitusvajaduste täitmisel uute julgeolekuprobleemide korral ning tunnustatakse koolituse pakutavate võimaluste ärakasutamist.

Tsiviil-ÜJKP kokkulepe: nõukogu järeldused 9. detsember 2019, 14611/19

Leitav aadressil: https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/et/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Civilian+CSDP+Compact%3a+Council

Tsiviiljulgeoleku ühise julgeoleku- ja kaitsepoliitika (ÜJKP) kokkulepe kinnitab veelkord oma pühendumust tsiviil-ÜJKP võimekamaks, tõhusamaks, paindlikumaks, reageerimisvõimelisemaks ja sidusamaks muutmisel.

Järeldustes rõhutatakse ÜJKP tsiviilmissioonide olulist panust rahvusvahelise rahu ja stabiilsuse tagamisse kui olulist osa ELi integreeritud lähenemisviisist väliskonfliktidele ja

[29] Civilian CSDP Compact

kriisidele. Samuti rõhutatakse vajadust tugevdada ÜJKP kaudu ELi rolli ja suutlikkust tegutseda turvalisuse pakkujana.

Pärast esimest iga-aastast ülevaatekonverentsi (ARC),[30] mis toimus 14. novembril 2019 Brüsselis, tervitab nõukogu viimase aasta positiivseid üldisi edusamme ja kõigi sidusrühmade tugevat pühendumust kompakti täielikule elluviimisele.

Nõukogu kiidab heaks ülevaatekoverentsil kindlaks määratud teekonnapunktid, mille eesmärk on aidata kaasa kokkuleppe üldisele rakendamisele, tagades ristühendused eri piirkondade vahel. Samuti püüavad nad juhtumipõhiselt edendada tihedat koostööd asjaomaste partneritega.

Missiooni tugiplatvormi 2019 aastaaruanne 14. aprill 2020, (Euroopa välisteenistus) WK3795 / 2020 INIT[31]

Aruanne annab iga-aastase ülevaate missioonide toetustest. Lähtudes Euroopa välisteenistuse töödokumendist „Küberjulgeoleku integreerimise ÜJKP tsiviilmissioonide kavandamise ja läbiviimise idee" toetas MSP CIS[32] meeskond mõnede soovituste rakendamist.

Tsiviilmissioonide planeerimise ning läbiviimise võimekuse (CPCC)[33] küberekspert ja mõnede missioonide kübereksperdid osalesid CERT-EU küberturvalisuse konverentsil 2019. aasta novembris. MSP on otseses kontaktis CERT-EUga ja annab korrapäraselt infot missiooni CIS ametnikele.

Nende 2019. aasta kohtumiste tulemused hõlmasid järgmist: (i) küberjulgeolekumeetmete kasutuselevõtt operatsioonide kavas (OPLAN) igal missioonil; ja ii) küberkeskuse määramine kõikidele missioonidele, et tõhustada tegevuse koordineerimist missiooni tasandil, CPSSi ja Euroopa välisteenistuse julgeoleku operatsioonikeskust.

MSP CIS on toetanud ka küberturvalisuse institutsioonidevahelise raamlepingu kasutamist. Varude II küberkaitse põhivarustuse hankeprotsess on lõpule viidud ja seonduvad seadmed on missioonil nüüd saadaval.

2019. aastal õnnestus MSP CIS meeskonnal katta kõik tsiviil-CSDP missioonid CERT-EU põhiteenuste kaudu. (Kokku 4 missiooni, 2019. aastal lisati 2. Missioonid on sõlmitud erikokkuleppel CERT-EUga ning on registreerunud CERT-EU edasijõudnud (ingl k *advanced*) teenuste saamiseks k.a võrgu järelevalve, läbitungimiskatse ja juhtumite käsitlemise.)

ESDC koolituskursuste portfell pakkus missioonidele välja koolitustegevusi, et suurendada ettevõttesisest küberturvalisuse kultuuri.

[30] Annual Review Conference
[31] *The Annual report of the Mission Support Platform 2019. Brussels, 14 April 2020 WK 3795/2020 INIT.* Dokumentil on AK märge.
[32] Misson Support Platform Communication and Information Systems
[33] Civilian Planning and Conduct Capability

Töödokument: Mini-kontseptsioon ÜJKP tsiviiltoetuse kohta hübriidohtude vastu võitlemisel 20. mai 2020 (Euroopa välisteenistus 8077/20)[34]

Euroopa välisteenistuse väljatöötatud mini-kontseptsioon tutvustab ÜJKP tsiviilkontseptsiooni - hübriidohtu -, mis tuleneb uuest julgeolekukeskkonnast. Minikontseptsioon määrab kindlaks vajaliku uue väljaõppe, koostöö asjaomaste ELi institutsioonidega, muudatused missiooniprotokollides ja protsessides jne. Kontseptsioon käsitleb ÜJKP tsiviilmissioonide kontekstis hübriidohtude kindlakstegemise, neile reageerimise ja neile vastupanuvõime suurendamise prioriteetset valdkonda. See põhineb jätkuvatel jõupingutustel hübriidohtudele vastupanuvõime suurendamiseks nii missioonide endi kui ka vastuvõtvate riikide toetuseks, ning pakub välja viise, kuidas parandada vastupanuvõimet nende väljakutsete vastu.

