EUROOPAN
KOMISSIO

UNIONIN ULKOASIOIDEN
JA TURVALLISUUSPOLITIIKAN
KORKEA EDUSTAJA

Bryssel 6.4.2016
JOIN(2016) 18 final

YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

Yhteinen kehys hybridiuhkien torjumiseksi:

Euroopan unionin toimet

1. JOHDANTO

Euroopan unionin turvallisuusympäristö on muuttunut viime vuosina voimakkaasti. Mittavat rauhaan ja vakauteen kohdistuvat haasteet EU:n itäisillä ja eteläisillä naapuruusalueilla osoittavat jatkuvasti, että unionin on mukautettava ja lisättävä voimavarojaan turvallisuuden takaajana. Painopisteen olisi oltava ulkoisen ja sisäisen turvallisuuden läheisessä suhteessa. Monet rauhaan, turvallisuuteen ja vaurauteen tällä hetkellä kohdistuvat haasteet johtuvat epävakaudesta EU:n välittömillä naapurialueilla sekä uhkien muuttumisesta. Euroopan komission puheenjohtaja Jean-Claude Juncker totesi vuonna 2014 esittämissään poliittisissa suuntaviivoissa, että ”EU:ta on vahvistettava myös turvallisuus- ja puolustuskysymyksissä” ja että eurooppalaisia ja kansallisia välineitä on yhdistettävä aiempaa tehokkaammin. Lisäksi yhteisen ulko- ja turvallisuuspolitiikan korkea edustaja alkoi 18. toukokuuta 2015 kokoontuneen ulkoasiainneuvoston pyynnöstä laatia tiiviissä yhteistyössä komission yksiköiden ja Euroopan puolustusviraston kanssa sekä EU:n jäsenvaltioita kuullen tätä yhteistä kehystä ja siihen sisältyviä toteutettavissa olevia ehdotuksia hybridiuhkien torjumiseksi ja EU:n ja sen jäsenvaltioiden sekä kumppaneiden sietokyvyn parantamiseksi.[1] Eurooppa-neuvosto muistutti kesäkuussa 2015 tarpeesta ottaa EU:n välineitä käyttöön hybridiuhkien torjumiseksi.[2]

Hybridiuhkien määritelmät vaihtelevat, ja niiden on edelleenkin oltava joustavia, jotta voidaan ottaa huomioon uhkien muuttuva luonne. Käsitteellä tarkoitetaan erilaisia pakottavia ja turvallisuutta vaarantavia toimia ja (diplomaattisia, sotilaallisia, taloudellisia ja teknisiä) perinteisiä ja uusia menetelmiä, joita valtiolliset tai valtiosta riippumattomat toimijat voivat käyttää koordinoidusti tiettyjen tavoitteiden saavuttamiseksi ilman, että sotatilan virallisen julistamisen kynnys ylittyy. Yleensä tarkoituksena on käyttää hyväksi kohteen haavoittuvuutta ja luoda epäselvyyttä päätöksentekoprosessien haitaksi. Hybridiuhkia voidaan luoda laajamittaisilla disinformaatiokampanjoilla, ja sosiaalista mediaa voidaan käyttää poliittisen retoriikan valvontaan tai sijaistoimijoiden radikalisointiin, rekrytointiin ja ohjaamiseen.

Kun hybridiuhkien torjunta liittyy kansalliseen turvallisuuteen ja puolustukseen sekä yleisen järjestyksen ylläpitoon, pääasiallinen vastuu on jäsenvaltioilla, sillä suurin osa kansallisista haavoittuvuustekijöistä on maakohtaisia. Monilla EU:n jäsenvaltioilla on kuitenkin yhteisiä uhkia, joiden kohteena voivat olla myös rajatylittävät verkostot tai infrastruktuuri. Tällaisiin uhkiin voidaan puuttua tehokkaammin koordinoiduilla EU:n tason toimilla käyttämällä EU:n toimintamalleja ja välineitä ja perustamalla toimet eurooppalaiseen yhteisvastuuseen, keskinäiseen avunantoon ja kaikkiin Lissabonin sopimuksen tarjoamiin mahdollisuuksiin. EU:n politiikka ja välineet voivat olla, ja ovatkin jo merkittävissä määrin, keskeisessä lisäarvoa tuottavassa roolissa lisättäessä tietoisuutta asiasta. Näin parannetaan jäsenvaltioiden kestokykyä ja valmiuksia vastata yhteisiin uhkiin. Tässä kehyksessä ehdotettuja unionin ulkoisia toimia ohjaavat Euroopan

[1] Neuvoston päätelmät yhteisestä turvallisuus- ja puolustuspolitiikasta (YTPP), toukokuu 2015, neuvoston asiakirja 8971/15.
[2] Eurooppa-neuvoston päätelmät, kesäkuu 2015, EUCO 22/15.

unionista tehdyn sopimuksen (SEU) 21 artiklassa vahvistetut periaatteet, joihin kuuluvat demokratia, oikeusvaltioperiaate, ihmisoikeuksien yleismaailmallisuus ja jakamattomuus sekä Yhdistyneiden kansakuntien peruskirjan ja kansainvälisen oikeuden periaatteiden noudattaminen.[3]

Tämän yhteisen tiedonannon tarkoituksena on helpottaa kokonaisvaltaisen lähestymistavan laatimista. Näin EU voi torjua hybridiluonteisia uhkia kohdennetusti ja koordinoidusti jäsenvaltioiden kanssa luomalla synergiaa kaikkien asianomaisten välineiden välille ja edistämällä tiivistä yhteistyötä kaikkien asiaan liittyvien toimijoiden kesken.[4] Toimet perustuvat olemassa oleviin strategioihin ja alakohtaisiin politiikkoihin, joilla pyritään parantamaan turvallisuutta. Hybridiuhkia voidaan torjua erityisesti Euroopan turvallisuusagendan[5], EU:n tulevan globaalin ulko- ja turvallisuuspoliittisen strategian ja Euroopan puolustusalan toimintasuunnitelman[6], Euroopan unionin kyberturvallisuusstrategian[7], Euroopan energiaturvallisuusstrategian[8] ja Euroopan unionin merellisen turvallisuusstrategian[9] avulla.

Koska myös Nato työskentelee hybridiuhkien torjumiseksi ja ulkoasiainneuvosto on ehdottanut yhteistyön ja koordinoinnin vauhdittamista tällä alalla, joillakin ehdotuksilla pyritään lisäämään EU:n ja Naton yhteistyötä hybridiuhkien torjumisessa.

Ehdotuksen painopisteitä ovat tietoisuuden parantaminen, kestokyvyn lisääminen, ennaltaehkäisy, kriisitilanteisiin reagoiminen ja palautuminen.

2. UHAN HYBRIDILUONTEEN TUNNISTAMINEN

Hybridiuhat pyritään kohdentamaan tietyn maan haavoittuvuustekijöihin, ja usein niillä halutaan vaarantaa demokraattiset perusarvot ja vapaudet. Korkea edustaja ja komissio tekevät ensivaiheessa jäsenvaltioiden kanssa yhteistyötä tilannetietoisuuden lisäämiseksi valvomalla ja arvioimalla riskejä, jotka voidaan kohdistaa EU:n haavoittuvuustekijöihin. Komissio on kehittämässä turvallisuusriskien arviointimenetelmiä avuksi päätöksentekijöiden informoimiseen ja riskeihin perustuvan politiikan suunnitteluun monilla aloilla ilmailun turvaamisesta terrorismin rahoittamiseen ja rahanpesun torjuntaan. Lisäksi olisi hyödyllistä, jos jäsenvaltiot tekisivät selvityksen hybridiuhille alttiista aloista. Tavoitteena olisi hybridiuhkien indikaattorien kartoittaminen ja sisällyttäminen ennakkovaroitusjärjestelmiin ja olemassa oleviin riskinarviointimekanismeihin sekä niistä tiedottaminen tarpeen mukaan jäsenvaltioiden kesken.

[3] EU:n perusoikeuskirja sitoo toimielimiä ja jäsenvaltioita unionin lainsäädännön täytäntöönpanossa.
[4] Mahdollisiin säädösehdotuksiin sovelletaan komission parempaa sääntelyä koskevia vaatimuksia, jotka esitetään parempaa sääntelyä koskevissa komission suuntaviivoissa (SWD(2015) 111).
[5] COM(2015) 185 final.
[6] Esitetään vuonna 2016.
[7] EU:n kyberpuolustuspolitiikan kehys, neuvoston asiakirja 15585/14, ja yhteinen tiedonanto ”Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö”, helmikuu 2013, JOIN(2013)1.
[8] Yhteinen tiedonanto ”Euroopan energiavarmuusstrategia”, toukokuu 2014, SWD(2014) 330.
[9] Yhteinen tiedonanto ”Tavoitteena kansainvälisten merialueiden avoimuus ja turvallisuus: Euroopan unionin merellisen turvallisuusstrategian osatekijät”, JOIN(2014) 9 final, 6.3.2014.

