EUROOPAN
KOMISSIO

Bryssel 24.7.2020
COM(2020) 605 final

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

EU:n turvallisuusunionistrategiasta

I. Johdanto

Komission poliittisissa suuntaviivoissa tehtiin selväksi, että meidän on tehtävä kaikkemme unionin kansalaisten suojelemiseksi. Turvallisuus on ensiarvoisen tärkeää henkilötasolla, mutta se suojelee myös perusoikeuksia sekä luo perustan taloutemme, yhteiskuntamme ja demokratiamme luottamukselle ja dynaamisuudelle. Euroopan turvallisuusympäristö on muutostilassa. Syynä tähän ovat muuttuvat uhat sekä muut tekijät, kuten ilmastonmuutos, väestönkehityksen suuntaukset ja poliittinen epävakaisuus rajojemme ulkopuolella. Globalisaatio, vapaa liikkuvuus ja digitalisaatio tuovat jatkossakin vaurautta, helpottavat elämäämme sekä vauhdittavat innovointia ja kasvua. Näihin hyötyihin sisältyy kuitenkin myös riskejä ja kustannuksia. Eurooppalaiseen elämäntapaan kohdistuvat välittömät uhat, kuten terrorismi, järjestäytynyt rikollisuus sekä huume- ja ihmiskauppa, voivat käyttää niitä hyväkseen. Kyberhyökkäykset ja -rikollisuus lisääntyvät jatkuvasti. Turvallisuusuhat ovat muuttumassa monimutkaisemmiksi: rajatylittävät työskentelymahdollisuudet ja yhteenliitettävyys hyödyttävät niitä, ne käyttävät hyväkseen fyysisen ja digitaalisen maailman välisiä hämärtyviä rajoja, heikossa asemassa olevia ryhmiä sekä sosiaalisia ja taloudellisia eroja. Hyökkäykset voivat tapahtua hetkessä, eikä niistä välttämättä jää lainkaan jälkiä. Sekä valtiolliset että valtiosta riippumattomat toimijat voivat hyödyntää monenlaisia hybridiuhkia[1], ja EU:n ulkopuolisilla tapahtumilla voi olla kriittisiä vaikutuksia EU:n sisäiseen turvallisuuteen.

Myös covid-19-kriisi on muuttanut käsitystämme turvallisuudesta, turvallisuusuhista ja niihin liittyvistä politiikoista. Se on tuonut esiin tarpeen taata turvallisuus sekä fyysisissä että digitaalisissa ympäristöissä. Se on korostanut avoimen strategisen riippumattomuuden merkitystä toimitusketjuillemme kriittisten tuotteiden, palvelujen, infrastruktuurien ja teknologioiden suhteen. Se on lisännyt tarvetta ottaa jokainen ala ja yksilö mukaan yhteisiin toimiin, jotta voimme varmistaa, että EU on alusta asti valmistautuneempi, sietokykyisempi ja paremmin varustautunut reagoimaan tarpeen vaatiessa.

Jäsenvaltiot eivät voi suojella kansalaisia vain toimimalla yksin. Vahvuuksiemme hyödyntäminen yhteistyöllä ei ole koskaan ollut tärkeämpää, eikä EU:lla ole koskaan ollut parempia mahdollisuuksia vaikuttaa asioihin. Unioni voi näyttää esimerkkiä parantamalla yleistä kriisinhallintajärjestelmäänsä ja työskentelemällä rajojensa sisä- ja ulkopuolella maailmanlaajuisen vakauden edistämiseksi. Vaikka ensisijainen vastuu turvallisuudesta on jäsenvaltioilla, viime vuodet ovat osoittaneet yhä selkeämmin, että yhden jäsenvaltion turvallisuus vaikuttaa kaikkien turvallisuuteen. Toteuttamalla monialaisia ja integroituja ratkaisuja EU voi auttaa jäsenvaltioiden turvallisuusalan toimijoita tarjoamalla tarvittavia välineitä ja tietoja.[2]

EU voi myös varmistaa, että turvallisuuspolitiikka perustuu yhteisiin eurooppalaisiin arvoihin – oikeusvaltioperiaatteen, tasa-arvon[3] ja perusoikeuksien kunnioittamiseen ja vaalimiseen sekä avoimuuden, vastuuvelvollisuuden ja demokraattisen valvonnan takaamiseen. Ne luovat politiikoille oikeanlaisen luottamusperustan. EU voi rakentaa

[1] Hybridiuhkien määritelmät vaihtelevat, mutta niillä tarkoitetaan erilaisia pakottavia ja turvallisuutta vaarantavia toimia ja (diplomaattisia, sotilaallisia, taloudellisia ja teknisiä) perinteisiä ja uusia menetelmiä, joita valtiolliset tai valtiosta riippumattomat toimijat voivat käyttää koordinoidusti tiettyjen tavoitteiden saavuttamiseksi (ilman, että sotatilan virallisen julistamisen kynnys ylittyy). Ks. JOIN(2016) 18 (final).

