Euroopan unionin neuvosto

Bryssel, 3. huhtikuuta 2025
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	2. huhtikuuta 2025
Vastaanottaja:	Thérèse BLANCHET, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	COM(2025) 148 final
Asia:	KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE ProtectEU – eurooppalainen sisäisen turvallisuuden strategia

Valtuuskunnille toimitetaan oheisena asiakirja COM(2025) 148 final.

Liite: COM(2025) 148 final

EUROOPAN
KOMISSIO

Strasbourg 1.4.2025
COM(2025) 148 final

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

ProtectEU – eurooppalainen sisäisen turvallisuuden strategia

1. ProtectEU: eurooppalainen sisäisen turvallisuuden strategia

Turvallisuus on peruskallio, jolle kaikki vapautemme rakentuvat. Demokratia, oikeusvaltioperiaate, perusoikeudet, eurooppalaisten hyvinvointi, kilpailukyky ja vauraus ovat kaikki riippuvaisia siitä, miten pystymme takaamaan perusturvallisuuden. Tänä turvallisuusuhkien aikana EU:n jäsenvaltioiden kyky taata ihmisten turvallisuus riippuu enemmän kuin koskaan **yhtenäisestä EU:n toimintamallista sisäisen turvallisuutemme suojelemiseksi**. Muuttuvassa geopoliittisessa toimintaympäristössä Euroopan on jatkossakin pidettävä lupauksensa rauhasta.

Ensimmäiset askeleet eurooppalaisen turvallisuuskoneiston rakentamiseksi on jo otettu. Olemme viimeisten kymmenen vuoden aikana parantaneet unionin kollektiivisia toimintamekanismeja lainvalvonnan ja oikeudellisen yhteistyön, rajaturvallisuuden, vakavan ja järjestäytyneen rikollisuuden torjunnan, terrorismin ja väkivaltaisten ääriliikkeiden torjunnan sekä EU:n fyysisen ja digitaalisen kriittisen infrastruktuurin suojelun osa-alueilla. Aiemmin hyväksytyn lainsäädännön ja aiemmin laaditun politiikan asianmukainen täytäntöönpano on edelleen keskeistä.

Tämänhetkisten uhkien luonne ja luontainen yhteys EU:n sisäisen ja ulkoisen turvallisuuden välillä edellyttävät, että teemme enemmän.

Uhkakuva on synkkä. Raja **hybridiuhkien** ja avoimen sodankäynnin välillä hämärtyy. Venäjä on käynyt EU:ta ja sen kumppaneita vastaan verkossa ja sen ulkopuolella hybridikampanjaa, jonka tarkoituksena on häiritä ja heikentää yhteiskunnallista yhteenkuuluvuutta ja demokraattisia prosesseja sekä testata EU:n solidaarisuutta Ukrainaa kohtaan. Vihamieliset vieraat valtiot ja niiden tukemat toimijat pyrkivät soluttautumaan kriittiseen infrastruktuuriin ja toimitusketjuihin ja häiritsemään niitä, anastamaan arkaluonteista tietoa ja hankkiutumaan asemaan, jossa niiden mahdollisuudet tehdä tuhoa tulevaisuudessa ovat maksimaaliset. Ne käyttävät rikollisuutta palveluna ja rikollisia välikäsinään. Toimitusketjujen osalta riippuvuus kolmansista maista tekee meistä myös haavoittuvampia vihamielisten valtioiden hybridikampanjoiden edessä.

Euroopassa leviää vahvoja **järjestäytyneen rikollisuuden verkostoja**, joita ruokitaan verkossa. Ne levittäytyvät talouteemme ja vaikuttavat yhteiskuntaamme, kuten Europolin äskettäin esittämässä vakavaa ja järjestäytynyttä rikollisuutta koskevassa EU:n uhkakuva-arviossa (SOCTA)[1] tuodaan esiin. Kun järjestäytynyt rikollisuus on saanut jalansijaa yhteisössä tai taloudessa, sen kitkemisestä tulee pitkä taistelu: kolmasosa suurimman uhkan aiheuttavista rikollisverkostoista on toiminnassa yli kymmenen vuoden ajan. Ne pystyvät kryptovaluuttojen ja rinnakkaisten rahoitusjärjestelmien avulla pesemään rahaa ja piilottamaan rikoksien tuottaman hyödyn.

Terrorismin uhka on EU:ssa edelleen suuri. Alueellisilla kriiseillä EU:n ulkopuolella on heijastusvaikutuksia, ja ne motivoivat eri ideologioita edustavia terroristeja rekrytoimaan ja mobilisoimaan väkeä tai kehittämään valmiuksiaan. Terroristit kohdistavat radikalisointi- ja rekrytointitoimintaansa erityisesti yhteiskunnan haavoittuvimpiin osiin ja tiettyihin nuoriin. Ne innoittavat yksittäisiä toimijoita iskuihin ja synnyttävät järjestelmävastaisia ääriliikkeitä, joiden tavoitteena on tuhota demokraattinen oikeusjärjestys.

Turvallisuuskoneistomme parantamisessa **teknologisen kehityksen** harppaukset ovat tärkeitä. Kyberhyökkäyksiä ja ulkomaista tiedonmanipulointia esiintyy kuitenkin yhä enemmän, ja niissä hyödynnetään tekoälyn kaltaisia uusia teknologioita. Erityisesti lapsiin, nuoriin ja

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

vanhempiin ihmisiin kohdistuu riskejä verkossa, jossa myös vihapuheen leviäminen uhkaa sananvapautta ja sosiaalista yhteenkuuluvuutta.

Yhä useammasta eurooppalaisesta tuntuu siltä, että elämä ei ole enää yhtä turvallista kuin aiemmin, ja **käsitys turvallisuudesta EU:ssa** on heikentynyt siinä määrin, että kysyttäessä tulevaisuudesta 64 prosenttia on huolissaan EU:n turvallisuudesta.[2] Huoli kasvaa myös yrityksissä: väärä ja tarkoituksella harhaanjohtava tieto, rikollisuus ja laiton toiminta sekä kybervakoilu on mainittu vuonna 2025 laaditussa maailmanlaajuisia riskejä koskevassa Maailman talousfoorumin raportissa[3] kymmenen suurimman riskin joukossa.

Eurooppalaisten olisi **voitava elää elämäänsä ilman pelkoa** niin kotona kuin julkisilla paikoilla, liikkuessaan kaduilla, kulkiessaan metrolla tai surffaillessaan internetissä. EU:n turvallisuustyössä on keskeistä, että erityisesti niitä, jotka ovat kaikkein haavoittuvaisimpia, suojellaan iskuilta, joilla on taipumusta vaikuttaa suhteettomasti lapsiin, naisiin ja vähemmistöihin, kuten juutalais- ja muslimiyhteisöihin. Tämä on selviytymiskykyisten ja yhteenkuuluvuutta edistävien yhteiskuntien rakentamisessa olennaista.

Komissio esittää **eurooppalaisen sisäisen turvallisuuden strategian**, jotta uhkia voitaisiin torjua paremmin. Tiukentamalla lainsäädäntöä, syventämällä yhteistyötä ja lisäämällä tiedonvaihtoa voimme parantaa selviytymiskykyämme ja kollektiivista kykyämme ennakoida, ehkäistä ja havaita turvallisuusuhkia ja reagoida niihin. Yhtenäisellä sisäisen turvallisuuden toimintamallilla voidaan auttaa jäsenvaltioita hyödyntämään teknologian mahdollisuuksia niin, että turvallisuus paranee eikä heikkene, ja myötävaikuttaa siihen, että digitaalinen ympäristö on kaikille turvallinen. Lisäksi sillä tuetaan jäsenvaltioiden yhteistä reagointia unionin sisäiseen turvallisuuteen vaikuttaviin maailmanlaajuisiin poliittisiin ja taloudellisiin muutoksiin.

Strategiaa ohjaa **kolme periaatetta**, ja sen ytimessä on oikeusvaltioperiaatteen ja perusoikeuksien kunnioittaminen.

Ensinnäkin päämääräksi asetetaan turvallisuuskulttuurin muuttaminen. Tarvitsemme **koko yhteiskunnan kattavan lähestymistavan**, jossa ovat mukana kaikki kansalaiset ja sidosryhmät, kuten kansalaisyhteiskunta, tutkimusmaailma, korkeakoululaitos ja yksityiset tahot. Näin ollen strategiaan kuuluvissa toimissa sovelletaan aina kun mahdollista yhdennettyä lähestymistapaa, jota useat sidosryhmät toteuttavat.

Toiseksi **turvallisuusnäkökohdat on otettava mukaan ja valtavirtaistettava kaikkeen EU:n lainsäädäntöön, politiikkaan ja ohjelmiin**, myös EU:n ulkosuhteissa. Kun lainsäädäntöä, politiikkaa ja ohjelmia valmistellaan, tarkastellaan uudelleen, pannaan täytäntöön ja toteutetaan, turvallisuusnäkökulma on pidettävä mielessä ja varmistettava, että tarvittavat turvallisuusnäkökohdat otetaan huomioon, jotta voidaan edistää johdonmukaista ja kattavaa lähestymistapaa turvallisuuteen.

Kolmanneksi turvallinen ja häiriönsietokykyinen Eurooppa edellyttää **EU:lta, sen jäsenvaltioilta ja yksityiseltä sektorilta merkittäviä investointeja**. Jotta tässä strategiassa esitetyt tavoitteet ja toimet voidaan toteuttaa, tarvitaan riittävästi henkilöresursseja ja varoja. Kuten seuraavaa monivuotista rahoituskehystä koskevassa tiedonannossa[4] todetaan, Euroopan on lisättävä turvallisuuden julkista rahoitusta ja edistettävä turvallisuustutkimusta ja -investointeja sekä vahvistettava strategista riippumattomuuttaan.

[2] Flash-eurobarometri FL550: EU:n haasteet ja painopisteet.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, s. 17.
[4] COM (2025) 46 final.

Strategia täydentää **varautumisunionistrategiaa**[5], jossa esitetään kaikki vaarat kattava yhtenäinen lähestymistapa, jolla varaudutaan ihmisen aiheuttamiin konflikteihin, luonnonkatastrofeihin ja kriiseihin, sekä **valkoista kirjaa Euroopan puolustusvalmiudesta vuoteen 2030 mennessä**[6], jolla tuetaan kaikkialla EU:ssa puolustusvoimavarojen kehittämistä ja hankkimista pelotteeksi ulkomaisille vastapuolille. Komissio aikoo ehdottaa myös **eurooppalaista demokratian kilpeä**, jolla vahvistetaan EU:n demokratioiden selviytymiskykyä. Näissä aloitteissa esitetään visio turvallisesta ja selviytymiskykyisestä EU:sta.

EU:n sisäisen turvallisuuden uudenlainen hallinta

Komissio tekee tiivistä yhteistyötä jäsenvaltioiden ja EU:n virastojen kanssa EU:n sisäisen turvallisuuden toimintamallin parantamiseksi sekä strategisella että operatiivisella tasolla.

Tässä yhteydessä

- **määritetään aina komission uusiin ja tarkistettaviin aloitteisiin liittyvät mahdolliset turvallisuus- ja varautumisnäkökohdat alusta lähtien ja koko neuvotteluprosessin ajan**
- **pidetään säännöllisesti Euroopan sisäistä turvallisuutta käsittelevän komission hankeryhmän kokouksia ja tuetaan ryhmän työtä komission sisällä tehtävällä strategisella monialaisella yhteistyöllä**
- **esitetään sisäiseen turvallisuuteen liittyviä uhka-analyyseja turvallisuusasioita käsittelevän kollegion työn tueksi**
- **keskustellaan neuvostossa jäsenvaltioiden kanssa muuttuvista sisäisen turvallisuuden haasteista uhka-analyysin pohjalta ja vaihdetaan ajatuksia keskeisistä politiikan painopisteistä**
- **raportoidaan säännöllisesti Euroopan parlamentille ja neuvostolle, jotta keskeisten turvallisuusaloitteiden järjestelmällistä toteuttamista voidaan seurata ja tukea**

2. Yhdennetty tilannekuva ja uhka-analyysi

Annamme EU:lle uusia tapoja jakaa ja yhdistää tietoja ja toimitamme säännöllisesti EU:n sisäisen turvallisuuden uhka-analyysin, jota hyödynnetään kattavassa riski- ja uhka-arvioinnissa.

Turvallisuus perustuu **toimivaan ennakointiin**. EU:n on tukeuduttava tässä kattavaan, riittävän riippumattomaan, ajantasaiseen tilannekuvaan ja uhka-analyysiin. Käyttökelpoinen tiedustelutieto, jota jäsenvaltioita kannustetaan edelleen parantamaan tiedonhankinnan keskitettynä yhteyspisteenä toimivan yhtenäisen tiedustelun analysointikyvyn (SIAC) avulla, on ratkaisevan tärkeää, jotta voidaan arvioida ja torjua uhkia ja viime kädessä antaa aineksia politiikkaa ja lainsäädäntöä koskeviin toimiin[7]. **Tiedusteluun perustuvia analyyseja** ja **uhka-arvioita** on hyödynnettävä EU:n tasolla tuloksellisemmin ja yhteistyössä.

[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.
[7] Safer Together – raportti EU:n siviili- ja puolustusvarautumisen parantamisesta, s. 23.

Komissio aikoo laatia EU:n tasolla ja tietyille aloille tehtyjen erilaisten riski- ja uhka-arvioiden[8] pohjalta **säännöllisesti EU:n sisäisen turvallisuuden uhka-analyyseja**, joissa määritetään tärkeimmät turvallisuushaasteet. Tarkoituksena on tuottaa tietoa politiikan painopisteiden määrittämiseen. Näiden uhka-analyysien avulla tullaan kehittämään ketterää ja reagoivaa sisäisen turvallisuuden politiikkaa, jolla tuloksellisesti torjutaan muuttuvia uhkia, parannetaan ihmisten ja yritysten suojelua hyökkäyksiltä ja mahdollistetaan oikea-aikaiset kohdennetut politiikkatoimet. Näistä EU:n sisäisen turvallisuuden uhka-analyyseista saadaan aineksia myös **kattavaan (eli monialaiseen ja kaikki vaarat huomioivaan) EU:n riski- ja uhka-arviointiin**, jonka komissio ja korkea edustaja laativat varautumisunionistrategiaa noudattaen.

Tiedon jakamisessa luottamus ja tietojen turvallinen käsittely ovat olennaisen tärkeitä, ja ne edellyttävät luotettavaa ja suojattua infrastruktuuria. EU:n toimielinten, elinten ja virastojen on varmistettava, että ne voivat käyttää **suojattuja viestintäkanavia**, kun ne jakavat arkaluonteisia ja turvallisuusluokiteltuja tietoja toisilleen ja jäsenvaltioille. Investoinnit **yhteentoimiviin suojattuihin järjestelmiin** ja luotettavaan teknologiaan vahvistavat EU:n riippumattomuutta ja EU:n kykyä hallita kriisejä ja varmistaa operatiivinen häiriönsietokyky. Tässä yhteydessä komissio kehottaa lainsäätäjiä saattamaan päätökseen neuvottelut **asetusehdotuksesta, joka koskee tietoturvallisuutta unionin toimielimissä, elimissä ja laitoksissa**[9]. Näin voidaan varmistaa muun muassa, että EU:lla on yhteinen säännöstö arkaluonteisten turvallisuusluokittelemattomien ja turvallisuusluokiteltujen tietojen käsittelylle.

Oman operatiivisen turvallisuutensa ja tilannetietoisuutensa varmistamiseksi komissio aikoo tarkistaa omaa turvallisuuden hallintajärjestelmäänsä ja perustaa **yhdennetyn turvallisuusoperaatiokeskuksen (ISOC)** suojelemaan ihmisiä, fyysistä omaisuutta ja operaatioita kaikissa komission toimipaikoissa. Komissio aikoo myös parantaa operatiivisia ja analyyttisia valmiuksiaan tunnistaa ja lieventää hybridiuhkia.

Varautumis- ja turvallisuusnäkökohdat huomioidaan kaikissa EU:n säädöksissä, politiikoissa ja ohjelmissa varautumisunionistrategiaa noudattaen. Kun komissio valmistelee tai tarkastelee uudelleen lainsäädäntöä, politiikkoja tai ohjelmia varautumis- ja turvallisuusnäkökulma mielessään, se määrittää aina parhaaksi arvioidun toimintavaihtoehdon mahdolliset vaikutukset varautumiseen ja turvallisuuteen. Tätä tuetaan komission politiikan laatijoille säännöllisesti annettavalla koulutuksella.

Tukeakseen jäsenvaltioita komissio keskustelee neuvoston kanssa muuttuvista sisäisen turvallisuuden haasteista ja keskeisistä politiikan prioriteeteista ja tiedottaa sille säännöllisesti strategian toteuttamisesta. Lisäksi komissio pitää Euroopan parlamentin ja sidosryhmät ajan tasalla ja ottaa ne mukaan kaikkiin asiaankuuluviin toimiin.

Keskeiset toimet

Komissio aikoo

- **laatia ja esittää säännöllisesti uhka-analyyseja EU:n sisäisen turvallisuuden haasteista**

Jäsenvaltioita kehotetaan

[8] Alakohtaisia uhka-arvioita, joista uhka-analyysiin saadaan tietoa, ovat muun muassa vakavaa ja järjestäytynyttä rikollisuutta koskeva EU:n uhkakuva-arvio (SOCTA), selvitys terrorismitilanteesta ja -suuntauksista EU:ssa (TE-SAT), yhteinen kyberarviointiraportti (JCAR) sekä tulevat rahanpesuun ja terrorismin rahoitukseen liittyviä uhkia, riskejä ja menetelmiä koskevat arviot, jotka komission ja rahanpesuntorjuntaviranomaisen on määrä tehdä.

[9] COM (2022)119 final.