<u>Toimi 1</u>: Jäsenvaltioita kehotetaan käynnistämään tarpeen mukaan komission ja korkean edustajan tuella hybridiriskiselvitys sellaisten tärkeimpien haavoittuvuustekijöiden ja erityisten hybridiuhkiin liittyvien indikaattorien kartoittamiseksi, jotka saattavat vaikuttaa kansallisiin ja Euroopan laajuisiin rakenteisiin ja verkostoihin.

3. EU:N TOIMIEN ORGANISOINTI: TIETOISUUDEN LISÄÄMINEN

3.1. EU:n hybridianalyysikeskus

On keskeisen tärkeää, että EU saavuttaa koordinoidusti jäsenvaltioiden kanssa riittävän tilannetietoisuuden, jotta voidaan havaita turvallisuusympäristön muutokset, jotka liittyvät valtiollisten ja/tai valtiosta riippumattomien toimijoiden hybriditoimintaan. Jotta hybridiuhkia voidaan torjua tehokkaasti, on tärkeää parantaa tietojenvaihtoa ja edistää asiaan liittyvien tiedustelutietojen jakamista eri aloilla ja Euroopan unionin, sen jäsenvaltioiden ja kumppaneiden välillä.

EU:n hybridianalyysikeskus perustetaan Euroopan ulkosuhdehallinnon (EUH) tiedusteluanalyysikeskuksen (EU INTCEN) yhteyteen, ja siihen keskitetään hybridiuhkien analysointi. Hybridianalyysikeskus vastaanottaa, analysoi ja jakaa turvallisuusluokiteltuja ja julkisista lähteistä saatavia tietoja, jotka liittyvät hybridiuhkien indikaattoreihin ja uhkia koskeviin varoituksiin eri sidosryhmiltä EUH:ssa (myös unionin edustustoissa), komissiossa (ja unionin virastoissa[10]) ja jäsenvaltioissa. Hybridianalyysikeskus analysoisi yhdessä EU:n[11] ja jäsenvaltioiden tasolla toimivien muiden samankaltaisten elinten kanssa EU:hun ja sen naapurialueeseen liittyviä hybridiuhkien ulkoisia osatekijöitä, jotta turvapoikkeamia voitaisiin tarkastella nopeasti ja EU:n strategiseen päätöksentekoprosessiin saataisiin tietoja esimerkiksi EU:n tasolla tehtävää turvallisuusriskien arviointia varten. Hybridianalyysikeskuksen tuottamat analyysit prosessoitaisiin ja käsiteltäisiin turvallisuusluokiteltuja tietoja ja tietosuojaa koskevien Euroopan unionin sääntöjen[12] mukaisesti. Hybridiuhkayksikön pitäisi olla yhteydessä olemassa oleviin EU:n ja kansallisen tason elimiin. Jäsenvaltioiden olisi perustettava EU:n hybridianalyysikeskukseen liittyvät kansalliset yhteyspisteet. Myös henkilöstö EU:ssa ja sen ulkopuolella (mukaan lukien EU:n edustustoihin, operaatioihin ja tehtäviin lähetetty henkilöstö) sekä jäsenvaltioissa olisi koulutettava havaitsemaan hybridiuhkien ensimmäisiä merkkejä.

<u>Toimi 2</u>: Perustetaan hybridiuhkia koskevien turvallisuusluokiteltujen ja julkisista lähteistä saatavien tietojen vastaanottamiseen ja analysoimiseen kykenevä EU:n hybridianalyysikeskus EU INTCENin rakenteeseen. Jäsenvaltioita kehotetaan perustamaan hybridiuhkia käsittelevät kansalliset yhteyspisteet, jotta voidaan varmistaa yhteistyö ja turvallinen viestintä EU:n hybridianalyysikeskuksen kanssa.

[10] Niiden tehtävänannon mukaisesti.
[11] Esimerkiksi Europolin Euroopan verkkorikostorjuntakeskus ja Euroopan terrorismintorjuntakeskus, Frontex ja tietotekniikan kriisiryhmä CERT-EU.
[12] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24. lokakuuta 1995.

3.2. Strateginen viestintä

Hybridiuhkien toteuttajat saattavat levittää järjestelmällisesti disinformaatiota esimerkiksi kohdennetuilla sosiaalisen median kampanjoilla. Näin pyritään radikalisoimaan henkilöitä, horjuttamaan yhteiskuntaa ja valvomaan poliittista retoriikkaa. On hyvin tärkeää, että hybridiuhkiin kyetään vastaamaan pätevällä **strategisen viestinnän** strategialla. Yhteiskunnan valmiuksia vastata hybridiuhkiin voidaan parantaa ensisijaisesti antamalla nopeasti asiatietoihin perustuvia vastauksia ja lisäämällä yleistä tietoisuutta.

Strategisessa viestinnässä olisi perinteisen audiovisuaalisen ja verkkomedian lisäksi käytettävä täysimääräisesti hyväksi sosiaalista mediaa. EUH:n pitäisi käyttää East StratCom- ja Arab StratCom -työryhmien toiminnasta saatujen kokemusten pohjalta lingvistejä, jotka osaavat sujuvasti asianomaisia muita kuin EU-kieliä, parhaalla mahdollisella tavalla. Lisäksi olisi käytettävä sosiaalisen median asiantuntijoita. Nämä voivat seurata EU:n ulkopuolista tiedottamista ja varmistaa, että disinformaatioon vastataan kohdennetulla viestinnällä. Lisäksi jäsenvaltioiden olisi kehitettävä koordinoituja strategisen viestinnän mekanismeja lähteiden ilmoittamisen tueksi ja disinformaation torjumiseksi, jotta hybridiuhat voidaan paljastaa.

Toimi 3: Korkea edustaja tarkastelee jäsenvaltioiden kanssa tapoja päivittää ja koordinoida valmiuksia proaktiiviseen strategiseen viestintään sekä optimoida median seurannan ja kielten erityisosaajien käyttöä.

3.3. Hybridiuhkien torjunnan osaamiskeskus

Yksi monikansallinen laitos tai laitosten verkosto voisi toimia tiettyjen jäsenvaltioiden ja kumppaniorganisaatioiden[13] kokemusten pohjalta hybridiuhkien torjunnan osaamiskeskuksena. Se voisi keskittyä hybridistrategioiden soveltamisen tutkimiseen ja edistää uusien käsitteiden ja teknologian kehittämistä yksityisellä sektorilla ja toimialalla jäsenvaltioiden kestokyvyn parantamiseksi. Tutkimuksen avulla voitaisiin lähentää EU:n ja jäsenvaltioiden toimintalinjoja, oppeja ja käsitteitä sekä varmistaa, että päätöksenteossa voidaan ottaa huomioon hybridiuhkien monimutkaisuus ja epävarmuus. Tällaisen osaamiskeskuksen olisi suunniteltava ohjelmia tutkimuksen edistämiseksi ja kehitettävä harjoituksia käytännön ratkaisujen löytämiseksi hybridiuhkien asettamille haasteille. Tällaisen osaamiskeskuksen vahvuus riippuisi asiantuntemuksesta, jonka saavat aikaan siihen osallistuvat monikansalliset ja -alaiset edustajat siviili- ja sotilasaloilta, yksityiseltä sektorilta ja tiedemaailmasta.

Osaamiskeskus tekisi tiiviisti yhteistyötä jo toiminnassa olevien EU:n[14] ja Naton[15] osaamiskeskusten kanssa. Näin voitaisiin hyötyä eri näkökulmista, joita hybridiuhkiin on

[13] Naton osaamiskeskukset.
[14] Esim. Euroopan unionin turvallisuusalan tutkimuslaitos (EUTT), CBRN-kysymyksiä käsittelevät alakohtaiset EU:n osaamiskeskukset.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

saatu kyberpuolustuksesta, strategisesta viestinnästä, siviili- ja sotilasyhteistyöstä, energia-asioista sekä kriisitoiminnasta.

<u>Toimi 4</u>: Jäsenvaltioita kehotetaan harkitsemaan osaamiskeskusten perustamista hybridiuhkien torjumiseksi.

4. EU:N TOIMIEN ORGANISOINTI: KESTOKYVYN PARANTAMINEN

Kestokyvyllä tarkoitetaan valmiuksia kestää painetta ja toipua haasteista entistä vahvempana. Jotta hybridiuhkia voitaisiin torjua tehokkaasti, on puututtava tärkeimmän infrastruktuurin, toimitusketjujen ja yhteiskunnan mahdollisiin haavoittuvuustekijöihin. EU:n tason infrastruktuurin kestokykyä voidaan parantaa EU:n välineillä ja toimintalinjoilla.

