



Euroopan unionin  
neuvosto

Bryssel, 18. lokakuuta 2023  
(OR. en)

14372/23

|                 |                |
|-----------------|----------------|
| JAI 1332        | COPEN 363      |
| COSI 179        | FREMP 292      |
| ENFOPOL 431     | JAIEX 66       |
| ENFOCUSTOM 110  | CFSP/PESC 1410 |
| IXIM 194        | COPS 489       |
| CT 155          | HYBRID 73      |
| CRIMORG 137     | DISINFO 85     |
| FRONT 327       | TELECOM 306    |
| ASIM 92         | DIGIT 223      |
| VISA 208        | COMPET 1008    |
| CYBER 247       | RECH 456       |
| DATAPROTECT 278 | CULT 122       |
| CATS 58         | COTER 185      |
| DROIPEN 151     | CORDROGUE 94   |

#### SAATE

---

Lähtettäjä: Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine  
DEPREZ

Saapunut: 18. lokakuuta 2023

Vastaanottaja: Thérèse BLANCHET, Euroopan unionin neuvoston pääsihteeri

---

Kom:n asiak. nro: COM(2023) 665 final

---

Asia: KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA  
NEUVOSTOLLE EU:n turvallisuusunionistrategian täytäntöönpanoa  
koskeva kuudes edistymiskertomus

---

Valtuuskunnille toimitetaan oheisena asiakirja COM(2023) 665 final.

---

Liite: COM(2023) 665 final



Bryssel 18.10.2023  
COM(2023) 665 final

**KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE**

**EU:n turvallisuusunionistrategian täytäntöönpanoa koskeva kuudes edistymiskertomus**

## I. Johdanto

Komissio hyväksyi kolme vuotta sitten vuosien 2020–2025 turvallisuusunionistrategian<sup>1</sup>, jossa määritellään unionin tärkeimmät turvallisuutta koskevat painopisteet. Sittenkin olemme edistyneet hyvin strategian kaikkien neljän pilarin edistämässä – olemme antaneet käänteentekevää lainsäädäntöä kaikilla osa-alueilla kriittisten toimijoiden suojelusta aina kyberuhkien sietokyvyn parantamiseen. Samaan aikaan Euroopan ja naapurustomme turvallisuusuhkaympäristö kuitenkin kehittyi edelleen. Eräissä kouluissa Ranskassa ja Brysselin kaduilla viime päivinä tapahtuneet terrori-iskut ovat selkeä muistutus siitä, että turvallisuusarkkitehtuurimme mukauttamista ja vahvistamista on jatkettava kiireellisesti. Kyberhyökkäysten aiheuttama vaara kasvaa edelleen, ja sitä lisää myös se, että pahantahtoiset toimijat valitsevat puolensa käynnissä olevissa konflikteissa. Hybridiuhat, mukaan lukien disinformaatio, lisääntyvät edelleen. Europol on todennut, että Venäjän hyökkäyssota Ukrainaa vastaan on syynä EU:n kohteisiin kohdistuvien kyberhyökkäysten merkittävään lisääntymiseen, ja suurimmat hyökkäykset ovat poliittisesti motivoituja ja venäläismielisten hakkeriryhmien koordinoimia.<sup>2</sup> Tämä on ilmennyt internetyhteyksien estämisenä ja keskeisten palvelujen, kuten energiaverkkojen, keskeytyksinä.<sup>3</sup>

Turvallisuusunionistrategian tarkoituksena on antaa EU:lle valmiudet selviytyä paremmin muuttuvassa uhkaympäristössä. Pandemian ja sodan aiheuttamat kriisit ovat osoittaneet, että strategiassa omaksuttu lähestymistapa – pyrkimyksemme sovittaa yhteen koko EU:n turvallisuusekosysteemi ja siirtyä pois turvallisuuden kyberulottuvuuden ja fyysisen ulottuvuuden välisestä kapeasta ajattelusta, järjestäytyneen rikollisuuden ja terrorismin sekä radikalisoitumisen torjunta mukaan luettuna – on tärkeä.

On kuitenkin pysyttävä valppaana ja tutkittava jatkuvasti, mitä puutteita kansalaisten suojelemiseksi toteuttamissamme toimissa on. Strategiassa määritetään painopistealat, joilla unioni voi tuoda lisäarvoa tukemalla jäsenvaltioita kaikkien Euroopassa asuvien ihmisten turvallisuuden edistämässä. Sen hyväksymisen jälkeen kaikkia määritettyjä toimia on käsitelty ja uusia toimia on lisätty, jotta voidaan vastata jatkuviin turvallisuushaasteisiin.

Komissio on esittänyt turvallisuusunionistrategian puitteissa kaiken kaikkiaan 36 lainsäädäntöaloitetta. Yli puolesta näistä ehdotuksista on jo käyty toimielinten väliset neuvottelut, joiden myötä on annettu vankkaa uutta lainsäädäntöä, kuten liitteen taulukossa kuvataan. Euroopan parlamentti ja neuvosto neuvottelevat kuitenkin edelleen useista komission ehdottamista keskeisistä aloitteista. Nykyinen vaalikausi päättyy kesäkuussa 2024 pidettäviin Euroopan parlamentin vaaleihin, joten on toimittava nopeasti, jotta nämä ratkaisematta olevat asiat saadaan käsiteltyä ja kansalaiset voivat hyötyä kaikilta osin turvallisuusunionista. Tässä turvallisuusunionin kuudennessa edistymiskertomuksessa keskitytään sen vuoksi hahmottelemaan niitä keskeisiä komission hyväksymiä turvallisuusunionia koskevia lainsäädännöllisiä ja muita kuin lainsäädännöllisiä asiakirjoja, joiden viimeistelyyn ja tehokkaaseen täytäntöönpanoon on vielä keskityttävä.

---

<sup>1</sup> COM(2020) 605.

<sup>2</sup> Hajautetut palvelunestohyökkäykset (DDoS-hyökkäykset): ks. Europolin Spotlight-raportti ”Cyber-attacks: the apex of crime-as-a-service”, 13. syyskuuta 2023.

<sup>3</sup> Wiper-tyyppisiä haittaohjelmia on käytetty paljon Ukrainan konfliktin aikana tuhoamaan tietoja ja järjestelmiä, mikä on vaikuttanut esimerkiksi tuhansien tilaajien internetyhteyksiin EU:ssa sekä internetyhteyksiin eräissä suuressa saksalaisessa energiayrityksessä, joka menetti yli 5 800 tuuliturbiinin etävalvontayhteyden. ”The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict”, Euroopan parlamentin tutkimus, syyskuu 2023, PE 702.594.

Jo sovittujen EU:n säädösten hyödyt ilmenevät vasta, kun säädökset pannaan täytäntöön. Työssä on keskityttävä niiden asianmukaiseen ja täysimittaiseen saattamiseen osaksi kansallista lainsäädäntöä, täytäntöönpanoon ja soveltamiseen jäsenvaltioissa. Vuonna 2023 komissio on edelleen varmistanut EU:n turvallisuusunionistrategian täytäntöönpanon edistymisen käyttämällä institutionaalisia valtuuksiaan käynnistää rikkomusmenettelyjä aina, kun jäsenvaltiot eivät ole saattaneet EU:n lainsäädäntöä osaksi kansallista lainsäädäntöään tai kun ne ovat saattaneet sen osaksi kansallista lainsäädäntöään virheellisesti.

Tässä kertomuksessa esitetään myös yhteenveto niistä aiheista, joissa jäsenvaltioiden ja/tai EU:n virastojen toiminta on keskeisellä sijalla strategian toteuttamisessa. EU:n virastot ovat keskeisessä asemassa turvallisuusunionin aloitteiden täytäntöönpanon tukemisessa, ja niiden vastuut ovat kehittyneet viime vuosina. Kertomuksessa esitetään eräitä tärkeimpiä uusia tehtäviä, joita niille on osoitettu tehostetun tuen antamiseksi jäsenvaltioille turvallisuusunionin keskeisten aloitteiden täytäntöönpanossa.

Lisäksi geopoliittinen tilanne on korostanut ulkoisen turvallisuuden merkitystä sisäiselle turvallisuudellemme. EU:n vahvempi sisäinen turvallisuuskehys on kiinteässä yhteydessä vahvempiin kumppanuuksiin ja yhteistyöhön kolmansien maiden kanssa. EU:n on jatkossakin pyrittävä aktiivisesti selvittämään, miten maailmanlaajuinen sitoutuminen voi auttaa turvaamaan kansalaisten turvallisuuden EU:ssa.

## **II. Tulevaisuudenkestävä turvallisuusympäristö**

### ***Kriittisen infrastruktuurin kyberturvallisuus ja häiriönsietokyky***

Unioni on sitoutunut turvallisuusunionin puitteissa varmistamaan, että kaikkia Euroopan kansalaisia ja yrityksiä suojellaan asianmukaisesti niin verkossa kuin sen ulkopuolellakin, sekä edistämään avointa, turvallista ja vakaata kybertoimintaympäristöä. Kyberhäiriötilanteiden kasvava laajuus, esiintymistiheys ja vaikutus muodostavat merkittävän uhan verkko- ja tietojärjestelmien toiminnalle ja sisämarkkinoille. Venäjän Ukrainaa vastaan käymä hyökkäyssota on kasvattanut tätä uhkaa entisestään, ja tämänhetkisiä geopoliittisia jännitteitä pahentavat useiden valtiollisten ja rikollisten toimijoiden ja haktivistien toimet. Nord Stream -kaasuputkien viimeisyksyinen sabotaasi on korostanut keskeisten alojen, kuten energian, digitaalisen infrastruktuurin, liikenteen ja avaruusalan, riippuvaisuutta häiriönsietokykyisestä kriittisestä infrastruktuurista. Hiljattainen Viron ja Suomen väliseen merenalaiseen kaasuputkeen ja datakaapeliin liittyvä häiriötilanne osoittaa, että tällaisiin tilanteisiin on valmistauduttava hyvin. Vaikka vahinkojen syy on edelleen epäselvä ja tutkimukset jatkuvat, jäsenvaltioiden ja komission välinen tietojenvaihto eri tasoilla on ollut rohkaisevaa. Häiriöillä ei ollut välitöntä vaikutusta internetyhteyksiin eikä kaasun toimitusvarmuuteen Euroopan tasolla tai paikallisella tasolla. Tämä on osoitus viime kuukausien aikana saavutetusta edistyksestä ja tehostetuista valmiustoimista.

Selkeä ja vankka oikeudellinen kehys on sen vuoksi olennaisen tärkeä näiden kriittisten infrastruktuurien suojelun ja häiriönsietokyvyn varmistamiseksi. Tässä yhteydessä saavutettiin ratkaiseva läpimurto, kun samanaikaisesti hyväksyttiin tarkistettu direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa

(NIS 2 -direktiivi)<sup>4</sup> ja direktiivi kriittisten toimijoiden häiriönsietokyvystä<sup>5</sup>, jotka molemmat tulivat voimaan 16. tammikuuta 2023. Jäsenvaltioita kehoitetaan nyt saattamaan nämä keskeiset säädökset osaksi kansallista lainsäädäntöään nopeasti ja kaikilta osin viimeistään 17. lokakuuta 2024, jotta voidaan luoda vankka unionin kehys sen kriittisten infrastruktuurien suojaamiseksi fyysisiltä uhkilta ja kyberuhkilta.

Komissio vahvisti heinäkuussa 2023 komission delegoidussa asetuksessa keskeiset palvelut 11:llä kriittisten toimijoiden häiriönsietokykyä koskevan direktiivin soveltamisalaan kuuluvalla alalla.<sup>6</sup> Seuraavaksi jäsenvaltioiden on tehtävä näitä palveluja koskevat riskinarvioinnit. Neuvoston 8. joulukuuta 2022 antaman suosituksen<sup>7</sup> jälkeen työtä on tehostettu kriittisten infrastruktuurien stressitestien parissa, alkaen energia-alasta, ja yhteistyön vahvistamiseksi Naton ja keskeisten kumppanimaiden kanssa. Tämän työn tuloksena syntyi kesäkuussa 2023 kriittisen infrastruktuurin häiriönsietokykyä käsittelevän EU:n ja Naton työryhmän raportti, jossa kartoitettiin kriittisen infrastruktuurin nykyiset turvallisuushaasteet neljällä keskeisellä alalla (energia, liikenne, digitaalinen infrastruktuuri ja avaruus) ja annettiin suosituksia häiriönsietokyvyn parantamiseksi. EU:n ja Naton henkilöstöt panevat parhaillaan häiriönsietokykyä koskevan jäsennellyn vuoropuhelun yhteydessä täytäntöön suosituksia, jotka koskevat muun muassa koordinoinnin, tiedonvaihdon ja harjoitusten lisäämistä.