- **parantamaan tiedustelutietojen jakamista yhtenäisen tiedustelun analysointikyvyn (SIAC) kanssa ja varmistamaan parempi tietojen jakaminen EU:n virastojen ja elinten kanssa**

Euroopan parlamenttia ja neuvostoa kehotetaan

- **viemään päätökseen neuvottelut asetusehdotuksesta, joka koskee tietoturvallisuutta unionin toimielimissä, elimissä ja laitoksissa**

3. EU:n turvallisuusvalmiuksien vahvistaminen

Kehitämme uusia työkaluja lainvalvontaan, esimerkiksi uudistamalla Europolia, ja parannamme keinoja koordinoida toimintaa ja keinoja varmistaa, että datanvaihto on suojattua ja pääsy dataan on laillista.

Jotta EU voi tuloksellisesti torjua muuttuvia uhkia, sen on parannettava turvallisuusvalmiuksiaan ja edistettävä innovointia. Koska lainvalvonta- ja oikeusviranomaiset ovat ensisijaisia toimijoita sisäisten turvallisuusuhkien torjunnassa, ne tarvitsevat oikeanlaiset operatiiviset välineet ja valmiudet toimiakseen nopeasti ja vaikuttavasti. On tärkeää, että näillä viranomaisilla on mahdollisuus viestiä ja koordinoida toimintaansa valtioiden rajojen yli ja eri viranomaisten välillä, jotta rikoksia voidaan tehokkaasti ehkäistä, havaita ja tutkia ja nostaa niistä syytteitä.

EU:n sisäisen turvallisuuden virastot ja elimet

Oikeuden, sisäasioiden ja kyberturvallisuuden alalla toimivilla EU:n virastoilla ja elimillä on EU:n turvallisuusrakenteessa keskeinen rooli, joka kasvaa edelleen virastojen ja elinten tehtävien laajentuessa.

Tänään, 25 vuotta perustamisensa jälkeen, **Europol** on EU:n turvallisuusrakenteessa tärkeämpi kuin koskaan. Se tukee monimutkaisia valtioiden rajat ylittäviä tutkintatoimia, helpottaa tiedonvaihtoa, kehittää innovatiivisia välineitä poliisitoimintaan ja tarjoaa kehittynyttä asiantuntemusta lainvalvontaan. On kuitenkin monia tekijöitä, jotka estävät Europolia hyödyntämästä koko operatiivista potentiaaliaan valtioiden rajat ylittävän rikollisuuden torjumiseksi toteutettavien tutkinta- ja operatiivisten toimien tukemisessa. Näiden tekijöiden kirjo ulottuu resurssien riittämättömyydestä siihen, että sen tämänhetkinen toimeksianto ei kata uusia turvallisuusuhkia, kuten sabotointia, hybridiuhkia tai tiedon manipulointia. Siksi komissio aikookin ehdottaa **Europolin toimeksiannon kunnianhimoista tarkistamista**, jotta siitä tulisi aidosti operatiivinen poliisivirasto, joka tukee jäsenvaltioita paremmin. Tavoitteena on vahvistaa Europolin teknistä asiantuntemusta ja valmiuksia tukea kansallisia lainvalvontaviranomaisia, parantaa koordinointia muiden virastojen ja elinten sekä jäsenvaltioiden kanssa, vahvistaa strategisia kumppanuuksia kumppanimaiden ja yksityisen sektorin kanssa sekä varmistaa, että Europoliin kohdistuvaa valvontaa vahvistetaan.

Lisäksi komissio pyrkii entisestään **parantamaan sisäisen turvallisuuden alalla toimivien EU:n virastojen ja elinten vaikuttavuutta ja täydentävyyttä ja vahvistamaan saumatonta yhteistyötä** niiden välillä.

Eurojustin toimeksiantoa tullaan arvioimaan ja vahvistamaan oikeudellisen yhteistyön vaikuttavuuden lisäämiseksi parantaen näin täydentävyyttä ja yhteistyötä Europolin kanssa. Tähän sisältyy Eurojustin tehokkuuden ja sen valmiuksien parantaminen, jotta se voi tarjota ennakoivaa tukea ja analysointia jäsenvaltioiden oikeusviranomaisille. Lisäksi, koska **EPPOlla** on ainutlaatuinen toimivalta tutkia unionin taloudellisia etuja vahingoittavia rikoksia ja nostaa niistä syytteitä, komissio aikoo pohtia, miten EPPOn valmiuksia suojata unionin varoja voidaan parhaiten parantaa. Tähän kuuluu myös EPPOn ja Europolin välisen yhteistyön vahvistaminen.

Tehokas ja suojattu tietojenvaihto virastojen välillä on yhteistyön kannalta ratkaisevan tärkeää. Europol ja Frontex tarvitsevat tammikuussa 2024 antamansa yhteisen lausunnon[10] jatkotoimena nopeaa keskinäistä tietojenvaihtoa, myös operatiivisia tarkoituksia varten. **eu-LISAlla** on keskeinen rooli datan suojatun tallentamisen ja saatavuuden varmistamisessa virastojen välisen tietojenvaihdon paremman koordinoinnin ja tehostamisen osalta. **EU:n perusoikeusvirasto** tarjoaa perusoikeuksien suojelua koskevaa asiantuntemusta turvallisuustoimenpiteiden kehittämiseen ja toteuttamiseen.

EU:n rahanpesuntorjuntaviranomaiselle (AMLA) on annettu valtuudet verrata tietoja osuma /ei osumaa -periaatteella tietoihin, joita Europol, EPPO, Eurojust ja EU:n petostentorjuntavirasto asettavat saataville, jotta ne voivat tehdä yhteisiä analyyseja valtioiden rajat ylittävistä tapauksista.

ENISAlla on keskeinen rooli EU:n kyberturvallisuuslainsäädännön täytäntöönpanossa. Komissio aikoo tulevassa **kyberturvallisuusasetuksen tarkistuksessa** arvioida sen toimeksiantoa ja ehdottaa sen nykyaikaistamista EU:n tason lisäarvon vahvistamiseksi.

Tulliviranomaisten ja muiden lainvalvontaviranomaisten välinen yhteistyö lisääntyy, kun EU:n tulliuudistuspaketissa ehdotetut **EU:n tulliviranomainen** ja **EU:n tullidatakeskus** perustetaan. Tulevalta keskukselta saatavat tiedot ja niihin liittyvä Europolin, Eurojustin, EPPOn, OLAFin, rahanpesuntorjuntaviranomaisen ja Frontexin toimivaltuuksien piiriin kuuluva data parantavat yhteistä analysointia ja osaltaan lisäävät operatiivisten toimien johdonmukaisuutta erityisesti ulkorajoilla. Komissio kannustaa lainsäätäjiä saattamaan neuvottelut EU:n tulliuudistuksesta nopeasti päätökseen ja avustaa niitä edelleen tässä asiassa.

EPPOn, OLAFin, Europolin, Eurojustin, rahanpesuntorjuntaviranomaisen ja ehdotetun EU:n tulliviranomaisen tekemän työn keskinäisen täydentävyyden parantamisessa tukeudutaan myös **EU:n petostentorjuntarakenteen** käynnissä olevan uudelleentarkastelun tuloksiin. Sisäiselle turvallisuudelle voi olla hyötyä tästä kokonaisvaltaisesta toimintamallista, jossa keskitytään sekä rikosoikeudellisten että hallinnollisten keinojen parempaan käyttöön, tietojärjestelmien yhteentoimivuuteen ja yhteistyön parantamiseen.

Kriittinen viestintä

Tällä hetkellä **kriittisen viestinnän järjestelmiä**[11] käytetään useimmissa tapauksissa erillisinä kansallisella tasolla. Tämä tarkoittaa sitä, että ensitoimijat eivät useinkaan voi viestiä kollegoidensa kanssa ylittäessään rajan toiseen jäsenvaltioon. Joissakin jäsenvaltioissa myös erityyppisten ensitoimijoiden (esim. poliisin ja ambulanssien) välistä viestintää on rajoitettu. Useimpien järjestelmien standardit eivät täytä tämänhetkisiä toiminnallisuutta ja häiriönsietokykyä koskevia vaatimuksia, mikä rajoittaa merkittävästi ensitoimijoiden reagointikykyä erityisesti valtioiden rajat ylittävissä tilanteissa.

Parantaakseen EU:n valmiuksia reagoida kriiseihin komissio aikoo ehdottaa lainsäädäntöä, jolla perustetaan **eurooppalainen kriittisen viestinnän järjestelmä (EUCCS)** jäsenvaltioiden seuraavan sukupolven kriittisen viestinnän järjestelmien liittämiseksi yhteen. Tarkoituksena on, että EUCCS perustuu kolmeen strategiseen pilariin: operatiiviseen liikkuvuuteen, vahvaan häiriönsietokykyyn ja strategiseen riippumattomuuteen. EUCCS-aloitteessa tullaan asettamaan yhdenmukaiset vaatimukset jäsenvaltioiden kriittisen viestinnän järjestelmille ja autetaan nykyaikaistamaan niitä, jotta ne voivat toimia saumattomasti. Myös järjestelmän kattavuutta

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

[11] Näitä ovat lainvalvontaviranomaisten, rajavartijoiden, tulliviranomaisten, pelastuspalvelun, palokuntien, ensivasteen työntekijöiden ja muiden yleisen turvallisuuden kannalta keskeisten toimijoiden käyttämät verkostot.

laajennetaan tulevan monikiertorataisen IRIS[2] [12]-järjestelmän avulla. EU:n rahoittamilla hankkeilla kehitetään EUCCS:n teknisiä valmiuksia pääasiassa eurooppalaisiin teknologian tarjoajiin turvautuen, jotta voidaan edistää EU:n strategista riippumattomuutta tällä herkällä alalla.

Laillinen datan saatavuus

Lainvalvonta- ja oikeusviranomaisten on voitava tutkia rikoksia ja toteuttaa toimia niiden torjumiseksi. Tällä hetkellä lähes kaikista vakavan ja järjestäytyneen rikollisuuden muodoista jää digitaalinen jalanjälki.[13] Nykyään noin 85 prosenttia rikostutkintatoimista perustuu lainvalvontaviranomaisten mahdollisuuksiin saada digitaalista tietoa.[14]

Tehokkaan lainvalvonnan edellyttämää tietojen saatavuutta käsittelevä korkean tason työryhmä korosti loppuraportissaan[15], että lainvalvonta ja oikeuslaitos ovat joutuneet antamaan jalansijaa rikollisille viimeisten kymmenen vuoden aikana rikollisten hyödyntäessä välineitä ja tuotteita, jotka ovat peräisin muilta lainkäyttöalueilta palveluntarjoajilta, jotka ovat ottaneet käyttöön toimenpiteitä, joilla on viety mahdollisuus tehdä yhteistyötä laillisten pyyntöjen osalta yksittäisissä rikostapauksissa. Järjestelmällinen yhteistyö lainvalvontaviranomaisten ja yksityisten tahojen välillä, palveluntarjoajat mukaan lukien, on sen vuoksi olennaisen tärkeää tulevissa pyrkimyksissä päästä eroon kaikkein uhkaavimmista rikollisverkostoista ja rikollisista unionissa ja sen ulkopuolella.

Koska digitalisaatio ulottuu koko ajan laajemmalle ja tarjoaa rikollisille jatkuvasti uusia välineitä, on olennaisen tärkeää luoda datan käyttöä koskeva säännöstö, joka vastaa tarpeeseen valvoa lainsäädäntömme noudattamista ja suojata arvojamme. Yhtä tärkeää on huolehtia siitä, että digitaaliset järjestelmät pysyvät suojassa luvattomalta käytöltä, jotta voidaan ylläpitää kyberturvallisuutta ja suojautua uusilta turvallisuusuhkilta. Tällaisissa käyttöoikeuksia koskevissa säännöissä on myös kunnioitettava perusoikeuksia ja varmistettava muun muassa yksityisyyden ja henkilötietojen asianmukainen suoja.

EU on viime vuosina toteuttanut toimia **verkkorikollisuuden torjumiseksi ja digitaalisen todistusaineiston saatavuuden helpottamiseksi kaikissa rikoksissa**, kun se on hyväksynyt sähköistä todistusaineistoa koskevat säännöt, joita sovelletaan kaikilta osin elokuusta 2026 alkaen.[16] Niitä tullaan täydentämään tiedon ja todistusaineiston vaihtoa koskevilla kansainvälisillä välineillä. Komissio ehdottaa piakkoin uuden **kyberrikollisuuden vastaisen YK:n yleissopimuksen** allekirjoittamista ja tekemistä.

Korkean tason työryhmän suositusten[17] noudattamiseksi komissio esittää vuoden 2025 alkupuoliskolla **etenemissuunnitelman, jossa esitetään lainsäädännölliset ja käytännön toimenpiteet**, joita se ehdottaa toteutettavan **datan laillisen ja tosiasiallisen saatavuuden varmistamiseksi**. Etenemissuunnitelman jatkotoimena komissio asettaa etusijalle **datan säilyttämistä koskevien sääntöjen** EU-tason vaikutusten arvioinnin ja **salausta koskevan teknologisen etenemissuunnitelman** valmistelun. Tarkoituksena on määrittää ja arvioida

[12] Resilienssiä, yhteenliitettävyyttä ja turvallisuutta satelliittien avulla parantava EU:n infrastruktuuri.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52019PC0070).
[15] Tehokkaan lainvalvonnan edellyttämää tietojen saatavuutta käsittelevän korkean tason työryhmän loppuraportti – 15.11.2024, 4802e306-c364-4154-835b-e986a9a49281_en.
[16] Euroopan parlamentin ja neuvoston asetus (EU) 2023/1543, annettu 12 päivänä heinäkuuta 2023, eurooppalaisista esittämismääräyksistä ja eurooppalaisista säilyttämismääräyksistä sähköisten todisteiden hankkimiseksi rikosoikeudellisissa menettelyissä ja rikosoikeudellisten menettelyjen perusteella annettujen vapaudenmenetyksen käsittävien rangaistusten täytäntöönpanoa varten, EUVL L 191, 28.7.2023.
[17] Neuvoston päätelmät tehokkaan lainvalvonnan edellyttämästä tietojen saatavuudesta (12. joulukuuta 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/fi/pdf..

teknisiä ratkaisuja, joiden avulla lainvalvontaviranomaiset voisivat käyttää salattua dataa laillisesti varmistaen kyberturvallisuuden ja kunnioittaen perusoikeuksia.

Operatiivinen yhteistyö

Komissio tekee yhteistyötä jäsenvaltioiden, EU:n virastojen ja elinten sekä kumppanimaiden kanssa vahvistaakseen operatiivista yhteistyötä, joka on olennaisen tärkeää, jotta voidaan lisätä kansainvälisen järjestäytyneen rikollisuuden ja terrorismin torjunnan vaikuttavuutta.

Euroopan monialainen rikosuhkien torjuntafoorumi (EMPACT) on saanut aikaan merkittäviä operatiivisia tuloksia. Se on EU:n tärkein kehys vakavan ja järjestäytyneen rikollisuuden vastaiselle yhteiselle toiminnalle. Seuraavalla EMPACT-kaudella 2026–2029 on tilaisuus vahvistaa tätä kehystä entisestään. Jotta kaikkein uhkaavimmista rikollisverkostoista ja rikollisista päästään eroon, unionin on virtaviivaistettava ja keskitettävä toimensa kiireellisimpiin prioriteetteihin, vahvistettava jäsenvaltioiden sitoumuksia ja varmistettava resurssien tuloksellinen käyttö.

Tätä varten komissio aikoo tehdä yhteistyötä neuvoston puheenjohtajavaltioiden ja jäsenvaltioiden kanssa, jotta voidaan **maksimoida EMPACTin potentiaali ja pureutua seuraavan EMPACT-kauden 2026–2029 keskeisiin prioriteetteihin**. Näillä painopistealoilla tarvitaan tiedustelutietoa kaikkein uhkaavimmista rikollisverkostoista, yhteisiä tutkintatoimia ja operatiivisia työryhmiä sekä vahvoja oikeuslaitoksen toimia, joihin kuuluu myös rahavirtojen seuraaminen. Lisäksi unionin on torjuttava rikollisten värväystä ja soluttautumista sekä vahvistettava virastojen välistä ja kansainvälistä lainvalvontayhteistyötä ja -koulutusta.

Komissio aikoo tukea myös muita **valtioiden rajat ylittävän operatiivisen lainvalvontayhteistyön muotoja jäsenvaltioiden ja Schengenin säännöstöön osallistuvien maiden välillä**. Schengen-alueella, jonka sisärajoilla ei tehdä tarkastuksia, tarvitaan tiivistä yhteistyötä ja tietojenvaihtoa jäsenvaltioiden lainvalvontaviranomaisten välillä sisäisen turvallisuuden korkean tason varmistamiseksi. Lainvalvontaviranomaisilla on edelleen haasteita, kun ne seuraavat tai toteuttavat kiireellisiä toimia toisessa valtiossa[18], ja myös hybridiuhkien torjunta edellyttää valtioiden rajat ylittävän yhteistyön parantamista. Yhteisen strategisen vision luomiseksi olisi perustettava **operatiivisen lainvalvontayhteistyön tulevaisuutta käsittelevä korkean tason työryhmä**.

Tehokas datanvaihto lainvalvontaviranomaisten välillä on olennaisen tärkeää myös tuloksellisen valtioiden rajat ylittävän yhteistyön kannalta. Kun **yhteentoimivuusarkkitehtuuri** on perustettu, se antaa lainvalvontaviranomaisille ja Europolille tosiasiallisen pääsyn keskeisiin tietoihin. Samalla EU:n ja sen jäsenvaltioiden olisi priorisoitava kahden- ja monenvälistä tietojenvaihtoa **Prüm II -asetuksen**[19] oikeudellisen ja teknisen täytäntöönpanon kautta yhteistyössä eu-LISAn ja Europolin kanssa. Tämä mahdollistaa sormenjälkien, DNA-tunnisteiden, ajoneuvorekisteritietojen, kasvokuvien ja rikosrekisteritietojen suojatun automaattisen vaihdon EU:n reitittimien kautta. Kansallisella tasolla jäsenvaltioiden on pantava täytäntöön **tietojenvaihtodirektiivi**[20], jolla parannetaan

[18] Tämä todetaan komission arviossa siitä, miten jäsenvaltiot ovat noudattaneet operatiivisesta lainvalvontayhteistyöstä 9 päivänä kesäkuuta 2022 annettua neuvoston suositusta (EU) 2022/915 (5909/25).