4.1. Kriittisen infrastruktuurin suojaaminen

Kriittisen infrastruktuurin (esim. energiantoimitusketjujen ja liikenteen) suojaaminen on tärkeää, sillä hybridiuhkien toteuttajien epätavanomainen hyökkäys nk. pehmeään kohteeseen voisi häiritä vakavasti taloutta tai yhteiskuntaa. Euroopan elintärkeiden infrastruktuureiden suojaamisohjelma[16] (EPCIP) tarjoaa kriittisen infrastruktuurin suojaamiseksi kaikki vaaratekijät kattavan, monialaisiin järjestelmiin perustuvan toimintamallin. Siinä otetaan huomioon riippuvuussuhteet, ja se perustuu ennaltaehkäisyn, varautumisen ja reagoinnin toimintalinjoissa toteutettuihin toimiin. Euroopan elintärkeää infrastruktuuria koskevassa direktiivissä[17] vahvistetaan menettely, jonka avulla määritetään ja nimetään Euroopan elintärkeät infrastruktuurit, sekä yhteinen lähestymistapa infrastruktuurien suojaamisen parantamistarpeen arviointiin. Erityisesti direktiivin nojalla olisi aloitettava uudelleen työ liikenteeseen liittyvän kriittisen infrastruktuurin (esim. EU:n suurimmat lentoasemat ja kauppasatamat) kestokyvyn parantamiseksi. Komissio arvioi, onko kaikilla asianomaisilla aloilla tarpeen kehittää yhteisiä välineitä, kuten indikaattoreita, kriittisen infrastruktuurin kestokyvyn parantamiseksi hybridiuhkia vastaan.

<u>Toimi 5</u>: Komissio määrittää yhteistyössä jäsenvaltioiden ja sidosryhmien kanssa yhteiset välineet, myös indikaattorit, kriittisen infrastruktuurin suojelun ja kestokyvyn parantamiseksi hybridiuhkia vastaan tärkeillä aloilla.

4.1.1. Energiaverkot

Energian häiriintymätön tuotanto ja jakelu ovat elintärkeitä EU:lle, ja merkittävät sähkökatkot voivat olla haitallisia. Hybridiuhkien torjunnan kannalta on tärkeää monipuolistaa EU:n energialähteitä, -toimittajia ja -reittejä edelleen turvallisempien ja kestävämpien energiatoimitusten varmistamiseksi. Komissio on myös tekemässä EU:n

[16] Komission tiedonanto elintärkeiden infrastruktuurien suojaamista koskevasta EU:n ohjelmasta, 12.12.2006, KOM(2006) 786 lopullinen.

[17] Neuvoston direktiivi 2008/114/EY, annettu 8 päivänä joulukuuta 2008, Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista, EUVL L 345, 23.12.2008.

voimaloista riski- ja turvallisuusarviointeja (stressitestejä). Energiantarjonnan monipuolistamiseksi ollaan lisäämässä energiaunionistrategian puitteissa tehtävää työtä. Esimerkiksi eteläisen kaasukäytävän avulla voidaan saada kaasua Kaspianmeren alueelta Eurooppaan, ja Pohjois-Euroopassa on perustettu nestekaasuterminaaleja, joihin tulee toimituksia useilta toimittajilta. Tätä esimerkkiä olisi seurattava Keski- ja Itä-Euroopassa ja Välimeren alueella, jossa on kehitteillä kaasuterminaali.[18] Myös koko ajan kehittyvät nesteytetyn maakaasun markkinat edistävät tätä tavoitetta.

Komissio tukee tiukkojen ydinaineita ja -laitoksia koskevien turvallisuusnormien laatimista ja käyttöönottoa, mikä parantaa kestokykyä. Komissio kannustaa jäsenvaltioita saattamaan ydinturvallisuusdirektiivin[19]johdonmukaisesti osaksi kansallista lainsäädäntöä ja panemaan sen täytäntöön. Direktiivissä vahvistetaan säännöt onnettomuuksien estämiselle ja niiden seurausten lieventämiselle. Sama koskee perusnormidirektiiviä[20], jossa käsitellään valmiusjärjestelyjä ja -toimintaa koskevaa kansainvälistä yhteistyötä erityisesti naapurijäsenvaltioiden ja muiden naapurimaiden kesken.

<u>Toimi 6</u>: Komissio tukee yhteistyössä jäsenvaltioiden kanssa työtä energialähteiden monipuolistamiseksi ja turvallisuusnormien edistämiseksi, jotta ydinenergiainfrastruktuurin kestokyky paranee.

4.1.2. Liikenteen ja toimitusketjujen turvallisuus

Liikenne on keskeisen tärkeää unionin toiminnalle. Liikenneinfrastruktuuriin (esimerkiksi lentoasemille, maantieinfrastruktuuriin, satamiin ja rautateille) kohdistuvilla hybridi-iskuilla voi olla vakavat seuraukset, jotka johtavat matkailun ja toimitusketjujen häiriöihin. Pannessaan ilmailun ja meriliikenteen turvallisuutta koskevaa lainsäädäntöä[21] täytäntöön komissio tekee säännöllisiä tarkastuksia[22] ja pyrkii puuttumaan esiin tuleviin hybridiuhkiin maantieliikenteen turvallisuutta koskevilla toimillaan. EU:n kehyksestä

[18] Edistyminen toistaiseksi, ks. energiaunionin tilaa koskeva katsaus 2015, COM(2015) 572 final.

[19] Neuvoston direktiivi 2009/71/Euratom, annettu 25 päivänä kesäkuuta 2009, ydinlaitosten ydinturvallisuutta koskevan yhteisön kehyksen perustamisesta, sellaisena kuin se on muutettuna 8 päivänä heinäkuuta 2014 annetulla neuvoston direktiivillä 2014/87/Euratom.

[20] Neuvoston direktiivi 2013/59/Euratom, annettu 5 päivänä joulukuuta 2013, turvallisuutta koskevien perusnormien vahvistamisesta ionisoivasta säteilystä aiheutuvilta vaaroilta suojelemiseksi ja direktiivien 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom ja 2003/122/Euratom kumoamisesta.

[21] Euroopan parlamentin ja neuvoston asetus (EY) N:o 300/2008, annettu 11 päivänä maaliskuuta 2008, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta; komission täytäntöönpanoasetus (EU) 2015/1998, annettu 5 päivänä marraskuuta 2015, yksityiskohtaisista toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi; Euroopan parlamentin ja neuvoston direktiivi 2005/65/EY, annettu 26 päivänä lokakuuta 2005, satamien turvallisuuden parantamisesta; Euroopan parlamentin ja neuvoston asetus (EY) N:o 725/2004, annettu 31 päivänä maaliskuuta 2004, alusten ja satamarakenteiden turvatoimien parantamisesta.

[22] Komission on EU:n lainsäädännön mukaan tehtävä tarkastuksia sen varmistamiseksi, että jäsenvaltiot panevat ilmailun ja meriliikenteen turvallisuutta koskevia vaatimuksia täytäntöön oikein. Tämä merkitsee asianomaisen viranomaisen tarkastuksia jäsenvaltioissa sekä lentoasemien, satamien, lentoyhtiöiden, laivojen ja turvatoimia toteuttavien tahojen tarkastuksia. Komission tarkastuksilla pyritään varmistamaan, että jäsenvaltiot panevat EU:n normit täysimääräisesti täytäntöön.

keskustellaan muutetun lentoturvallisuusasetuksen[23] nojalla osana Euroopan ilmailustrategiaa[24]. Lisäksi Euroopan unionin merellisessä turvallisuusstrategiassa ja siihen liittyvässä toimintasuunnitelmassa[25] käsitellään merelliseen turvallisuuteen kohdistuvia uhkia. Sen ansiosta EU ja sen jäsenvaltiot voivat puuttua merelliseen turvallisuuteen kohdistuviin uhkiin, myös hybridiuhkien torjuntaan, kattavasti siviili- ja sotilastoimijoiden monialaisen yhteistyön kautta, jotta voidaan suojella kriittistä meri-infrastruktuuria, maailmanlaajuista toimitusketjua, kauppamerenkulkua ja merten luonnon- ja energiavaroja. Kansainvälisen toimitusketjun turvallisuutta käsitellään myös tullialan riskienhallintaa koskevassa EU:n strategiassa ja toimintasuunnitelmassa[26].

Toimi 7: Komissio seuraa liikennealalla esiin tulevia uhkia ja päivittää lainsäädäntöä tarvittaessa. Pannessaan täytäntöön Euroopan unionin merellistä turvallisuusstrategiaa ja tullialan riskienhallintaa koskevaa EU:n strategiaa ja toimintasuunnitelmaa komissio ja korkea edustaja tarkastelevat (osana omaa toimivaltaansa) koordinoidusti jäsenvaltioiden kanssa, miten vastata hybridiuhkiin ja erityisesti kriittistä liikenneinfrastruktuuria koskeviin uhkiin.