Samanaikaisesti komissio hyväksyi 6. syyskuuta 2023 ehdotuksen<sup>8</sup> neuvoston suositukseksi suunnitelmaksi koordinoitusta EU:n tason reagoinnista kriittisen infrastruktuurin häiriöihin, joilla on huomattavaa rajatylittävää merkitystä. Suunnitelmasta järjestettiin 4. lokakuuta 2023 skenaarioperusteisen keskustelun muodossa harjoitus, jonka tarkoituksena oli testata, miten sitä sovellettaisiin käytännössä, ja antaa tietoa neuvostossa parhaillaan käytäviin ehdotusta koskeviin neuvotteluihin.

Neuvoston kehotuksesta<sup>9</sup> komissio, korkea edustaja ja verkko- ja tietoturva-alan yhteistyöryhmä ovat tehneet riskinarviointeja ja laatineet riskiskenaarioita kyberturvallisuuden näkökulmasta. Tässä työssä keskitytään aluksi televiestintä- ja sähköalaan. Koska työhön osallistuvat kaikki asiaankuuluvat siviili- ja sotilasalan virastot ja verkostot, aikaan saadaan ensimmäistä kertaa kattava ja osallistava unionin laajuinen arviointi. Se täydentää edelleen kriittisiä toimitusketjuja koskevia koordinoituja turvallisuusriskinarviointeja, joita tehdään NIS 2 -direktiivin puitteissa, sekä kriittisten infrastruktuurien riskinarviointeja ja stressitestejä energian, digitaalisen viestintäinfrastruktuurin, liikenteen ja avaruuden aloilla. Koordinoinnin ja johdonmukaisuuden vuoksi näiden toimien olisi perustuttava toisiinsa vakiomuotoisen lähestymistavan luomiseksi ja niiden olisi ohjattava tulevien harjoitusten kehittämistä. Näiden toimien onnistuminen riippuu nyt jäsenvaltioiden aktiivisesta sitoutumisesta.

Talouksien ja yhteiskuntien toiminta on erityisesti turvallisuuden ja puolustuksen alalla yhä riippuvaisempi avaruuteen liittyvistä palveluista ja datasta. Avaruus on yhä kiistellympi

---

<sup>4</sup> Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi).

<sup>5</sup> Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta.

<sup>6</sup> C(2023) 4878.

<sup>7</sup> Neuvoston suositus, annettu 8 päivänä joulukuuta 2022, unionin koordinoitusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen.

<sup>8</sup> COM(2023) 526.

<sup>9</sup> Neuvoston päätelmät Euroopan unionin kyberturvallisuuden tason kehityksestä, 23. toukokuuta 2022, ja EU:n kyberturvallisuusvalmiuksien lujittamista koskeva Neversissä esitetty kehotus, 9. maaliskuuta 2022.

strateginen alue, ja sen merkitys turvallisuudelle on kasvanut erityisesti Venäjän hyökättyä Ukraina. Maaliskuussa 2023 hyväksyttiin turvallisuutta ja puolustusta tukeva EU:n avaruusstrategia, jonka tarkoituksena on vahvistaa EU:n strategista asemaa ja riippumattomuutta avaruudessa. Tämän strategian keskeisenä toimenä komissio ehdottaa vuonna 2024 EU:n avaruuslakia, jolla säännellään EU:n avaruustoiminnan turvallisuutta, kestävyyttä ja häiriönsietokykyä/vaarattomuutta.

Ulkoisen ulottuvuuden osalta voidaan todeta, että turvallinen infrastruktuuri tukee maailmantalouden ja toimitusketjujen häiriönsietokykyä, ja tästä syystä EU:n Global Gateway -strategiaan<sup>10</sup> sisältyy vahva turvallisuusulottuvuus. Kun otetaan huomioon EU:n ja kumppanimaiden infrastruktuurien väliset yhteydet, kansainvälisen yhteistyön lisääminen on välttämätöntä, jotta voidaan vahvistaa maailmanlaajuisista kyberuhkien sietokykyä ja tukea vapaata, avointa, turvallista ja varmaa kybertoimintaympäristöä.

### ***Kyberkestävyyssäädös***

Euroopan kyberturvallisuuden kannalta on keskeisen tärkeää, että kuluttajat ja yritykset voivat luottaa turvallisiin digitaalisiin tuotteisiin. Komissio on pyrkinyt vastaamaan tähän tarpeeseen 15. syyskuuta 2022 antamassaan ehdotuksessa<sup>11</sup> kyberkestävyyssäädökseksi. Sillä otettaisiin käyttöön pakolliset horisontaaliset kyberturvavaatimukset digitaalisia elementtejä sisältäville tuotteille viiden vuoden ajaksi tai niiden koko elinkaaren ajaksi (riippuen siitä, kumpi ajanjaksoista on lyhyempi). Sillä luotaisiin edellytykset digitaalisia elementtejä sisältävien turvallisten tuotteiden suunnittelulle ja kehittämiselle varmistamalla, että markkinoille saatetaan laitteisto- ja ohjelmistotuotteita, joissa on mahdollisimman vähän haavoittuvuuksia. Tämä olisi tärkeä virstanpylväs Euroopan kyberturvallisuusstandardien parantamisessa kaikilla aloilla, ja siitä tulisi todennäköisesti kansainvälinen vertailukohta, joka tarjoaisi unionin kyberturvallisuusteollisuudelle selkeitä etuja maailmanlaajuisilla markkinoilla. Euroopan parlamentti ja neuvosto vahvistivat omat kantansa heinäkuussa 2023, ja neuvottelujen pitäisi edetä ripeästi.

Kyberturvallisuuden sertifiointi auttaa myös merkittävästi lisäämään luottamusta tieto- ja viestintätekniisiä tuotteita ja palveluja kohtaan, sillä sen avulla kuluttajat, yritykset ja viranomaiset voivat tehdä tietoon perustuvia valintoja siten, että kyberturvallisuuden taso on asianmukainen. Kyberturvallisuuden sertifiointia koskeva työ etenee, ja EU:n yhteisiin kriteereihin perustuvaa kyberturvallisuuden sertifiointijärjestelmää arvioidaan komiteamenettelyssä. Euroopan unionin kyberturvallisuusvirasto (ENISA) valmistelee parhaillaan ehdolla olevaa EU:n pilvipalvelujen turvallisuuden sertifiointijärjestelmää (Cloud Security Certification Scheme, EUCS), ja siitä keskustellaan Euroopan kyberturvallisuuden sertifiointiryhmässä. Eri alojen asiantuntijoiden, kuluttajien ja palveluntarjoajien kanssa tehtävän tiiviin työn pitäisi johtaa vankkaan oikeudelliseen ja tekniseen lähestymistapaan, joka tarjoaa tarvittavat turvatakuut unionin lainsäädännön, kansainvälisten sitoumusten ja WTO-velvoitteiden mukaisesti. Lisäksi ENISA valmistelee ehdolla olevaa EU5G-järjestelmää ja EU:n digitaalisen identiteetin lompakkoa. Kaikkien jäsenvaltioiden yhteiset toimet ovat olennaisen tärkeitä tieto- ja viestintätekniisten tuotteiden, palvelujen ja prosessien yleisen turvallisuuden parantamiseksi.

### ***EU:n toimielinten, elinten ja laitosten tietoturvaa ja kyberturvallisuutta koskevat asetukset***

Maaliskuussa 2022 yhdessä ehdotetut asetukset, joilla säännellään unionin omien toimielinten kyberturvallisuutta ja tietoturvaa, ovat edenneet eri tahtiin. Kyberturvallisuutta koskevasta

---

<sup>10</sup> JOIN(2021) 30.

<sup>11</sup> COM(2022) 454.

asetuksesta päästiin viime kesäkuussa poliittiseen yhteisymmärrykseen, mikä mahdollistaa kaikkien EU:n toimielinten, elinten, toimistojen ja virastojen kyberturvallisuusaseman vahvistamisen ja osoittaa, että EU pitää tärkeänä tämän ehdotuksen nopeaa täytäntöönpanoa. Tässä tilanteessa on erityisen huolestuttavaa, että tietoturvaa koskeva rinnakkaisehdotus, joka on olennaisen tärkeä EU:n toimielinten, elinten ja laitosten vankan lainsäädäntökehyksen täydentämiseksi, on edennyt odottamattoman hitaasti. Molemmat ehdotukset olisi hyväksyttävä ennen Euroopan parlamentin vaaleja, jotta EU:n hallinto olisi uskottava ja kestävä nykyisessä geopoliittisessa tilanteessa. Kaikkia EU:n toimielimiä, elimiä ja laitoksia koskevat tietoturvasääntöjen ja -standardien vähimmäisvaatimukset loisivat varmuutta kaikille osapuolille ja varmistaisivat johdonmukaisen suojan sekä EU:n turvallisuusluokiteltuihin että muihin kuin turvallisuusluokiteltuihin tietoihin kohdistuvia kehittyviä uhkia vastaan. Yhdessä nämä uudet säännöt tarjoaisivat vakaan perustan turvalliselle tietojenvaihdolle EU:n toimielinten, elinten ja laitosten välillä ja jäsenvaltioiden kanssa sekä standardoidut käytännöt ja toimenpiteet tietovirtojen suojaamiseksi. Näin ollen ne vastaavat neuvoston useisiin kehotuksiin parantaa EU:n toimielinten, elinten ja laitosten häiriönsietokykyä ja suojella unionin päätöksentekoprosessia paremmin pahantahtoiselta sekaantumiselta.

### ***Kybersolidaarisuussäädös***

Komission 18. huhtikuuta 2023 hyväksymällä ehdotetulla kybersolidaarisuussäädöksellä<sup>12</sup>, joka perustuu jo olemassa olevaan vahvaan strategiseen, poliittiseen ja lainsäädännölliseen kehykseen, parannettaisiin entisestään kyberuhkien havaitsemista sekä sietokykyä ja varautumista unionin kyberturvallisuusekosysteemin kaikilla tasoilla. Nämä tavoitteet toteutettaisiin seuraavien kolmen päätoimen avulla:

- 1) Otetaan käyttöön ***kyberturvallisuuden eurooppalainen suojakilpi*** yhteisten havaitsemis- ja tilannetietoisuusvalmiuksien luomiseksi ja parantamiseksi. Se koostuisi kansallisista turvaoperaatiokeskuksista ja rajojen yli toimivista turvaoperaatiokeskuksista.
- 2) Perustetaan ***kyberhätätilanteiden mekanismi***, jolla tuetaan jäsenvaltioita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä välittömässä palautumisessa niiden jälkeen. Poikkeamiin reagoimisen tukemiseen kuuluisi EU:n kyberturvallisuusreservi, joka olisi myös Euroopan unionin toimielinten, elinten, toimistojen ja virastojen sekä Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden käytettävissä edellyttäen, että niiden Digitaalinen Eurooppa -ohjelmaan liittyvässä assosiaatiosopimuksessa niin määrätään.
- 3) Perustetaan ***kyberturvallisuuspoikkeamien eurooppalainen jälkitarkastelumekanismi***, jonka avulla voidaan tarkastella ja arvioida erityisiä merkittäviä tai laajamittaisia poikkeamia. ENISA koordinoisi ja laatisi häiriötilanteiden jälkitarkasteluraportin.

Keskustelut ovat alkaneet neuvostossa ja Euroopan parlamentissa. Neuvottelujen saattaminen päätökseen ennen Euroopan parlamentin nykyisen vaalikauden päättymistä vauhdittaisi huomattavasti pyrkimyksiä suojella kansalaisia ja yrityksiä kaikkialla unionissa.