[19] Euroopan parlamentin ja neuvoston asetus (EU) 2024/982, annettu 13 päivänä maaliskuuta 2024, automaattisesta tietojen hausta ja -vaihdosta poliisiyhteistyössä sekä neuvoston päätösten 2008/615/YOS ja 2008/616/YOS ja Euroopan parlamentin ja neuvoston asetusten (EU) 2018/1726, (EU) 2019/817 ja (EU) 2019/818 muuttamisesta (Prüm II -asetus), EUVL L, 2024/982, 5.4.2024.

[20] Euroopan parlamentin ja neuvoston direktiivi (EU) 2023/977, annettu 10 päivänä toukokuuta 2023, jäsenvaltioiden lainvalvontaviranomaisten välisestä tietojenvaihdosta ja neuvoston puitepäätöksen 2006/960/YOS kumoamisesta, EUVL L 134, 22.5.2023, s. 1–24.

tiedonvaihtokanavia saumatonta valtioiden rajat ylittävää tiedonkulkua varten, samalla kun varmistetaan niiden integrointi unionin tason järjestelmiin, kuten SIENAan[21].

Tuloksellinen valtioiden rajat ylittävä yhteistyö perustuu myös **EU:n yhteisen lainvalvontakulttuurin** edistämiseen. Olennaisen tärkeitä tämän tavoitteen saavuttamiseksi ovat yhteinen koulutus, osaamiskeskukset ja vaihto-ohjelmat. Komissio aikoo selvittää, miten EU voi parhaiten tukea jäsenvaltioiden viranomaisille annettavaa koulutusta, tukeutuen **CEPOLiin**, joka on EU:n lainvalvontakoulutusvirasto.

Rajaturvallisuuden vahvistaminen

Ulkorajojen häiriönsietokyvyn ja turvallisuuden vahvistaminen on ratkaisevan tärkeää, jotta voidaan torjua hybridiuhkia, kuten muuttoliikkeen käyttöä aseena, estää uhkan muodostavien toimijoiden ja tavaroiden pääsy EU:hun ja tuloksellisesti torjua valtioiden rajat ylittävää rikollisuutta ja terrorismia. **Schengenin tietojärjestelmää (SIS) on tarkoitus parantaa** vuonna 2026, jotta jäsenvaltiot voivat kolmansien maiden Europolille jakaman datan perusteella tehdä kuulutuksia terrorismiin osallistuneista kolmansien maiden kansalaisista, kuten terrorismiin syyllistyvistä vierastaistelijoista, ja muihin vakaviin rikoksiin osallistuneista kolmansien maiden kansalaisista.

EU:n laajojen tietojärjestelmien parempi **yhteentoimivuus** antaa jäsenvaltioille olennaista tietoa kolmansista maista tulevista henkilöistä, jotka ylittävät tai aikovat ylittää ulkorajan, mikä auttaa viranomaisia arvioimaan maahantulon edellytyksiä jäsenvaltioiden alueelle[22]. Komissio jatkaa tiivistä yhteistyötä jäsenvaltioiden ja eu-LISAn kanssa, jotta nämä järjestelmät, erityisesti **rajanylitystietojärjestelmä (EES), Euroopan matkustuslupajärjestelmä (ETIAS) ja tarkistettu viisumitietojärjestelmä (VIS)** voidaan ottaa nopeasti käyttöön ja varmistaa niiden sujuva toiminta ja turvallisuushyödyt.

Jotta rajaturvallisuutta voitaisiin entisestään parantaa ja EU:n yhteistyötä lujittaa muuttuvien uhkien torjumiseksi, **komissio aikoo ehdottaa Frontexin vahvistamista**. Eurooppalainen raja- ja merivartiosto olisi vähitellen kolminkertaistettava vahvuudeltaan 30 000:een henkilöön. Valvontaa ja tilannetietoisuutta varten sillä olisi oltava käytössään kehittynyttä teknologiaa, kuten myös Euroopan yhdennetyn rajaturvallisuuden kannalta merkityksellistä tiedustelutietoa, ja rajavalvontaa varten sen olisi saatava pääsy vakaisiin EU:n maanhavainnointipalveluihin, jotka on määrä ottaa käyttöön vuoteen 2027 mennessä. Tällä tavoin voitaisiin entisestään parantaa kykyä havaita, ehkäistä ja torjua valtioiden rajat ylittävää rikollisuutta ulkorajoilla ja vahvistaa tukea jäsenvaltioille palauttamisten toteuttamisessa, erityisesti turvallisuusriskin aiheuttavien kolmansien maiden kansalaisten osalta.

Asiakirja- ja henkilöllisyyspetokset helpottavat maahantulijoiden salakuljetusta, ihmiskauppaa, laitonta rikollista liikkumista ja laittomien tavaroiden kauppaa. Kun **rinnakkaishenkilöllisyyksien tunnistin (MID)**[23] on toiminnassa, se parantaa kansallisten viranomaisten kykyä tunnistaa henkilöt, jotka käyttävät rinnakkaishenkilöllisyyksiä, ja torjua henkilöllisyyspetoksia. Komissio aikoo tutkia keinoja parantaa EU:n kansalaisille ja

[21] Suojatun tiedonvaihdon verkkosovellus.

[22] Rajanylitystietojärjestelmän (EES) avulla jäsenvaltiot voivat määrittää kolmansien maiden kansalaisten henkilöllisyyden Schengen-alueen ulkorajoilla ja rekisteröidä heidän maahantulonsa ja maastalähtönsä, minkä ansiosta on mahdollista järjestelmällisesti tunnistaa sallitun oleskeluajan ylittäneet henkilöt. Euroopan matkustustieto- ja -lupajärjestelmän (ETIAS) ja viisumitietojärjestelmän (VIS) avulla jäsenvaltiot voivat arvioida ennen kolmannen maan kansalaisen saapumista ulkorajalle, aiheuttaako hänen oleskelunsa EU:n alueella turvallisuusriskin.

[23] MID on yksi asetuksella (EU) 2019/818 ja asetuksella 2019/817 käyttöön otetuista yhteentoimivuuskomponenteista.

kolmansien maiden kansalaisille myönnettävien matkustus- ja oleskeluasiakirjojen turvallisuutta. Lisäksi komissio arvioi, miten EU:n digitaalisen identiteetin lompakot, jotka on määrä ottaa käyttöön eurooppalaisen digitaalisen identiteetin kehyksen puitteissa vuoden 2026 loppuun mennessä, voivat osaltaan parantaa matkustusasiakirjojen turvallisuutta ja henkilöllisyyden todentamista. Tämä täydentää digitaalisia matkustustunnisteita ja EU:n digitaalista matkustussovellusta koskevia ehdotuksia[24].

Matkustustiedot ovat viranomaisille ratkaisevan tärkeitä, jotta ne voivat tunnistaa ja tutkia rikollisten, terroristien ja muiden turvallisuusuhkia aiheuttavien henkilöiden liikkeitä. Vaikka kaupalliseen lentomatkustukseen liittyviä tietoja varten on olemassa EU:n säännöstö[25], muita liikennemuotoja koskevan datan käsittely lainvalvontatarkoituksessa on hajanaista. Rikolliset ja terroristit voivat näin ollen paljastumatta hyödyntää eri liikennemuotoja laittomaan toimintaan. Komissio aikoo tehdä yhteistyötä jäsenvaltioiden ja liikenteen toimialan kanssa **matkustustietosäännöstön vahvistamiseksi**. Tarkoituksena on tehdä selvitys unionin järjestelmästä, jossa yksityislentotoiminnan harjoittajat velvoitettaisiin keräämään ja siirtämään matkustajadataa, arvioida matkustajarekisteritietojen käsittelyä koskevia sääntöjä ja tutkia, miten meriliikenteen matkustustietojen käsittelyä voitaisiin sujuvoittaa. Maantieliikenteen osalta komissio aikoo selvittää **rekisterikilpien automaattisten tunnistusjärjestelmien (ANPR)** laajempaa käyttöä ja lisätä mahdollisuuksia synergiaan SIS-järjestelmän kanssa.

Ennakointi, innovointi ja voimavaravetoinen toimintamalli

Komissio kehittää EU:n tasolla **kattavan ennakointiin perustuvan sisäisen turvallisuuden toimintamallin**, joka perustuu kansallisella tasolla määritettyihin parhaisiin käytäntöihin. Tällä toimintamallilla tuetaan päätöksentekoa ja ohjataan investointeja EU:n rahoittamaan turvallisuustutkimukseen ja -innovointiin.

Tutkimuksella ja innovoinnilla on keskeinen rooli sisäisessä turvallisuudessa, sillä niiden avulla voidaan luoda ratkaisuja, joilla voidaan torjua uusia uhkia, kuten teknologian väärinkäyttöä[26]. EU:n täytyy jatkaa EU:n rahoittaman turvallisuustutkimuksen ja -innovoinnin[27] avulla investoimista innovatiivisten välineiden ja ratkaisujen kehittämiseen turvallisuusuhkien torjumiseksi noudattaen samalla EU:n sääntöjä ja perusoikeuksia. Komission olisi tuettava tutkimustulosten siirtämistä käytäntöön, jotta tällaisten modernien voimavarojen käyttöönotto voidaan varmistaa, ja asetettava etusijalle tekoälyn kaltaiset **nykyteknologiat**. Jotta lainvalvonta- ja oikeusviranomaiset voivat paremmin hyödyntää tekoälyjärjestelmiä ja muita teknisiä voimavaroja, tähän toimintamalliin olisi sisällyttävä koulutusta. Lisäksi teknologioiden kaksikäyttöpotentiaalia olisi tarvittaessa hyödynnettävä molempiin suuntiin (siviilipuolelta puolustukseen ja puolustuksesta siviilikäyttöön)[28].

Sisäisen turvallisuuden EU-innovaatiokeskus[29], innovaatiolaboratorioiden verkosto, joka tukee sisäisen turvallisuuden toimijoiden työtä EU:ssa ja jäsenvaltioissa uusimmilla innovaatiopäivityksillä ja toimivilla ratkaisuilla, auttaa sisällyttämään tutkimustyön tulokset käytännön toimintaan ja politiikkaan. Europolin työn vaikuttavuuden parantaminen edellyttää Europolin ohjelmistotyökalupakin (ETR) vahvistamista, jotta sen on mahdollista tunnistaa ja

[24] https://ec.europa.eu/commission/presscorner/detail/fi/ip_24_5047.
[25] Matkustajarekisteriä (PNR) ja matkustajien ennakkotietoja (API) koskeva säännöstö, joka sisältyy direktiiviin (EU) 2016/681 (PNR-direktiivi) ja asetuksiin (EU) 2025/12 ja (EU) 2025/13 (API-asetukset).
[26] Ks. komission Yhteisen tutkimuskeskuksen raportti ”Emerging risks and opportunities for EU internal security from new technologies”, https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025, https://data.europa.eu/doi/10.2837/0004501.
[28] Niinistön raportin mukaisesti.
[29] Sisäisen turvallisuuden EU-innovaatiokeskus | Europol.

kehittää kehittyneitä teknologioita, hankkia niitä yhdessä ja soveltaa operatiivisesti. Lisäksi komissio perustaa yhteisen tutkimuskeskuksensa yhteyteen tutkijoita yhteen kokoavan **turvallisuustutkimus- ja innovointikampuksen**, jotta voitaisiin lyhentää aikaa, joka kuluu tutkimustuloksista innovointiin, kehittämiseen ja onnistuneeseen toteutukseen ja samalla vähentää kehittämis-, testaus- ja validointikustannuksia.

Eurooppalainen tutkimusalueemme on luonteeltaan yhteistyöhön perustuva, joten se on altis ulkomaiselle sekaantumiselle ja disinformaatiolle. Neuvoston hyväksyttyä suosituksen tutkimuksen turvallisuudesta[30] komissio ja jäsenvaltiot toteuttavat toimenpiteitä toimijoiden vaikutusmahdollisuuksien lisäämiseksi muun muassa perustamalla tutkimuksen turvallisuuteen keskittyvän osaamiskeskuksen.

Keskeiset toimet

Komissio aikoo hyväksyä

- **vuonna 2026 lainsäädäntöehdotuksen, jolla muutetaan Europol aidosti toimintakykyiseksi lainvalvontavirastoksi**
- **vuonna 2026 lainsäädäntöehdotuksen, jolla Eurojustia vahvistetaan**
- **vuonna 2026 lainsäädäntöehdotuksen, jolla Frontexin roolia ja tehtäviä lujitetaan**
- **vuonna 2026 lainsäädäntöehdotuksen, jolla perustetaan eurooppalainen kriittisen viestinnän järjestelmä**

Komissio aikoo

- **vuonna 2025 esittää etenemissuunnitelman, jolla toteutetaan lainvalvontaviranomaisten laillinen ja tosiasiallinen pääsy dataan**
- **vuonna 2025 laatia vaikutustenarvioinnin datan säilyttämistä koskevien EU:n tason sääntöjen päivittämiseksi tarpeen mukaan**
- **vuonna 2026 esittää salausta koskevan teknologisen etenemissuunnitelman, jotta voidaan määrittää ja arvioida teknisiä ratkaisuja, jotka mahdollistavat lainvalvontaviranomaisille laillisen pääsyn dataan**
- **tehdä työtä sen eteen, että voidaan perustaa korkean tason työryhmä operatiivisen lainvalvontayhteistyön lujittamiseksi**
- **vuonna 2026 perustaa yhteisen tutkimuskeskuksensa yhteyteen turvallisuustutkimus- ja innovointikampuksen**

Komissio aikoo yhteistyössä jäsenvaltioiden ja EU:n virastojen kanssa

- **vahvistaa Euroopan monialaista rikosuhkien torjuntafoorumia (EMPACT)**
- **tehdä työtä sen eteen, että yhteentoimivuusarkkitehtuurin käyttöönotto ja Prüm II -asetuksen täytäntöönpano on nopeaa**
- **vahvistaa matkustustietosäännöstöä**

Jäsenvaltioita kehotetaan

- **saattamaan tietojenvaihtodirektiivi osaksi kansallista lainsäädäntöä ja panemaan se kaikilta osin täytäntöön**

[30] EUVL C/2024/3510, 30.5.2024.

4. Hybridiuhkien ja muiden vihamielisten tekojen vastustuskyky

Kasvatamme hybridiuhkien vastustuskykyä parantamalla kriittisen infrastruktuurin suojelua, vahvistamalla kyberturvallisuutta, suojaamalla liikenteen solmukohtia ja satamia ja torjumalla verkkouhkia.

EU:n turvallisuutta heikentävät vihamieliset teot ovat yleistyneet ja kehittyneet, ja pahantahtoiset toimijat ovat laajentaneet arsenaaliaan merkittävästi. Hybridikampanjat, joita EU:hun, sen jäsenvaltioihin ja kumppaneihin kohdistuu, ovat voimistuneet, ja niihin liittyy kriittiseen infrastruktuuriin kohdistuvaa sabotointia, tuhopolttoja, kyberhyökkäyksiä, vaaleihin sekaantumista, ulkomaista sekaantumista ja tiedon manipulointia, kuten disinformaatiota, sekä muuttoliikkeen käyttöä aseena. Poliittisen ja operatiivisen roolinsa sekä käsittelemiensä tietojen luonteen vuoksi unionin toimielimet, elimet, toimistot ja virastot, jäljempänä ’unionin toimijat’, eivät ole niiltä suojassa.

EU:n on **parannettava häiriönsietokykyään**, käytettävä nykyisiä välineitä tuloksellisesti ja kehitettävä uusia tapoja vastata näihin valtiollisten ja valtiosta riippumattomien toimijoiden aiheuttamiin muuttuviin uhkiin sekä nyt että tulevaisuudessa.

Kriittinen infrastruktuuri

Kriittiseen infrastruktuuriin kohdistuvat uhkat, kuten sabotoinnin ja haitallisen kybertoiminnan kaltaiset hybridiuhkat, ovat merkittävä huolenaihe erityisesti jäsenvaltioita yhdistävän infrastruktuurin kannalta, olipa kyse sitten energiayhdysjohdoista, valtioiden rajat ylittävistä tietoliikennekaapeleista tai liikenteestä. Venäjän käynnistettyä sodan Ukrainaa vastaan kriittiseen infrastruktuuriin kohdistuva sabotointi on useissa jäsenvaltioissa lisääntynyt erityisesti vuonna 2024. Lainvalvonta-, turvallisuus- ja kyberturvallisuusviranomaisten, puolustusvoimien ja pelastuspalvelun sekä yksityisten toimijoiden välinen yhteistyö on olennaisen tärkeää, jotta tällaisten toimien ennakoiminen, havaitseminen, ehkäiseminen ja niihin reagoiminen on tuloksellista.

Haavoittuvuuksien vähentäminen ja kriittisten toimijoiden häiriönsietokyvyn vahvistaminen on välttämätöntä, jotta keskeisten talouden ja yhteiskunnan kannalta elintärkeiden palvelujen keskeytymätön tarjonta voidaan varmistaa. Sen vuoksi on ratkaisevan tärkeää, että **direktiivi kriittisten toimijoiden häiriönsietokyvystä**[31] ja **direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa (NIS2)**[32] saatetaan ripeästi osaksi kansallista lainsäädäntöä ja pannaan asianmukaisesti täytäntöön kaikissa jäsenvaltioissa.