Kuigi hübriidohtude määratlused on erinevad ja nende muutuvale olemusele reageerimiseks peavad need olema paindlikud, on selle minikontseptsiooni eesmärk käsitleda kahjulike hübriidtoimingute järgmisi põhijooni: sunniviisilise ja õõnestava tegevuse segu, tavapärased ja ebakonventsionaalsed meetodid (nt diplomaatilised, sõjalised, majanduslikud, tehnoloogilised, meedia-, religioossed institutsioonid jne), mida riiklikud või valitsusvälised osalejad saavad koordineeritult kasutada konkreetsete poliitiliste eesmärkide saavutamiseks, jäädes samal ajal ametlikult välja kuulutatud sõja piiriks.

Kõik ÜJKP tsiviilmissioonid võivad tugineda jätkuvatele ELi jõupingutustele hübriidohtude vastu võitlemisel, sealhulgas ELi hübriidohtude ühisüksus,[35] Euroopa välisteenistuse strateegilise kommunikatsiooni rakkerühmade ja hübriidsete riskiuuringute kaudu.

Suuremad jõupingutused ÜJKP tsiviilmissioonide vastu suunatud hübriidohtude vastu võitlemiseks hõlmavad hübriidohtude väljaõpet vastupanuvõime suurendamiseks, olukorrateadlikkuse suurendamist ja valmisolekut missiooni kaitsmiseks, samuti missiooni suurenenud rolli seoses ELi üldise olukorrateadlikkusega hübriidohtude osas. Lisaks peaks missioon olema ette valmistatud nii, et see aitaks suurendada vastuvõtva riigi vastupanuvõimet hübriidohtude vastu, mis võib hõlmata hübriidse riskiuuringu läbiviimist ja strateegiliste nõuannete tagamist, abi desinformatsiooni vastu võitlemisel ning koolituse pakkumist vastuvõtvale riigile.

[34] Dokument on hetkel kooskõlatamata.
[35] EU Hybrid Fusion Cell

2. ÜJKP MISSIOONIDEGA SEONDUVATE HÜBRIIDSETE OHTUDE JA KÜBERPOLIITIKA NING ÕIGUSLIKU RAAMISTIKU ANALÜÜS

2.1. TULEMUSED

I. Dokumendid esitavad laia teadlikkust sellest, et küberruum on selgelt piirideta sfäär, mille tõttu kõik seda kasutavad inimese ja kõik sellega seotud riigid / institutsioonid on silmitsi võimalike ohtudega.

II. Dokumendid keskenduvad ohumaastiku muutustele, sealhulgas kirjeldatakse, et ohud võivad tekkida ka mittetraditsioonilisel viisil, nt desinformatsioonikampaaniad jne. Sellega on võimalik tuvastada dokumentides kasvavat tähelepanu mõistele „hübriidoht".

III. ELi poliitikadokumentides pööratakse üha enam tähelepanu küber- ja hübriidohtudele, sealhulgas rõhutatakse vajadust tõsta teadlikkust ja vajadust rakendada asjakohaseid meetmeid (nt personali koolitus, asjakohaste üksuste loomine; suurem koostöö liikmesriikide ja asjaomaste asutuste vahel jne) ning suutma reageerida nendele uutele ja kiiresti arenevatele ohu vormidele.

IV. Kehtivad kogu ELi hõlmavad lepingud, samuti teiste rahvusvaheliste institutsioonidega, nt NATO, et teha koostööd ja üksteist toetada nende uute ohtude vastu võitlemisel.

V. Dokumendid kinnitavad, et küberjulgeoleku alase institutsioonilise koostöö jaoks on välja töötatud plaan, kuid näib, et seni pole kõnealust plaani töösse rakendatud.

VI. Euroopa välisteenistuselt oodatakse ÜJKP missioonide osas teatavaid otseseid meetmeid, et lisada uute ohtude hindamine / teadlikkus missiooni kavandamisse, samuti suurendada missiooni liikmete valmisolekut nende ohtudega missioonil olles toime tulla ja pakkuda asukohariigile asjakohast tuge.

a. Asjakohase koolituse osas eeldatakse, et liikmesriigid pakuvad seda koolitust või pakuvad sellest suurema osa.

b. Vaja on täiendavalt hinnata asjakohaseid koolitusvajadusi uute, tekkida võivate ohtude osas ja leida asjakohased koolitusvõimalused (sealhulgas asjakohaste asutuste, nt ESDC, CEPOL jne) juba pakutavad koolitused.