[2] Esimerkiksi EU:n Copernicus-avaruusohjelman tuottamat palvelut tarjoavat maanhavainnointitietoja ja sovelluksia rajavalvontaan, meriturvallisuuteen, lainvalvontaan, merirosvouksen ja huumeiden salakuljetuksen torjuntaan sekä hätätilanteiden hallintaan.

[3] Tasa-arvon unioni: sukupuolten tasa-arvostrategia 2020–2025, COM(2020) 152.

toimivan ja aidon turvallisuusunionin, jossa yksilöiden oikeudet ja vapaudet on turvattu. Turvallisuus ja perusoikeuksien kunnioittaminen eivät ole ristiriitaisia vaan yhdenmukaisia tavoitteita, ja ne täydentävät toisiaan. Turvallisuuspolitiikkojen on perustuttava arvoihimme ja perusoikeuksiimme. Niillä taataan tarpeellisuuden, suhteellisuuden ja laillisuuden periaatteet sekä asianmukaiset vastuuvelvollisuudet ja oikeussuojakeinot. Niiden on mahdollistettava tehokkaat toimet erityisesti heikoimmassa asemassa olevien ihmisten suojaamiseksi.

Tärkeitä oikeudellisia, käytännöllisiä ja tukivälineitä on jo käytössä, mutta niitä on vahvistettava ja niiden täytäntöönpanoa on parannettava. Jäsenvaltioiden välisessä tietojen ja tiedustelutietojen vaihdossa sekä terroristien ja muiden rikollisten toimintatilan kaventamisessa on edistytty huomattavasti. Parantamisen varaa kuitenkin on.

Työtä on jatkettava myös EU:n rajojen ulkopuolella. Unionin ja sen kansalaisten suojelemisessa ei ole enää kyse turvallisuuden varmistamisesta vain EU:n rajojen sisällä, vaan myös turvallisuuden ulkoisen ulottuvuuden huomioimisesta. EU:n lähestymistapa ulkoiseen turvallisuuteen yhteisen ulko- ja turvallisuuspolitiikan (YUTP) ja yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) mukaisesti on edelleen olennainen osa EU:n pyrkimyksiä parantaa turvallisuutta EU:ssa. Tehokkaat ja kattavat toimet edellyttävät kolmansien maiden kanssa tehtävää ja maailmanlaajuista yhteistyötä yhteisiin haasteisiin vastaamiseksi, sillä vakaus ja turvallisuus EU:n naapurustossa ovat ratkaisevan tärkeitä myös EU:n oman turvallisuuden kannalta.

Tämä uusi strategia perustuu Euroopan parlamentin[4], neuvoston[5] ja komission[6] aiempaan työhön ja osoittaa, että toimivan ja todellisen turvallisuusunionin on oltava yhdistelmä vahvoja välineitä ja politiikkoja, joilla turvallisuus voidaan taata käytännössä. Lisäksi on tiedostettava, että turvallisuudella on vaikutuksia yhteiskunnan kaikkiin osiin ja kaikkiin julkisiin politiikkoihin. EU:n on varmistettava turvallinen elinympäristö kaikille rodusta tai etnisestä alkuperästä, uskonnosta, vakaumuksesta, sukupuolesta, iästä tai sukupuolisesta suuntautumisesta riippumatta.

Strategia kattaa vuodet 2020–2025, ja siinä keskitytään tulevaisuuden kannalta kestävän turvallisuusympäristön edellyttämien voimavarojen ja valmiuksien kehittämiseen. Strategiassa esitetään koko yhteiskunnan kattava lähestymistapa, joka mahdollistaa tehokkaan ja koordinoidun reagoimisen nopeasti muuttuviin uhkaympäristöihin. Siinä määritellään strategiset painopisteet ja niihin liittyvät toimet, joilla digitaalisiin ja fyysisiin riskeihin voidaan puuttua yhdenmukaisella tavalla koko turvallisuusunionin ekosysteemissä keskittyen siihen, missä EU voi tuoda lisäarvoa. Tavoitteena on kaikkien ihmisten turvallisuuden takaaminen EU:ssa.

---

[4] Esimerkiksi Euroopan parlamentin terrorismia käsittelevän erikoisvaliokunnan (TERR) laatima mietintö marraskuulta 2018.

[5] Uudistetusta sisäisen turvallisuuden strategiasta kesäkuussa 2015 annetuista neuvoston päätelmistä neuvoston viimeaikaisiin päätelmiin joulukuulta 2019.

[6] ”Euroopan turvallisuusagendan valjastaminen terrorismin torjuntaan ja toimivan ja todellisen turvallisuusunionin perustamisen valmisteluun”, COM(2016) 230 final, 20.4.2016. Ks. viimeaikainen arvio sisäistä turvallisuutta koskevan lainsäädännön täytäntöönpanosta: Sisäasioita koskevan lainsäädännön täytäntöönpano sisäisen turvallisuuden alalla – 2017–2020, (SWD(2020) 135).