Nopean edistymisen varmistamiseksi komissio tukee jäsenvaltioita kriittisten toimijoiden[33] määrittämisessä ja keskeisiin palveluihin liittyviä kansallisia strategioita ja riskinarviointeja koskevien hyvien käytäntöjen vaihtamisessa yhteistyössä **kriittisten toimijoiden häiriönsietokykyä käsittelevän ryhmän ja verkko- ja tietoturva-alan yhteistyöryhmän** kanssa. Jos kriittisen infrastruktuurin häiriöillä on merkittäviä valtioiden rajat ylittäviä vaikutuksia, EU:n tason toimia koordinoidaan **kriittistä infrastruktuuria koskevan EU:n suunnitelman** avulla. Komissio kannustaa neuvostoa hyväksymään nopeasti **EU:n**

[31] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta.

[32] 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).

[33] Direktiivin soveltamisalaan kuuluvat energia, liikenne, pankkitoiminta, rahoitusmarkkinoiden infrastruktuuri, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, julkishallinto, avaruusala sekä elintarvikkeiden tuotanto, jalostus ja jakelu.

kybersuunnitelman, jolla entisestään vahvistetaan koordinointia kriisinhallinnan yhteydessä ja tiivistetään yhteistyötä viranomaisten välillä fyysisen ja digitaalisen häiriönsietokyvyn osalta. Vuonna 2023 toteutettiin onnistuneesti stressitestejä energia-alalla, ja komissio aikookin edistää **vapaaehtoisia stressitestejä** muilla sisäisen turvallisuuden kannalta keskeisillä aloilla. Lisäksi komissio laatii **yleiskatsauksen keskeisten palvelujen tarjoamiseen kohdistuvista rajat ylittävistä ja monialaisista riskeistä**. Sillä tuetaan jäsenvaltioiden riskinarviointeja, ja se antaa aineksia kattavaan EU:n tason riskinarviointiin. Komissio tekee varautumisunionistrategiaa noudattaen jäsenvaltioiden kanssa yhteistyötä määrittääkseen muita aloja ja palveluja, jotka eivät kuulu nykyisen lainsäädännön soveltamisalaan mutta joiden suhteen voi olla tarve ryhtyä toimiin.

Kriittisen infrastruktuurin häiriönsietokykyä käsittelevä EU:n ja Naton työryhmä on edistänyt erinomaista yhteistyötä parhaiden käytäntöjen jakamisessa ja häiriönsietokyvyn parantamisessa energia-, liikenne-, digitaali- ja avaruusalalla. Tätä työtä jatketaan **häiriönsietokykyä koskevassa EU:n ja Naton jäsennellyssä vuoropuhelussa**. **EU:n hybridivälineistö** tarjoaa jäsenvaltioille ja kumppaneille vankkaa tukea hybridiuhkiin valmistautumisessa ja niiden torjunnassa. **Hybridialan nopean toiminnan ryhmät**[34] antavat pyynnöstä räätälöityä lyhytaikaista apua jäsenvaltioille, EU:n eri operaatioille ja kumppaneille. Lisäksi komissio aikoo viedä eteenpäin sabotoinnin torjuntaa koskevaa EU:n yhteistyötä asiantuntijatoimilla[35], joihin kuuluu asiantuntijoille tarkoitettu **yhteinen työohjelma** tietojenvaihdon virtaviivaistamiseksi ja vastatoimien kartoittamiseksi.

Euroopan **merenalaisiin kaapeleihin** vaikuttavat häiriötilanteet osoittavat, että tarvitaan vahvempia toimenpiteitä ja selkeämpää reagointia. Kuten **kaapelien turvallisuutta koskevassa EU:n toimintasuunnitelmassa**[36] todetaan, komissio tulee korkean edustajan rinnalla tekemään yhteistyötä jäsenvaltioiden, EU:n virastojen ja Naton kaltaisten kumppaneiden kanssa, jotta merenalaisiin kaapeleihin kohdistuvia uhkia voidaan ehkäistä, ja havaita, niihin voidaan reagoida ja niitä voidaan torjua. Jotta uhkista voitaisiin laatia yhdennetty tilannekuva, komissio aikoo tehdä yhteistyötä jäsenvaltioiden kanssa kehittääkseen ja ottaakseen vapaaehtoisuuden pohjalta käyttöön yhdennetyn merenalaisten kaapeleiden valvontamekanismin merialueittain alkaen Pohjoismaiden ja Baltian maiden välisestä alueellisesta keskuksesta.

Kyberturvallisuus

Pahantahtoiseen kybertoimintaan, joka on usein osa laajempaa moniulotteisten ja hybridien uhkien kirjoa, on kiinnitettävä jatkuvasti huomiota ja se edellyttää toimia Euroopan tasolla. Unioni on viime vuosina hyväksynyt kyberturvallisuuslainsäädäntöä, jolla vahvistetaan EU:n kriittisillä aloilla toimivien NIS2-toimijoiden ja unionin toimijoiden kyberuhkien sietokykyä[37], parannetaan digitaalisten tuotteiden turvallisuutta (kyberresilienssisäädös) ja luodaan säännöstö varautumisen ja poikkeamiin reagoinnin tukemiselle (kybersolidaarisuussäädös). Komissio hyväksyi tammikuussa 2025 **sairaaloiden ja terveydenhuoltopalvelujen tarjoajien**

[34] EU:n turvallisuus- ja puolustusalan strateginen kompassi 2022, s. 22.

[35] EU:n suojaavien turvatoimien neuvonantajat, eurooppalainen räjähteiden raivausverkosto (EEODN), Atlas-verkosto, EU:n suuria turvallisuusriskejä käsittelevä verkosto (EU HRSN), CBRN-turvallisuuden neuvoa-antava ryhmä, kriittisten toimijoiden häiriönsietokykyä käsittelevä ryhmä (CERG).

[36] JOIN (2025) 9 final.

[37] Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2023/2841, annettu 13 päivänä joulukuuta 2023, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi unionin toimielimissä, elimissä, toimistoissa ja virastoissa, EUVL L, 2023/2841, 18.12.2023.

kyberturvallisuutta koskevan eurooppalaisen toimintasuunnitelman[38], jonka avulla on tarkoitus parantaa uhkien havaitsemista, niihin varautumista ja kriiseihin reagoimista. Sen toteuttaminen kokonaisuudessaan on keskeistä. Samaan aikaan meidän on nostettava toimemme erityisesti tietojenvaihdon, toimitusketjujen turvallisuuden, kiristysohjelmien ja kyberhyökkäysten sekä teknologisen suvereniteetin osalta uudelle tasolle, jotta voimme vastata uusiin uhkiin ja kehityskulkuihin.

Toimintasuunnitelman toteuttaminen edellyttää myös, että nykyinen kyberturvallisuuteen liittyvä 299 000 hengen osaamisvaje paikataan. Komissio aikoo tehdä yhteistyötä jäsenvaltioiden kanssa osaamisunionin[39] puitteissa kyberturvallisuuteen perehtyneen työvoiman lisäämiseksi erityisesti uuden kyberturvallisuusakatemian avulla. STEM-aineiden (luonnontieteet, matematiikka, tekniikka ja teknologiat) opetusta koskevalla strategisella suunnitelmalla[40] edistetään osaamisjatkumon parantamista ja Euroopan reagointia kyberturvallisuuden työmarkkinoiden tarpeisiin.

Samalla kun EU parantaa häiriönsietokykyään, se aikoo edelleen hyödyntää kaikilta osin EU:n yhteistä diplomaattista reagointia haitallisiin kybertoimiin (**kyberdiplomatian välineistö**) ehkäistäkseen ja torjuakseen valtiollisten ja valtiosta riippumattomien toimijoiden aiheuttamia kyberuhkia ja reagoidakseen niihin.

Tieto- ja viestintätekniikan toimitusketjujen turvallisuus

5G-kyberturvallisuusvälineistö tarjoaa asianmukaisen kehyksen 5G-verkkojen suojaamiseksi, mutta välineistön käyttöönotto jäsenvaltioissa on vielä riittämätöntä. Jäljellä on turvallisuusriskejä, joita ei voida hyväksyä. Ne koskevat erityisesti suuririskisten toimittajien korvaamista. Yhdenmukaisella tieto- ja viestintätekniikan toimitusketjun turvallisuutta koskevalla toimintamallilla voidaan vähentää sisämarkkinoiden hajanaisuutta, joka johtuu erilaisista kansallisen tason toimintamalleista, välttää kriittistä riippuvuutta ja vähentää suuririskisistä toimittajista tieto- ja viestintätekniikan toimitusketjuille aiheutuvia riskejä ja näin suojata kriittistä infrastruktuuriamme.

Komissio tarkastelee laajemmin tieto- ja viestintätekniikan toimitusketjujen ja infrastruktuurin turvallisuutta ja häiriönsietokykyä tulevassa **kyberturvallisuusasetuksen tarkistuksessa** tätä toimintamallia noudattaen. Lisäksi komissio aikoo ehdottaa **eurooppalaisen kyberturvallisuuden sertifiointikehyksen** parantamista sen varmistamiseksi, että tulevat sertifiointijärjestelmät voidaan hyväksyä nopeasti ja että ne vastaavat tarpeisiin.

Komissio aikoo kehittää tehtyjen tai käynnissä olevien alakohtaisten arviointien[41] pohjalta yhdessä jäsenvaltioiden kanssa **strategisen suunnittelun koordinoituja kyberturvallisuusriskien arviointeja**.

Pilvi- ja tietoliikennepalveluista on tullut keskeinen osa kriittisten infrastruktuurien, yritysten ja viranomaisten toimitusketjuja. Komissio aikoo toteuttaa toimia kannustaakseen kriittisiä toimijoita valitsemaan sellaisia **pilvi- ja tietoliikennepalveluita, joissa kyberturvallisuus on asianmukaisella tasolla**, ottaen huomioon teknisten riskien lisäksi myös strategiset riskit ja riippuvuudet.

[38] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM(2025) 90 final.
[40] COM(2025) 89 final.
[41] Esim. 5G-verkot, tietoliikenne, sähkö, uusiutuva energia ja verkkoon liitetyt ajoneuvot.

Kiristysohjelmat ja kyberhyökkäykset

Merkittävä sitkeä haaste EU:ssa ja maailmanlaajuisesti ovat **kiristysohjelmat**, joiden vuotuisten kokonaiskustannusten arvioidaan erään raportin[42] mukaan kasvavan vuoteen 2031 mennessä yli 250 miljardiin euroon. Sekä **NIS2-direktiivi** että **kyberresilienssisäädös** tulevat parantamaan merkittävästi toimijoiden turvallisuustasoa, sillä hyökkäysten toteuttamisesta tulee kiristysohjelmaverkostoille kalliimpaa. Lisäksi komissio aikoo tehdä tiivistä yhteistyötä jäsenvaltioiden kanssa sen varmistamiseksi, että kiristysohjelmahyökkäyksistä, erityisesti edistyneistä pitkäkestoisista uhkista, ja lunnasmaksuista ilmoitetaan lainvalvontaviranomaisille entistä useammassa tapauksessa, mikä helpottaa tutkintaa.

Kyberhyökkäysten ehkäisemiseksi ja pysäyttämiseksi EU:n on vahvistettava lainvalvontaviranomaisten, kyberturvallisuusviranomaisten ja -toimijoiden sekä yksityisten tahojen välistä tietojenvaihtoa Europolin ja EU:n kyberturvallisuusviraston (ENISA) suojissa.

Europolin ja Eurojustin olisi lainvalvontayhteistyötä tukien jatkettava työtä niiden saavutusten pohjalta, joita niillä on kiristysohjelmaoperaatioiden purkamisessa. Tätä varten lainvalvontaviranomaisten olisi maksimoitava yhteistyömekanismien, kuten **Europolin IRRM-mallin (International Ransomware Response Model, kansainvälinen reagointimalli kiristysohjelmiin)** ja **kansainvälisen kiristyshaittaohjelmien vastaisen aloitteen (International Counter Ransomware Initiative, CRI)**[43], käyttö, ja ENISAn ja Europolin olisi tehtävä yhteistyötä kiristysohjelmatyyppien salauksenpurkuvälineiden tietovaraston[44] laajentamiseksi.

Teknologinen suvereniteetti

Kyberturvallisuus ja teknologinen suvereniteetti liittyvät läheisesti toisiinsa, ja teknologiseen riippuvuuteen on puututtava ensi tilassa. Unionin täytyy **ohjata uusien teknologioiden kehittämistä ja käyttöönottoa**, joten komissio pyrkii parantamaan **strategisten teknologioiden**, kuten tekoälyn, kvanttiteknologian, kehittyneiden tietoliikenneyhteyksien, pilvipalvelujen, reunalaskennan ja esineiden internetin[45], valmiuksia tulevien aloitteiden, kuten tekoälytoimintasuunnitelman, kvanttistrategian ja muiden vastaavien avulla[46]. Komissio tukee edelleen viimeisimpien saatavilla olevien kansainvälisesti sovittujen **internetprotokollien** nopeaa käyttöönottoa, sillä ne ovat olennaisen tärkeitä, jotta voidaan ylläpitää skaalautuvaa ja tehokasta internetiä, jossa kyberturvallisuus on paremmalla tasolla. Lisätoimia tarvitaan myös, jotta voidaan vastata **radiotaajuuksiin liittyviin haasteisiin**, kuten GNSS-signaalien harhauttamiseen ja peittämiseen, toimitusketjujen riskeihin ja riippuvuuksiin, kuten kvanttitunnistusteknologioiden käyttöön, ja tutkia radiotaajuuksien seurantakapasiteetin kehittämistä.

Uudella kvanttiaikakaudella **kvanttiturvallisen salauksen** (PQC) käyttöönotto on ratkaisevan tärkeää arkaluonteisen viestinnän ja lepäävän datan suojaamiseksi ja digitaalisten identiteettien suojelemiseksi. Komissio tekee kvanttiturvalliseen salaukseen siirtymisen koordinoidusta

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Saatavilla No More Ransom -hankkeen kautta, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] e.g. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, the Quantum Flagship Homepage of Quantum Flagship | Quantum Flagship, 3C-verkostot (COM(2024) 81 final) ja kaapelien turvallisuutta koskeva EU:n toimintasuunnitelma (JOIN(2025) 9 final).

toteutussuunnitelmasta vuonna 2024 annetun suosituksen[47] pohjalta jäsenvaltioiden kanssa yhteistyötä edistääkseen tätä siirtymistä. Tähän liittyen jäsenvaltioiden olisi määritettävä kriittisten toimijoiden keskuudessa suuririskiset tapaukset ja varmistettava niiden osalta kvanttiturvallisuus mahdollisimman pian ja viimeistään vuoden 2030 loppuun mennessä. Lisäksi komissio tekee yhteistyötä jäsenvaltioiden ja Euroopan avaruusjärjestön (ESA) kanssa kehittääkseen ja ottaakseen käyttöön osana EU:n turvallisten yhteyksien ohjelmaa (**IRIS²**) kvanttiavaimen jakamiseen (QKD) perustuvan **eurooppalaisen kvanttiviestintäinfrastruktuurin (EuroQCI)**[48]. Molemmat aloitteet antavat toimijoille mahdollisuuden siirtää ja tallentaa tietoa turvallisesti.

Kvanttiteknologialla tulee olemaan keskeinen rooli myös turvallisuussovelluksissa: osana **kvanttistrategiaa** laaditaan **turvallisuussovellusten kvanttitunnistuksen edistämissuunnitelma**. Komissio pyrkii varmistamaan kvanttiturvallisuuden myös turvallisuuden kannalta kriittisissä sisäisissä järjestelmissään, kuten turvallisuusluokitelluissa tietojärjestelmissä.

Yritysystävällinen kyberturvallisuussäännöstö

Kyberturvallisuusasetuksen tuleva tarkistus tarjoaa tilaisuuden **yksinkertaistaa EU:n kyberturvallisuuslainsäädäntöä**, kuten kilpailukykykompassissa linjataan. Komissio aikoo tehdä tiivistä yhteistyötä jäsenvaltioiden kanssa varmistaakseen, että NIS2-direktiivissä, kyberresilienssisäädöksessä ja kybersolidaarisuussäädöksessä vahvistettu horisontaalinen kyberturvallisuussäännöstö pannaan nopeasti, johdonmukaisesti ja yritysystävällisesti täytäntöön. Näin lisätään yksinkertaisuutta ja johdonmukaisuutta ja vältetään kyberturvallisuussääntöjen hajanaisuutta tai päällekkäisyyttä EU:n ja kansallisessa lainsäädännössä.

Jotta verkkopalveluja olisi turvallisesti saatavilla ja digitaalinen turvallisuus vahvistuisi kaikkialla EU:ssa, **eurooppalainen digitaalisen identiteetin kehys** tulee tarjoamaan kaikille EU:n kansalaisille ja asukkaille luotettavia digitaalisen identiteetin lompakoita vuoden 2026 loppuun mennessä. Tuleva **eurooppalainen yrityslompakko** helpottaa suojattua valtioiden rajat ylittävää vuorovaikutusta yritysten ja julkishallinnon välillä. Nämä molemmat ovat ennakkoedellytyksiä sille, että datavetoiset sisämarkkinat, joilla ovat käytössä esimerkiksi yhteinen digitaalinen palveluväylä, sähköinen laskutus, sähköiset hankinnat ja digitaalinen tuotepassi, voivat toimia suojatusti ja tehokkaammin.

Turvallisuus verkossa

Osa kaikkein vakavimmista hybridiuhkista, jotka vaarantavat eurooppalaisten turvallisuuden ja kohdistuvat EU:n demokraattiseen toimintaympäristöön, ilmenee verkossa. Näihin uhkiin kuuluvat verkossa tapahtuva laiton toiminta ja laiton verkkosisältö, tiedonmanipulointi, johon liittyy keinotekoista vahvistamista, harhaanjohtavaa tietoa sekä ulkomaista tiedonmanipulointia ja häirintää.