4.1.3. Avaruus

Avaruusinfrastruktuuri voi olla hybridiuhkien kohteena, millä on vaikutuksia moneen alaan. EU on laatinut avaruusesineiden valvonnan ja seurannan tukikehyksen[27], jotta jäsenvaltioiden omistuksessa oleva avaruusinfrastruktuuri voidaan verkostoida. Tarkoituksena on tarjota avaruusvalvonta- ja -seurantapalveluja[28] tietyille käyttäjille (jäsenvaltiot, EU:n toimielimet, avaruusalusten omistajat ja operoijat ja pelastuspalveluviranomaiset). Komissio tarkastelee tulevan Euroopan avaruusstrategian yhteydessä sen kehittämistä edelleen avaruusinfrastruktuuriin kohdistuvien hybridiuhkien valvomiseksi.

Satelliittiviestintä on keskeisessä asemassa kriisinhallinnassa, katastrofiavun antamisessa, poliisin työssä ja raja- ja rannikkovartioinnissa. Se on suurten infrastruktuurien, kuten liikenteen, avaruusinfrastruktuurin ja kauko-ohjattujen ilma-alusten käytön kokonaisjärjestelmien, selkäranka. Eurooppa-neuvosto on kehottanut valmistelemaan valtiollisen satelliittiviestinnän seuraavaa sukupolvea. Tämän vuoksi komissio arvioi Euroopan avaruusstrategian ja Euroopan puolustusalan toimintasuunnitelman yhteydessä yhteistyössä Euroopan puolustusviraston kanssa keinoja keskittää kysyntää.

---

[23] Komission asetus (EU) 2016/4, annettu 5 päivänä tammikuuta 2016, Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008 muuttamisesta keskeisten ympäristönsuojeluvaatimusten osalta; asetus (EY) N:o 216/2008, annettu 20 päivänä helmikuuta 2008, yhteisistä siviili-ilmailua koskevista säännöistä.

[24] Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Ilmailustrategia Euroopalle, COM(2015) 598 final, 7.12.2015.

[25] Komissio hyväksyi joulukuussa 2014 toimintasuunnitelman Euroopan unionin merellisen turvallisuusstrategian toteuttamiseksi; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

[26] Komission tiedonanto Euroopan parlamentille, neuvostolle ja Euroopan talous- ja sosiaalikomitealle tullialan riskienhallintaa koskevasta strategiasta ja toimintasuunnitelmasta: Riskien torjunta, toimitusketjun turvallisuuden vahvistaminen ja kaupan helpottaminen, COM(2014) 527 final.

[27] Ks. Euroopan parlamentin ja neuvoston päätös 541/2014/EU.

[28] Esimerkiksi varoitukset kiertoradalla tapahtuvien törmäysten estämiseksi, varoitukset rikkoutumisista tai törmäyksistä sekä avaruusesineiden riskialttiista palaamisesta maan ilmakehään.

Monet kriittiset infrastruktuurit ovat riippuvaisia tarkoista aikatiedoista verkkojen (esimerkiksi energia ja televiestintä) tai kaupanteon aikaleimojen (esim. rahoitusmarkkinat) synkronoimiseksi. Riippuvuus yhdestä maailmanlaajuisen satelliittinavigointijärjestelmän aikasynkronointisignaalista ei riitä varmistamaan hybridiuhkien torjuntaan tarvittavaa kestokykyä. Toinen luotettava aikalähde voisi olla eurooppalainen maailmanlaajuinen satelliittinavigointijärjestelmä Galileo.

Toimi 8: Komissio ehdottaa tulevien Euroopan avaruusstrategian ja Euroopan puolustusalan toimintasuunnitelman yhteydessä, että avaruusinfrastruktuurin kestokykyä hybridiuhkia vastaan parannetaan erityisesti laajentamalla mahdollisesti avaruusesineiden valvontaa ja seurantaa koskemaan myös hybridiuhkia, valmistelemalla valtiollisen satelliittiviestinnän seuraavaa sukupolvea Euroopan tasolla ja ottamalla Galileo käyttöön sellaisessa kriittisessä infrastruktuurissa, joka on riippuvainen aikasynkronoinnista.

4.2. Puolustusvoimavarat

Puolustusvoimavaroja on lisättävä, jotta voidaan parantaa EU:n kestokykyä hybridiuhkia vastaan. On tärkeää määritellä keskeiset voimavaroja parantavat alat, esimerkiksi seuranta- ja tunnistamisvalmiudet. Euroopan puolustusvirasto voisi toimia hybridiuhkiin liittyvän sotilaallisen valmiuden kehittämisen moottorina (esim. lyhentämällä puolustusvoimavarojen kehittämissykliä, investoimalla teknologiaan, järjestelmiin ja prototyyppeihin, avaamalla puolustusliiketoiminnan innovatiiviselle kaupalliselle teknologialle). Mahdollisia toimia voitaisiin tarkastella tulevan Euroopan puolustusalan toimintasuunnitelman yhteydessä.

Toimi 9: Korkea edustaja ehdottaa tarvittaessa jäsenvaltioiden tuella ja yhdessä komission kanssa hankkeita, joilla selvitetään, miten puolustusvoimavaroja voitaisiin mukauttaa ja EU:n kannalta merkityksellisiä seikkoja kehittää erityisesti yhtä tai useampaa jäsenvaltiota koskevien hybridiuhkien torjumiseksi.

4.3. Kansanterveyden ja elintarviketurvan suojaaminen

Väestön terveys voi joutua vaaraan, jos tartuntatauteja manipuloidaan tai elintarvikkeita, maaperää, ilmaa ja juomavettä saastutetaan kemiallisilla, biologisilla, säteily- ja ydintekijöillä (CBRN). Lisäksi eläin- tai kasvitautien tahallinen levittäminen voi haitata vakavasti unionin elintarviketurvaa, ja sillä voi olla merkittäviä taloudellisia ja yhteiskunnallisia vaikutuksia EU:n elintarvikeketjun tärkeimmillä alueilla. Tällaisiin hybridiuhkiin vastaamiseen voidaan käyttää EU:n olemassa olevia terveysturvallisuus-, ympäristönsuojelu- ja elintarviketurvarakenteita.

Rajatylittäviä terveysuhkia koskevan EU:n lainsäädännön[29] nojalla nykyisillä mekanismeilla koordinoidaan valmiutta valtioiden rajat ylittävien vakavien terveysuhkien

[29] Euroopan parlamentin ja neuvoston päätös N:o 1082/2013/EU, annettu 22 päivänä lokakuuta 2013, valtioiden rajat ylittävistä vakavista terveysuhkista ja päätöksen N:o 2119/98/EY kumoamisesta, EUVL L 293, 5.11.2013, s. 1.

varalta. Jäsenvaltiot, EU:n virastot ja tiedekomiteat[30] ovat toisiinsa yhteydessä varhaisvaroitus- ja reagointijärjestelmän kautta. Terveysturvakomitea, joka koordinoi jäsenvaltioiden vastauksia uhkiin, voi toimia yhteystahona kansanterveyden haavoittuvuustekijöiden suhteen[31] sekä sisällyttää hybridiuhat (erityisesti bioterrorismin) kriisiviestintää koskeviin suuntaviivoihin ja valmiuksien kehittämistä koskeviin harjoituksiin (kriisisimulaatioihin) jäsenvaltioiden kanssa. Elintarviketurvan alalla toimivaltaiset viranomaiset vaihtavat elintarvikkeita ja rehuja koskevan nopean hälytysjärjestelmän (RASFF) ja tullialan riskienhallintajärjestelmän (CRMS) kautta riskianalyysitietoja saastuneiden elintarvikkeiden aiheuttamien terveysriskien valvomiseksi. Eläinten ja kasvien terveyden osalta EU:n säädöskehyksen[32] tarkistamisen avulla voidaan lisätä uusia keinoja olemassa olevaan valikoimaan[33], jotta myös hybridiuhkiin voidaan varautua paremmin.

<u>Toimi 10</u>: Komissio lisää yhteistyössä jäsenvaltioiden kanssa tietoisuutta hybridiuhista ja parantaa kestokykyä niitä vastaan olemassa olevien valmius- ja koordinointimekanismien puitteissa erityisesti terveysturvakomiteassa.