### ***Kyberturvallisuusakatemia***

Kyberuhkien lisääntyessä EU tarvitsee kipeästi ammattilaisia, joilla on taidot ja pätevyys ehkäistä, havaita ja estää kyberhyökkäyksiä ja puolustaa EU:ta niiltä. EU:n kyberturvallisuustyövoiman tarve on tällä hetkellä arviolta 883 000 ammattilaista, kun taas

---

<sup>12</sup> COM(2023) 209.

täyttämättä olevien avoimien työpaikkojen määrä vaihteli 260 000:sta 500 000:een vuonna 2022. Kaikkia yhteiskuntaryhmiä olisi kannustettava auttamaan tämän aukon täyttämässä, mutta esimerkiksi vuonna 2022 naisia oli ainoastaan 20 prosenttia kyberturvallisuuteen liittyvän tutkinnon suorittaneista ja 19 prosenttia tieto- ja viestintäteknikan asiantuntijoista. Osana Euroopan osaamisen teemavuotta 2023 komissio hyväksyi 18. huhtikuuta 2023 kyberturvallisuuteen liittyvän osaamisvajeen pienentämiseksi aloitteen<sup>13</sup> kyberturvallisuusakatemia perustamisesta, johon jäsenvaltiot suhtautuivat myönteisesti<sup>14</sup>. Kyberturvallisuusakatemia kokoaisi yhteen nykyiset kyberturvallisuustaitoja koskevat aloitteet ja parantaisi koordinoitua. Komissio kannustaa jäsenvaltioita, alue- ja paikallisviranomaisia sekä eurooppalaisia julkisyhteisöjä hyväksymään erityisiä kyberturvallisuustaitoja koskevia strategioita tai aloitteita tai sisällyttämään kyberturvallisuustaidot sellaisiin asiaankuuluviin strategioihin tai aloitteisiin, joilla on laajempi soveltamisala (muun muassa kyberturvallisuus, digitaaliset taidot ja työllisyys). Myös yksityisten sidosryhmien osallistuminen on olennaisen tärkeää, jotta kyberturvallisuuteen liittyvää osaamisvajetta ja siihen liittyvää työvoimapulaa voidaan pienentää Euroopassa.

### ***Droonit***

Toinen julkisiin tiloihin ja kriittisiin infrastruktuureihin kohdistuva kasvava uhka on droonien pahantahtoinen käyttö. Drooneihin liittyvät tapaukset ovat yleistyneet sekä unionissa että sen ulkopuolella, ja droonien torjuntaratkaisut ovat keskeinen väline unionin lainvalvontaviranomaisille ja muille viranomaisille sekä kriittisen infrastruktuurin yksityisille ylläpitäjille. Samalla droonien laillinen käyttö edistää merkittävästi vihreää ja digitaalista siirtymää.<sup>15</sup> Kuten marraskuussa 2022 hyväksytyssä droonistrategiassa 2.0 ilmoitettiin, komissio antaa tänään tiedonannon siitä, miten droonien aiheuttamia mahdollisia uhkia voidaan torjua, sekä kaksi käsikirjaa, jotka sisältävät käytännön ohjeita keskeisistä teknisistä näkökohdista.<sup>16</sup> Aloitteella pyritään tarjoamaan kattava ja yhdenmukainen poliittinen kehys, jossa vallitsee yhteisymmärrys niistä käytössä olevista säännöistä, joiden avulla voidaan torjua droonien aiheuttamia mahdollisia uhkia ja mukautua tarpeen mukaan teknologian nopeaan kehitykseen. Jäsenvaltioita ja asianomaisia yksityisiä infrastruktuurin ylläpitäjiä kehoitetaan tekemään tiivistä yhteistyötä komission kanssa aloitteen täysimittaisen täytäntöönpanon varmistamiseksi.

### ***Merenkulun ja ilmailun turvallisuus***

Laiton toiminta, kuten merirosvous, aseelliset ryöstöt merellä, muuttajien salakuljetus, ihmis-, ase- ja huumekauppa sekä terrorismi, ovat edelleen meriturvallisuuden haasteita, ja niitä pahentavat kehittyvät uhkat, kuten hybridi- ja kyberhyökkäykset. Komissio ja korkea edustaja antoivat 10. maaliskuuta 2023 yhteisen tiedonannon EU:n merellisen turvallisuusstrategian päivittämisestä<sup>17</sup>, joka olisi nyt pantava täytäntöön päivitetyn toimintasuunnitelman mukaisesti.

Ilmailun turvaamisen alalla komissio hyväksyi 2. helmikuuta 2023 tehokkaampaa ja kestävämpää ilmailun turvaamispoliittikkaa koskevan komission yksiköiden valmisteluasiakirjan<sup>18</sup>. Se sisältää kunnianhimoisen ohjelman, jonka tavoitteena on 1) uudenaikaistaa ilmailun turvaamista koskeva sääntelyrakenne, 2) edistää innovatiivisempien ratkaisujen kehittämistä ja käyttöönottoa sekä 3) päivittää ilmailun turvaamisen perustasoa

---

<sup>13</sup> COM(2023) 207.

<sup>14</sup> Neuvoston päätelmät EU:n kyberpuolustuspolitiikasta, 22. toukokuuta 2023.

<sup>15</sup> COM(2022) 652.

<sup>16</sup> COM(2023) 659.

<sup>17</sup> JOIN(2023) 8.

<sup>18</sup> SWD(2023) 37.

siten, että EU:n lentoasemat pystyvät täysimittaisesti hyödyntämään uutta huipputeknologiaa, jonka avulla voidaan torjua ensisijaisimpia uhkia. Kahden vuoden kuluessa on pantava täytäntöön neljätoista lippulaivatoimea.

Komissio kehottaa Euroopan parlamenttia ja neuvostoa saattamaan kiireellisesti ja joka tapauksessa ennen nykyisen Euroopan parlamentin vaalikauden päättymistä päätökseen neuvottelut seuraavista asioista:

- ehdotus kyberkestävyysäädökseksi
- ehdotus kybersolidaarisuusäädökseksi
- ehdotus EU:n toimielinten, elinten ja laitosten tietoturvaä asetukseksi.

Komissio kehottaa jäsenvaltioita

- jatkamaan kriittisten toimijoiden häiriönsietokykyä koskevan direktiivin saattamista osaksi kansallista lainsäädäntöä ensisijaisena tavoitteena sekä energia-alan kriittisen infrastruktuurin stressitestien tekemistä
- hyväksymään neuvoston suosituksen suunnitelmaksi koordinoidusta reagoinnista kriittisen infrastruktuurin merkittäviin häiriöihin, joilla on huomattavaa rajatylittävää merkitystä
- saattamaan NIS 2 -direktiivin kaikilta osin ja kiireellisesti osaksi kansallista lainsäädäntöä keskeisten ja tärkeiden toimijoiden kyberturvallisuuden parantamiseksi
- osallistumaan aktiivisesti kyberturvallisuusriskien arviointeihin ja kriittisen infrastruktuurin ja toimitusketjujen riskiskenaarioiden laatimiseen
- toteuttamaan kyberturvallisuusakatemiaan jatkotoimia, jotka perustuvat vahvaan sitoutumiseen Euroopan tasolla ja kyberturvallisuustaitoja koskeviin kansallisiin strategioihin tai aloitteisiin, joissa keskeiset sidosryhmät, myös alue- ja paikallisviranomaiset, ovat mukana
- tekemään yhteistyötä asianomaisten yksityisten infrastruktuurin ylläpitäjien ja komission kanssa sen varmistamiseksi, että kaikki droonien aiheuttamien mahdollisten uhkien torjumista koskevassa tiedonannossa luetellut toimet pannaan täytäntöön
- panemaan täytäntöön EU:n merellisen turvallisuusstrategian toimintasuunnitelman ja raportoimaan säännöllisesti saavutuksista
- toteuttamaan 14 lippulaivatoimea, jotka on määritelty ilmailun turvaamisen parantamiseksi.

### III. Muuttuvien uhkien torjuminen

Uudet geopoliittiset jännitteet ovat selvä todiste siitä, että EU:n turvallisuushaasteet eivät ainoastaan kasva, vaan ne ovat myös yhä epävakaita, ja monien uhkien hybridimuotoinen luonne korostaa niitä entisestään. Turvallisuudessa on otettava huomioon myös yhteiskunnan ja teknologian muutokset. Covid-19-pandemia lisäsi kyberrikollisten mahdollisuuksia, ja erityisesti lasten seksuaalista hyväksikäyttöä koskevan aineiston uhka verkossa kasvoi. Rikolliset ja pahantahtoiset toimijat ovat aina valmiita hyödyntämään teknologian kehitystä. Tällaiset usein monimutkaiset ja moniulotteiset uhat edellyttävät EU:lta vahvaa ja johdonmukaista toimintaa.

### ***Verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan torjumista koskeva asetus***

Europolin järjestäytynyttä verkkorikollisuutta koskevasta uhka-arviosta käy ilmi, että vuonna 2022 lapsiin kohdistuva seksuaalinen riisto ja väkivalta lisääntyi edelleen sekä esiintyvyyden että vakavuuden osalta ja rikoksenteijät käyttivät edelleen hyväkseen teknisiä mahdollisuuksia peittää tekonsa ja henkilöllisyytensä.<sup>19</sup> Nykyinen järjestelmä, joka perustuu yritysten suorittamaan vapaaehtoiseen havaitsemiseen ja ilmoittamiseen, on osoittautunut riittämättömäksi lasten suojelun kannalta. Väliaikainen asetus mahdollistaa yritysten suorittaman vapaaehtoisen havaitsemisen ja ilmoittamisen edellyttäen, että se on lainmukaista yleisen tietosuoja-asetuksen mukaisesti. Tämän asetuksen voimassaolo päättyy elokuussa 2024. Komissio ehdotti toukokuussa 2022 asetusta<sup>20</sup>, jolla puututaan verkkopalvelujen väärinkäyttöön lapsiin kohdistuvan seksuaaliväkivallan tarkoituksiin. Ehdotetussa kehyksessä painotetaan voimakkaasti ennaltaehkäisyä. Yritykset olisivat velvollisia arvioimaan järjestelmiensä kautta tapahtuvan, lapsiin kohdistuvan seksuaaliväkivallan riskiä ja ryhtymään ennaltaehkäiseviin toimenpiteisiin. Kansalliset tuomioistuimet tai riippumattomat hallintoviranomaiset voisivat antaa palveluntarjoajille kohdennettuja tunnistamismääräyksiä viimeisenä keinona ainoastaan silloin, kun riski on merkittävä. Uusi riippumaton EU-keskus helpottaisi palveluntarjoajien työtä toimimalla asiantuntemuksen keskuksena, ja se tarjoaisi luotettavaa tietoa tunnistetusta materiaalista, vastaanottaisi ja analysoisi palveluntarjoajilta saatuja verkkovälitteistä lapsiin kohdistuvaa seksuaaliväkivaltaa koskevia ilmoituksia virheellisten ilmoitusten tunnistamiseksi sekä tarjoaisi tukea uhreille. On erittäin tärkeää, että uudet säännöt hyväksytään ja pannaan täytäntöön mahdollisimman pian, jotta voidaan suojella lapsia uusilta väärinkäytöksiltä, estää aineiston uudelleensiintyminen verkossa ja saattaa rikoksenteijät oikeuteen. Neuvottelut ovat käynnissä neuvostossa ja parlamentissa, ja tavoitteena on päästä asiasta sopimukseen ennen parlamentin vaalikauden päättymistä.

### ***Naisiin kohdistuvan väkivallan ja lähisuhdeväkivallan torjumista koskeva direktiivi***

Naisiin kohdistuva verkkoväkivalta, myös lähisuhdeväkivallan yhteydessä, on noussut tällaisen väkivallan uudeksi muodoksi, joka leviää yksittäisten jäsenvaltioiden rajojen yli internetin ja tietoteknisten välineiden kautta. Komissio ehdotti maaliskuussa 2022 direktiiviä naisiin kohdistuvaan väkivaltaan ja lähisuhdeväkivaltaan puuttumiseksi. Siihen sisältyy verkkoväkivaltaa koskevat erityiset säännöt ja toimenpiteet suojelussa, oikeussuojan saatavuudessa ja ennaltaehkäisyssä olevien puutteiden korjaamiseksi. Varhainen hyväksyminen ja täytäntöönpano antaisi jäsenvaltioille lisävälineitä tämältyyppisen rikollisuuden torjuntaan. Lainsäätäjät aloittivat toimielinten väliset neuvottelut heinäkuussa 2023 ja pyrkivät saamaan ne päätökseen ennen Euroopan parlamentin nykyisen vaalikauden päättymistä.