VII. Kuigi ÜJKP missioonide jaoks on kokku lepitud meetmed missioonipõhise teadlikkuse tõstmiseks ja uute ohtude suhtes vastupidavuse suurendamiseks, nt. „Minikontseptsioonid", on nende tegevuste elluviimist alustatud suhteliselt hiljuti. Selle tõttu puudub veel välja töötatud küberi minikontseptsioon, mis keskenduks konkreetselt ÜJKP missioonidele.

2.2. SOOVITUSED

Dokumendi kokkuvõte ja analüüs näitavad ELi kasvavat teadlikkust ja ennetavat reageerimist hübriidohtudele ja kübervarustusele nii seoses ELi sise- kui ka välispoliitika ja määrustega.

Samuti on dokumendid üldiselt hästi välja töötatud ja vastavad suuresti ÜJKP missioonide vajadustele.

Analüüsi ja järelduste kohaselt esitatakse järgmised soovitused ÜJKP missiooni liikmete tegevuse tõhususe suurendamiseks:

- Analüüsitud poliitikadokumendid sisaldavad nii praeguseid ELi põhiväärtusi kui ka lähenemisviise hübriidohtude ja küberi osas ning soovitavad asjakohastele ELi institutsioonidele küberintsidentidele reageerimise tõhustamiseks koolitusvahendeid, koolituse prioriteetide seadmist ja nii edasi. Missiooni liikmete koolitusse tuleks integreerida ELi poliitika- ja strateegiadokumentide vastavad osad.

- Hübriidohtude ja kübervara pidevalt muutuva iseloomu tõttu peaksid ÜJKP missioonidega õigeaegse teabevahetuse tagamiseks (asjakohased) missiooni liikmed saama ajakohastatud teavet ja juurdepääsu asjakohastele dokumentidele.

- Veendumaks, et ELi poliitika ja strateegiad jätkavad ÜJKP missioonide vajaduste rahuldamist, peaksid ÜJKP missioonide tippjuhid olema kaasatud ELi hübriidohtude ning küberpoliitika ja strateegiate väljatöötamisse.

- ÜJKP missioonide jaoks asjakohase teabe liikumise ja teadlikkuse tagamiseks tuleks jälgida ELi poliitika- ja strateegiadokumentide rakendamist ÜJKP missioonidel. Samuti tuleks protsessi muutmiseks vajaduse korral süstemaatiliselt koguda tagasisidet tuvastatud takistuste ja lünkade kohta.

- Küberturvalisuse küsimusi on ELi poliitikadokumentides hästi käsitletud, samas kui hübriidohud, sealhulgas nende määratlus, pole veel täielikult välja töötatud. Selle vajakajäämise addresseerimine peaks viima ühiste jõupingutusteni, pöörates piisavalt tähelepanu hübriidohtude pidevalt arenevatele nähtustele, nende erinevale iseloomule ja selle kajastamisele vastavates poliitikadokumentides.

II OLEMASOLEVATE KOOLITUSTE ANALÜÜS

Vastavalt EUCTG strateegilistele juhistele ÜJKP tsiviilõppe kohta viidi läbi saadaolevate koolituste uuring, mille eesmärk oli välja selgitada ÜJKP tsiviilmissioonide tulemuslikkuse seisukohast asjakohane koolitus, eriti seoses võimekaklastri „hübriidohud ja küber".

Olemasolevate koolitusvõimaluste kaardistamine toimus kooskõlas EUCTG ÜJKP tsiviilõppe strateegiliste suuniste punktis 18 sätestatud põhimõtetega, milles öeldakse, et „EUCTG peaks tagama, et ÜJKP koolitustegevused ja koolitusvõimalused järgivad ELi poolehoiu ja läbipaistvuse põhimõtteid ning on avatud kõigile ELi liikmesriikidele ". Arvestades, et paljud koolitused, mida pakutakse liikmesriikides, ei ole kõigile ELi liikmesriikidele avatud, näiteks asutuste olemuse tõttu, kus koolitust pakutakse nt kraadiõppe osa või keele tõttu, milles koolitust pakutakse, on koolituse kaardistamine suunatud ainult ELi institutsioonidele, kes peaksid pakkuma asjakohast koolitust.

Kuna puuduvad asjakohased ja hiljutised andmed olemasolevate koolitusstandarditest ja hübriidohtude-ning küberi-teemalistest koolitusvõimalustest liikmesriikides või muudes rahvusvahelistes organisatsioonides, viis CCT läbi koolitusvõimluste kaardistamiseks asjakohastele asutustele suunatud küsimustikuuringu. Uuringutulemuste kohaselt moodustati loetelu saadaolevatest koolitustest teemal „Hübriidohud ja küber" (vt: LISA 1).