Digipalvelusäädöksen tiukka täytäntöönpano on ensiarvoisen tärkeää, jotta vastuuvelvollisten toimijoiden kanssa voidaan varmistaa, että verkkoympäristö on turvallinen ja esteetön sekä myös hybridiuhkia kestävä. Digipalvelusäädöksessä velvoitetaan erittäin suurten verkkoalustojen ja erittäin suurten verkossa toimivien hakukoneiden tarjoajat tekemään riskinarviointeja ja ottamaan käyttöön toimenpiteitä, joilla lievennetään niiden palvelujen muotoilusta, toiminnasta tai käytöstä aiheutuvia järjestelmäriskejä. Tällaisia riskejä voivat olla kielteiset vaikutukset kansalaiskeskusteluun ja vaaliprosesseihin sekä yleiseen turvallisuuteen,

[47] Suositus kvanttiturvalliseen salaukseen siirtymisen koordinoidusta toteutussuunnitelmasta | Euroopan digitaalista tulevaisuutta rakentamassa.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

kuten pahantahtoisten vieraan vallan toimijoiden pitkälle menevä puuttuminen esimerkiksi vaaliprosesseihin. Jäsenvaltioiden toimivaltaisten viranomaisten kouluttaminen lainsäädäntöön sisältyvien työkalujen käytössä on tärkeää erityisesti sukupuoleen perustuvan verkkoväkivallan osalta, jotta laiton verkkosisältö voidaan poistaa nopeasti. Digipalvelusäädöksessä säädetään kriisinhallintamenettelystä, joka voidaan ottaa käyttöön, jos poikkeukselliset olosuhteet johtavat yleiseen turvallisuuteen tai kansanterveyteen kohdistuvaan vakavaan uhkaan unionissa tai sen merkittävissä osissa. Tämän menettelyn täydentämiseksi komissio ja digitaalisten palvelujen koordinaattoreiksi nimetyt kansalliset toimivaltaiset viranomaiset ovat laatineet myös vapaaehtoisen **digipalvelusäädökseen liittyvän poikkeamavastekehyksen**. Digitaalisten palvelujen koordinaattorit ovat toteuttaneet toimia myös vaalien luotettavuuden suojelemiseksi esimerkiksi järjestämällä pyöreän pöydän kokouksia ja stressitestejä[49]. Digipalvelusäädös on yhdessä poliittista mainontaa koskevan asetuksen[50] kanssa yksi monista säikeistä, jotka kytkeytyvät demokratian ja demokraattisten prosessien luotettavuuden turvaamiseen. Demokratia ja demokraattiset prosessit voivat joutua vihamielisten toimijoiden kohteeksi, myös digitaalisten välineiden ja sosiaalisen median kautta.

Ulkomaisen tiedonmanipuloinnin ja häirinnän torjuntavälineistön täytäntöönpano on toinen tärkeä komponentti, joka tarjoaa keskeistä tukea EU:n tasolla. Näissä pyrkimyksissä keskeistä on myös digitaalisen lukutaidon ja medialukutaidon sekä kriittisen ajattelun tukeminen[51].

Muuttoliikkeen välineellistämisen torjunta

Venäjä on Valko-Venäjän avulla ja merkittävällä tuella käyttänyt tarkoituksellisesti muuttoliikettä aseena ja laittomasti ohjannut muuttovirtoja EU:n ulkorajoille horjuttaakseen yhteiskuntiemme vakautta ja heikentääkseen Euroopan unionin yhtenäisyyttä. Tämä vaarantaa paitsi EU-maiden kansallisen turvallisuuden ja suvereniteetin myös Schengen-alueen turvallisuuden ja eheyden ja koko unionin turvallisuuden. Lokakuussa 2024 antamissaan päätelmissä Eurooppa-neuvosto tähdensi, että Venäjän ja Valko-Venäjän tai minkään muunkaan maan ei saa antaa käyttää väärin arvojamme, kuten oikeutta turvapaikkaan, ja heikentää demokratiaamme.

Jotta näitä uhkia voidaan tosiasiallisesti torjua, unioni on vahvan poliittisen tuen lisäksi toteuttanut taloudellisia, operatiivisia ja diplomaattisia toimenpiteitä, joihin kuuluu myös yhteistyö lähtö- ja kauttakulkumaiden kanssa, kuten vuonna 2024 annetussa komission tiedonannossa muuttoliikkeen käyttämisestä aseena todetaan[52]. Näihin toimenpiteisiin kuuluu neuvoston luoman uuden säännöstön käyttäminen pakotteiden määräämiseksi varojen jäädyttämisen ja matkustuskieltojen muodossa yksityishenkilöille ja organisaatioille, jotka osallistuvat senkaltaiseen toimintaan, jota Venäjä harjoittaa käyttämällä muuttoliikettä aseena[53]. EU käyttää edelleen tarvittaessa tätä säännöstöä ja tukee jäsenvaltioita tämän uhkan torjumisessa.

[49] DSA Elections Toolkit for Digital Services Coordinators 2025 (digipalvelusäädökseen liittyvä vaalivälineistö digitaalisten palvelujen koordinaattoreita varten) https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.

[50] Euroopan parlamentin ja neuvoston asetus (EU) 2024/900, annettu 13 päivänä maaliskuuta 2024, poliittisen mainonnan avoimuudesta ja kohdentamisesta, EUVL L, 2024/900, 20.3.2024.

[51] Digitaalisen koulutuksen toimintasuunnitelma (2021–2027) – Eurooppalainen koulutusalue.

[52] COM(2024) 570 final.

[53] Neuvoston asetus (EU) 2024/2642, annettu 8 päivänä lokakuuta 2024, Venäjän epävakauttavien toimien johdosta määrättävistä rajoittavista toimenpiteistä, ST/8744/2024/INIT, EUVL L, 2024/2642, 9.10.2024.

Liikenteen turvaaminen

Merisatamat, lentoasemat ja maainfrastruktuuri ovat ratkaisevan tärkeitä saapumis- ja lähtöpaikkoja. Niillä on keskeinen rooli EU:n taloudessa ja yhteiskunnassa, ja ne ovat olennaisen tärkeitä sotilaallisen liikkuvuuden kannalta. Nämä liikenteen solmukohdat ja välineet ovat kuitenkin myös ensisijaisia ulkoisten uhkien ja rikollisen toiminnan kohteita. Viimeaikaiset häiriötilanteet, kuten lentorahtiin liittyvät turvallisuuspoikkeamat ja rautatieinfrastruktuuriin kohdistuvat iskut, ovat tuoneet esiin vakavia riskejä. **Liikenteenharjoittajat** voivat olla pahantahtoisille toimijoille sekä kohteita että välineitä. EU:n voimassa olevat säädökset ovat parantaneet ilmailun turvaamista[54], mutta siviili-ilmailun korkea uhkataso edellyttää keinoja ennakoida häiriötilanteita ja kuulla nopeasti asianomaisia jäsenvaltioita. Komissio aikoo tehdä yhteistyötä jäsenvaltioiden kanssa muuttaakseen voimassa olevaa ilmailun turvaamista koskevaa täytäntöönpanolainsäädäntöä, jotta voidaan jakaa **ilmailun turvallisuuteen vaikuttavia tapahtumia** koskevia turvallisuusluokiteltuja tietoja. Lisäksi komissio harkitsee **sääntelytoimenpiteitä**, joilla torjutaan uusia uhkia, kuten **lentorahtia koskevia vaaratilanteita**, ja vahvistetaan ilmailun turvaamista koskevia normeja. Tähän kuuluu myös **ilmailun turvaamista koskevan lainsäädännön (AVSEC)** vahvistaminen, jotta on mahdollista toteuttaa välittömiä toimenpiteitä ja samalla säilyttää yhden turvatarkastuksen periaate EU:n lentoasemilla.

Laatiessaan tulevaa **EU:n satamastrategiaa eurooppalaisen satama-allianssin** pohjalta komissio tutkii keinoja vahvistaa edelleen meriturvallisuutta koskevaa lainsäädäntöä, jotta uusia uhkia voidaan torjua tuloksellisesti, turvata satamat ja parantaa EU:n toimitusketjun turvallisuutta. Tätä varten komissio tulee varmistamaan lainsäädännön vankan täytäntöönpanon ja pyrkii yhdenmukaistamaan kansallisia käytäntöjä ja vahvistamaan taustan tarkistuksia satamissa. Lentorahtia varten laadittujen turvaprotokollien lisäksi komissio aikoo tehdä yhteistyötä jäsenvaltioiden ja yksityisen sektorin kanssa tällaisten protokollien ulottamiseksi meriliikenneketjujen turvaamiseen.

Ehdotettu EU:n tulliviranomainen tulee analysoimaan ja arvioimaan riskejä, joita EU:hun saapuviin, EU:sta lähteviin ja EU:n kautta kuljetettaviin tavaroihin **tullitietojen** perusteella liittyy, ja toimii näin jäsenvaltioiden tukena estämässä pahantahtoisia toimijoita hyödyntämästä kansainvälisiä toimitusketjuja. Tulevalla **eurooppalaisella valtamerisopimuksella** on EU:n merellisen turvallisuusstrategian[55] mukaisesti keskeinen rooli merellisen turvallisuuden parantamisessa EU:ta ympäröivillä merialueilla ja laajemmin, muun muassa sitä kautta, että kannustetaan monitavoitteisten merioperaatioiden ja -harjoitusten laajentamiseen.

Toimitusketjujen häiriönsietokyky

Euroopan on vähennettävä tukeutumistaan kolmansien maiden teknologioihin, sillä se voi johtaa riippuvuuteen ja turvallisuusriskeihin. Komissio pyrkii lieventämään riippuvuutta yksittäisistä ulkomaisista toimittajista, vähentämään suuririskisistä toimittajista toimitusketjuille aiheutuvia riskejä ja suojaamaan EU:n maaperällä olevaa kriittistä infrastruktuuria ja teollista kapasiteettia, kuten **kilpailukykykompassissa**[56] ja **puhtaan teollisen kehityksen ohjelmassa**[57] on esitetty. Komissio aikoo edistää **sisäisen turvallisuuden näkökohtia teollisuuspolitiikassa** tekemällä yhteistyötä EU:n teollisuuden kanssa keskeisissä asioissa (esim. liikenteen solmukohdat ja kriittiset infrastruktuurit), jotta voidaan tuottaa

[54] Euroopan parlamentin ja neuvoston asetus (EY) N:o 300/2008, annettu 11 päivänä maaliskuuta 2008, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä, EUVL L 97, 9.4.2008, s. 72–84.
[55] JOIN (2023) 8 final.
[56] COM (2025) 30 final.
[57] COM (2025) 85 final.

turvallisuusratkaisuja, kuten ilmaisinlaitteita, biometristä teknologiaa ja miehittämättömiä ilma-aluksia, joissa turvallisuus on sisäänrakennettuna ominaisuutena. Komissio aikoo **tarkastella EU:n hankintasääntöjä** ja arvioida, ovatko vuoden 2009 puolustus- ja turvallisuusalan julkisia hankintoja koskevan direktiivin[58] turvallisuusnäkökohdat riittäviä vastaamaan lainvalvontaa ja kriittisten toimijoiden häiriönsietokykyä koskeviin tarpeisiin.

Komissio tukee jäsenvaltioita **suorien ulkomaisten investointien** ja logistiikkakeskusten laitehankintojen **seurannassa**, jotta kriittisen infrastruktuurin ja teknologian turvallisuus voidaan varmistaa.

Kun **sisämarkkinoiden hätätilaa ja häiriönsietokykyä koskevaa säädöstä (IMERA)** aletaan soveltaa, se auttaa EU:ta hallitsemaan kriisejä, jotka häiritsevät kriittisiä toimitusketjuja sekä tavaroiden, palvelujen ja ihmisten vapaata liikkuvuutta. Se mahdollistaa kriisien nopean koordinoinnin, kriisien kannalta olennaisten tavaroiden ja palvelujen määrittämisen ja antaa välineistön niiden saatavuuden varmistamiseksi. Lisäksi komissio aikoo ehdottaa tiiviissä yhteistyössä jäsenvaltioiden kanssa, että perustetaan **virastojen välinen kuljetus- ja toimitusketjuturvallisuutta edistävä hälytysmekanismi**, jolla taataan uhkien ennakoimisessa ja torjumisessa tarvittavien tietojen suojattu ja oikea-aikainen jakaminen.

Kriittisiä raaka-aineita koskevan säädöksen ja nettonollateollisuussäädöksen täytäntöönpanon myötä kestävyyttä, häiriönsietokykyä ja eurooppalaisuuden suosimista koskevien kriteerien käytön lisääminen EU:n julkisissa hankinnoissa edistää edelläkävijämarkkinoiden kehitystä. Kauppasuhteiden vahvistaminen esimerkiksi raaka-ainekumppanuuksien ja puhtaan kaupan ja puhtaiden investointien kumppanuuksien avulla auttaa monipuolistamaan toimitusketjuja.

Kyky selviytyä kemiallisista, biologisista, säteily- ja ydinuhkista ja varautua niihin

Venäjän hyökkäyssota Ukrainaa vastaan on kasvattanut **kemiallisten, biologisten, säteily- ja ydinuhkien (CBRN)** riskiä. Jotta CBRN-materiaalien mahdollista hankintaa ja niiden käyttämistä aseena voidaan torjua, komissio aikoo tukea jäsenvaltioita ja kumppanimaita koulutuksen ja harjoitusten avulla. Komissio aikoo myös parantaa CBRN-uhkiin varautumista ja reagointikykyä uhkien priorisoinnin, vastatoimiin kohdennetun innovointirahoituksen, rescEU-valmiusvarastojen ja vasta-aineiden varastoinnin avulla uuden **CBRN-uhkiin varautumisen ja reagoinnin toimintasuunnitelman** puitteissa. Lisäksi **lääkinnällisten vastatoimien EU-strategialla** tuetaan lääkinnällisten vastatoimien kehittämistä tutkimuksesta valmistukseen ja jakeluun EU:n suojelemiseksi pandemioilta ja CBRN-uhkilta.

EU on covid-19-pandemiasta saatujen kokemusten pohjalta vahvistanut terveysturvasäännöstöä[59]. Komissio nimeää kansanterveysalan EU:n vertailulaboratorioita vahvistamaan EU:n ja jäsenvaltioiden valmiuksia valvontaan ja nopeaan havaitsemiseen. Varautumista, ennaltaehkäisyä ja reagointia edistävä unionin terveysturvasuunnitelma julkaistaan vuonna 2025.

Keskeiset toimet

Komissio aikoo

- **vuonna 2025 tarkastella uudelleen ja tarkistaa kyberturvallisuusasetusta**
- **kehittää toimenpiteitä pilvipalvelujen kyberturvallisen käytön varmistamiseksi**
- **vuonna 2025 ehdottaa EU:n satamastrategiaa**

[58] Direktiivi 2009/81/EY hankintaviranomaisten ja hankintayksiköiden tekemien rakennusurakoita sekä tavara- ja palveluhankintoja koskevien sopimusten tekomenettelyjen yhteensovittamisesta puolustus- ja turvallisuusalalla, EUVL L 216, 20.8.2009.

[59] Erityisesti rajatylittävistä vakavista terveysuhkista annetulla asetuksella (EU) 2022/2371.

- **vuonna 2026 tarkistaa puolustus- ja turvallisuusalaa koskevia EU:n hankintasääntöjä**
- **vuonna 2026 esittää uuden CBRN-uhkiin varautumisen ja reagoinnin toimintasuunnitelman**

Komissio aikoo yhteistyössä jäsenvaltioiden kanssa

- **kehittää ja ottaa käyttöön eurooppalaisen kvanttiviestintäinfrastruktuurin (EuroQCI)**
- **varmistaa digipalvelusäädöksen noudattamisen valvonnan**
- **ryhtyä toimiin torjuakseen muuttoliikkeen käyttämistä aseena**
- **perustaa ilmailun turvapoikkeamajärjestelmän**
- **ryhtyä toimiin virastojen välisen kuljetus- ja toimitusketjuturvallisuutta edistävän hälytysmekanismin perustamiseksi**

Neuvostoa kehotetaan

- **hyväksymään neuvoston suositus EU:n kybersuunnitelmasta**

Jäsenvaltioita kehotetaan

- **saattamaan kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi ja tarkistettu kyberturvallisuusdirektiivi osaksi kansallista lainsäädäntöä ja panemaan ne kaikilta osin täytäntöön**

5. Vakavan ja järjestäytyneen rikollisuuden kitkeminen

Autamme kitkemään järjestäytynyttä rikollisuutta ehdottamalla tiukempia sääntöjä järjestäytyneen rikollisuuden verkostojen torjumiseksi, myös tutkinnan osalta, vähentämällä EU:n nuorten alttiutta tulla värvätyksi rikolliseen toimintaan ja ottamalla käyttöön parempia toimenpiteitä rikoksentekovälineiden ja rikoksella saatujen varojen käytön estämiseksi.

Järjestäytynyt rikollisuus hyödyntää muuttuvaa toimintaympäristöä ja leviää eksponentiaalisesti. Se hyötyy kehittyneistä teknologioista, se toimii useilla lainkäyttöalueilla ja sillä on vahvat yhteydet EU:n rajojen ulkopuolelle. Koska uhkat ovat monitahoisia ja ylikansallisia, EU:n tason koordinointi ja tuki on ratkaisevan tärkeää.

Rikollisuuden torjunta

Nuorten värvääminen järjestäytyneeseen rikollisuuteen on kasvava huolenaihe EU:ssa. Järjestäytyneen rikollisuuden torjunta edellyttää, että puututaan sen **perimmäisiin syihin** tarjoamalla koulutusta ja vaihtoehtoja rikolliselle elämäntavalle koko yhteiskunnan kattavan lähestymistavan avulla. Komissio tukee turvallisuusnäkökohtien sisällyttämistä EU:n koulutus-, sosiaali-, työllisyys- ja aluepolitiikkaan. EU tulee edistämään **näyttöön perustuvaa rikoksentorjuntapolitiikkaa**[60], joka on räätälöity paikallisiin olosuhteisiin.