### ***5G-verkkojen kyberturvallisuus***

5G-verkkojen turvallisuus on yksi komission tärkeimmistä painopisteistä ja olennainen osa sen turvallisuusunionistrategiaa. 5G-verkot ovat keskeinen infrastruktuuri, joka tarjoaa perustan monille erilaisille palveluille, jotka ovat välttämättömiä sisämarkkinoiden toiminnalle ja elintärkeille yhteiskunnallisille ja taloudellisille toiminnoille. Verkko- ja tietoturva-alan yhteistyöryhmässä edustettuina olevat EU:n jäsenvaltioiden viranomaiset julkaisivat 15. kesäkuuta 2023 komission ja ENISAn tuella toisen tilannekatsauksen 5G-verkkojen kyberturvallisuutta koskevan EU:n välineistön täytäntöönpanosta. Tilannekatsauksen mukaan 24 jäsenvaltiota on hyväksynyt tai valmistelee lainsäädäntötoimia, joilla annetaan kansallisille viranomaisille valtuudet arvioida toimittajia ja asettaa rajoituksia, ja kymmenen jäsenvaltiota

<sup>19</sup> Europol (2023), järjestäytynyttä verkkorikollisuutta koskeva uhka-arvio 2023.

<sup>20</sup> COM(2022) 209.

on asettanut tällaisia rajoituksia. Tarvitaan kuitenkin lisätoimia, jotta voidaan välttää koko unionin haavoittuvuus, jolla voi olla vakavia kielteisiä vaikutuksia yksittäisten käyttäjien ja yritysten turvallisuuteen kaikkialla unionissa sekä unionin kriittiseen infrastruktuuriin. Kaikkien jäsenvaltioiden on pantava välineistö täytäntöön viipymättä. Komissio antoi samana päivänä tiedonannon välineistön täytäntöönpanosta jäsenvaltioissa sekä komission omasta yhteisötiedotuksesta ja unionin rahoitustoiminnasta. Tämä korosti vahvaa huolta matkaviestinverkon tietoliikennelaitteiden toimittajien Huaweiin ja ZTE:n aiheuttamista riskeistä EU:n turvallisuudelle. Tässä yhteydessä komissio toteuttaa toimenpiteitä välttääkseen yhteisötiedotuksensa altistumisen Huaweiin ja ZTE:tä toimittajina käyttäville matkaviestinverkoille. Hankinnoissa suljetaan pois sellaiset uudet yhteyspalvelut, jotka perustuvat kyseisten toimittajien laitteisiin, ja komissio tekee yhteistyötä jäsenvaltioiden ja teleoperaattoreiden kanssa varmistaa, että kyseiset toimittajat poistetaan asteittain komission toimipaikkojen olemassa olevista yhteyspalveluista. Komissio tutkii myös, miten tämä päätös voitaisiin ottaa huomioon asiaankuuluvissa unionin rahoitusohjelmissä ja -välineissä täysin unionin oikeuden mukaisesti.

### ***Tietojen saatavuus tehokasta lainvalvontaa varten***

Nykyisenä digitaaliaikana lähes jokaisessa rikoksessa on digitaalinen osatekijä. Teknologioita ja välineitä käytetään myös rikollisiin tarkoituksiin, mukaan lukien ne teknologiat ja välineet, jotka ovat välttämättömiä yhteiskuntamme kyberturvallisuuden, tietosuojan ja yksityisyyden suojan takaamiseksi. Tämän vuoksi on yhä haastavampaa ylläpitää tehokasta lainvalvontaa kaikkialla EU:ssa yleisen turvallisuuden takaamiseksi sekä rikosten ehkäisemiseksi, havaitsemiseksi ja tutkimiseksi ja niitä koskeviin syytetoimiin ryhtymiseksi, ja vaikka unionin tasolla ja kansallisella tasolla on toteutettu merkittäviä toimia muun muassa lainsäädännöllä sekä valmiuksien kehittämistä ja innovaatioita koskevilla aloitteilla, oikeudellisia ja teknisiä haasteita on edelleen olemassa. Komissio on perustanut neuvoston puheenjohtajavaltion tuella korkean tason työryhmän, joka käsittelee tehokkaasti lainvalvonnan edellyttämää tietojen saatavuutta. Sen tehtävänä on tarjota monenlaisille sidosryhmille ja asiantuntijoille yhteistyöfoorumi, jossa voidaan tarkastella haasteita, joita rikosoikeudellisen valvonnan harjoittajat kohtaavat (esimerkiksi salaus, tietojen säilyttäminen, 5G ja standardointi). Komissio odottaa, että korkean tason työryhmä laatii kesäkuuhun 2024 mennessä tasapainoiset, vankat ja toteutettavissa olevat suositukset, joissa otetaan huomioon näiden kysymysten monimutkaisuus myös kyberturvallisuuden ja tietosuojan näkökulmasta. Jäsenvaltioita ja osallistuvia asiantuntijoita kannustetaan sen vuoksi osallistumaan aktiivisesti tähän prosessiin ja pyrkimään tehokkaisiin, lainmukaisiin ja yhteisesti hyväksytyihin ratkaisuihin.

### ***Hybridiuhat***

EU:n turvallisuus- ja puolustusalan strateginen kompassi<sup>21</sup> on nykyisessä geopoliittisessa tilanteessa, jossa hybridiuhat ovat yhä monimutkaisempia ja kehittyneempiä, tarjonnut yhteisen arvion unionin kohtaamista uhkista ja haasteista sekä strategisen toimintasuunnitelman. Valtioiden ja valtiosta riippumattomien toimijoiden pahantahtoisen toiminnan lisääntyminen kybertoimintaympäristössä, myös Ukrainan vastaisen sodan yhteydessä, on entisestään korostanut kybertoimintaympäristön merkitystä ulko- ja turvallisuuspolitiikan alana. Pahantahtoisten toimien ja disinformaation mahdolliset riskit edellyttävät erityistä valppautta vaalien yhteydessä, myös vuoden 2024 Euroopan parlamentin vaalien alla.

Koska heijastusvaikutusten riski on suuri, EU on jatkanut kybervalmiuksien kehittämiseen tähtäviä toimia ja edistänyt kumppanuuksia kolmansien maiden kanssa muun muassa

---

<sup>21</sup> Neuvoston asiakirja 7371/22.

erityisten kybervuoropuhelujen avulla edistääkseen aktiivisesti EU:n yleistä häiriönsietokykyä. Useita välineitä on kehitetty, tarkistettu ja vahvistettu, jotta voidaan parantaa unionin kykyä puuttua tehokkaasti hybridiuhkiin, kuten 14. syyskuuta 2023 julkaistussa hybridiuhkia koskevassa seitsemännessä tilannekatsauksessa<sup>22</sup> kuvataan. Näitä ovat muun muassa seuraavat:

- EU:n hybridivälineistö, jolla varmistetaan kehys koordinoitulle ja tietoon perustuvalla reagoinnilla hybridiuhkiin ja -kampanjoihin;
- meneillään oleva työ EU:n hybridialan nopean toiminnan ryhmien perustamiseksi jäsenvaltioille, kumppanimaille ja yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) operaatioille annettavaa lyhytaikaista mukautettua tukea varten;
- tarkistettu EU:n protokolla hybridiuhkien torjumiseksi (”EU Playbook”)<sup>23</sup>, jossa kuvataan unionin prosessit ja rakenteet hybridiuhkien ja -kampanjoiden torjumiseksi;
- tarkistetut täytäntöönpano-ohjeet EU:n yhteistä diplomaattista vastausta haitallisiin kybert toimiin koskeville puitteille<sup>24</sup> (”kyberdiplomatian välineistö”), joiden avulla voidaan kehittää kestäviä, mukautettuja, johdonmukaisia ja koordinoituja strategioita pysyviä kyberuhkatoimijoita vastaan;
- ulkomaisen tiedonmanipuloinnin ja häirinnän torjuntavälineistö, jolla vahvistetaan unionin nykyisiä välineitä ulkomaisen tiedonmanipuloinnin ja häirinnän ehkäisemiseksi, estämiseksi ja torjumiseksi;
- EU:n kyberpuolustuspolitiikka<sup>25</sup>, jonka tarkoituksena on lisätä EU:n kyberpuolustusvalmiuksia, parantaa tilannetietoisuutta ja koordinoita kaikkia käytettävissä olevia puolustautumisvaihtoehtoja, jotta voidaan vahvistaa häiriönsietokykyä, vastata kyberhyökkäyksiin ja varmistaa solidaarisuus ja keskinäinen avunanto.

Jäsenvaltioita kannustetaan sen vuoksi jatkamaan ja tehostamaan yhteistyötään tällä alalla varmistamalla edellä mainittujen välineistöjen tehokas täytäntöönpano muun muassa säännöllisten harjoitusten avulla ja pääsemällä yhteisymmärrykseen hybridialan nopean toiminnan ryhmien käsitteestä, jota voidaan käyttää ohjeena ryhmien perustamiseen tähtäviä jatkotoimissa.

### ***Tekoäly lainvalvonnassa***

Tekoälystä on tullut nopeasti arkipäiväinen osa elämää. Tekoälyn käytön vaikutuksia kyberrikollisuuteen ja -turvallisuuteen ei vielä täysin tunneta, mutta ne asettavat selvästi uusia haasteita. Vaikka tekoälystä voi olla hyötyä, kun sitä käytetään turvallisesti ja hallitusti, se voi tarjota vaarallisia mahdollisuuksia pahantahtoosille toimijoille, esimerkiksi auttaa rikollisia piilottamaan henkilöllisyytensä terrorismin ja lasten seksuaalisen hyväksikäytön kaltaisissa rikoksissa. Siksi viranomaisten on tärkeää pysyä ajan tasalla kehityksestä väärinkäytösten ehkäisemiseksi ja niihin puuttumiseksi.<sup>26</sup> Ehdotettua tekoälysäädöstä koskevissa neuvotteluissa pyritään käsittelemään näitä aiheita, ja neuvottelut ovat nyt ratkaisevassa vaiheessa, kun lainsäätäjät keskustelevat teknisistä ja poliittisista kysymyksistä, jotka määrittävät tulevien vuosien vuorovaikutuksen tämän teknologian kanssa. On tärkeää löytää tasapainoisia ratkaisuja erityisesti riskialttiiden sovellusten osalta, myös lainvalvonnan alalla.

---

<sup>22</sup> SWD(2023) 315.

<sup>23</sup> SWD(2023) 116.

<sup>24</sup> 10289/23, 8. kesäkuuta 2023.

<sup>25</sup> JOIN(2022) 49.

<sup>26</sup> Ks. esimerkiksi 17. huhtikuuta 2023 julkaistu Europolin raportti ”ChatGPT - the impact of Large Language Models on Law Enforcement”.

Komissio kehottaa Euroopan parlamenttia ja neuvostoa saattamaan kiireellisesti ja joka tapauksessa ennen nykyisen Euroopan parlamentin vaalikauden päättymistä päätökseen toimielinten väliset neuvottelut seuraavista vireillä olevista asioista:

- ehdotus lasten verkossa tapahtuvan seksuaalisen hyväksikäytön torjumista koskevaksi asetukseksi
- ehdotus naisiin kohdistuvan väkivallan ja lähisuhdeväkivallan torjumista koskevaksi direktiiviksi
- ehdotus tekoälyä koskevia yhdenmukaistettuja sääntöjä koskevaksi asetukseksi (tekoälysäädös).

Komissio kehottaa jäsenvaltioita

- ottamaan viipymättä ja täysimittaisesti käyttöön 5G-kyberturvallisuutta koskevan EU:n välineistön
- tukemaan tehokkaan lainvalvonnan edellyttämää tietojen saatavuutta käsittelevän korkean tason työryhmän työtä, jotta voidaan laatia selkeitä, vankkoja ja toteuttamiskelpoisia suosituksia nykyisten ja odotettavissa olevien haasteiden ratkaisemiseksi oikeasuhteisella tavalla
- toteuttamaan yhteistyössä korkean edustajan kanssa toimia, joilla varmistetaan EU:n hybridivälineistön, tarkistetun kyberdiplomatian välineistön ja ulkomaisen tiedonmanipuloinnin ja häirinnän torjuntavälineistön tehokas täytäntöönpano, muun muassa säännöllisten harjoitusten avulla ja maailmanlaajuinen dynamiikka huomioon ottaen
- pääsemään yhteisymmärrykseen hybridialan nopean toiminnan ryhmien käsitteestä.