4.4. Kyberturvallisuus

EU hyötyy paljon siitä, että yhteiskunta on yhdistetty verkkoihin ja digitoitu. Hybridiuhkien toteuttajat voivat kuitenkin tehdä kyberhyökkäyksiä, joilla häiritään digitaalipalveluja eri puolilla EU:ta. Viestintä- ja tiedotusjärjestelmien kestokyvyn parantaminen Euroopassa on tärkeää digitaalisten sisämarkkinoiden tukemiseksi. Euroopan unionin kyberturvallisuusstrategiassa ja Euroopan turvallisuusagendassa esitetään strateginen kokonaiskehys kyberturvallisuutta ja -rikollisuutta koskeville EU:n aloitteille. EU on toiminut aktiivisesti lisätäkseen tietoisuutta ja kehittääkseen yhteistyömekanismeja ja toimia kyberturvallisuusstrategian mukaisesti. Erityisesti ehdotetulla verkko- ja tietoturvadirektiivillä[34] puututaan monien olennaisten palveluntarjoajien kyberturvallisuusriskeihin energian, liikenteen, rahoituksen ja terveydenhuollon aloilla. Näiden samoin kuin tärkeimpien digitaalipalveluiden (esim. pilvipalvelujen) tarjoajien olisi toteutettava asianmukaiset turvallisuustoimenpiteet ja raportoitava kansallisille viranomaisille vakavista vaaratilanteista ja niiden mahdollisista hybriditekijöistä. Kun lainsäätäjät antavat direktiivin ja jäsenvaltiot saattavat sen

[30] Komission päätös C(2015) 5383, annettu 7 päivänä elokuuta 2015, kansanterveyden, kuluttajien turvallisuuden ja ympäristön alan tiedekomiteoiden perustamisesta.

[31] Euroopan parlamentin ja neuvoston päätös N:o 1082/2013/EU, annettu 22 päivänä lokakuuta 2013, valtioiden rajat ylittävistä vakavista terveysuhkista ja päätöksen N:o 2119/98/EY kumoamisesta , EUVL L 293, 5.11.2013, s. 1.

[32] Euroopan parlamentin ja neuvoston asetus (EU) 2016/429, annettu 9 päivänä maaliskuuta 2016, tarttuvista eläintaudeista sekä tiettyjen eläinterveyttä koskevien säädösten muuttamisesta ja kumoamisesta (”eläinterveyssäännöstö”), EUVL L 84, 31.3.2016. Euroopan parlamentti ja neuvosto pääsivät 16. joulukuuta 2015 poliittiseen yhteisymmärrykseen Euroopan parlamentin ja neuvoston asetuksesta kasvintuhoojien vastaisista suojatoimenpiteistä (kasvien terveyttä koskeva asetus).

[33] Esim. EU:n rokotepankit, pitkälle kehitetty eläintautien tietojärjestelmä, tiukemmat vaatimukset laboratorioiden ja muiden taudinaiheuttajia käsittelevien tahojen toimenpiteille.

[34] Komission ehdotus: Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa, COM(2013) 48 final, 7.2.2013. Neuvosto ja Euroopan parlamentti ovat saavuttaneet ehdotetusta direktiivistä poliittisen yhteisymmärryksen, ja se hyväksyttäneen virallisesti piakkoin.

tehokkaasti osaksi lainsäädäntöään ja panevat sen täytäntöön, se edistää kyberturvallisuusvalmiuksia kaikissa jäsenvaltioissa, sillä sen nojalla alan yhteistyötä lujitetaan hybridiuhkien torjuntaa koskevalla tietojenvaihdolla ja parhailla käytänteillä. Erityisesti direktiivillä perustetaan 28 kansallisen CSIRT-toimijan (tietotekniikan kriisiryhmät) ja CERT-EU-ryhmän[35] verkosto, joka toteuttaa vapaaehtoista operationaalista yhteistyötä.

Edistääkseen julkisen ja yksityisen sektorin yhteistyötä ja kyberturvallisuuden EU:n laajuista lähestymistapaa komissio perusti verkko- ja tietoturvafoorumin, joka ohjaa riskienhallinnan parhaita käytänteitä. Jäsenvaltiot määrittelevät turvallisuusvaatimukset ja kansallisista turvapoikkeamista ilmoittamista koskevat säännöt, mutta komissio kannustaa lähentämään riskienhallinnan lähestymistapoja hyödyntäen erityisesti Euroopan verkko- ja tietoturvavirastoa (ENISA).

<u>Toimi 11</u>: Komissio kehottaa jäsenvaltioita perustamaan ensi tilassa 28 kansallisen CSIRT-toimijan ja CERT-EU-ryhmän verkoston ja käyttämään sitä täysimääräisesti sekä laatimaan strategisen yhteistyön kehyksen. Komission olisi varmistettava koordinoidusti jäsenvaltioiden kanssa, että alakohtaiset kyberuhkia koskevat aloitteet (esim. ilmailun, energian, merenkäynnin aloilla) vastaavat verkko- ja tietoturvadirektiivin monialaista kapasiteettia, jotta tiedotus, asiantuntemus ja nopea reagointi voidaan koota yhteen.

4.4.1. Toimiala

Pilvipalveluista ja massadatasta ollaan koko ajan riippuvaisempia, mikä on lisännyt haavoittuvuutta hybridiuhkien suhteen. Digitaalisten sisämarkkinoiden strategiassa otetaan käyttöön kyberturvallisuutta koskeva julkisen ja yksityisen sektorin sopimusperusteinen kumppanuus[36], jossa keskitytään tutkimukseen ja innovointiin. Näin unioni saa hyvät teknologiset valmiudet alalla. Kumppanuuden avulla rakennetaan luottamusta eri markkinatoimijoiden kesken ja kehitetään synergiaa kysyntä- ja tarjontapuolen välille. Julkisen ja yksityisen sektorin sopimusperusteinen kumppanuus ja siihen liittyvät toimenpiteet painottuvat pääasiassa siviilipuolen kyberturvallisuustuotteisiin ja -palveluihin, mutta näiden aloitteiden ansiosta teknologian käyttäjät saavat paremman suojan myös hybridiuhilta.

<u>Toimi 12</u>: Komissio työskentelee koordinoidusti jäsenvaltioiden kanssa yhdessä toimialan kanssa kyberturvallisuutta koskevan julkisen ja yksityisen sektorin sopimusperusteisen kumppanuuden puitteissa teknologian kehittämiseksi ja testaamiseksi, jotta käyttäjiä ja infrastruktuuria voitaisiin suojata paremmin hybridiuhkiin liittyviltä kyberturvallisuusongelmilta.

[35] EU:n toimielinten tietotekniikan kriisiryhmä.
[36] Aloitetaan vuoden 2016 puolivälissä.

4.4.2. Energia

Älykotien ja -laitteiden yleistyminen, älykkäiden energiaverkkojen kehittäminen ja energiajärjestelmän digitalisoituminen myös altistavat kyberhyökkäyksille. Euroopan energiavarmuusstrategialla[37] ja energiaunionistrategialla[38] tuetaan kaikki vaaratilanteet kattavaa lähestymistapaa, johon on sisällytetty kestokyky hybridiuhkien suhteen. Kriittisen energiainfrastruktuurin suojelun teemaverkosto edistää energiasektorin (öljy, kaasu, sähkö) toimijoiden yhteistyötä. Komissio on perustanut verkkopohjaisen foorumin[39] uhkia ja turvapoikkeamia koskevan tiedon analysointia ja jakamista varten. Se on haavoittuvuuden vähentämiseksi myös kehittämässä yhdessä sidosryhmien[40] edustajien kanssa älykkään verkon toiminnan kyberturvallisuutta koskevaa kattavaa energia-alan strategiaa. Sähkömarkkinat ovat yhä yhdennetymmät, mutta kriisitilanteiden hoitamista koskevat säännöt ja menettelyt ovat yhä kansallisia. Meidän on varmistettava, että hallitukset tekevät yhteistyötä valmistautuessaan kriiseihin ja estäessään ja lieventäessään niitä. Kaikkien keskeisten toimijoiden on myös noudatettava yhteisiä sääntöjä.

<u>Toimi 13</u>: Komissio antaa älykkäiden verkkojen omistajille ohjeistusta laitteistojen kyberturvallisuuden parantamisesta. Se tarkastelee sähkömarkkinoiden uutta markkinarakennetta koskevan aloitteen puitteissa mahdollisuutta laatia riskeihin varautumista koskevia suunnitelmia ja menettelysäännöt, jotka koskevat tietojenvaihtoa ja joiden avulla varmistetaan jäsenvaltioiden keskinäinen solidaarisuus kriisiaikoina. Tämä koskee myös kyberhyökkäysten estämistä ja niiden vaikutusten lieventämistä.