III VÕIMEKLASTER HÜBRIIDOHUD JA KÜBER: KÕRGETASEMELISED ÕPIVÄLJUNDID (CTALO)

Võimeklaster Hübriidohud ja küber

Kõrgetasemelised õpiväljundid (CTALO)

Selle kursuse läbimisel on õppuril:

Õppimise tasemed			
Õppimisalad	**Baastase**	**Edasijõudnud**	**Hübriidohtude/küberi ekspert / spetsialist**
ELI ÜLDINE VASTUS HÜBRIIDIOHTUDELE JA KÜBERILE			
Teadmised (T)	- nimetab ELi poliitikadokumentides toodud uute julgeolekuväljakutsete, sealhulgas hübriidohtudega seotud probleemide lahendamiseks toodud meetmed;	- kirjeldab ÜJKP missioonide kontekstis hübriidohtude ja kübervaldkonnaga seotud uute julgeolekuprobleemide lahendamiseks mõeldud ELi poliitika ja strateegia eesmärki ja rakendusmehhanismi; - selgitab ELi poliitika- ja strateegiadokumentide olulisust uute julgeolekuprobleemide, sealhulgas hübriidohtudega seotud probleemide lahendamisel, ja nende olulisust missiooni tegevuses;	-kirjeldab üksikasjalikult ÜJKP missioonide rolli ELi hübriidohtude ja küberriskide vastu võitlemise poliitika ja strateegia rakendamisele kaasa aitamisel
Oskused (O)		- tuvastab ELi hübriidohtude ja küberkuritegevuse vastu võitlemise strateegia ja muude poliitiliste dokumentide vahelised seosed missioonide tegevuse kontekstis;	- pakub missiooni liikmetele meetmeid hübriidohtude ja küberkuritegevuse vastaseks võitluseks vastavalt EL strateegia-ja poliitikadokumentide asjakohastes osades toodule;
Autonoomia / vastutus (A/V)			- vastutab ELi poliitika-ja strateegiadokumentide ajakohastamise

			ettepanekute tegemise eest hübriidohtude ja küberkuritegevuse vastu võitlemise valdkonnas;
TÖÖGA SEOTUD SÜSTEEMIDE JA SEADMETE OHUTU KASUTAMINE MISSIOONI RUUMIDES			
Teadmised (T)	-loetleb missioonireeglid, suunised ja / või protseduurid, mis puudutavad missiooniga seotud teabe, dokumentide, IT-süsteemide, riist- ja tarkvara, rakenduste, digitaalsuhtlusega seotud asjaolude ja missioonil kättesaadava teabe/ dokumentide ohutut ja turvalist käitlemist ja kasutamist;	-kirjeldab missiooniga seotud IT-süsteemide, ametliku, tundliku ja/või salastatud (salajase, konfidentsiaalse, piiratud) teabe / dokumentide, riistvara ja digitaalsete sidevahendite ning rakenduste sobimatu käitlemise ja kasutamisega seotud riske;	
Oskused (O)		-simuleeritud keskkonnas valib ohutud ja turvalised protseduurid missiooniga seotud IT-süsteemide, teabe/ dokumentide ning digitaalsete sidevahendite ja -rakenduste käitlemiseks ja kasutamiseks;	-hindab missiooni riistvara käitlemise ja kasutamise reegleid, suuniseid ja / või protseduure; digitaalsuhtlusega seotud küsimusi (e-post, vestlused), tarkvara ja rakenduste kasutamist (nt WhatsApp ja muud rakendused), missiooniga seotud IT-süsteemide turvalist kasutamist, tehes ettepanekuid mis tahes kohanduste või muudatuste tegemiseks, et tagada IT-süsteemide ja -vahendite ohutu ja turvaline kasutamine; - selgitab välja IT-toe probleemid ja puudused ametliku, tundliku ja/või salastatud (salajase, konfidentsiaalse, piiratud) teabe/ dokumentide turvalisel käsitlemisel põhjendades riistvara,