#### **IV. Eurooppalaisten suojeleminen terrorismilta ja järjestäytyneeltä rikollisuudelta**

Riski siitä, että maailmanlaajuiset tai paikalliset tapahtumat synnyttävät uusia terrori-iskuja, on aina olemassa. Järjestäytynyt rikollisuus ja laitton huumausainekauppa ovat vakavimpia EU:n turvallisuuteen kohdistuvia uhkia. Unionin näiden uhkien torjumista koskevien yhteisten toimien tehostamiseksi tehdään parhaillaan yhteistä työtä järjestäytyneen rikollisuuden torjuntaa koskevan EU:n strategian<sup>27</sup>, ihmiskaupan torjuntaa koskevan EU:n strategian<sup>28</sup>, EU:n huumeidenvastaisen ohjelman ja toimintasuunnitelman<sup>29</sup> sekä EU:n terrorisminvastaisen ohjelman<sup>30</sup> täytäntöönpanemiseksi. Järjestäytyneen rikollisuuden ja huumekaupan huolestuttavasti heikkenevään tilanteeseen vastaamiseksi jäsenvaltioiden ja EU:n on kuitenkin tehostettava entisestään työtään, jotta rikollisverkostojen vastaisia yhteisiä toimia voidaan tehostaa ja jotta rikoksen uhreja voidaan suojella paremmin. Samaan aikaan tämän kertomuksen kanssa julkaistaan EU:n etenemissuunnitelma huumekaupan ja järjestäytyneen rikollisuuden torjumiseksi<sup>31</sup>.

---

<sup>27</sup> COM(2021) 170.

<sup>28</sup> COM(2021) 171.

<sup>29</sup> COM(2020) 606.

<sup>30</sup> COM(2020) 795.

<sup>31</sup> COM(2023) 641.

Terrorismin torjunnan alalla EU vahvistaa myös ulkoisen toiminnan välineitään<sup>32</sup> hyödyntämällä täysimittaisesti terrorismintorjuntaa koskevaa korkean tason vuoropuhelua ja EU:n edustustojen terrorismintorjunnan ja turvallisuuden asiantuntijoiden verkostoa sekä osallistumalla monenvälisiin foorumeihin, muun muassa maailmanlaajuisen terrorisminvastaisen foorumin (GCTF) yhteispuheenjohtajana.

### ***Huumausaineiden laitton kauppa***

Euroopan unionin huumeviraston uusi toimeksianto, jota sovelletaan heinäkuusta 2024 alkaen, antaa EU:lle paremmat valmiudet puuttua monimutkaiseen turvallisuus- ja terveysongelmaan, joka vaikuttaa miljooniin ihmisiin EU:ssa ja maailmanlaajuisesti. Komissio on myös tarkistamassa<sup>33</sup> huumausaineiden lähtöaineita koskevia asetuksia<sup>34</sup>, jotta voidaan vastata vuoden 2020 arvioinnissa<sup>35</sup> havaittuihin tärkeimpiin haasteisiin. Arvioinnissa korostettiin tarvetta puuttua design-lähtöaineiden<sup>36</sup> aiheuttamiin haasteisiin laittomien huumausaineiden tarjonnan vähentämiseksi.

Koska Euroopassa saatavilla olevien laittomien huumausaineiden määrä on kuitenkin lisääntynyt ennennäkemättömällä tavalla, huumekaupan torjuntaa on tehostettava yhteistyössä kansainvälisten kumppaneiden kanssa. Jäsenvaltioiden ja EU:n on toteutettava lisätoimia rikollisverkostojen purkamiseksi ja rikoksen uhrien suojelemisen parantamiseksi. Komissio esittelee tänään EU:n etenemissuunnitelman huumekaupan ja järjestäytyneen rikollisuuden torjumiseksi. Siinä esitetään 17 toimea neljällä painopistealueella: vahvistetaan logistiikkakeskusten torjuntakykyä eurooppalaisen satama-allianssin avulla, hajotetaan rikollisverkostoja, lisätään ennaltaehkäisytoimia ja vahvistetaan yhteistyötä kansainvälisten kumppaneiden kanssa. Toimet on määrä toteuttaa vuosina 2024 ja 2025.

### ***Ampuma-aseet***

Ampuma-aseiden laitton kauppa ruokkii järjestäytyneitä rikollisuutta EU:ssa ja sen naapurialueilla. EU:ssa arvioidaan olevan siviilihenkilöiden käsissä jopa 35 miljoonaa laitonta ampuma-asetta, ja Schengenin tietojärjestelmässä noin 630 000 ampuma-asetta on merkitty varastetuiksi tai kadonneiksi. Nopeiden pakettitoimitusten ja 3D-tulostuksen kaltaisen uuden teknologian kehittyessä ampuma-aseiden laitton kauppa on saanut uusia muotoja, joissa voidaan välttyä valvonnalta. Venäjän Ukrainaa vastaan käymä hyökkäyssota on myös lisännyt ampuma-aseiden leviämisen riskiä. Komissio hyväksyi lokakuussa 2022 ehdotuksen siviilikäyttöön tarkoitettujen ampuma-aseiden tuontia, vientiä ja kauttakuljetusta koskevan nykyisen lainsäädännön ajantasaistamisesta, jotta voidaan sulkea nykyisissä säännöissä olevat porsaanreiät, jotka voivat lisätä EU:hun salakuljetettavien ja tarkoituksenvastaisesti siirrettävien ampuma-aseiden määrää.<sup>37</sup> Keskipitkällä aikavälillä nämä uudet säännöt auttavat vähentämään vientikieltojen kiertämisen riskiä siviilikäyttöön tarkoitettujen ampuma-aseiden viennissä ja lisäämään tällaisten ampuma-aseiden tuonnin valvontaa EU:n ulkopuolisista

---

<sup>32</sup> Kuten strategisessa kompassissa ja kesäkuussa 2022 hyväksytyissä terrorismin ja väkivaltaisten ääri liikkeiden jatkuvasti kehittyvän uhkan ulkoisen ulottuvuuden käsittelyä koskevissa neuvoston päätelmissä kehoitetaan.

<sup>33</sup> Huumausaineiden lähtöaineet – EU:n lainsäädännön tarkistaminen (europa.eu).

<sup>34</sup> Euroopan parlamentin ja neuvoston asetus (EY) N:o 273/2004, annettu 11 päivänä helmikuuta 2004, huumausaineiden lähtöaineista ja neuvoston asetus (EY) N:o 111/2005, annettu 22 päivänä joulukuuta 2004, unionin ja kolmansien maiden välisen huumausaineiden lähtöaineiden kaupan valvontaa koskevista säännöistä.

<sup>35</sup> COM(2020) 768.

<sup>36</sup> Huumeidenvastaisen toimintasuunnitelman toimi 23, COM(2020) 606.

<sup>37</sup> COM(2022) 480.

maista. Molempien lainsäätäjien on vielä vahvistettava kantansa tähän asiaan, jotta asiasta päästäisiin sopimukseen ennen parlamentin vaalikauden päättymistä.

### ***Ihmiskauppa***

Ihmiskauppa on erityisen vakava järjestäytyneen rikollisuuden muoto ja vakava perusoikeuksien loukkaus. Uhreja kaupataan EU:n sisällä pääasiassa seksuaalista hyväksikäyttöä ja työvoiman hyväksikäyttöä varten, mutta myös kerjäämiseen ja rikollisuuteen pakottamista ja muita muotoja varten. Komissio ehdotti joulukuussa 2022 ihmiskaupan ehkäisemistä koskevan direktiivin<sup>38</sup> muuttamista päivitettyillä säännöillä nykyisen oikeudellisen kehyksen puutteiden korjaamiseksi. Kun tarkistettu direktiivi on hyväksytty, sen soveltamisalaan lisättäisiin erityisesti pakkoavioliitot ja laittomat adoptiot ja siinä olisi nimenomainen maininta ihmiskaupan verkkoulottuvuudesta. Siihen sisältyisi myös rikoksentehtäjiä koskeva pakollinen seuraamusjärjestelmä, ja siinä virallistettaisiin kansallisten ohjautumismekanismien perustaminen, jotta voitaisiin parantaa uhrien varhaista tunnistamista ja rajatylittävää ohjaamista avun ja tuen saamiseksi uhreille. Ihmiskaupan uhrien tarjoamien palvelujen tietoisesta käyttämisestä tulisi rikos, ja ihmiskauppaa koskeva vuotuinen tietojenkeruu, jossa saadut tiedot Eurostat julkaisee, tulisi pakolliseksi. Neuvosto hyväksyi yleisnäkemyksensä kesäkuussa 2023, kun taas Euroopan parlamentin on vielä vahvistettava kantansa. On toimittava nopeasti, jotta sopimukseen päästään ennen tämän parlamentin toimikauden päättymistä.

### ***Ympäristörikollisuus***

Ympäristörikollisuudesta on tullut maailmanlaajuinen uhka, joka kasvaa vuosittain arviolta 5–7 prosenttia. Järjestäytyneitä rikollisuutta houkuttelevat merkittävät voitot, jäsenvaltioiden väliset lainsäädännölliset porsaanreiät ja alhainen paljastumisriski. Europolin mukaan on viitteitä siitä, että tästä toiminnasta saatuja tuloja käytetään terrorismin rahoittamiseen. Komissio hyväksyi joulukuussa 2021 ehdotuksen, jolla korvataan vuonna 2008 annettu direktiivi ympäristönsuojelusta rikosoikeudellisin keinoin. Ehdotuksessa keskitytään ympäristörikosluokkien määrittelyjen tarkentamiseen ja päivittämiseen sekä tehokkaiden, varoittavien ja oikeasuhteisten seuraamustyyppien ja -tasojen määrittelyyn luonnollisille henkilöille ja oikeushenkilöille. Uusia rikoksia ovat muun muassa laittomaan metsäkatoon, EU:n kemikaalilainsäädännön rikkomiseen, pinta- tai pohjaveden laittomaan ottoon ja alusten laittomaan kierrätykseen liittyvät rikokset. Ehdotuksen tavoitteena on vahvistaa merkittävästi lainvalvontaketjua ja rajatylittävää yhteistyötä jäsenvaltioiden viranomaisten sekä EU:n virastojen ja elinten välillä. Euroopan parlamentti ja neuvosto ovat vahvistaneet omat kantansa ehdotukseen ja käyvät parhaillaan neuvotteluja, jotka on tarkoitus saada päätökseen vuoden loppuun mennessä. Luonnonvaraisten eläinten ja kasvien laittoman kaupan torjumista koskeva tarkistettu toimintasuunnitelma<sup>39</sup> on pantava täytäntöön ennaltaehkäisyn ja täytäntöönpanon tehostamiseksi.

### ***Varojen takaisin hankinta ja menetetyksi tuomitseminen***

Rikollisten laittomien tulojen riistäminen on keskeisessä asemassa järjestäytyneen rikollisuuden torjunnassa. Tämän vuoksi ja sen lisäksi, että komissio oli tehnyt ehdotuksen<sup>40</sup>, jolla lainvalvontaviranomaisille annetaan pääsy pankkitilitietoihin koko EU:n alueella (josta päästiin poliittiseen yhteisymmärrykseen kesäkuussa 2023), komissio esitti toukokuussa 2022

---

<sup>38</sup> COM(2022) 732.

<sup>39</sup> COM(2022) 581.