4.4.3. Vakaat rahoitusjärjestelmät

EU:n talous edellyttää toimivaa ja turvallista rahoitus- ja maksujärjestelmää. On hyvin tärkeää, että rahoitusjärjestelmää ja siihen liittyvää infrastruktuuria suojataan kyberiskuilta riippumatta hyökkääjän motiiveista ja luonteesta. Jotta voitaisiin varautua EU:n rahoituspalveluihin kohdistuviin hybridiuhkiin, toimialalla on ymmärrettävä uhka, testattava puolustuskeinoja ja hankittava tarvittava teknologia hyökkäykseltä suojautumiseksi. Uhkia koskeva tietojenvaihto rahoitusmarkkinoiden toimijoiden kesken ja asianomaisten viranomaisten, tärkeimpien palvelujentarjoajien tai asiakkaiden kanssa on keskeisen tärkeää, mutta sen on myös oltava turvallista ja tietoturvavaatimusten mukaista. Komissio pyrkii yksilöimään kansainvälisillä foorumeilla tehdyn, myös G7:n, työn mukaisesti seikat, jotka haittaavat asianmukaista uhkia koskevaa tietojenvaihtoa, ja ehdottamaan ratkaisuja. On tärkeää varmistaa käytänteiden säännöllinen testaaminen ja hiominen, jotta yrityksiä ja alan infrastruktuuria voidaan suojata. Esimerkiksi turvallisuutta lisäävää teknologiaa on päivitettävä jatkuvasti.

[37] Komission tiedonanto Euroopan parlamentille ja neuvostolle: Euroopan energiavarmuusstrategia, COM(2014) 330 final.
[38] Joustavaa energiaunionia ja tulevaisuuteen suuntautuvaa ilmastonmuutospolitiikkaa koskeva puitestrategia, COM(2015) 80 final.
[39] EU:n häiriö- ja uhkatietokeskus (ITIS-EUC).
[40] Energy Expert CyberSecurity Platform (EECSP).

<u>Toimi 14</u>: Komissio edistää yhteistyössä ENISAn[41], jäsenvaltioiden ja alan kansainvälisten, eurooppalaisten ja kansallisten viranomaisten sekä rahoituslaitosten kanssa uhkia koskevan tietojenvaihdon foorumeja ja verkostoja ja helpottaa niiden toimintaa. Lisäksi se puuttuu seikkoihin, jotka haittaavat tällaisen tiedon vaihtamista.

4.4.4. Liikenne

Nykyaikaiset liikennejärjestelmät (rautateillä, maanteillä, lentoliikenteessä ja merillä) perustuvat tietojärjestelmiin, jotka ovat alttiina kyberhyökkäyksille. Koska liikenteellä on rajatylittävä ulottuvuus, EU:lla on erityinen rooli. Komissio jatkaa koordinoidusti jäsenvaltioiden kanssa kyberuhkien ja liikennejärjestelmien laittomaan häirintään liittyvien riskien analysoimista. Komissio on laatimassa ilmailun kyberturvallisuuden etenemissuunnitelmaa yhteistyössä Euroopan lentoturvallisuusviraston (EASA)[42] kanssa. Merelliseen turvallisuuteen kohdistuvia kyberuhkia käsitellään Euroopan unionin merellisessä turvallisuusstrategiassa ja siihen liittyvässä toimintasuunnitelmassa.

<u>Toimi 15</u>: Komissio ja korkea edustaja tarkastelevat osana omaa toimivaltaansa koordinoidusti jäsenvaltioiden kanssa, miten vastata hybridiuhkiin ja erityisesti liikennealan kyberhyökkäyksiä koskeviin uhkiin.

4.5. Hybridiuhkiin liittyvä rahoitus

Hybridiuhkien toteuttajat tarvitsevat rahoitusta toimintansa ylläpitämiseen. Rahoitusta käytetään terroristiryhmien tukemiseen tai hienovaraisempiin epävakautta aiheuttaviin toimiin, kuten painostusryhmien tai äärilaitojen poliittisten puolueiden tukemiseen. EU vauhditti Euroopan turvallisuusagendassa vahvistettuja rikosten ja terrorismin rahoituksen torjuntatoimia erityisesti toimintasuunnitelman[43] avulla. Uudistetulla rahanpesun vastaisella kehyksellä lujitetaan terrorismin rahoituksen ja rahanpesun torjuntaa, helpotetaan kansallisten rahanpesun selvittelykeskusten työtä epäilyttävien rahansiirtojen ja tietojenvaihdon havaitsemiseksi ja seuraamiseksi ja varmistetaan varainsiirtojen jäljitettävyys Euroopan unionissa. Sen avulla voitaisiin siis myös torjua hybridiuhkia. Myös YUTP-välineiden suhteen voitaisiin tarkastella räätälöityjä ja tehokkaita rajoittavia toimenpiteitä hybridiuhkien torjumiseksi.

<u>Toimi 16</u>: Komissio käyttää terrorismin rahoituksen torjuntaa koskevaa EU:n toimintasuunnitelmaa myös hybridiuhkien torjumiseen.

---

[41] Euroopan verkko- ja tietoturvavirasto.

[42] Komissio esitti joulukuussa 2015 ehdotuksen uudeksi EASA-asetukseksi, josta Euroopan parlamentti ja neuvosto keskustelevat parhaillaan. Ehdotus: Euroopan parlamentin ja neuvoston asetus yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan lentoturvallisuusviraston perustamisesta sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008 kumoamisesta, COM(2015) 613 final, 2015/0277 (COD).

[43] Komission tiedonanto Euroopan parlamentille ja neuvostolle: Toimintasuunnitelma terrorismin rahoituksen torjunnan vahvistamiseksi, COM(2016) 50 final.

4.6. Kestokyvyn lisääminen radikalisoitumista ja väkivaltaisia ääriliikkeitä vastaan

Vaikka terroriteot ja väkivaltaiset ääriliikkeet eivät sinänsä olekaan hybridinluonteisia, hybridiuhkien toteuttajat voivat ottaa yhteyttä haavoittuvassa asemassa oleviin yhteiskunnan jäseniin ja pyrkiä rekrytoimaan ja radikalisoimaan näitä nykyaikaisten viestintäkanavien (esimerkiksi internetin, sosiaalisen median ja sijaisryhmien) ja propagandan avulla.

Komissio analysoi uusien toimenpiteiden tarvetta torjuakseen ääriliikkeisiin liittyvää internetsisältöä osana digitaalisten sisämarkkinoiden strategiaa ja ottaa tässä huomioon niiden vaikutuksen ilmaisun- ja tiedonvapauden perusoikeuksiin. Toimenpiteisiin voisi kuulua laittoman sisällön tarkka poistaminen varoen, ettei laillista sisältöä poisteta (”notice and action”). Välikäsiltä olisi edellytettävä suurempaa vastuuta ja huolellisuutta verkkojen ja järjestelmien hallinnassa. Näin voitaisiin täydentää nykyistä vapaaehtoisuuteen perustuvaa lähestymistapaa, jossa internetyritykset ja sosiaalisen median yritykset poistavat terroristipropagandan nopeasti (erityisesti EU:n internetfoorumin puitteissa) yhteistyössä EU:n internetsisällöstä ilmoittamista käsittelevän Europolin yksikön kanssa.

Radikalisoitumista torjutaan osana Euroopan turvallisuusagendaa vaihtamalla kokemuksia ja kehittämällä parhaita käytänteitä esimerkiksi yhteistyössä EU:n ulkopuolisten maiden kanssa. Strategisen Syyria-viestinnän neuvoa-antavan ryhmän tavoitteena on tehostaa vaihtoehtoisen viestin laatimista ja jakamista terrorismipropagandan torjumiseksi. Radikalisoitumisen torjunnan verkosto tukee jäsenvaltioita ja tahoja, joiden on oltava yhteydessä radikalisoituneiden henkilöiden (esimerkiksi ulkomaisten terroristitaistelijoiden) tai radikalisoitumiselle alttiiksi katsottujen henkilöiden kanssa. Radikalisoitumisen torjunnan verkosto tarjoaa koulutusta ja opastusta. Se antaa myös tukea ensisijaisille kolmansille maille, jos niissä on halua sitoutua tähän toimintaan. Lisäksi komissio edistää oikeudellista yhteistyötä rikosoikeuden alalla esimerkiksi Eurojustin puitteissa terrorismin ja radikalisoitumisen torjumiseksi kaikissa jäsenvaltioissa. Tähän sisältyvät myös ulkomaisia terroristitaistelijoita ja palaavia vierastaistelijoita koskevat toimet.

EU edistää väkivaltaisten ääriliikkeiden torjuntaa täydentämällä edellä mainittuja lähestymistapoja **ulkoisissa toimissaan** esimerkiksi ulkoisella yhteistyöllä ja tiedotuksella, ennaltaehkäisyllä (radikalisoitumisen ja terrorismin rahoituksen torjunnalla) sekä puuttumalla taustalla oleviin taloudellisiin, poliittisiin ja yhteiskunnallisiin tekijöihin, jotka tarjoavat terrorismiryhmittymille mahdollisuuden menestyä.

<u>Toimi 17:</u> Komissio toteuttaa Euroopan turvallisuusagendassa vahvistettuja toimia radikalisoitumisen torjumiseksi ja analysoi tarvetta tehostaa menettelyjä laittoman sisällön poistamiseksi vetoamalla välikäsien vastuuseen verkkojen ja järjestelmien hallinnoinnissa.