Digipalvelusäädöksen nojalla toteutettavissa toimenpiteissä edellytetään, että alaikäisten käytettävissä olevien verkkoalustojen tarjoajat hallitsevat riskejä ja torjuvat laitonta sisältöä, kuten vihapuhetta, jotta verkkopalvelujen vastaanottajia ja erityisesti alaikäisiä voidaan suojella muun muassa lapsiin kohdistuvan seksuaaliväkivallan tekijöiltä, ihmiskauppiailta ja verkossa tapahtuvalta värväämiseltä rikolliseen toimintaan tai väkivaltaisiin ääriliikkeisiin. Komissio aikoo antaa **alaikäisten suojelemisesta ohjeita**, joilla verkkoalustojen tarjoajia autetaan varmistamaan, että alaikäisten yksityisyys ja turvallisuus on verkossa korkealla tasolla. Ohjeisiin sisällytetään kaikkia unionissa toimivia digitaalisia palveluita koskevia suosituksia

[60] https://www.eucpn.org/.

alaikäisten suojelun parantamiseksi verkossa. Lisäksi komissio aikoo vuonna 2025 helpottaa EU:ssa **yksityisyyttä suojaavan iänvarmistusratkaisun** käyttöönottoa. Sen on tarkoitus täyttää aukko siihen asti, kunnes digitaalinen lompakko tulee tarjolle vuoden 2026 lopussa. Komissio aikoo esittää myös nettikiusaamisen vastaisen toimintasuunnitelman.

Komissio tulee edelleen tukemaan myös vapaaehtoista yhteistyötä, jota sidosryhmät tekevät verkkoalustojen ja muiden toimijoiden kanssa muun muassa EU:n internetfoorumin kautta ja digipalvelusäädöksen nojalla laadittujen kohdennettujen käytännesääntöjen kautta. Viimeksi mainituista voidaan mainita esimerkkinä laittoman vihapuheen torjumista verkossa koskevat käytännesäännöt vuodelta 2025. Tavoitteena on lisätä tietoisuutta, vastata yhdessä jo olemassa oleviin ja uusiin uhkiin sekä kehittää ja jakaa riskinvähentämistoimenpiteitä koskevia hyviä käytäntöjä.

Järjestäytyneen rikollisuuden vaikutus paikallistasolla korostaa tarvetta alueellisiin ratkaisuihin, joilla alttiutta laittomaan toimintaan ja tällaisen toiminnan houkuttelevuutta voidaan vähentää. EU:n kaupunkiagendassa tullaan käsittelemään kaupunkien turvallisuushaasteita ”EU:n kaupungit radikalisoitumista vastaan” -aloitteen pohjalta. Komissio aikoo tukea jäsenvaltioita kaupunkien ja alueiden turvallisuuden parantamisessa Euroopan aluekehitysrahaston kautta.

Vahvempi koulutuspohja ja osaaminen tukevat selviytymiskykyisiä ja yhteenkuuluvuutta edistäviä yhteiskuntia. Unioni pyrkii **osaamisunionin** ja **kotouttamista ja osallisuutta koskevan toimintasuunnitelman** avulla parantamaan ihmisten kykyä vastustaa väärää tietoa ja tarkoituksella harhaanjohtavaa tietoa, radikalisoitumista ja rikolliseen toimintaan värväämisestä.

Yksi EU:n keskeisistä tavoitteista on lasten suojeleminen kaikenlaiselta väkivallalta, myös rikolliselta toiminnalta ja fyysiseltä tai henkiseltä väkivallalta, verkossa ja sen ulkopuolella. EU aikoo laatia **toimintasuunnitelman lasten suojelemiseksi rikollisuudelta**, jonka toimet ulottuvat sekä verkkoympäristöön että sen ulkopuolelle. Sillä on tarkoitus vastata erityisen haavoittuvassa asemassa olevien ryhmien erityistarpeisiin. Tällaisia ovat esimerkiksi lapset, jotka ovat yhä alttiimpia värväämiselle ja radikalisoitumiselle, verkkoviettelylle ja seksuaaliväkivallalle, nettikiusaamiselle, disinformaatiolle ja muille uhkille. Toimintasuunnitelmassa esitetään johdonmukainen ja koordinoitu toimintamalli, joka perustuu käytettävissä oleviin kehyksiin ja välineisiin, joihin kuuluvat tuleva lapsiin kohdistuvan seksuaaliväkivallan EU-torjuntakeskus sekä muut EU:n elimet ja virastot, ja ehdotetaan tapoja edetä siellä, missä on edelleen puutteita.

Rikollisverkostojen ja niiden toiminnan mahdollistajien kitkeminen

Korkean riskin rikollisverkostojen, niiden johtajien ja niiden toiminnan mahdollistajien torjuntaa on vahvistettava. Vaikka hiljattain on saatu merkittäviä tuloksia[61], vanhentuneet säännöt ja epäyhtenäinen rikollisverkostojen määrittely haittaavat tuloksellista rikosoikeudellista reagointia ja valtioiden rajat ylittävää yhteistyötä. Komissio aikoo tarkastella alan vanhentunutta lainsäädäntöä ja ehdottaa **järjestäytynyttä rikollisuutta koskevan lainsäädäntökehyksen** uudistamista rikostorjunnan vahvistamiseksi.

Hallinnollinen täytäntöönpano voi täydentää lainvalvontaa, jotta tuloksia voidaan saada aikaan nopeammin. Tästä on osoituksena EPPOn ja Euroopan petostentorjuntaviraston (OLAF) työ **EU:n taloudellisia etuja vahingoittavien valtioiden rajat ylittävien petosten ja rikosten torjumiseksi**. Tukipetoksia kohdistuu esimerkiksi uusiutuvaan energiaan, tutkimusohjelmiin ja maatalouteen[62]. Komissio aikoo tutkia tapoja koordinoida rikosoikeudellisten ja hallinnollisten

[61] Esim. äskettäiset EMPACT-tapaukset.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

välineiden käyttöä ja parantaa yhteistyötä Europolin, Eurojustin ja EPPOn kanssa. Komissio tukee edelleen myös **hallinnollisen lähestymistavan** laajempaa soveltamista, jotta paikallisviranomaiset ja muut hallintoviranomaiset voivat estää rikollisten soluttautumista[63].

EU on vahvistamassa **korruption** torjuntaa koskevaa lainsäädäntökehystään[64]. Euroopan parlamentin ja neuvoston olisi saatava nopeasti päätökseen neuvottelut komission ehdottamasta päivitetystä korruptiontorjuntasäännöstöstä. Komissio aikoo esittää EU:n korruptiontorjuntastrategian, jolla edistetään lahjomattomuutta ja vahvistetaan koordinointia viranomaisten ja sidosryhmien välillä.

Keskeinen järjestäytyneiden rikollisryhmien väkivallan lisääntymisen mahdollistava tekijä ovat ampuma-aseet. Komissio aikoo ehdottaa ampuma-aseiden laitonta kauppaa koskevia yhteisiä rikosoikeudellisia normeja. Uudessa **ampuma-aseiden laittoman kaupan torjuntaa koskevassa EU:n toimintasuunnitelmassa** keskitytään laillisten markkinoiden turvaamiseen ja rikollisen toiminnan rajoittamiseen paremman tiedustelun ja vahvemman kansainvälisen yhteistyön avulla keskittyen erityisesti Ukrainaan ja Länsi-Balkaniin.

Pyroteknisten tuotteiden laiton kauppa rikolliseen toimintaan edellyttää toimenpiteitä ennaltaehkäisyn ja jäljitettävyyden parantamiseksi. Komissio arvioi parhaillaan pyroteknisiä tuotteita koskevaa direktiiviä ja pohtii myös **pyroteknisten tuotteiden laittomasta kaupasta määrättäviä rikosoikeudellisia seuraamuksia**.

Rahavirtojen seuraaminen

Rahavirtojen seuraaminen on ratkaisevan tärkeää järjestäytyneen rikollisuuden ja terrorismin torjunnassa, mutta se on edelleen hyvin haastavaa. Järjestäytyneen rikollisuuden ja rahavirtojen välinen yhteys edellyttää vahvoja yhteisiä toimia, joilla voidaan pysäyttää rikollisverkostojen pääsy rahoituslähteisiin ja suojella paremmin ihmisiä, yrityksiä ja julkisia varoja.

EU on pönkittänyt toimiaan uusilla rahanpesuntorjuntasäännöillä ja muun muassa perustamalla **EU:n rahanpesuntorjuntaviranomaisen (AMLA)**[65]. Rahanpesuntorjuntaviranomaisen, petostentorjuntaviraston, Euroopan syyttäjänviraston, Eurojustin ja Europolin välinen yhteistyö on olennaisen tärkeää tuloksellisen talousrikostutkinnan toteuttamiseksi. Komissio aikoo tukea **kumppanuuksien** perustamista, sekä virastojen välisen yhteistyön helpottamiseksi että yksityisen sektorin kanssa.

Olennaisen tärkeässä asemassa on järjestäytyneen rikollisuuden taloudellisten motiivien poistaminen, varojen takavarikointi ja rikollisen hyödyn menetetyksi tuomitseminen. Jäsenvaltioiden olisi viipymättä saatettava **varojen takaisinhankintaa ja menetetyksi tuomitsemista** koskevat tiukemmat säännöt[66] osaksi kansallista lainsäädäntöään ja kaikin tavoin hyödynnettävä niitä. EU:n rahanpesunvastaisen säännöstön ulottumattomissa olevien rinnakkaisten rahoitusjärjestelmien, kuten kryptovaroihin perustuvien järjestelmien, torjunta edellyttää myös innovatiivisia toimia, parhaiden käytäntöjen jakamista jäsenvaltioiden kesken sekä Europolin ja Eurojustin antaman tuen lisäämistä. Komissio aikoo tutkia, voitaisiinko järjestäytyneen rikollisuuden tuottamien voittojen ja terrorismin rahoituksen jäljittämiseksi

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi korruption torjunnasta sekä neuvoston puitepäätöksen 2003/568/YOS ja sellaisen lahjonnan torjumisesta, jossa on osallisina Euroopan yhteisöjen virkamiehiä tai Euroopan unionin jäsenvaltioiden virkamiehiä, tehdyn yleissopimuksen korvaamisesta sekä Euroopan parlamentin ja neuvoston direktiivin (EU) 2017/1371 muuttamisesta, COM(2023) 234 final, 3.5.2023.

[65] https://www.amla.europa.eu/index_fi.

[66] Euroopan parlamentin ja neuvoston direktiivi (EU) 2024/1260, annettu 24 päivänä huhtikuuta 2024, varojen takaisinhankinnasta ja menetetyksi tuomitsemisesta, EUVL L, 2024/1260, 2.5.2024.

luoda uusi EU:n laajuinen järjestelmä. Lisäksi se kannustaa **rahanpesun selvittelykeskuksia** välittämään tietoa lainvalvontaviranomaisille nopeasti ja laajennetusti. Komissio aikoo selvittää tapoja tukkia porsaanreiät, tukea jäsenvaltioita valmiuksien kehittämisessä ja jatkaa yhteistyötä niiden kolmansien maiden kanssa, joita rikolliset hyödyntävät maanalaiseen pankkitoimintaan.

Vakavien rikosten torjunta

Rikollisverkostojen hajottamisen lisäksi myös vakavien rikosten torjunta edellyttää kohdennettuja toimia. Vahvistaakseen kykyä torjua **verkkopetoksia**, jotka aiheuttavat erittäin merkittävää taloudellista haittaa[67], komissio aikoo tukea ennaltaehkäiseviä toimenpiteitä ja tuloksellisempia lainvalvontatoimia. Lisäksi se aikoo tehdä yhteistyötä jäsenvaltioiden ja sidosryhmien kanssa uhrien tukemiseksi ja suojelemiseksi muun muassa avustamalla varojen takaisinhankinnassa. Nämä toimet tullaan kirjaamaan **verkkopetosten torjunnan toimintasuunnitelmaan**.

Komissio tukee **lapsiin kohdistuvan seksuaaliväkivallan** torjuntaa koskevan EU:n strategian (2020–2025)[68] pohjalta lainsäädäntövallan käyttäjiä annettujen kahden lainsäädäntöehdotuksen[69] viimeistelyssä verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan ehkäisemiseksi ja torjumiseksi ja lapsiin kohdistuvan seksuaaliväkivallan ja riiston vastaisten lainvalvontatoimien tuloksellisuuden lisäämiseksi. Koska väliaikaiset säännöt ovat voimassa huhtikuuhun 2026 saakka, on olennaisen tärkeää luoda pysyvä lainsäädäntökehys. Komissio kannustaa lainsäätäjiä aloittamaan neuvottelut asetusehdotuksesta, jossa vahvistetaan säännöt lapsiin kohdistuvan seksuaaliväkivallan ehkäisemiseksi ja torjumiseksi. Lainsäätäjiä kehotetaan myös edistämään neuvotteluja lapsiin kohdistuvan seksuaaliväkivallan ja seksuaalisen riiston sekä lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan materiaalin torjumista koskevasta direktiivistä, jossa vahvistetaan rikosten ja seuraamusten määrittelyä koskevat vähimmäissäännöt lasten seksuaalisen riiston osalta.

Puolet EU:n vaarallisimmista rikollisverkostoista on mukana väkivaltaisessa **huumausainekaupassa**. Vaikka EU on viime aikoina vahvistanut tällaisen rikollisuuden torjuntaa[70] erityisesti laajentamalla **EU:n huumausaineviraston** toimeksiantoa, lisätoimia tarvitaan. Komissio aikoo tehdä tiivistä yhteistyötä jäsenvaltioiden kanssa ehdottaakseen uutta **EU:n huumausainestrategiaa**. Se aikoo myös tarkistaa **huumausaineiden lähtöaineita koskevaa lainsäädäntökehystä** ja ehdottaa **huumekaupan vastaista EU:n toimintasuunnitelmaa** reittien ja liiketoimintamallien tuhoamiseksi. Satamien suojelun vahvistamiseksi perustettua **eurooppalaisen satama-allianssin julkisen ja yksityisen sektorin kumppanuutta** laajennetaan koskemaan pienempiä satamia ja sisävesisatamia ja varmistetaan, että meriturvallisuutta koskevia sääntöjä noudatetaan. Komissio tunnustaa laittoman huumausainekaupan vakavat paikalliset vaikutukset ja aikoo edelleen tukea tasapainoista, näyttöön perustuvaa ja monialaista huumausainepolitiikkaa, joka antaa valmiudet torjua äkillisiä huumausainevirtoja, erityisesti synteettisiä opioideja.

EU on ihmisten hyväksikäytön torjumiseksi hyväksynyt uusia sääntöjä[71], ja se aikoo ottaa käyttöön **ihmiskaupan torjuntaa koskevan uudistetun EU:n strategian** (2026–2030), joka

[67] Global Anti-Scam Report 2024.
[68] COM (2020) 607 final.
[69] COM (2022) 209 final ja COM (2024) 60 final.
[70] COM (2023) 641 final.
[71] Direktiivi (EU) 2024/1712, annettu 13 päivänä kesäkuuta 2024, ihmiskaupan ehkäisemisestä ja torjumisesta sekä ihmiskaupan uhrien suojelemisesta annetun direktiivin 2011/36/EU muuttamisesta, EUVL L, 2024/1712, 24.6.2024.

sisältää kaikki vaiheet ennaltaehkäisystä syytteeseenpanoon ja jossa keskitytään uhrien tukemiseen sekä EU:n että kansainvälisellä tasolla.

Maahantulijoiden salakuljetuksen torjunnassa komissio aikoo johtaa toimia keskeisten kumppaneiden kanssa uuden ihmissalakuljetuksen vastaisen maailmanlaajuisen allianssin kautta yhteistyössä Europolin, Eurojustin ja Frontexin kanssa, myös verkkoulottuvuuden osalta. Salakuljetuksen torjuntaa koskevat komission ehdotukset[72] olisi hyväksyttävä ja pantava täytäntöön viipymättä. Lisäksi komissio on **liikenteenharjoittajia koskevan välineistön**[73] hyväksymisen jälkeen lisännyt yhteydenpitoa ulkomaisten viranomaisten ja liikenteenharjoittajien kanssa ja jatkaa yhteistyötä ilmailualan ja siviili-ilmailujärjestöjen[74] kanssa lisätäkseen tietoisuutta ilmateitse tapahtuvasta maahantulijoiden salakuljetuksesta[75].

Ympäristörikollisuus uhkaa ympäristöä, kansanterveyttä ja taloutta pitkällä aikavälillä. Komissio aikoo tukea jäsenvaltioita ympäristörikosdirektiivin[76] täytäntöönpanossa ja vahvistaa operatiivisia verkostoja ja toimia tällä osa-alueella[77]. Olennaisen tärkeää on jämäkkä noudattamisen valvonta. Lisäksi äskettäin hyväksytty Euroopan neuvoston yleissopimus ympäristönsuojelusta rikosoikeudellisin keinoin[78] auttaa varmistamaan vahvat ja vertailukelpoiset ympäristörikollisuuden torjuntatoimet sekä Euroopassa että sen ulkopuolella.

Rikosoikeudelliset toimet

Rikollisuus ja terrorismi voivat vaikuttaa kaikkiin, minkä vuoksi on olennaisen tärkeää tukea ja turvata **uhrien** oikeudet, jotta voidaan vähentää haittoja ja lisätä yleistä turvallisuutta ja luottamusta viranomaisiin. Komissio aikoo esittää uhrien oikeuksia koskevan direktiivin pohjalta uuden **uhrien oikeuksia koskevan EU:n strategian**.