<sup>40</sup> COM(2021) 429.

varojen takaisin Hankintaa ja menetetyksi tuomitsemista koskevan ehdotuksen<sup>41</sup>, jolla pyritään vahvistamaan varojen jäljittämistä, tunnistamista, jäädyttämistä, menetetyksi tuomitsemista ja hallinnointia koskevia valmiuksia. Ehdotuksen keskeiset säännökset koskevat talousrikosten tutkintaa koskevia vaatimuksia, varallisuuden takaisin hankinnasta vastaavien toimistojen lisävaltuuksia ja -välineitä sekä tehokkaampia jäädyttämistä ja menetetyksi tuomitsemista koskevia toimenpiteitä, joita sovelletaan entistä laajempaan joukkoon rikoksia. Yksi uusista rikoksista, joihin näitä toimenpiteitä sovellettaisiin, on unionin rajoittavien toimenpiteiden rikkominen. Komissio hyväksyi joulukuussa 2022 erillisen ehdotuksen unionin rajoittavien toimenpiteiden rikkomiseen liittyvien rikosten ja seuraamusten määrittelyn yhdenmukaistamisesta. Komission ensisijaisena tavoitteena on edelleen unionin rajoittavien toimenpiteiden tehokas täytäntöönpano ja valvonta, joita vahvistaa komission vastauksena Venäjän Ukrainaa vastaan käymään hyökkäyssotaan perustaman jäädyttämis- ja takavarikointityöryhmän työ. Euroopan parlamentti ja neuvosto ovat hyväksyneet kantansa molempiin ehdotuksiin ja pyrkivät pääsemään sopimukseen tämän vuoden loppuun mennessä.

### ***Rahanpesun torjunnan paketti***

Rahanpesu liittyy käytännöllisesti katsoen kaikkeen rikolliseen toimintaan, josta kertyy rikoshyötyjä EU:ssa<sup>42</sup>, ja se on siten keskeinen tekijä, johon keskittymällä voidaan torjua rikollisuutta EU:ssa. Komissio esitti heinäkuussa 2021 kunnianhimoisia ehdotuksia EU:n rahanpesun ja terrorismin rahoittamisen estämiseen tähtäävien toimenpiteiden vahvistamiseksi<sup>43</sup> ja antoi neljä lainsäädäntöehdotusta, joilla pyritään tehostamaan sellaisten rikollisten toimien ehkäisemistä ja havaitsemista, joilla pyritään pesemään laittomia tuloja tai rahoittamaan terroristista toimintaa rahoitusjärjestelmän kautta. Toukokuussa 2023 lainsäätäjät hyväksyivät tästä paketista aloitteen, joka koskee kryptovarojen siirtojen jäljitettävyyden varmistamista.<sup>44</sup> Tätä asetusta aletaan soveltaa 30. joulukuuta 2024, johon mennessä kaikkien kryptovarapalvelun tarjoajien on kerättävä ja säilytettävä tiedot kryptovarojen siirtojen lähettäjistä ja saajasta. Kolmen muun ehdotuksen tavoitteena on i) perustaa uusi EU:n rahanpesuntorjuntaviranomainen, jonka tehtävänä on varmistaa yhdenmukainen ja korkealaatuinen valvonta koko sisämarkkinoilla, myös kaikkein riskialteimpien rajatylittävien yhteisöjen osalta, sekä tukea ja koordinoida rahanpesun selvittelykeskusten työtä, ii) vahvistaa yksityistä sektoria koskevat yhdenmukaiset säännöt, mukaan lukien EU:n laajuisen 10 000 euron ylärajan käyttöönotto suurille käteismaksuille, joilla maksetaan palveluja ja tavaroita, ja iii) vahvistaa toimivaltaisten viranomaisten valtuuksia ja yhteistyövälineitä. Paketin odotetaan parantavan merkittävästi EU:n kykyä torjua rahanpesua ja suojella EU:n kansalaisia terrorismilta ja järjestäytyneeltä rikollisuudelta. Lainsäätäjät neuvottelevat parhaillaan kolmesta jäljellä olevasta ehdotuksesta, ja tavoitteena on päästä asiasta yhteisymmärrykseen ennen tämän parlamentin toimikauden päättymistä.

Komissio kehottaa Euroopan parlamenttia ja neuvostoa saattamaan kiireellisesti ja joka tapauksessa ennen nykyisen Euroopan parlamentin vaalikauden päättymistä päätökseen toimielinten väliset neuvottelut seuraavista vireillä olevista asioista:

- ehdotus varojen takaisin Hankintaa ja menetetyksi tuomitsemista koskevaksi direktiiviksi

<sup>41</sup> COM(2022) 245.

<sup>42</sup> Europol, ”Enterprising criminals – Europe’s fight against the global networks of financial and economic crime”, 2020.

<sup>43</sup> COM(2021) 420.

<sup>44</sup> Euroopan parlamentin ja neuvoston asetukset (EU) 2023/1113, annettu 31 päivänä toukokuuta 2023, varainsiirtojen ja tiettyjen kryptovarojen siirtojen mukana toimitettavista tiedoista ja direktiivin (EU) 2015/849 muuttamisesta.

- ehdotus unionin rajoittavien toimenpiteiden rikkomiseen liittyvien rikosten ja seuraamusten määrittelyn yhdenmukaistamista koskevaksi direktiiviksi
- ehdotus ihmiskaupan ehkäisemistä koskevaksi direktiiviksi
- ehdotus direktiiviksi ympäristönsuojelun parantamisesta rikosoikeudellisin keinoin
- ehdotus rahanpesun torjuntaa koskevaksi paketiksi
- ehdotus siviilikäyttöön tarkoitettujen ampuma-aseiden tuontia, vientiä ja kauttakuljetusta koskevan nykyisen lainsäädännön ajantasaistamiseksi.

Komissio kehottaa jäsenvaltioita sekä EU:n virastoja ja elimiä

- tekemään yhteistyötä huumekaupan ja järjestäytyneen rikollisuuden torjuntaa koskevan EU:n etenemissuunnitelman 17 toimen täytäntöönpanemiseksi vuosina 2023 ja 2024.

## V. Vahva eurooppalainen turvallisuusekosysteemi

Viime vuosina turvallisuusuhat ovat muuttuneet luonteeltaan yhä enemmän rajatylittäviksi, mikä edellyttää synergian lisäämistä ja tiiviimpää yhteistyötä kaikilla tasoilla. Turvallisuusunionistrategian hyväksymisen jälkeen on tehty merkittäviä aloitteita rajatylittävän yhteistyön maksimoimiseksi, käytävissä olevien välineiden ja menettelyjen yksinkertaistamiseksi ja parantamiseksi sekä ulkorajoilla että Schengen-alueella sekä lainvalvonta- ja oikeusviranomaisten välisen tietojenvaihdon tehostamiseksi järjestäytyneen rikollisuuden torjunnan parantamiseksi. Tätä taustaa vasten tietojenvaihtoa koskevien yhteentoimivuuseriaatteiden tehokas täytäntöönpano on tärkeä pilari, jonka avulla voidaan parantaa turvallisuutta ja tehokasta eurooppalaista reagointia rajatylittäviin uhkiin siten, että samalla taataan sisäinen vapaa liikkuvuus.

### *Tehostettu tietojenvaihto Schengen-alueella: matkustajien ennakkotiedot (API-tiedot), matkustajarekisterit (PNR) ja Prüm II -asetus*

Komission joulukuussa 2022 hyväksymät kaksi API-tietoa koskevaa ehdotusta<sup>45</sup> parantaisivat unionin sisäistä turvallisuutta antamalla jäsenvaltioiden lainvalvontaviranomaisille lisävälineitä vakavan rikollisuuden ja terrorismin torjuntaan. Erityisesti EU:n sisäisten lentojen matkustajien ennakkotiedot, joita käytetään yhdessä PNR-tietojen kanssa, antaisivat jäsenvaltioiden lainvalvontaviranomaisille mahdollisuuden tehostaa huomattavasti tutkimuksiaan kohdennetummilla toimenpiteillä. On tärkeää, että ehdotetut säännöt hyväksytään mahdollisimman pian, sillä se tukisi järjestäytyneen rikollisuuden ja terrorismin torjuntaa ja vähentäisi merkittävästi kaikkien matkustajien järjestelmällisten tarkastusten tarvetta siinä tapauksessa, että sisärajarastukset otetaan väliaikaisesti uudelleen käyttöön, mikä helpottaisi lentomatkustamista ja vapaata liikkuvuutta. Komissio suositteli 6. syyskuuta 2023, että neuvosto antaisi luvan neuvotella Sveitsin, Islannin ja Norjan kanssa PNR-tietojen siirtoa koskevista sopimuksista. Näiden kolmen suosituksen hyväksyminen tukisi johdonmukaista ja tehokasta EU:n ulkoista PNR-politiikkaa.

<sup>45</sup> COM(2022) 729 ja COM(2022) 73.

Poliisi käyttää päivittäin Prüm-tietojenvaihtoa järjestäytyneen rikollisuuden, huumeiden, terrorismin, seksuaalisen riiston ja ihmiskaupan torjunnassa. Ehdotuksella asetukseksi automaattisesta tietojenvaihdosta poliisiyhteistyössä (Prüm II)<sup>46</sup> tarkistetaan nykyisiä Prüm-puitteita, jotta tiedonsaannin puutteet saataisiin poistettua ja rikosten ennaltaehkäisyä, paljastamista ja tutkintaa tehostettua EU:ssa. Poliisiyhteistyöhön liittyvää automaattista tietojenvaihtoa koskevat tarkistettavat säännöt täydentävät tämän toimeksiannon poliisiyhteistyötä koskevia ehdotuksia jo hyväksytyin operatiivista rajatylittävää yhteistyötä koskevan neuvoston suosituksen ja lainvalvontaviranomaisten välistä tietojenvaihtoa koskevan direktiivin ohella. Näiden välineiden nopea käyttöönotto ja täytäntöönpano parantaisi, helpottaisi ja nopeuttaisi lainvalvontaviranomaisten välistä tietojenvaihtoa ja auttaisi rikollisten tunnistamisessa.

### ***Täysin yhteentoimiva rajavalvontajärjestelmä turvallista, vahvaa, digitaalista ja yhtenäistä Schengen-aluetta varten***

Hyvin toimiva sisärajan Schengen-alue perustuu jäsenvaltioiden keskinäiseen luottamukseen. Tämä puolestaan perustuu tehokkaaseen valvontaan joko unionin ulkorajoilla tai vaihtoehtoisena toimenpiteenä jäsenvaltioiden alueella. Komission Schengenin rajasäännöstöön ehdottamassa muutoksessa<sup>47</sup> esitetään, miten jäsenvaltiot voivat hyödyntää paremmin sisärajanvalvonnan vaihtoehtoja, jotka voivat tarjota korkean turvallisuustason. On tärkeää, että Schengenin rajasäännöstön muutos hyväksytään ja pannaan täysimittaisesti täytäntöön, jotta varmistetaan korkea ja oikeasuhteinen turvallisuustaso Schengen-alueella. Myös EU:n tietojärjestelmien uutta rakennetta kehitetään edelleen, jotta voidaan paremmin tukea kansallisten viranomaisten työtä turvallisuuden ja rajaturvallisuuden varmistamiseksi. Siihen kuuluvat uudistettu Schengenin tietojärjestelmä, Euroopan matkustustieto- ja -lupajärjestelmä, rajanylitystietojärjestelmä, viisumitietojärjestelmän päivitys sekä yhteentoimivuusperiaatteet, joilla järjestelmät voidaan yhdistää toisiinsa täysin turvallisesti. Kun tämä uusi rakenne on täysin valmis, se tarjoaa kansallisille viranomaisille kattavampia ja luotettavampia turvallisuustietoja. Kaikki yhteentoimivuusperiaatteiden osatekijät ovat olennaisen tärkeitä, mikä tarkoittaa, että viivästyminen jollakin osa-alueella tai jossakin jäsenvaltiossa johtaa käyttöönoton viivästyamiseen kaikkien osalta. Viiveet rajanylitystietojärjestelmän teknisessä kehittämisessä olisi minimoitava, jotta rajanylitystietojärjestelmä voisi aloittaa toimintansa mahdollisimman pian ja jotta kaikki yhteentoimivuusperiaatteiden keskeiset osatekijät voitaisiin ottaa käyttöön.