4.7. Lisääntyvä yhteistyö EU:n ulkopuolisten maiden kanssa

Kuten Euroopan turvallisuusagendassa korostetaan, EU on keskittynyt aiempaa enemmän turvallisuusalan valmiuksien kehittämiseen ***kumppanimaissa***. Perustana on muun muassa turvallisuuden ja kehityksen välinen yhteys ja tarkistetun Euroopan naapuruuspolitiikan[44] turvallisuusulottuvuuden kehittäminen. Näillä toimilla voidaan myös parantaa kumppaneiden kestokykyä hybriditoimien suhteen.

Komissio aikoo lisätä edelleen operatiivisten ja strategisten tietojen vaihtoa laajentumismaiden kanssa sekä tarpeen mukaan itäisen kumppanuuden ja eteläisen naapurialueen maiden kanssa. Tietojenvaihdon avulla voidaan torjua järjestäytynyttä rikollisuutta, terrorismia, sääntöjenvastaista maahantuloa ja pienaseiden laitonta kauppaa. EU on myös vauhdittamassa terrorismin torjuntaa koskevaa yhteistyötään kolmansien maiden kanssa tehostettujen turvallisuusalan vuoropuhelujen ja toimintasuunnitelmien kautta.

EU:n ulkoisten rahoitusvälineiden avulla on tarkoitus perustaa EU:n ulkopuolisiin maihin toimivia ja luotettavia instituutioita[45], jotka ovat ennakkoedellytys tehokkaille toimille turvallisuusuhkiin vastattaessa ja kestokykyä lisättäessä. Tärkeimpiä keinoja ovat turvallisuusalan uudistaminen ja valmiuksien lisääminen turvallisuuden ja kehityksen tueksi.[46] Komissio on suunnitellut vakautta ja rauhaa edistävän välineen[47] osana toimia, joilla lisätään kyberuhkien sietokykyä ja kumppaneiden kykyä havaita kyberhyökkäyksiä ja -rikollisuutta ja reagoida niihin. Näin voidaan torjua hybridiuhkia EU:n ulkopuolisissa maissa. EU rahoittaa kumppanimaissa valmiuksia kehittävää toimintaa CBRN-kysymyksiin liittyvien turvallisuusriskien lieventämiseksi.[48]

Jäsenvaltiot voisivat auttaa kumppaneita parantamaan valmiuksiaan käyttämällä kriisinhallinnan kattavan lähestymistavan mukaisesti yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) välineitä ja operaatioita yhdistettyinä EU:n välineisiin tai niiden täydentämiseksi. Seuraavia toimia voitaisiin harkita: i) tuki strategiselle viestinnälle, ii) neuvonta ministeriöille, joihin kohdistuu suurin hybridiuhka ja iii) lisätuki rajavalvontaan hätätilanteissa. Lisäksi voitaisiin tarkastella synergiaa YTPP-

[44] Yhteinen tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Euroopan naapuruuspolitiikan tarkistus, 18.11.2015, JOIN(2015) 50 final.

[45] Sama kuin edellä; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Enlargement Strategy, 10.11.2015, COM(2015) 611 final (ei käännetty suomeksi); Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle: EU:n kehitysyhteistyöpolitiikan vaikutuksen lisääminen: muutossuunnitelma, 13.10.2011, COM(2011) 637 final.

[46] Yhteinen tiedonanto: Turvallisuuden ja kehityksen edistäminen valmiuksia kehittämällä – Euroopan unionin kumppanimaille lisää keinoja kriisien ehkäisyyn ja hallintaan, JOIN(2015) 17 final.

[47] Euroopan parlamentin ja neuvoston asetus (EU) N:o 230/2014, annettu 11 päivänä maaliskuuta 2014, vakautta ja rauhaa edistävän välineen perustamisesta, EUVL L 77, 15.3.2014, s. 1.

[48] Aloja ovat muun muassa rajavalvonta, kriisinhallinta, nopeat toimet, kaksikäyttötuotteiden laittoman vientikaupan valvonta, tautien seuranta ja valvonta, rikosoikeudellinen ydinmateriaalitutkimus, turvapoikkeamista selviytyminen ja suuririskisten laitosten suojelu. EU:n ulkopuolisille maille voidaan jakaa myös parhaat käytänteet, jotka on kehitetty EU:n CBRN-toimintasuunnitelman mukaisesti. Näitä ovat esimerkiksi ydinturvan eurooppalainen koulutuskeskus ja EU:n osallistuminen kansainväliseen rajavalvontatyöryhmään.

välineiden ja turvallisuus-, tulli- ja oikeusalan toimijoiden välillä. Näihin kuuluvat myös asianomaiset EU:n virastot[49], Interpol ja Euroopan santarmijoukot, kukin oman tehtävänantonsa mukaisesti.

<u>Toimi 18</u>: Korkea edustaja aloittaa koordinoidusti komission kanssa hybridiriskiselvityksen naapurialueilla.

Korkea edustaja, komissio ja jäsenvaltiot käyttävät saatavilla olevia välineitä kumppaneiden valmiuksien ja hybridiuhkia koskevan kestokyvyn parantamiseen. YTPP-operaatioita voidaan käyttää EU-välineistä riippumatta tai niiden täydentämiseksi kumppaneiden avustamiseen valmiuksien kehittämisessä.

5. KRIISIEN ENNALTAEHKÄISY, KRIISEIHIN REAGOIMINEN JA KRIISEISTÄ PALAUTUMINEN

Kuten 3.1 kohdassa todetaan, ehdotetun EU:n hybridianalyysikeskuksen on tarkoitus analysoida asiaa koskevia indikaattoreita, jotta hybridiuhkia voitaisiin estää ja niihin vastata ja EU:n päättäjiä voitaisiin informoida. Heikkouksia voidaan lieventää kansallisen ja EU:n tason pitkän aikavälin toimintalinjoilla, mutta lyhyellä aikavälillä on tärkeää parantaa jäsenvaltioiden ja unionin kykyä estää hybridiuhkia, reagoida niihin ja palautua niistä nopeasti ja koordinoidusti.

Hybridiuhkien aiheuttamiin tapahtumiin on keskeisen tärkeää vastata nopeasti. Eurooppalainen hätäavun koordinointikeskus[50] voisi helpottaa kansallisia pelastuspalvelutoimia ja -valmiuksia, mikä voisi olla tehokas mekanismi niiden hybridiuhkien osatekijöiden suhteen, jotka edellyttävät pelastuspalveluun liittyvää reagointia. Tämä voitaisiin toteuttaa koordinoidusti muiden EU:n reagointimekanismien ja ennakkovaroitusjärjestelmien kanssa: ulkoisen turvallisuusulottuvuuden osalta erityisesti EUH:n tilannekeskuksen kanssa ja sisäisen turvallisuusulottuvuuden osalta strategisten analyysien ja valmiustoimien keskuksen kanssa.

Yhteisvastuulausekkeen (Euroopan unionin toiminnasta tehdyn sopimuksen eli SEUT-sopimuksen 222 artikla) mukaan unioni voi toteuttaa toimia ja sen jäsenvaltiot voivat toteuttaa yhteisiä toimia, jos jäsenvaltio joutuu terrori-iskun taikka luonnon tai ihmisen aiheuttaman suuronnettomuuden kohteeksi. Unionin toimia jäsenvaltioiden avuksi toteutetaan soveltamalla neuvoston päätöstä 2014/415/EU[51]. Koordinointijärjestelyjen neuvostossa olisi perustuttava EU:n hätätila- ja kriisinkoordinointijärjestelyihin[52]. Komissio ja korkea edustaja yksilöivät näiden järjestelyjen puitteissa osana omaa toimivaltaansa asianmukaiset unionin välineet ja esittävät neuvostolle ehdotuksia poikkeuksellisia toimenpiteitä koskevien päätösten tekemiseksi.

[49] Europol, Frontex, Cepol ja Eurojust.
[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] Neuvoston päätös 2014/415/EU yhteisvastuulausekkeen täytäntöönpanojärjestelyistä unionissa, EUVL L 192, 1.7.2014, s. 53.
[52] http://www.consilium.europa.eu/fi/documents-publications/publications/2014/eu-ipcr/

SEUT-sopimuksen 222 artiklassa mainitaan myös tilanteet, jotka edellyttävät yhden tai useamman jäsenvaltion antamaa suoraa apua terrori-iskun tai luonnononnettomuuden kohteeksi joutuneelle jäsenvaltiolle. Tällöin neuvoston päätöstä 2014/415/EU ei sovelleta. Koska hybriditoiminnalla aiheutetaan epäselvyyttä, komission ja korkean edustajan olisi tarkasteltava osana omaa toimivaltaansa yhteisvastuulausekkeen mahdollista soveltamista viimeisenä keinona tilanteissa, joissa EU:n jäsenvaltio on merkittävien hybridiuhkien kohteena.