			tarkvara ja rakenduste uuenduste valikut ja valitud uuenduste asjakohasust teabe turvalisema haldamise ja kasutamise tagamiseks;
Autonoomia / vastutus (A/V)			-võtab vastutuse dokumentide, IT-süsteemide, riist- ja tarkvara, nende rakenduste käitlemist ja kasutamist sätestavate, digitaalse suhtlusega seotud (e-post, vestlused) ELi ja missiooni eeskirjade, suuniste ja/või protseduuride muutmise/täiendamise eest põhjendades meetmete valikut;
ISIKLIKE SEADMETE OHUTU KASUTAMINE VÄLJASPOOL MISSIOONI RUUME			
Teadmised (T)	-kirjeldab riistvara kasutamise protseduure, digitaalsuhtlusega seotud turvalisuse probleeme e-posti, vestluste, sotsiaalmeedia, tarkvara ja rakenduste, nt WhatsApp ja muud rakendused, kasutamisel väljaspool missiooni ruume (nt kodus);	-annab hinnangu potentsiaalsetele riskidele, mis võivad tekkida riistvara kasutamisel, digitaalsuhtluses (e-post, vestlused, sotsiaalmeedia), tarkvara ja rakenduste (nt WhatsApp ja muud rakendused) kasutamisel väljaspool missiooni ruume (nt vastuvõtva riigi ametiasutustes, kodus);	
Oskused (O)		-valib simuleeritud keskkonnas turvalised riist- ja tarkvara, digitaalsuhtlusega seotud rakendused, milliseid kasutab väljaspool missiooni ruume (nt kodus);	-tuvastab missiooni liikmete probleemid ja riskid riistvara käitlemisel digitaalsuhtluses (e-post, vestlused, sotsiaalmeedia), tarkvara ja rakenduste (nt WhatsApp ja muud rakendused), kasutamisel väljaspool missiooni ruume (nt kodus);
Autonoomia/vastutus (A/V)			-võtab vastutuse riistvara ohutu ja turvalise kasutamise, digitaalse

			suhtlusega seotud probleemide (e-post, vestlused, sotsiaalne meedia), tarkvara ja rakendustega seotud protseduuride täiendamise meetmete väljatöötamise eest;
OLUKORRATEADLIKKUS			
Teadmised (T)	-kirjeldab missiooni keskkonda puudutavate regulaarsete/perioodiliste ülevaadete rolli seoses võimalike küber-/ hübriidohtudega, mis võivad tekkida missiooni riigis/piirkonnas;	- selgitab missiooni regulaarsete/ perioodiliste ülevaadete põhjal, kuidas hübriidohud ja küber võivad olukorda vastuvõtvas riigis ja missioonil mõjutada; - teatab tähelepanekutest, mis viitavad hübriidohtudele ja/või küberile kasutades selleks kokku lepitud suhtluskanaleid;	
Oskused (O)			- tuvastab simuleeritud stsenaariumi põhjal hübriidohtude ja küberruumiga seotud olukorrad ja teabe, mida tuleks kajastada missioonide regulaarsetes/ perioodilistes ülevaadetes;
Autonoomia/vastutus (A/V)			- hindab kriitiliselt missiooni vastuvõtva riigi jaoks tekkida võivaid erinevaid hübriidohte ja küberküsimusi analüüsides missiooni vastu võtva riigi julgeolekut, majandust ning rahvusvahelisi suheteid, pakkudes vastumeetmeid; - teeb ettepanekuid meetmete kohta, mis võimaldavad missiooni toetust asukohariigile hübriidohtude ja küberjuhtumite vastu võitlemisel;

HÜBRIIDOHUD			
Teadmised (T)	- kirjeldab hübriidohu peamisi iseloomulikke jooni; -kirjeldab erinevaid hübriidohtusid ja erinevaid viise, kuidas need võivad esineda; -kirjeldab protseduure selle kohta, kuidas ja kellega (missioonil) ühendust võtta, kui on tõendeid või kahtlustatakse juba aset leidnud hübriidohu juhtumit;	-selgitab hübriidohtusid puudutava missioonil kogutava asukohapõhise teabe olulisust missiooni otsustusprotsessi jaoks; -selgitab protseduure, kuidas ja kelle poole pöörduda (missioonil/Brüsselis), kui on tõendeid või kahtlustatakse juba aset leidnud hübriidohu juhtumit;	- kirjeldab peamisi ülesandeid ja tegevusi, mida täidavad ELi Hübriidsünteesirakud, Hübriidkeskuse Oivakeskus, Euroopa välisteenistuse strateegilise kommunikatsiooni rakkerühmad ja/või seonduvad hübriidsed riskiuuringutega tegelevad üksused; -defineerib laia valikut protseduure ja suhtluskanaleid, mida rakendada ja kasutada juhul, kui on tõendeid või kahtlustatakse juba aset leidnud hübriidohtu juhtumit (missioonil/ Brüsselis);
Oskused (O)		-hindab simuleeritud juhtumistsenaariumi põhjal teavet, mis võib viidata võimalikule hübriidohule;	- teeb simuleeritud stsenaariumi põhjal kindlaks erinevad hübriidohud, hinnates võimalikku asukohapõhist teavet hübriidohtude võimalikkuse kohta, võttes ja põhjendades võetavaid meetmeid;
Autonoomia/vastutus (A/V)			-võtab simuleeritud keskkonnas vastutuse hübriidohu tuvastamise ja sellest teavitamise eest kasutades kokkulepitud suhtluskanaleid ja protseduure;
KÜBEROHUD			
Teadmised (T)	-kirjeldab EL poliitikadokumentides kajastatud kõige enam levinumaid küberohtude tüüpe;	-selgitab küberohu määratlust - loetleb erinevad küberohtude tüübid, sealhulgas need, mis on kajastatud ELi poliitikadokumentides;	-selgitab mitmesuguseid ELi poliitikadokumente, millised kajastavad küberohtude temaatikat ÜJKP missioonide tegevuse kontekstis;