Seulontaehdotuksella<sup>48</sup> parannettaisiin Schengen-alueen turvallisuutta luomalla yhdenmukaiset säännöt sellaisten kolmansien maiden kansalaisten tunnistamiseksi, jotka eivät täytä Schengenin rajasäännöstön mukaisia maahantulon edellytyksiä, ja ohjaamalla heidät terveys- ja turvallisuustarkastuksiin ulkorajoilla. Jos seulonnan jälkeen vaikuttaa siltä, että henkilö voi muodostaa uhan sisäiselle turvallisuudelle, ehdotettu Eurodac-järjestelmä osoittaisi tämän ja tukisi näin näitä tavoitteita Tämä puolestaan helpottaisi ehdotetun turvapaikka-asioiden ja muuttoliikkeen hallintaa koskevan asetuksen täytäntöönpanoa. Komissio kannustaa lainsäätäjiä saattamaan näitä asioita koskevat neuvottelut nopeasti päätökseen ennen nykyisen vaalikauden päättymistä.

### ***Korruptiontorjunta***

Korruptio on erittäin vahingollista demokratiollemme, taloudellemme ja turvallisuudellemme, sillä se edistää järjestäytyneitä rikollisuutta ja vihamielisiä ulkomaista sekaantumista.

---

<sup>46</sup> COM(2021) 784.

<sup>47</sup> COM(2021) 891.

<sup>48</sup> COM(2020) 612.

Korruption onnistunut ehkäiseminen ja torjunta on olennaisen tärkeää sekä EU:n arvojen ja EU:n politiikkojen vaikuttavuuden turvaamiseksi että oikeusvaltioperiaatteen ja hallintoelimiä ja julkisia instituutioita kohtaan koettavan luottamuksen säilyttämiseksi. Kuten puheenjohtaja Ursula von der Leyen ilmoitti vuonna 2022 pitämässään unionin tilaa koskevassa puheessa, komissio hyväksyi 3. toukokuuta 2023 korruption vastaisen toimenpidepaketin<sup>49</sup>. Komission ehdotus korruption torjuntaa koskevaksi direktiiviksi sisältää tiukennettuja sääntöjä, joilla kriminalisoidaan korruptiorikokset ja yhdenmukaistetaan rangaistuksia kaikkialla EU:ssa. Se mahdollistaa myös tehokkaan tutkinnan ja syytteenpanon, ja siinä keskitytään voimakkaasti ennaltaehkäisyyn ja sellaisen lahjomattomuuden kulttuurin luomiseen, jossa korruptiota ei suvaita. Ehdotuksesta on aloitettu keskustelut Euroopan parlamentissa ja neuvostossa. Lisäksi jäsenvaltioita kehoitetaan panemaan täytäntöön 5. heinäkuuta 2023 hyväksytyin vuoden 2023 oikeusvaltiokertomuksen korruptiontorjunnan pilarin suositukset. Korkean edustajan esittämässä ja komission tukemassa ehdotuksessa esitetään lisäksi, että perustetaan erityinen yhteiseen ulko- ja turvallisuuspolitiikkaan kuuluva pakotejärjestelmä, jonka tarkoituksena on torjua vakavaa korruptiota maailmanlaajuisesti.

### ***Uhrien oikeuksien vahvistaminen***

Komissio ehdotti 12. heinäkuuta 2023 muutoksia uhrien oikeuksia koskevaan direktiiviin, jotta voitaisiin parantaa uhrien tiedonsaantia, tukea ja suojelua, osallistumista rikosoikeudenkäynteihin ja korvausten saantia. Yksi tarkistuksen yleistavoitteista on edistää korkeaa turvallisuustasoa luomalla uhreille turvallisempi ympäristö, joka kannustaa ilmoittamaan rikoksista ja vähentää kostotoimien pelkoa.

Komissio kehottaa Euroopan parlamenttia ja neuvostoa saattamaan kiireellisesti ja joka tapauksessa ennen nykyisen Euroopan parlamentin vaalikauden päättymistä päätökseen toimielinten väliset neuvottelut seuraavista vireillä olevista asioista:

- ehdotus Prüm II -asetukseksi
- matkustajien ennakkotietoja (API-tiedot) koskevat ehdotukset
- ehdotukset korruption torjunnasta ja erityisesti yhteisen ulko- ja turvallisuuspolitiikan (YUTP) pakotejärjestelmän perustamisesta
- ehdotus Schengenin rajasäännöstöä koskevan asetuksen muuttamiseksi
- ehdotus uhrien oikeuksia koskevaksi direktiiviksi
- seulontaa koskeva ehdotus.

Komissio kehottaa jäsenvaltioita

- varmistamaan, että rajanylitystietojärjestelmä tulee voimaan mahdollisimman pian, jotta EU:n tietojenvaihtorakenteen täytäntöönpano saadaan päätökseen.

## **VI. Täytäntöönpano**

Euroopan kokonaisturvallisuuden varmistaminen on jaettu vastuu, jossa jokaisen toimijan on tehtävä oma osuutensa: komission ja lainsäätäjien on annettava uusia, vahvoja, kattavia ja käytännöllisiä sääntöjä, jäsenvaltioiden on saatettava nämä säännöt ajoissa osaksi kansallista lainsäädäntöään, pantava ne täytäntöön ja sovellettava niitä, minkä lisäksi monien eri viranomaisten, organisaatioiden ja sidosryhmien on toteutettava operatiivisia toimia ruohonjuuritasolla. EU:n virastoilla on myös keskeinen asema oikeuden, sisäasioiden ja

<sup>49</sup> COM(2023) 234.

kyberturvallisuuden alalla, ja aseman merkitys on kasvanut, kun niiden vastuualueita on hiljattain laajennettu.

### ***EU:n rahoituksen saajien tehostettu seulonta***

EU:n talousarviota toteuttaessaan komissio on vastuussa siitä, että EU:n rahoituksen saajat noudattavat EU:n arvoja. Mekanismit ja valvontajärjestelmät, joilla määritetään, kuka voi saada EU:n rahoitusta, ovat jo vankat, ja meneillään olevilla varainhoitoasetuksen uudelleenlaadintaa koskevilla neuvotteluilla pyritään myös antamaan komissiolle vahvemmat oikeudelliset keinot toimia tarvittaessa. Lisäksi komissio tarkastelee parhaillaan keinoja tehostaa nykyisten ja mahdollisten tulevien EU:n rahoituksen saajien seulontaa parantamalla ohjeistusta, joka koskee EU:n arvojen kunnioittamista koskevia velvoitteita ja EU:n arvojen rikkomisesta aiheutuvia seurauksia. Tämä selventää sekä edunsaajien että EU:n tasolla tarkastuksia toteuttavien tahojen vastuualueita ja voi toimia inspiraation lähteenä kansallisella tasolla. Jos rahoitusehtoja rikotaan, komissio ei epäröi keskeyttää yhteistyötä kyseisen hankkeen edunsaajien kanssa ja tarvittaessa periä varoja takaisin. On tärkeää, että jäsenvaltiot jakavat ennakoivasti tietoja komissiolle, kun ne ovat tietoisia EU:n rahoitusta hakeviin organisaatioihin liittyvistä mahdollisista riskeistä.

### ***Rikkomukset***

Komissio on toteuttanut turvallisuuden alalla useita rikkomusmenettelyjä. Esimerkiksi vuonna 2023 on pantu vireille suuri määrä rikkomustapauksia, sillä vuonna 2021 annettuun terroristisen verkkosisällön levittämistä koskevaan asetukseen<sup>50</sup> perustuvia velvoitteita ei ollut täytetty (16 jäsenvaltiota), ja vuosien 2022 ja 2023 aikana 20 jäsenvaltiota on saanut lisää virallisia ilmoituksia lasten seksuaalisen hyväksikäytön torjumisesta vuonna 2011 annetun direktiivin<sup>51</sup> virheellisen täytäntönnäpönnön vuoksi. Huomattava määrä rikkomustapauksia on edelleen vireillä, koska kansallinen lainsäädäntö ei ole sopusoinnussa terrorismin torjumisesta vuonna 2017 annetun direktiivin<sup>52</sup> kanssa ja koska kansallisen lainsäädännön osaksi ei ole saatettu sääntöjä, joilla helpotetaan rahoitus- ja muiden tietojen käyttöä tiettyjen rikosten ennalta estämistä, paljastamista, tutkimista tai niihin liittyviä syytetoimia varten<sup>53</sup>. Muita aloja, joilla rikkomusmenettelyjä on käynnissä, ovat ampuma-aselainsäädäntö, huumausaineissa käytettäviä psykoaktiivisia aineita koskevat säännöt, muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennösten torjunta, rahanpesun torjunta, rikosrekisteritietojen vaihto EU:n jäsenvaltioiden välillä ja uhrien oikeuksia koskeva direktiivi. Jäsenvaltioille, jotka toteuttavat sovittuja aloitteita ja toimia, on annettu (teknistä ja taloudellista) tukea, ja komissio on edelleen valmis työskentelemään jäsenvaltioiden kanssa täytäntönnäpönnön optimoimiseksi.

### ***Seuranta Schengen-arviointien ja Schengen-alueen uuden hallinnointijärjestelmän avulla***

---

<sup>50</sup> Euroopan parlamentin ja neuvoston asetukset (EU) 2021/784, annettu 29 päivänä huhtikuuta 2021, verkossa tapahtuvaan terroristisen sisällön levittämiseen puuttumisesta.

<sup>51</sup> Euroopan parlamentin ja neuvoston direktiivi 2011/93/EU, annettu 13 päivänä joulukuuta 2011, lasten seksuaalisen hyväksikäytön torjumisesta.

<sup>52</sup> Euroopan parlamentin ja neuvoston direktiivi (EU) 2017/541, annettu 15 päivänä maaliskuuta 2017, terrorismin torjumisesta sekä neuvoston puitepäätöksen 2002/475/YOS korvaamisesta sekä neuvoston päätöksen 2005/671/YOS muuttamisesta.

<sup>53</sup> Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/1153, annettu 20 päivänä kesäkuuta 2019, säännöistä, joilla helpotetaan rahoitus- ja muiden tietojen käyttöä tiettyjen rikosten ennalta estämistä, paljastamista, tutkimista tai niihin liittyviä syytetoimia varten, ja neuvoston päätöksen 2000/642/YOS kumoamisesta.

Schengenin arviointi- ja seurantamekanismi on edelleen edistänyt niiden Schengenin sääntöjen tehokasta täytäntöönpanoa, joilla pyritään parantamaan turvallisuutta alueella, jolla ei tehdä sisäraajatarkastuksia. Vuonna 2023 on toteutettu ensimmäiset tehostetun Schengenin arviointi- ja seurantamekanismin mukaiset arvioinnit, jotka mahdollistavat sellaisten strategisten heikkouksien oikea-aikaisen tunnistamisen ja korjaamisen, joilla on rajatylittävää vaikutusta EU:n turvallisuuteen. Lisäksi komissio on käynnistänyt vuonna 2023 temaattisen Schengen-arvioinnin, jonka tarkoituksena on arvioida niiden jäsenvaltioiden käytäntöjä, joilla on samanlaisia haasteita EU:hun suuntautuvan laittoman huumausainekaupan torjunnassa, ja keskittyä erityisesti laajamittaiseen laittomaan huumausainekauppaan. Näissä arvioinneissa kiinnitettiin entistä enemmän ja kattavammin huomiota Schengenin turvallisuustekijöihin. Neuvosto vahvisti kesäkuussa 2023 määräaikaisten, aihekohtaisten ja ennalta ilmoittamattomien Schengen-arviointien tulosten perusteella vuosien 2023–2024 Schengen-syklin painopisteet. Niissä määritellään kohdealat, joilla tarvitaan lisätoimia turvallisemman ja vahvemman Schengen-alueen luomiseksi. Näiden painopisteiden tehokas ja nopea täytäntöönpano yhdessä Schengen-neuvoston tehostetun poliittisen koordinoinnin kanssa vahvistaa entisestään järjestäytyneen rikollisuuden torjuntaa ja maksimoi rajatylittävän operatiivisen yhteistyön.