SEUT-sopimuksen 222 artiklasta poiketen, jos useat vakavat hybridiuhat muodostavat aseellisen hyökkäyksen EU:n jäsenvaltiota kohtaan, voidaan vedota SEU-sopimuksen 42 artiklan 7 kohtaan, jotta tilanteeseen voidaan vastata soveltuvalla tavalla ja oikea-aikaisesti. Hybridiuhkien laajamittainen ja vakava esiintulo saattaa edellyttää myös yhteistyön ja koordinoinnin lisäämistä Naton kanssa.

Jäsenvaltioita kehotetaan ottamaan joukkojaan valmistellessaan huomioon myös mahdolliset hybridiuhat. Jotta jäsenvaltiot kykenisivät tekemään hybridi-iskun aikana päätöksiä nopeasti ja tehokkaasti, niiden on pidettävä harjoituksia säännöllisesti niin käytännön kuin poliittisellakin tasolla kansallisen ja monikansallisen päätöksentekokyvyn testaamiseksi. Tavoitteena olisi laatia jäsenvaltioille, komissiolle ja korkealle edustajalle yhteiset operatiiviset käytänteet, joissa hahmotellaan menettely hybridiuhkatilannetta varten ensimmäisestä havainnosta hyökkäyksen loppuvaiheeseen ja joissa kartoitetaan kunkin unionin toimielimen ja toimijan rooli prosessissa.

Tämä on YTPP:n tärkeä osa. Siihen voisi kuulua a) siviilien ja sotilashenkilöiden koulutusta, b) mentorointi- ja neuvontakäyntejä uhan kohteena olevan valtion turvallisuus- ja puolustuskyvyn parantamiseksi, c) valmiussuunnitelmien laatiminen hybridiuhkien merkkien havaitsemiseksi ja varhaisvaroituskapasiteetin lisäämiseksi, d) rajavalvonnan tukeminen hätätilanteissa, e) tuki erityisaloilla, esimerkiksi CBRN-riskien lieventäminen ja siviilien evakuoiminen.

<u>Toimi 19</u>: Korkea edustaja ja komissio laativat koordinoidusti jäsenvaltioiden kanssa yhteiset operatiiviset käytänteet ja toteuttavat säännöllisesti harjoituksia, joilla parannetaan valmiuksia strategisten päätösten tekemiseen vastauksena monimuotoisiin hybridiuhkiin EU:n hätätila- ja kriisinkoordinointijärjestelyjen pohjalta.

<u>Toimi 20</u>: Komissio ja korkea edustaja tarkastelevat osana omaa toimivaltaansa SEUT-sopimuksen 222 artiklan ja SEU-sopimuksen 42 artiklan 7 kohdan soveltamista ja käytännön vaikutusta laajamittaisen ja vakavan hybridi-iskun tilanteessa.

<u>Toimi 21</u>: Korkea edustaja sisällyttää koordinoidusti komission kanssa sotilaalliset toimintavalmiudet osaksi hybridiuhkien torjuntaa ja käyttää ja koordinoi niitä osana yhteistä turvallisuus- ja puolustuspolitiikkaa.

6. YHTEISTYÖN LISÄÄMINEN NATON KANSSA

Hybridiuhat ovat haaste paitsi EU:lle, myös muille suurille kumppaniorganisaatioille, kuten Yhdistyneille kansakunnille, Euroopan turvallisuus- ja yhteistyöjärjestölle (Etyj) ja erityisesti Natolle. Tehokkaat toimet edellyttävät vuoropuhelua ja koordinointia organisaatioiden välillä sekä poliittisella että operatiivisella tasolla. EU:n ja Naton yhteistyön lähentäminen auttaisi molempia organisaatioita valmistautumaan ja vastaamaan hybridiuhkiin paremmin ja täydentämään ja tukemaan toistensa toimia osallistavuuden periaatteen pohjalta siten, että samalla kunnioitetaan molempien osapuolten päätöksenteon riippumattomuutta ja tietosuojasääntöjä.

Organisaatioilla on samat arvot ja samanlaiset haasteet. Sekä EU:n jäsenvaltiot että Nato-liittolaiset odottavat omien organisaatioidensa tukevan niitä nopeasti, päättäväisesti ja koordinoidusti kriisitilanteessa tai ihannetapauksessa jopa estävän kriisin toteutumisen. EU:n ja Naton läheisemmälle yhteistyölle ja koordinoinnille on yksilöity useita aloja, esimerkiksi tilannetietoisuus, strateginen viestintä, kyberturvallisuus sekä kriisien välttäminen ja niihin reagointi. EU ja Nato käyvät parhaillaan epävirallista vuoropuhelua hybridiuhista. Sitä olisi lisättävä, jotta niiden toiminta alalla voidaan synkronoida.

Jotta voitaisiin kehittää täydentäviä EU:n ja Naton yhteisiä toimia, on tärkeää, että molemmilla on sama tilannekuva ennen kriisiä ja sen aikana. Tämä voitaisiin toteuttaa analyysitietojen ja kokemusten säännöllisellä jakamisella sekä EU:n ja Naton hybridianalyysikeskusten suoralla yhteydellä. Samoin on tärkeää tuntea toisen osapuolen kriisinhallintamenettelyt nopeiden ja tehokkaiden toimien varmistamiseksi. Kestokykyä voitaisiin lisätä varmistamalla, että kriittisten infrastruktuurien vertailuarvot täydentävät toisiaan sekä tekemällä läheistä yhteistyötä strategisessa viestinnässä ja kyberpuolustuksessa. Yhteiset harjoitukset, joihin molemmat organisaatiot voivat osallistua täysimääräisesti sekä poliittisella että teknisellä tasolla, tehostaisivat kummankin osapuolen päätöksentekokykyä. Uusien koulutusmahdollisuuksien kartoittamisen avulla voitaisiin kehittää yhtenevä asiantuntemus kriittisillä aloilla.

<u>Toimi 22</u>: Korkea edustaja jatkaa koordinoidusti komission kanssa epävirallista vuoropuhelua Naton kanssa ja lisää yhteistyötä ja koordinointia sen kanssa tilannetietoisuuden, strategisen viestinnän, kyberturvallisuuden ja kriisien ehkäisyn ja niihin reagoinnin aloilla. Näin torjutaan hybridiuhkia ja samalla noudatetaan molempien organisaatioiden osallistamisen ja päätöksenteon riippumattomuuden periaatteita.

7. PÄÄTELMÄT

Tässä yhteisessä tiedonannossa esitetään toimia, joiden tarkoituksena on edistää hybridiuhkien torjuntaa sekä parantaa EU:n, jäsenvaltioiden ja kumppaneiden kestokykyä. Koska painopiste on **tietoisuuden lisäämisessä**, ehdotetaan erityisiä mekanismeja, joiden avulla voidaan vaihtaa tietoja jäsenvaltioiden kanssa ja koordinoida EU:n valmiuksia strategiseen viestintään. Lisäksi esitetään toimia **kestokyvyn parantamiseksi** esimerkiksi kyberturvallisuuden ja kriittisen infrastruktuurin aloilla, suojattaessa rahoitusjärjestelmää laittomalta käytöltä ja torjuttaessa väkivaltaisia

ääriliikkeitä ja radikalisoitumista. Kaikilla näillä aloilla ensimmäinen tärkeä askel on, että EU:n ja jäsenvaltioiden sopimat strategiat toteutetaan ja jäsenvaltiot panevat olemassa olevan lainsäädännön täysimääräisesti täytäntöön. Samaan aikaan näiden toimien tueksi toteutetaan joitakin konkreettisempia toimia.

Hybridiuhkien estämisen, niihin reagoimisen ja niistä palautumisen suhteen ehdotetaan, että yhteisvastuulausekkeen eli SEUT-sopimuksen 222 artiklan (sellaisena kuin se on määriteltynä asiaa koskevassa päätöksessä) ja SEU-sopimuksen 42 artiklan 7 kohdan soveltamista laajamittaisen ja vakavan hybridi-iskun tilanteessa tarkastellaan. Strategista päätöksentekokykyä voitaisiin parantaa laatimalla yhteiset operatiiviset käytänteet.

Lisäksi ehdotetaan, että **EU:n ja Naton välistä yhteistyötä ja koordinaatiota vauhditetaan** yhteisillä toimilla hybridiuhkien torjumiseksi.

Korkea edustaja ja komissio sitoutuvat käyttämään tämän yhteisen kehyksen täytäntöönpanon yhteydessä asianmukaisia EU:n välineitä, jotka niillä on käytössään. EU:lle on tärkeää yhdessä jäsenvaltioiden kanssa pyrkiä vähentämään riskejä, jotka liittyvät valtiollisten tai valtiosta riippumattomien toimijoiden esittämiin mahdollisiin hybridiuhkiin.