EU:n rikosoikeusjärjestelmät tarvitsevat vaikuttavia välineitä uusien uhkien torjumiseksi. Tätä varten komissio on käynnistänyt **EU:n rikosoikeuden tulevaisuutta käsittelevän korkean tason foorumin**. Foorumi kokoaa yhteen jäsenvaltioita, Euroopan parlamentin edustajia, EU:n virastoja ja elimiä sekä muita sidosryhmiä. Tavoitteena on keskustella tavoista varmistaa, että rikosoikeusjärjestelmien vaikuttavuus, oikeudenmukaisuus ja häiriönsietokyky pysyy muuttuvien haasteiden tasalla, samalla kun vahvistetaan oikeudellista yhteistyötä ja lisätään keskinäistä luottamusta, myös digitalisaation avulla[79].

Keskeiset toimet

Komissio aikoo

- **esittää vuonna 2026 lainsäädäntöehdotuksen järjestäytyneen rikollisuuden torjunnan uudistamiseksi**

[72] COM (2023) 755 final ja COM (2023) 754 final.

[73] Välineistö, jolla torjutaan kaupallisten kuljetusvälineiden käyttöä EU:hun suuntautuvan laittoman muuttoliikkeen helpottamisessa.

[74] Kansainvälinen siviili-ilmailujärjestö (ICAO) mukaan lukien.

[75] Komissio aikoo tukea myös ihmiskauppaa tai maahanmuuttajien salakuljetusta helpottavien tai harjoittavien liikenteenharjoittajien vastaisista toimenpiteistä annetun asetuksen, COM(2021) 753 final, viimeistelyä.

[76] Euroopan parlamentin ja neuvoston direktiivi (EU) 2024/1203, annettu 11 päivänä huhtikuuta 2024, ympäristön suojelusta rikosoikeudellisin keinoin, EUVL L, 2024/1203, 30.4.2024.

[77] Ympäristölainsäädännön täytäntöönpanoa ja sen noudattamisen valvontaa edistävä EU:n verkosto (IMPEL), ympäristöoikeuteen erikoistuneiden syyttäjien eurooppalainen verkosto (ENPE), ympäristörikollisuuden torjuntaverkosto (EnviCrimeNet) ja ympäristöoikeuteen erikoistuneiden tuomareiden eurooppalainen foorumi (EUFJE).

[78] Ympäristönsuojelua rikosoikeudellisin keinoin käsittelevä asiantuntijakomitea (PC-ENV) – rikosongelmia käsittelevä eurooppalainen komitea.

[79] Muun muassa perustamalla eCODEX-tiedonvaihtojärjestelmä (e-Justice Communication via Online Data Exchange) ja kolmansien maiden kansalaisia koskeva eurooppalainen rikosrekisteritietojärjestelmä (ECRIS-TCN).

- **esittää vuonna 2025 lainsäädäntöehdotuksen huumausaineiden lähtöaineita koskevan lainsäädäntökehyksen tarkistamiseksi**
- **esittää vuonna 2025 lainsäädäntöehdotuksen ampuma-aseiden laitonta kauppaa koskeviksi yhteisiksi rikosoikeudellisiksi normeiksi**
- **arvioida tarvetta tarkistaa pyroteknisiä tuotteita ja siviilikäyttöön tarkoitettuja räjähteitä koskevia direktiivejä**
- **arvioida tarvetta vahvistaa edelleen eurooppalaista tutkintamääräystä ja eurooppalaista pidätysmääräystä**
- **esittää vuonna 2026 EU:lle uuden ihmiskaupan torjuntaa koskevan strategian**
- **esittää vuonna 2026 EU:lle uuden uhrien oikeuksia koskevan strategian**
- **esittää vuoteen 2027 mennessä toimintasuunnitelman lasten suojelemiseksi rikollisuudelta**
- **esittää vuonna 2025 EU:n toimintasuunnitelman huumekaupan torjumiseksi**
- **esittää vuonna 2026 EU:n toimintasuunnitelman ampuma-aseiden laittoman kaupan torjumiseksi**
- **laajentaa onnistuneesti eurooppalaista satama-allianssia vuodesta 2025 alkaen**
- **hyväksyä vuonna 2026 digipalvelusäädökseen liittyviä ohjeita alaikäisten suojelemisesta**
- **esittää vuonna 2026 nettikiusaamisen vastaisen EU:n toimintasuunnitelman**

Jäsenvaltioita kehotetaan

- **saattamaan varojen takaisinhankintaa ja menetetyksi tuomitsemista koskevat uudet säännöt kaikilta osin osaksi kansallista lainsäädäntöä vuoden 2026 loppuun mennessä ja hyödyntämään niitä kaikilta osin**
- **toteuttamaan rikollisten soluttautumisen torjunnassa hallinnollista lähestymistapaa**
- **perustamaan julkisen ja yksityisen sektorin kumppanuuksia rahanpesun torjumiseksi**
- **saattamaan naisiin kohdistuvan väkivallan ja lähisuhdeväkivallan ehkäisemistä ja torjumista koskevan direktiivin osaksi kansallista lainsäädäntöä ja panemaan sen kaikilta osin täytäntöön**

Euroopan parlamenttia ja neuvostoa kehotetaan

- **edetä kohti neuvotteluja asetuksesta, jossa vahvistetaan säännöt lapsiin kohdistuvan seksuaaliväkivallan ehkäisemiseksi ja torjumiseksi, ja direktiivistä, joka koskee lapsiin kohdistuvan seksuaaliväkivallan ja seksuaalisen riiston sekä lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan materiaalin torjumista**
- **saattamaan päätökseen neuvottelut korruption torjuntaa koskevasta direktiivistä**

6. Terrorismin ja väkivaltaisten ääriliikkeiden torjunta

Otamme käyttöön kattavan terrorisminvastaisen agendan, jotta voimme ehkäistä radikalisoitumista, turvata verkkoympäristöä ja julkisia tiloja, tukkia rahoituskanavia ja reagoida iskuihin, kun niitä tapahtuu.

Terrorismin uhka on EU:ssa edelleen suuri. Se liittyy läheisesti geopoliittisten tapahtumien heijastusvaikutuksiin, uusiin teknologioihin ja terrorismin uusiin rahoituskeinoihin. Meidän on varmistettava, että EU on varustautunut hyvin ennakoimaan uhkia, ehkäisemään radikalisoitumista (sekä verkossa että sen ulkopuolella), suojelemaan kansalaisia ja julkisia tiloja iskuilta ja reagoimaan tuloksellisesti iskuihin, kun niitä tapahtuu. Vuoden 2025 aikana esitetään **EU:n uusi agenda terrorismin ja väkivaltaisten ääriliikkeiden ehkäisemiseksi ja**

torjumiseksi. Uutta agendaa noudattaen EU ja Länsi-Balkanin kumppanit allekirjoittavat vuonna 2025 **yhteisen toimintasuunnitelman** terrorismin ja väkivaltaisten ääriliikkeiden ehkäisemiseksi ja torjumiseksi.

Radikalisoitumisen ehkäiseminen ja ihmisten suojelu verkossa

Järjestäytyneen rikollisuuden torjunnan tavoin terrorismin ja väkivaltaisten ääriliikkeiden torjunta alkaa siitä, että **puututaan niiden perimmäisiin syihin**. **Radikalisoitumisen ehkäisemisen EU-tietokeskus** lisää tukeaan alan toimijoille ja päättäjille luomalla uuden **kattavan ennaltaehkäisyvälineistön**, joka mahdollistaa radikalisoitumisen varhaisen tunnistamisen ja siihen puuttumisen keskittyen haavoittuvassa asemassa oleviin henkilöihin ja erityisesti alaikäisiin. Radikalisoitumista tapahtuu usein vankiloissa, ja tukeakseen jäsenvaltioita tämän ongelman ratkaisemisessa komissio antaa uusia suosituksia.

Terroristiset ja väkivaltaiset ääriliikkeet käyttävät verkkoalustoja terroristisen ja haitallisen sisällön levittämiseen, varojen keräämiseen ja värväämiseen. Haavoittuvassa asemassa olevia käyttäjiä, erityisesti alaikäisiä, radikalisoidaan verkossa hälyttävää vauhtia. **Terroristista verkkosisältöä koskeva asetus** on ollut keskeisessä asemassa torjuttaessa terroristisen verkkosisällön leviämistä, ja se on mahdollistanut kaikkein pahimman ja vaarallisimman materiaalin nopean poistamisen[80]. Komissio arvioi parhaillaan asetuksen toimivuutta ja aikoo selvittää, miten tätä säännöstöä voitaisiin parhaiten vahvistaa.

Terrori-iskujen yhteydessä noudatettavaa **EU:n kriisiprotokollaa**, joka mahdollistaa lainvalvontaviranomaisten ja teknologia-alan nopean yhteisen reagoinnin, tullaan muuttamaan, jotta voidaan varmistaa skaalautuvuus ja joustavuus ja näin vastata terrori-iskujen lisääntyvään verkkoulottuvuuteen. EU:n internetfoorumi on jatkossakin tärkein keino tehdä vapaaehtoista yhteistyötä teknologia-alan kanssa terroristisen ja haitallisen verkkosisällön torjumiseksi. Lisäksi komissio on mukana kansainvälisissä aloitteissa, kuten Christchurch Call Foundation -säätiössä ja terrorismintorjunnan maailmanlaajuisessa internetfoorumissa (GIFCT).

Terrorismin rahoituksen torjunta

Terroristit rahoittavat toimintaansa joukkorahoituskampanjoiden, kryptovarojen, uuspankkien tai verkkomaksualustojen kautta. Lainvalvontaviranomaisten on havaittava nämä rahoitusvirrat ja tutkittava niitä. Tähän tarvitaan varoja, välineitä ja asiantuntemusta. Keskeinen rooli tässä on **terrorisminvastaisella talousrikostutkijoiden verkostolla**. Komissio tutkii mahdollisuutta luoda **uusi EU:n laajuinen terrorismin rahoituksen seurantajärjestelmä**, joka kattaisi EU:n sisäiset ja SEPA-maksutapahtumat, kryptovarojen siirrot sekä verkkomaksut ja sähköiset varojen siirrot. Järjestelmä täydentäisi EU:n ja Yhdysvaltojen välistä terrorismin rahoituksen jäljittämisohjelmaa (TFTP) koskevaa sopimusta.

EU:n varoja on **suojeltava väärinkäytöltä radikaalien ja äärinäkemysten edistämiseen** jäsenvaltioissa. Tarkistettuun **varainhoitoasetukseen** sisältyy nyt perusteena EU:n rahoituksen ulkopuolelle jättämiselle tuomio ”yllyttämisestä syrjintään, vihaan tai väkivaltaan”. Komissio jatkaa sen selvittämistä, mikä olisi paras tapa hyödyntää välineistöä, myös mahdollisia tuensaajia valittaessa. EU:n varojen suojaaminen edellyttää myös vahvaa yhteistyötä ja tiedonvaihtoa kansallisten viranomaisten, EU:n virastojen ja elinten välillä.

[80] Joulukuun 31. päivään 2024 mennessä oli annettu 1 426 määräystä poistaa terroristista sisältöä tai estää pääsy siihen. Suurin osa määräyksistä koski jihadista terroristista sisältöä mutta myös oikeistolaista terroristista sisältöä.

Iskuilta suojeleminen

Radikalisoitumisen ehkäisemiseen panostamisen lisäksi tärkeä osa kansalaisten suojelua on rajoittaa terroristien ja rikollisten mahdollisuuksia tehdä iskuja. Toimia tarvitaan sekä terroristien käyttämien välineiden osalta että vaarassa olevien kohteiden suojelemiseksi.

Ampuma-aseita koskevien toimien lisäksi komissio aikoo **tarkistaa räjähteiden lähtöaineita koskevia sääntöjä** ja sisällyttää niihin suuririskiset kemikaalit. **Julkiset tilat** ovat edelleen yleisin terrori-iskujen kohde, erityisesti silloin, kun tekijä on yksittäinen toimija. Kansalaisten suojelemiseksi vahingoittumiselta **EU:n suojaavien turvatoimien neuvontaohjelmaa** vahvistetaan, jotta jäsenvaltioiden pyynnöstä voidaan tehdä julkisten tilojen, kriittisen infrastruktuurin ja suuririskisten tapahtumien haavoittuvuusarviointeja, joita rahoitetaan EU:n varoin sisäisen turvallisuuden rahastosta. EU pyrkii lisäämään julkisten tilojen suojeluun käytettävissä olevaa rahoitusta. Komissio tarjoaa tukea jäsenvaltioiden viranomaisille ja yksityisille toimijoille tarkoitettujen ohjeiden ja välineiden avulla. Näistä voidaan mainita julkisten tilojen suojaamisen tietokeskus[81]. Julkisten tilojen suojaamisen tukemiseen on vuodesta 2020 lähtien myönnetty jo 70 miljoonaa euroa.

Komissio aikoo myös yhteistyössä paikallisviranomaisten ja yksityisten kumppanien kanssa tutkia mahdollisuutta vaatia organisaatioita harkitsemaan tai ottamaan käyttöön turvatoimia julkisissa tiloissa.

Komission toimia juutalaisyhteisön suojelemiseksi ohjaa edelleen **EU:n strategia antisemitismin torjumiseksi ja juutalaisen elämäntavan vaalimiseksi (2021–2030)**, sillä haavoittuvuudet ovat ilmeisiä. Yhtä lailla komissio aikoo varmistaa, että käytössä on asianmukaiset välineet, joilla tuetaan jäsenvaltioita **muslimivihan** torjunnassa.

Droonien käyttö vakoilussa ja iskujen tekemisessä on kasvava turvallisuushaaste. Komissio aikoo kehittää **droonientorjuntajärjestelmien yhdenmukaistetun testausmenetelmän**, perustaa **droonientorjunnan osaamiskeskuksen** ja arvioida tarvetta yhdenmukaistaa jäsenvaltioiden lainsäädäntöä ja menettelyjä[82].

Terrorismiin syyllistyvät vierastaistelijat

Jotta terrorismiin syyllistyvät vierastaistelijat, jotka palaavat tai saapuvat EU:hun voidaan tunnistaa ulkorajoilla, tarvitaan dataa terroriuhan aiheuttavista henkilöistä. Tätä varten komissio vahvistaa yhdessä Europolin kanssa **yhteistyötään keskeisten kolmansien maiden kanssa saadakseen henkilöistä, jotka saattavat aiheuttaa terroriuhan**, kuten terrorismiin syyllistyvistä vierastaistelijoista, **biografista ja biometristä dataa**, joka voidaan syöttää Schengenin tietojärjestelmään sovellettavaa EU:n ja jäsenvaltioiden lainsäädäntöä kaikilta osin noudattaen. Siksi on ratkaisevan tärkeää, että jäsenvaltiot hyödyntävät kaikkia olemassa olevia välineitä. Tähän kuuluvat kaikkien asiaankuuluvien tietojen syöttäminen **SIS-järjestelmään**, biometristen tarkastusten vahvistaminen ja järjestelmällisten tarkastusten suorittaminen pakollisina kaikille henkilöille EU:n ulkorajoilla[83]. Lisäksi Frontexin kehittämillä **yhteisillä riski-indikaattoreilla** tuetaan edelleen jäsenvaltioiden rajavalvontaviranomaisia, jotta ne voivat tunnistaa mahdollisten terrorismiin syyllistyvien vierastaistelijoiden epäilyttävän matkustamisen riskin ja arvioida sitä.

Lisäksi sen varmistamiseksi, että jäsenvaltioilla säilyy pääsy **taistelukentiltä saatuihin todisteisiin**, jotka YK:n UNITAD-tutkintaryhmä, joka pyrkii saattamaan syylliset vastuuseen Daeshin/ISILin tekemistä rikoksista, on kerännyt terrorismiin syyllistyvien vierastaistelijoiden

[81] Julkisten tilojen suojaamisen tietokeskus.
[82] Vuonna 2023 annetussa droonientorjuntatiedonannossa COM(2023) 659 final esitettyjen keskeisten toimien pohjalta.
[83] Kaikilta osin Schengenin rajasäännöstöä ja seulonta-asetusta noudattaen.

syytteeseenpanoa varten, komissio aikoo yhdessä Eurojustin kanssa arvioida mahdollisuutta tallentaa nämä todisteet Eurojustin keskeiseen kansainväliseen rikosaineistotietokantaan. Lisäksi uusi eurooppalainen **terrorismintorjuntarekisteri** on edelleen jäsenvaltioiden oikeuslaitosten tukena valtioiden rajat ylittävien kytkösten nopeassa tunnistamisessa terrorismitapauksissa.

Keskeiset toimet

Komissio aikoo

- **hyväksyä vuonna 2025 EU:lle uuden agendan terrorismin ja väkivaltaisten ääriliikkeiden ehkäisemiseksi ja torjumiseksi**
- **allekirjoittaa vuonna 2025 Länsi-Balkanin kumppaneiden kanssa uuden yhteisen toimintasuunnitelman terrorismin ja väkivaltaisten ääriliikkeiden ehkäisemiseksi ja torjumiseksi**
- **luoda uuden kattavan ennaltaehkäisyvälineistön radikalisoitumisen ehkäisemisen EU-tietokeskuksen kanssa**
- **arvioida vuonna 2026 terroristista verkkosisältöä koskevan asetuksen soveltamista**
- **muuttaa vuonna 2025 EU:n kriisiprotokollaa**
- **esittää vuonna 2026 ehdotuksen räjähteiden lähtöaineiden markkinoille saattamista ja käyttöä koskevan asetuksen tarkistamiseksi**
- **tehdä EU:n laajuista terrorismin rahoituksen seurantajärjestelmää koskevan toteutettavuustutkimuksen**

Jäsenvaltioita kehotetaan

- **parantamaan biometrisiä tarkastuksia ja tekemään järjestelmällisiä tarkastuksia pakollisina EU:n ulkorajoilla**
- **kaikilta osin hyödyntämään eurooppalaista terrorismintorjuntarekisteriä**

7. EU on vahva turvallisuustoimija globaalissa mittakaavassa

Parantaaksemme EU:n turvallisuutta aiomme lisätä operatiivista yhteistyötä kumppanuuksien kautta keskeisten alueiden, kuten laajentumis- ja naapuruuskumppaniemme, Latinalaisen Amerikan ja Välimeren alueen maiden kanssa. EU:n turvallisuusedut tullaan ottamaan huomioon kansainvälisessä yhteistyössä muun muassa hyödyntämällä EU:n työkaluja ja välineitä.