	- kirjeldab kõige sagedamini kasutatavaid küberrünnaku meetodeid;	- kirjeldab küberrünnaku meetodeid;	- selgitab küberintsidentide ja riskide vähendamise ja ennetamise meetmeid ja meetodeid ÜJKP missioonide kontekstis;
Oskused (O)		-simuleeritud keskkonnas valib reageerimisvõimalused / tööriistad / seadmed küberohu ennetamiseks vastavalt ELi ja missiooni protseduuridele	-kavandab simuleeritud juhtumistsenaariumi põhjal tegevused küberrünnakute vastu võitlemiseks, riskide maandamiseks ja küberintsidentide haldamiseks, taastades sealhulgas missiooni jaoks olulised süsteemid pärast küberintsidendi toimumist; - pakub küberintsidentide ennetamiseks vajalikud tööriistad / seadmed pakkudes meetmeid olemasolevate tööriistade/ seadmete täiendamiseks; -analüüsib riskide vähendamise meetmeid, et tulla toime küberohtude ja -intsidentidega vastavalt andmekaitse eeskirjadele; - kehtestab protseduurid missiooni jaoks oluliste süsteemide taastamiseks pärast küberintsidenti
Autonoomia/vastutus (A/V)			-vastutab küberintsidentide ennetamise eest ja nende aset leidmise korral missiooni oluliste süsteemide haldamise ja taastamisega seotud meetmete kooskõlastamise eest vastavalt kehtestatud korrale;

FÜÜSILISED OHUD IT-JA MUUDELE SÜSTEEMIDELE			
Teadmised (T)	-kirjeldab kõige sagedamini esinenud füüsilisi ohte ja haavatavusi, mis võivad missiooni jaoks olulisi IT-süsteeme/andmesalvestusi mõjutada/kahjustada;	-kirjeldab vahendeid, mida tavaliselt kasutatakse küber-/hübriidohu tekitamiseks või käivitamiseks;	-selgitab mitmeid tunnustatud füüsilisi ohte ja haavatavusi, mis võivad missiooni jaoks olulisi IT-süsteeme/ andmesalvestusüksusi mõjutada/ kahjustada; - kirjeldab üksikasjalikult tööriistu, mida tavaliselt kasutatakse IT-süsteemi/ andmesalvestite mõjutamiseks/ kahjustamiseks või küber-/hübriidohu tekitamiseks või käivitamiseks;
Oskused (O)		-valib simuleeritud keskkonnas meetmed, mis võimaldavad tuvastada ja kõrvaldada füüsilised ohud ja nõrgad kohad, mis võivad missiooni jaoks olulisi IT-süsteeme/andmesalvestusi mõjutada/kahjustada;	-teavitab mis tahes võetavatest meetmetest olles tuvastanud missiooni jaoks olulised füüsilised ohud ja nõrkused, mis võivad missiooni jaoks olulisi IT-süsteeme/ andmesalvestusüksusi mõjutada/ kahjustada; - tagab küber- ja hübriidohu minimeerimise vahendite püsiva kasutamise; -pakub riskide vähendamise meetmeid.
Autonoomia/vastutus (A/V)			-võtab simuleeritud juhtumistsenaariumi põhjal vastutuse tegevuse koordineerimise eest, mille eesmärk on vähendada missiooni jaoks hädavajalikke IT-süsteeme/ andmesalvestusüksusi mõjutavaid füüsilisi ohte ja haavatavusi.