### ***EU:n virastojen ja elinten rooli***

Kumppanuus on keskeisessä asemassa turvallisuusunionia koskevien aloitteiden täytäntöönpanossa, sillä konkreettisten tulosten aikaansaamiseksi tarvitaan eri kansallisten ja EU:n viranomaisten ja elinten työtä. Esimerkiksi EMPACT (Euroopan monialainen rikosuhkien torjuntafoorumi) mahdollistaa jäsenvaltioiden jäsennellyn monialaisen yhteistyön, jota tukevat kaikki EU:n toimielimet, elimet ja virastot (kuten Europol, Frontex, Eurojust, CEPOL, OLAF ja eu-LISA). EMPACTin toteuttamalla toimilla, myös erityisten operatiivisten toimintaryhmien avulla, koordinoidaan jäsenvaltioiden ja operatiivisten kumppaneiden toimia rikollisverkostojen ja vakavan rikollisuuden torjumiseksi. Pelkästään vuonna 2022 EMPACT johti yhteensä 9 922 pidätykseen, yli 180 miljoonan euron arvoisen omaisuus- ja rahamäärän takavarikointiin, 9 263 tutkinnan aloittamiseen, 4 019 uhrin tunnistamiseen, yli 62 tonnin huumausainemäärän takavarikointiin, 51 merkittävän kohteen tunnistamiseen ja 12 tällaisen kohteen pidätykseen sekä operaatioihin Ukrainan vastaisen hyökkäyssodan yhteydessä, erityisesti ihmiskauppaan ja ampuma-aseisiin liittyviin uhkiin puuttumiseksi.<sup>54</sup>

Frontex, Euroopan meriturvallisuusvirasto (EMSA) ja Euroopan kalastuksenvalvontavirasto (EFCA) lujittavat edelleen yhteistyötään rannikkovartiointitehtävissä tukeakseen kansallisia viranomaisia meriturvallisuuden parantamisessa. Nämä virastot osallistuvat merkittäväällä tavalla EU:n merellisen turvallisuusstrategian täytäntöönpanoon.

Useat turvallisuusunionin aloitteet ovat tuoneet asianomaisille virastoille uusia vastuualueita ja tehtäviä, joilla on toisinaan vaikutuksia henkilöstöresursseihin.

### ***Euroopan unionin kyberturvallisuusvirasto (ENISA)***

Kyberturvallisuuden parantamiseen tähtäävän varautumisen ja poikkeamiin reagoimisen osalta komissio on käynnistänyt lyhyen aikavälin toimen jäsenvaltioiden tukemiseksi siirtämällä rahoitusta Digitaalinen Eurooppa -ohjelmasta **Euroopan unionin kyberturvallisuusvirastolle (ENISA)**, jotta voidaan parantaa varautumista ja valmiuksia reagoida suuriin

<sup>54</sup> EMPACTin tietosivut vuoden 2022 tuloksista:

[https://www.consilium.europa.eu/media/65450/2023\\_225\\_empact-factsheets-2022\\_web-final.pdf](https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf)

kyberturvallisuuspoikkeamiin. Huhtikuussa 2023 hyväksytty ehdotus kybersolidaarisuussäädökseksi perustuu tähän toimeen, ja kun lainsäätäjät ovat hyväksyneet sen, ENISAlle voidaan antaa lisätehtäviä, kuten unionin tulevan kyberturvallisuusreservin toiminta ja hallinnointi tai laajamittaisten kyberhäiriötilanteiden jälkitarkasteluraportin laatiminen. Ehdotetun kyberkestävyyssäädöksen mukaisesti ENISAn tehtävänä olisi vastaanottaa valmistajilta ilmoituksia digitaalisia elementtejä sisältävien tuotteiden haavoittuvuuksista ja näiden tuotteiden turvallisuuteen vaikuttavista poikkeamista ja toimittaa ne ENISAn asianomaisille CSIRT-yksiköille tai jäsenvaltioiden asianomaisille keskitetyille yhteyspisteille. ENISAn odotetaan myös laativan joka toinen vuosi teknisen raportin digitaalisia elementtejä sisältävien tuotteiden kyberturvariskien uusista suuntauksista ja toimittavan sen verkko- ja tietoturva-alan yhteistyöryhmälle.

### *Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus*

**Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus** on yhdessä kansallisten koordinoitikeskusten verkoston kanssa unionin uusi elin, joka tukee innovointia ja teollisuuspolitiikkaa kyberturvallisuuden alalla. Tämä ekosysteemi tehostaa kyberturvallisuusteknologiayhteisön valmiuksia, ylläpitää tutkimuksen huippuosaamista ja vahvistaa unionin teollisuuden kilpailukykyä tällä alalla. Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus ja kansalliset koordinoitikeskukset tekevät strategisia investointipäätöksiä ja yhdistävät unionin, sen jäsenvaltioiden ja välillisesti teollisuuden resursseja teknologian ja teollisuuden kyberturvallisuusvalmiuksien parantamiseksi ja vahvistamiseksi. Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus on näin ollen keskeisessä asemassa Digitaalinen Eurooppa -ohjelman ja Horisontti Eurooppa -puiteohjelman kunnianhimoisten kyberturvallisuustavoitteiden saavuttamisessa.

Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus on rekrytoinut yli puolet henkilöstöstään, ja se palkkaa pian pääjohtajan. Jo käynnissä olevaan työhön sisältyy Digitaalinen Eurooppa -ohjelman kyberturvallisuutta koskeva osa ja uusi teknologian kehittämistä ja käyttöönottoa koskeva strateginen ohjelma<sup>55</sup>, jossa esitetään ensisijaisia toimia pk-yritysten tukemiseksi strategisten kyberturvallisuusteknologioiden, -palvelujen ja -prosessien kehittämisessä ja käytössä, ammattitaitoisen työvoiman tukemiseksi ja kasvattamiseksi sekä tutkimus-, kehitys- ja innovaatioasiantuntemuksen lisäämiseksi laajemmassa eurooppalaisessa kyberturvallisuusekosysteemissä.

### *Europol*

Täysin uuden toimeksiannon myötä **Europolilla** on paremmat valmiudet tukea jäsenvaltioita järjestäytyneen rikollisuuden torjunnassa. Laittoman huumausainekaupan torjunta on keskeinen painopiste, sillä sen merkitys kasvaa ja sen kielteiset vaikutukset EU:n kansalaisten turvallisuuteen lisääntyvät. Euroopan unionin neuvoston 15. toukokuuta 2023 antaman valtuutuksen jälkeen komissio on pyrkinyt aktiivisesti tekemään Bolivian, Brasilian, Ecuadorin, Meksikon ja Perun kanssa kansainvälisiä sopimuksia henkilötietojen vaihtamisesta Europolin kanssa vakavan rikollisuuden ja terrorismin ehkäisemiseksi ja torjumiseksi.

### *Eurojust*

**Eurojustilla** on yli 20 vuoden kokemus oikeudellisesta tuesta kansallisille viranomaisille monenlaisten vakavien ja monimutkaisten rajatylittävien rikosten torjunnassa, ja se on vakiinnuttanut asemansa EU:n vapauden, turvallisuuden ja oikeuden alueella. Vahvistaakseen yhteistyötä kautta linjan komissio neuvottelee parhaillaan kansainvälisiä sopimuksia, joilla

<sup>55</sup> [https://cybersecurity-centre.europa.eu/strategic-agenda\\_en](https://cybersecurity-centre.europa.eu/strategic-agenda_en)

helpotetaan Eurojustin ja 13 kolmannen maan<sup>56</sup> välistä yhteistyötä henkilötietojen vaihtamiseksi järjestäytyneen rikollisuuden ja terrorismin torjumiseksi. Neuvottelut on jo saatettu päätökseen Armenian ja Libanonin kanssa, niitä käydään Algerian ja Kolumbian kanssa ja ne on aloitettu Bosnia ja Hertsegovinan kanssa. Komissio kannustaa Euroopan parlamenttia ja neuvostoa saattamaan päätökseen sopimusten tekemisen näiden maiden kanssa ennen vaalikauden päättymistä, jotta voidaan vahvistaa rajatylittävää oikeudellista yhteistyötä ja laajentaa rajatylittävän rikollisuuden torjuntaa.

#### *Euroopan syyttäjänvirasto (EPPO)*

Siitä lähtien, kun **Euroopan syyttäjänvirasto (EPPO)** aloitti toimintansa kesäkuussa 2021, se on osoittautunut unionin työkalupakin tehokkaaksi välineeksi unionin talousarvioon vaikuttavien rikosten, myös rikollisjärjestöön osallistumiseen liittyvien rikosten, tutkinnassa ja syytteenpanossa, kun painopiste on unionin talousarvioon kohdistuvissa rikoksissa. Komissio kannustaa sellaisia jäsenvaltioita, jotka eivät vielä osallistu EPPOn tiiviimpään yhteistyöhön, tekemään niin mahdollisimman pian, jotta EPPOn tarjoamia mahdollisuuksia EU:n veronmaksajien rahojen suojelemiseksi voidaan hyödyntää täysimittaisesti.

#### *EUDA*

Koska lainsäätäjät hyväksyivät uuden toimeksiannon kesäkuussa 2023, nykyisestä Euroopan huumeaineiden ja niiden väärinkäytön seurantakeskuksesta (EMCDDA) tulee täysivaltainen virasto eli **Euroopan unionin huumevirasto (EUDA)**, jolla on entistä vahvempi asema. Virasto pystyy arvioimaan kattavammin laittomien huumeaineiden aiheuttamia uusia terveys- ja turvallisuushaasteita ja osallistumaan tehokkaammin jäsenvaltioiden ja kansainvälisen tason työhön. Tietojen kerääminen, analysointi ja levittäminen on edelleen viraston päätehtävä, mutta laajennetun toimeksiannon ansiosta se voi myös kehittää yleisiä terveys- ja turvallisuusuhkien arviointivalmiuksia uusien uhkien, myös sekakäytön, tunnistamiseksi, vahvistaa yhteistyötään kansallisten yhteyspisteiden kautta ja perustaa laboratorioiden verkoston, josta virasto saa rikosteknistä ja toksikologista tietoa. Tämä auttaa virastoa antamaan varoituksia, kun markkinoille tulee erityisen vaarallisia aineita, ja lisäämään tietoisuutta.

Komissio kehottaa Euroopan parlamenttia ja neuvostoa saattamaan kiireellisesti ja joka tapauksessa ennen nykyisen Euroopan parlamentin vaalikauden päättymistä päätökseen toimielinten väliset neuvottelut seuraavasta vireillä olevasta asiasta:

- ehdotus varainhoitoasetuksen uudelleenlaatimisesta.

Komissio kehottaa jäsenvaltioita

- jakamaan ennakoivasti tietoja komissiolle, kun ne ovat tietoisia EU:n rahoitusta hakeviin organisaatioihin liittyvistä mahdollisista riskeistä
- panemaan nopeasti täytäntöön vuosien 2023–2024 Schengen-syklin painopisteet turvallisemman ja vahvemman Schengen-alueen luomiseksi
- käsittelemään niitä vastaan vireillä olevia rikkomusmenettelyjä sen varmistamiseksi, että kyseinen lainsäädäntö saatetaan asianmukaisesti osaksi kansallista lainsäädäntöä.

<sup>56</sup> Algeria, Argentiina, Armenia, Bosnia ja Hertsegovina, Brasilia, Egypti, Israel, Jordania, Kolumbia, Libanon, Marokko, Tunisia ja Turkki.

## **VII. Päätelmät**

Viimeisten kolmen vuoden aikana on pyritty jatkuvasti ja määrätietoisesti edistämään EU:n turvallisuusunionin luomista. Turvallisuuspolitiikan kaikilla osa-alueilla on edistytty valtavasti. Jatkuvasti kehittyvien uhkien todellisuus vaatii nyt entistä motivoituneempia jatkuvia toimia. Lainsäädäntökehystä koskeva työ on saatava päätökseen hyvissä ajoin ennen vaalikauden päättymistä keväällä 2024. Jäsenvaltioilla on jatkuva velvollisuus saattaa uudet lait osaksi kansallista lainsäädäntöä, panna ne täytäntöön ja soveltaa niitä. Täytäntöönpano edellyttää yhteisiä toimia, myös EU:n virastojen tuella, ja hyvin usein yhä tiiviimpää yhteistyötä kansainvälisten kumppaniemme kanssa.

Voimme saavuttaa EU:ssa kansalaisten odottaman turvallisuustason ainoastaan kaikkien asianosaisten yhteisillä ja määrätietoisilla ponnisteluilla, ja nykyisessä tilanteessa jokaisen toimijan olisi asetettava etusijalle oma osuutensa EU:n turvallisuuden vahvistamisessa.