Viime vuosina on käynyt ilmi, että EU:n sisäinen ja ulkoinen turvallisuus kytkeytyvät luontaisesti toisiinsa. Venäjän hyökkäyssodalla Ukrainaa vastaan, Gazan konfliktilla, Syyrian tilanteella ja eri puolilla maailmaa esiin nousevilla konflikteilla on ollut vakavia heijastusvaikutuksia EU:n sisäiseen turvallisuuteen. Torjuakseen maailmanlaajuisen epävakauden vaikutuksia sisäiseen turvallisuuteensa **EU:n on puolustettava turvallisuusetujaan aktiivisesti** torjumalla ulkoisia uhkia, katkaisemalla ihmiskauppareittejä ja turvaamalla strategisesti tärkeitä käytäviä, kuten kauppareittejä. Samalla EU on edelleen vahva liittolainen kumppanimailleen, joiden kanssa tehdään yhteistyötä, jotta maailmanlaajuista turvallisuutta voidaan parantaa ja molemmin puolin lisätä kykyä selviytyä uhkista.

EU on viime vuosina toteuttanut merkittäviä toimia turvallisuusyhteistyönsä parantamiseksi. Kumppanimaiden kanssa on tehty sopimuksia operatiivisesta lainvalvontayhteistyöstä ja oikeudellisesta yhteistyöstä, kuten myös sovittu muuntyyppisistä järjestelyistä. EU pyrkii aktiivisesti uusiin kansainvälisiin sopimuksiin, neuvoston

neuvotteluohjeita noudattaen, ja valmiuksien kehittämistä koskeviin aloitteisiin EU:n virastojen ja elinten tukemana. Keskeinen tekijä turvallisuuden vahvistamisessa kumppanimaiden kanssa on myös naapuruus-, kehitys- ja kansainvälisen yhteistyön väline – Globaali Eurooppa.

Sääntöpohjainen monenvälinen maailmanjärjestys on globaalin turvallisuuden vahvistamisen kulmakivi. Keskeisessä asemassa sitä tukevien toimien vahvistamisessa ovat turvallisuusvuoropuhelut, myös eri teemoihin keskittyvät. **Turvallisuus- ja puolustusalan strategisen kompassin** tavoitteiden saavuttaminen sekä kahden- ja monenväliset yhteistyökehykset, kuten vakautus- ja assosiaatiosopimukset ja assosiaatiosopimukset, sekä yhteistyö YK:n ja Naton kaltaisten järjestöjen kanssa ovat ratkaisevan tärkeitä toimivien turvallisuusratkaisujen kehittämiseksi. EU tulee jatkamaan työtään monenvälisillä foorumeilla[84] ja parantamaan yhteistyötään kansainvälisten ja alueellisten järjestöjen ja kehysten kanssa, mukaan lukien Nato, YK, Euroopan neuvosto, Interpol, G7, Etyj ja kansalaisyhteiskunta.

Alueellinen yhteistyö

EU:n **Ukrainalle** antaman horjumattoman tuen jatkaminen ja **EU:n laajentumismaiden** turvallisuuden ja häiriönsietokyvyn vahvistaminen ovat prioriteetti sekä poliittinen ja geostrateginen välttämättömyys. EU:n turvallisuuden tukemisen rinnalla olisi **nopeutettava ehdokasmaiden yhdentymistä EU:n turvallisuusrakenteisiin** ja samaan aikaan vahvistettava niiden alueellista yhteistyötä. Komissio aikoo EU:n laajentumispolitiikan kautta tukea EU:n ehdokasmaiden ja mahdollisten ehdokasmaiden valmiuksia vastata uhkiin, lisätä operatiivista yhteistyötä ja tietojenvaihtoa sekä varmistaa mukautumisen EU:n periaatteisiin, lainsäädäntöön ja välineisiin. Ratkaisevan tärkeitä välineitä turvallisuuden vahvistamiseksi sekä ehdokasmaissa että mahdollisissa ehdokasmaissa ovat liittymistä valmisteleva tukiväline (IPA III) sekä Ukrainan, Moldovan ja Länsi-Balkanin tukivälineet.

EU aikoo myös nivoa **naapuruuskumppaninsa** tiiviimmin osaksi EU:n turvallisuusrakenteita. Unioni pyrkii **Välimeren aluetta koskevan uuden sopimuksen** ja tulevan **Mustanmeren strategisen toimintamallin** avulla jatkamaan turvallisuusnäkökohdat kattavan alueellisen yhteistyön ja kahdenvälisten strategisten kokonaisvaltaisten kumppanuuksien kehittämistä, tarvittaessa käymällä säännöllistä korkean tason turvallisuusvuoropuhelua. Operatiivista yhteistyötä Pohjois-Afrikan, **Lähi-idän ja Persianlahden** maiden kanssa aiotaan vahvistaa erityisesti terrorismin, rahanpesun, ampuma-aseiden laittoman kaupan sekä huumausaineiden (erityisesti captagonin) tuotannon ja kaupan torjunnassa.

Torjuakseen terrorismin ja rikollisen toiminnan lisääntymistä ja sen mahdollisia heijastusvaikutuksia **Saharan eteläpuolisessa Afrikassa, erityisesti Sahelissa, Afrikan sarvessa ja Länsi-Afrikassa** EU vahvistaa tukeaan Afrikan unionille, alueellisille talousyhteisöille ja alueen maille. EU:n merellistä turvallisuusstrategiaa[85] noudattaen EU vahvistaa yhteistyötä **Guineanlahdella, Punaisellamerellä ja Intian valtamerellä** laittoman kaupan ja merirosvouksen torjumiseksi tukemalla Afrikan sisäistä ja alueellista yhteistyötä tukeutuen EU:n koordinoituun läsnäoloon merialueilla (CMP) ja huumausaineiden merikuljetusten analysointi- ja torjuntakeskukseen (MAOC-N).

EU aikoo vahvistaa operatiivista yhteistyötään **Latinalaisen Amerikan ja Karibian maiden** kanssa, jotta korkean riskin rikollisverkostoja voidaan hajottaa ja panna syytteeseen, saada laitonta toimintaa lakkaamaan ja katkaista salakuljetusreittejä, ja parantaa yhteistyörakenteita,

[84] Maailmanlaajuinen terrorisminvastainen foorumi, Da'eshin vastainen maailmanlaajuinen liittoutuma, terrorismintorjunnan maailmanlaajuinen internetfoorumi (GIFCT), Christchurch Call Foundation, synteettisten huumausaineiden uhkia käsittelevä maailmanlaajuinen liittouma.
[85] JOIN (2023) 8 final.

kuten EU:n ja Latinalaisen Amerikan sisäisen turvallisuuden komitea (CLASI) ja EU:n ja Latinalaisen Amerikan ja Karibian valtioiden yhteisön (CELAC) huumeidentorjunnan koordinointi- ja yhteistyöjärjestelmä. Prioriteetteihin kuuluvat logistiikkakeskusten häiriönsietokyky ja kumppanuudet sekä rahavirtoja seuraavat toimintamallit. EU aikoo edelleen tukea Amerikkojen poliisiyhteisön (AMERIPOL) kehittämistä Europolin alueelliseksi vastineeksi ja vahvistaa EU:n jäsenvaltioiden ja kyseisen alueen välistä oikeudellista yhteistyötä. EU tulee tekemään yhteistyötä myös **Etelä- ja Keski-Aasian** kanssa terrorismiin, tavaroiden laittomaan kauppaan, huumekauppa mukaan lukien, ihmiskauppaan ja maahantulijoiden salakuljetukseen liittyvien yhteisten turvallisuushaasteiden osalta.

Lisäksi EU aikoo tukea kolmansien maiden alueellisia yhteistyörakenteita auttaakseen niitä lopettamaan laittoman kaupan sen lähteellä sillä periaatteella, että vastuu on yhteinen koko rikollisen toimitusketjun osalta. Lisäksi EU pyrkii osaltaan vahvistamaan logistiikkakeskusten turvallisuutta ulkomailla koordinoimalla **yhteisiä tarkastuksia kolmansien maiden satamissa**.

Operatiivinen yhteistyö

Global Gateway -strategialla tuetaan kestäviä ja laadukkaita infrastruktuurihankkeita, jotka liittyvät digitalisaatioon, ilmastoon ja energiaan, liikenteeseen, terveydenhuoltoon, koulutukseen ja tutkimukseen. Komissio aikoo sisällyttää tuleviin Global Gateway -investointeihin soveltuvin osin turvallisuusnäkökohtia. Tämä koskee EU:n ja sen kumppanimaiden strategisen autonomian kannalta kriittisiä aloitteita, kuten infrastruktuurihankkeita, joihin sisältyy turvallisuusarviointeja ja riskinhallintatoimenpiteitä.

Komissio aikoo tehdä lisää **EU:n ja kolmansien maiden välisiä sopimuksia yhteistyöstä Europolin ja Eurojustin kanssa**, erityisesti Latinalaisen Amerikan maiden kanssa.

Yksi vaikuttavimmista keinoista vahvistaa operatiivista yhteistyötä on EU:n ulkopuolisten maiden aktiivinen osallistuminen **Euroopan monialaiseen rikosuhkien torjuntafoorumin (EMPACT)**. EU aikoo edelleen kannustaa kolmansia maita, erityisesti Länsi-Balkania, itäistä naapurustoa, Saharan eteläpuolista Afrikkaa, Pohjois-Afrikkaa, Lähi-itää, Latinalaista Amerikkaa ja Karibian aluetta, osallistumaan foorumiin. Toinen väline, jolla rikostentorjuntayhteistyötä kolmansien maiden kanssa voidaan parantaa, ovat jäsenvaltioiden väliset ja Europolin koordinoimat operatiiviset toimintaryhmät, joihin kolmannet maat voivat osallistua. Komissio pyrkii myös saattamaan päätökseen neuvottelut **EU:n ja Interpolin** kansainvälisestä sopimuksesta[86], jolla voitaisiin varmistaa yhtenäisempi maailmanlaajuisia turvallisuusuhkia koskeva toimintamalli ja torjua kansainvälistä rikollisuutta.

Unionin on oltava Team Europe -hengessä läsnä kentällä. Unionin ja jäsenvaltioiden asiantuntijahenkilöstöllä on ratkaiseva rooli sen varmistamisessa, että unionin ulkoista toimintaa hoidetaan hyvin perehtyen, koordinoidusti ja tilanteeseen reagoiden. Nostaakseen tämän toimintamallin uudelle tasolle komissio aikoo unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan tukemana vahvistaa **yhteysverkostoja** ja helpottaa **Europolin ja Eurojustin yhteyshenkilöiden** lähettämistä eri alueille jäsenvaltioiden operatiivisten tarpeiden mukaisesti.

EU pyrkii tiiviimpään operatiiviseen lainvalvonta- ja oikeudelliseen yhteistyöhön, edistää reaaliaikaista tietojenvaihtoa ja yhteisiä operaatioita kolmansissa maissa toimivien **yhteisten tutkintaryhmien** kautta Europolin ja Eurojustin tuella. Komissio aikoo tukea jäsenvaltioita myös sellaisten **yhteisten fuusiokeskusten** perustamisessa, jotka kokoavat yhteen

[86] Neuvoston päätös (EU) 2021/1312, annettu 19 päivänä heinäkuuta 2021, ja neuvoston päätös (EU) 2021/1313, annettu 19 päivänä heinäkuuta 2021.

asiantuntijoita ja paikallisten lainvalvontaviranomaisten edustajia strategisissa kolmansissa maissa.

Yhteisen ulko- ja turvallisuuspolitiikan (YUTP) välineet

Jotta EU:n sisäiseen turvallisuuteen kohdistuvia ulkoisia uhkia voitaisiin paremmin tunnistaa ja torjua, myös **yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) operaatioita** tullaan hyödyntämään täysipainoisesti, neuvoston operaatioille asettamia toimeksiantoja noudattaen. Kolmansien maiden valmiuksien kehittämiseksi unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja ja komissio aikovat tukea YTPP-toimia erityisillä rahoitusvälineillä ja tutkivat kaikkia sopivia rahoitusmahdollisuuksia.

EU:n rajoittavat toimenpiteet ovat vakiintunut YUTP:n väline, jota käytetään myös terrorismin torjunnassa. Neuvosto voisi ulkoasioiden ja turvallisuuspolitiikan korkean edustajan, jäsenvaltioiden tai komission ehdotusten perusteella arvioida, miten EU:n nykyisistä yksipuolisista rajoittavista toimenpiteistä (EU:n terroristiluettelo) voitaisiin tehdä vaikuttavampia, toimivampia ja ketterämpiä. Lisäksi voitaisiin harkita rikollisverkostoihin kohdistettavien rajoittavien lisätoimenpiteiden tutkimista YUTP:n tavoitteiden mukaisesti.

Viisumipolitiikka ja tietojenvaihto

EU:n viisumipolitiikka on keskeinen väline kolmansien maiden kanssa tehtävässä yhteistyössä ja EU:n rajojen turvaamisessa, kun EU:hun saapumista valvotaan ja asetetaan sille ehdot. Komissio aikoo ottaa **turvallisuusnäkökohdat kaikilta osin huomioon EU:n viisumipolitiikassa** tulevan EU:n viisumipolitiikan strategian kautta. Komissio aikoo tehdä yhteistyötä lainsäätäjien kanssa hyväksyäkseen ehdotuksen viisumivapauden keskeyttämismekanismin tarkistamisesta ja virtaviivaistamisesta erityisesti yksittäisten viisumivapauden väärinkäyttötapausten osalta[87]. Kolmansia maita on tarkoitus kannustaa tietojen jakamiseen henkilöistä, jotka saattavat aiheuttaa turvallisuusuhkia, ja tiedot syötetään EU:n tietojärjestelmiin ja tietokantoihin.

Politiikan koordinoinnin ja alkuvaiheen toimien aikaansaamiseksi sekä tehokkaamman, nopeamman ja sujuvamman yhteistyön toteuttamiseksi komissio pyrkii luomaan lainvalvontaa ja rajavalvontaa varten **datankulkujärjestelyjä** ja tutkimaan tapoja **parantaa tietojenvaihtoa** luotettavien kolmansien maiden kanssa perusoikeuksia ja tietosuojasääntöjä noudattaen.

Keskeiset toimet

Komissio aikoo

- **tehdä EU:n ja priorisoitavien kolmansien maiden välillä kansainvälisiä sopimuksia yhteistyöstä Europolin ja Eurojustin kanssa**
- **kannustaa kumppanimaita osallistumaan Euroopan monialaiseen rikosuhkien torjuntafoorumiin (EMPACT) järjestäytyneen rikollisuuden ja terrorismin torjumiseksi**
- **tukea EU:n virastoja ja elimiä työjärjestelyjen luomisessa ja vahvistamisessa kumppanimaiden kanssa**
- **ottaa turvallisuusnäkökohdat paremmin huomioon EU:n viisumipolitiikassa tulevan viisumistrategian kautta**
- **vahvistaa tietojenvaihtoa luotettavien kolmansien maiden kanssa lainvalvontaa ja rajavalvontaa varten**

Komissio aikoo yhteistyössä EU:n ulkoasiainedustajan kanssa

[87] COM(2023) 642.

- **hyödyntää täysipainoisesti yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) siviilioperaatioita**
- **koordinoida yhteisiä tarkastuksia kolmansien maiden satamissa viimeistään vuonna 2027**

Komissio aikoo yhteistyössä EU:n ulkoasiainedustajan ja jäsenvaltioiden kanssa

- **vahvistaa yhteysverkostoja ja yhteistyötä Team Europe -lähestymistapaa noudattaen**
- **perustaa yhteisiä toimintaryhmiä ja fuusiokeskuksia kolmansiin maihin vuodesta 2025 alkaen**

Euroopan parlamenttia ja neuvostoa kehotetaan

- **saattamaan päätökseen neuvottelut viisumivapauden keskeyttämismekanismin tarkistamisesta**

8. Päätelmät

Epävarmassa maailmantilanteessa unionin valmiuksia ennakoida ja ehkäistä turvallisuusuhkia ja reagoida niihin on parannettava.

Pelkkä kriiseihin reagoiminen niitä kohdattaessa ei riitä. Meidän on terävöitettävä tietoisuuttamme uhkista, ja meillä on oltava niistä kattava kuva niiden kehittyessä. Meidän on varmistettava, että työkalumme ja voimavaramme ovat tehtävän tasalla.

Tässä strategiassa esitetty kattava toimenpidekokonaisuus auttaa luomaan unionin, joka on tässä maailmassa vahvempi: unionin, joka pystyy ennakoimaan ja suunnittelemaan omia turvallisuustarpeitaan ja huolehtimaan niistä, unionin, joka voi vastata tuloksellisesti sisäiseen turvallisuuteensa kohdistuviin uhkiin ja saattaa tekijät vastuuseen, unionin, joka suojelee avoimia, vapaita ja vauraita yhteiskuntiaan ja demokratioitaan.

Käsityksemme sisäisestä turvallisuudesta on muututtava. Aiomme tehdä työtä edistääksemme EU:ssa uutta turvallisuuskulttuuria, jossa turvallisuusnäkökohdat otetaan huomioon kaikessa lainsäädännössä, politiikoissa ja ohjelmissa – alusta lähtien täytäntöönpanoon asti – ja jossa eri politiikanalojen välinen yhteistyö antaa meille mahdollisuuden luoda uutta.

Kyseessä ei ole vain yhden toimielimen, hallituksen tai toimijan tehtävä vaan Euroopan yhteinen hanke.