KÜBER-TEEMALISED KOOLITUSED (Andmed originaalkeeles)

	KOOLITUSE NIMETUS	KOOLITUSE PAKKUJA	KOOLITUSE KVALIFIKATSIOONITASE	KOOLITUSE SIHTRÜHM	KOOLITUSE MEETOD	MÄRKUSED
1.	Challenges of EU Cyber Security	European Security and Defence College (ESDC)	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
2.	Cyber Security/Defence Training Programme	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
3.	Infrastructures in the Context of Digitization	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
4.	Cybersecurity basics for non-experts	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
5.	Cybersecurity Organisational and Defensive Capabilities	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
6.	Information Security Management and ICT security	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
7.	The role of the EU cyber ecosystem in the global cyber security stability	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
8.	Civil-Military Dimension of Cyberattacks	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
9.	Cyber Diplomacy	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	

10.	Cyber Defence policy on national and international levels	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
11.	Cybersecurity and smart city: challenges for residents, visitors and businesses	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
12.	Cyber Threat Intelligence and Information Sharing using MISP	ESDC	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
13.	AKU 104b Information Security Management Implementation Course Part 1_v1.1	European Security and Defence College (ESDC) – AKU (Autonomous knowledge units)			e-learning	
14.	AKU 104c Information Security Management Implementation Course Part 2_v1.1	ESDC – AKU			e-learning	
15.	AKU 104c Information Security Management Implementation Course Part 3_v1.1	ESDC – AKU			e-learning	
16.	AKU 105 Cyber Situational awareness for senior decision makers	ESDC – AKU		Senior officials	e-learning	
17.	Open source intelligence (OSINT) and IT solutions. (1st)	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Law enforcements analysts, officers who have some experience of High-Tech crime investigations or are about to be appointed as network investigators or IT forensic analysts, and prosecutors working in cyber-Investigations.	Residential	
18.	Open source intelligence (OSINT) and IT solutions. (2nd)	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Law enforcements analysts, officers who have some experience of High-Tech crime	Residential	

				investigations or are about to be appointed as network investigators or IT forensic analysts, and prosecutors working in cyber-Investigations.		
19.	Darkweb and cryptocurrencies	CEPOL	Expert level/specialised training	OPERATIONS STAFF - LE officials and prosecutors dealing with Darkweb and VCs, in cybercrime but also other relevant crime areas (e.g. online trafficking of firearms, drugs, payment card credentials).	Residential	
20.	Conducting forensic searches in various IT devices	CEPOL	Expert level/specialised training	OPERATIONS STAFF- Forensic experts with advanced professional experience on investigating IT devices.	Residential	
21.	Cybercrime - advanced Windows file systems forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Computer forensics practitioners who need to improve file systems knowledge in order to supervise forensic analysis and provide explanation at court.	Residential	
22.	Cross border exchange of e-evidence	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Head of Operations, Deputy Head of Operations, Head of Component, Head of Unit X, Deputy Head of Unit X, Head of Field Office, Deputy Head of Field Office, Head of Regional Coordination/Outreach Unit, Deputy Head of Regional Coordination/Outreach Unit, Head of Project Cell/Project Manager, Head of Training Unit, Justice Adviser, Legal Adviser	Residential	

				(Operations), Senior Adviser/Expert, Adviser/Expert, Human Rights Adviser, Gender Adviser, Project Management Officer, Programme Officer, Coordination and Cooperation Officer, Monitor, Operational Officer, Training Officer, BSE Policy Support Officer		
23.	Digital forensic investigators training	CEPOL	Expert level/specialised training	OPERATIONS STAFF - Law enforcement officials who have experience of High-Tech crime investigations or are about to be appointed as network investigators or IT forensic analysts.	Residential	
24.	Cyber Intelligence	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law enforcement officials working in the field of cyber intelligence at the operational and technical level, and prosecutors working in cyber-investigations.	Residential	
25.	Malware Investigations	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement Investigators who have a good knowledge of Computer Networking and the Microsoft Windows OS architecture.	Residential	
26.	Live Data Forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement Investigators who have a good knowledge of Computer Networking and the Microsoft Windows OS architecture.	Residential	

27.	Mac Forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement investigator involved in computer forensics with at least 1 year experience of computer forensics	Residential	
28.	Linux Forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law Enforcement investigator involved with computer forensics which must have been working with computer forensics for at least 1 year.	Residential	
29.	First responders and cyber forensics	CEPOL	Expert level/specialised training	OPERATIONS STAFF Law enforcement officials – IT crime first responders (first responders in cases of cyber-attacks).	Residential	

HÜBRIIDOHTUDE-TEEMALISED KOOLITUSED (Andmed originaalkeeles)

	KOOLITUSE NIMETUS	**KOOLITUSE PAKKUJA**	**KOOLITUSE KVALIFIKATSIOONITASE**	**KOOLITUSE SIHTRÜHM**	**KOOLITUSE MEETOD**	**MÄRKUSED**
1.	EU facing “hybrid threats” challenges	European Security and Defence College (ESDC)	EQF/SQF - 6 and 7	Middle-ranking to senior officials (Civ-Mil)	Residential & e-learning	
2.	The Challenges of securing Maritime Areas	ESDC	Advanced/specialised training	Civilian and military personnel (incl. police) from EU Member States, EU institutions/agencies.	Residential & e-learning	
3.	Advanced Course for Political Advisors in EU Missions and Operations	ESDC	Advanced/specialised training	Personnel working in political advisory positions/departments in national capitals, EU institutions, EU agencies as well as in EU missions and operations.	Residential & e-learning	

4.	EU Energy security: implications fot the CSDP	ESDC	Advanced/specialised training	Civilian and military personnel (incl. police) from EU Member States, EU institutions/agencies.	Residential	2020 course held online
5.	Regional seminars on security and defence	ESDC				
	E.g. *CSDP Seminar (Bi-regional Security and Defence Seminar) EU-South America and Mexico*	ESDC	Basic training/ Orientation Course	Civilians, Military, Police (Participants should be senior-level officials, preferable representing both Ministry of Foreign Affairs, Ministry of Defence and the police forces/services from the respective participant country.)	Residential & e-learning	
6.	AKU 106a Hybrid-CoE Adversarial Behaviour	European Security and Defence College (ESDC) - AKU (Autonomous knowledge units) (Course developed by Hybrid CoE)			e-learning	
7.	AKU 106b Hybrid-CoE The Landscape of Hybrid Threats	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
8.	AKU 106c Hybrid-CoE: The changing security environment (HS2)	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
9.	AKU 106d Hybrid-CoE Introduction to Hybrid Deterrence	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	

10.	AKU 106e Hybrid-CoE: Hybrid Warfare (JS)	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
11.	AKU 106f Hybrid-CoE: Hybrid Threats & Maritime Security (JS)	ESDC - AKU (Course developed by Hybrid CoE)			e-learning	
12.	Prevention of election interference	Hybrid CoE		Practitioners	Residential	Courses held up to date: a. Canada (January 2019, two trainings), around 105 practitioners b. Lithuania (February 2019), 40 practitioners c. Finland (March 2019), 35 practitioners d. Poland (April 2019) 50 practitioners e. EU RAS (only exercise April 2019) 30+ practitioners f. Montenegro (January 2020) 40 practitioners

KOOLITUSED, MIS HÕLMAVAD HÜBRIIDOHTUDE JA/VÕI KÜBERI TEEMAT (Andmed originaalkeeles)

	KOOLITUSE NIMETUS	**KOOLITUSE PAKKUJA**	**KOOLITUSE KVALIFIKATSIOONITASE**	**KOOLITUSE SIHTRÜHM**	**KOOLITUSE MEETOD**	**MÄRKUSED**
1.	CSDP High Level Course (HLC) (e.g. 2020-2021 JEAN REY - 4 modules)	European Security and Defence College (ESDC)		senior experts (mil-civ); incl. diplomats and police officers, who work in key positions or have a clear potential to achieve leadership posts particular CFSP/CSDP. Suitable academics, members of NGOs and the business community may be invited to participate	Residential and e-learning	.

2.	CSDP orientation course	ESDC		Nominated participants from civilian and military personnel from EU Member States, EU Institutions and Agencies, working the field of CSFP/CSDP (1 person per country, or more upon availability.)	Residential	
3.	AKU 01 - History and Context of ESDP/CSDP Development	European Security and Defence College (ESDC) – AKU (Autonomous knowledge units)			e-learning	
4.	AKU 02 - The European Global Strategy (EUGS)	ESDC – AKU			e-learning	
5.	AKU 03 - Role of EU Institutions in the field of CFSP/ CSDP	ESDC – AKU			e-learning	
6.	AKU4 - CSDP Crisis Management Structures and the Chain of Command	ESDC – AKU			e-learning	
7.	AKU6 - CSDP Decision Shaping/Making	ESDC – AKU			e-learning	
8.	AKU 07 - Impact of Lisbon Treaty on CSDP	ESDC – AKU			e-learning	
9.	AKU 11A - Gender and the UNSCR 1325 women, peace and security agenda	ESDC – AKU			e-learning	
10.	AKU 11B - Gender aspects in missions and operations	ESDC – AKU			e-learning	
11.	AKU 15 - European Armaments Cooperation (EAC)	ESDC – AKU			e-learning	
12.	AKU16 - An introduction to the Protection of Civilians (PoC) v.2	ESDC – AKU			e-learning	
13.	AKU 17 - Fragility and Crisis Management	ESDC – AKU			e-learning	
14.	AKU 21- Intercultural Competence	ESDC – AKU			e-learning	

15.	AKU 25 - The EU's Mutual Assistance Clause	ESDC – AKU			e-learning	
16.	AKU 34: PM2 - The EC's Project Management Methodology	ESDC – AKU			e-learning	
17.	AKU 200 Conflicts and crisis management - The EU as a global actor (Gorgio Porzio Adviser of CivOpsCrd)	ESDC – AKU			e-learning	
18.	AKU 300: Intercultural Competence in Civilian Crisis Management	ESDC – AKU			e-learning	