II. Euroopan nopeasti muuttuva turvallisuusuhkaympäristö

Turvallisuus on kansalaisten vaurauden ja hyvinvoinnin edellytys. Tähän turvallisuuteen kohdistuvat uhat riippuvat siitä, miten haavoittuvia ihmisten elämät ja toimeentulo ovat. Mitä haavoittuvampia ne ovat on, sitä suuremmalla todennäköisyydellä niitä voidaan hyödyntää. Sekä haavoittuvuudet että uhat kehittyvät jatkuvasti, ja EU:n on mukauduttava niihin.

Päivittäinen elämämme on monenlaisten palvelujen varassa – näitä ovat esimerkiksi energia-, liikenne- ja rahoituspalvelut sekä terveydenhuolto. Ne ovat riippuvaisia sekä fyysisestä että digitaalisesta infrastruktuurista, mikä lisää haavoittuvuutta ja häiriöiden mahdollisuutta. Covid-19-pandemian aikana uudet teknologiat ovat pitäneet monet yritykset ja julkiset palvelut toiminnassa, esimerkiksi mahdollistamalla etätyöskentelyn tai pitämällä toimitusketjut liikkeessä. Tämä on kuitenkin myös lisännyt poikkeuksellisen paljon vihamielisiä hyökkäyksiä, joiden tavoitteena on saada rikollista hyötyä pandemian aiheuttamista häiriöistä ja ihmisten siirtymisestä koteihinsa digitaaliseen etätyöhön.[7] Tarvikepula on luonut järjestäytyneelle rikollisuudelle uusia mahdollisuuksia. Seuraukset olisivat voineet olla hengenvaarallisia ja aiheuttaa häiriöitä keskeisille terveyspalveluille aikana, jolloin niihin kohdistui eniten paineita.

Digitaaliteknologia helpottaa elämäämme yhä useammilla tavoilla, mutta se on myös tehnyt teknologian **kyberturvallisuudesta** strategisesti tärkeän kysymyksen.[8] Kyberhyökkäyksillä on huomattavia haittavaikutuksia koteihin, pankkeihin, rahoituspalveluihin ja yrityksiin (erityisesti pk-yrityksiin). Fyysisten ja digitaalisten järjestelmien keskinäinen riippuvuus pahentaa mahdollisia vahinkoja entisestään: kaikilla fyysisillä iskuilla on vaikutusta digitaalisiin järjestelmiin, ja tietojärjestelmiin ja digitaalisiin infrastruktuureihin kohdistuvat kyberhyökkäykset voivat lamauttaa keskeisiä palveluita.[9] Esineiden internetin laajeneminen ja tekoälyn käytön lisääntyminen tuovat sekä uusia hyötyjä että uusia riskejä.

Maailma on riippuvainen digitaalisista infrastruktuureista, teknologioista ja verkkojärjestelmistä, joiden avulla voidaan harjoittaa liiketoimintaa, kuluttaa tuotteita ja nauttia palveluista. Kaikki on viestinnän ja vuorovaikutuksen varassa. Verkkoriippuvuus on avannut oven **kyberrikollisuuden** aallolle.[10] Kyberrikospalvelut ja maanalainen kyberrikollistalous tarjoavat helpon pääsyn kyberrikollisuuden tuotteisiin ja palveluihin verkossa. Rikolliset oppivat nopeasti käyttämään uutta teknologiaa omiin tarkoituksiinsa. Esimerkiksi lääkevääreennöksiä on päässyt lääkkeiden lailliseen toimitusketjuun.[11] Verkossa olevan lasten seksuaalista hyväksikäyttöä kuvaavan materiaalin räjähdysmäinen kasvu[12] on

---

7 Europol: ”Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU”, huhtikuu 2020.

8 Komission 5G-verkkojen kyberturvallisuutta koskeva suositus, C(2019) 2335; tiedonanto ”5G:n turvallinen käyttöönotto EU:ssa – EU:n välineistön täytäntöönpano”, COM(2020) 50.

9 Tšekissä sijaitsevaan Brnon yliopistolliseen sairaalaan kohdistui maaliskuussa 2020 verkkohyökkäys, joka pakotti sen siirtämään potilaita ja lykkäämään leikkauksia (Europol: ”Pandemic Profiteering. How criminals exploit the COVID-19 crisis”). Tekoälyä voidaan väärinkäyttää digitaalisissa, poliittisissa ja fyysisissä hyökkäyksissä sekä vakoilussa. Esineiden internetin suorittamaa tiedonkeruuta voidaan käyttää ihmisten tarkkailemiseen (älykellot, virtuaaliavustajat jne.).

10 Joidenkin ennusteiden mukaan tietoturvaloukkausten kustannukset nousevat 5 biljoonaan dollariin vuodessa vuoteen 2024 mennessä, kun ne vuonna 2015 olivat 3 biljoonaa dollaria (Juniper Research, The Future of Cybercrime & Security).

11 Eräässä vuonna 2016 tehdyssä tutkimuksessa (Legiscript) arvioitiin, että maailmanlaajuisesti internetapteekeista vain 4 prosenttia toimii laillisesti ja että EU:n kuluttajat ovat verkossa toimivien 30 000 – 35 000 laittoman apteekin tärkein kohderyhmä.

12 EU:n strategia lasten seksuaalisen hyväksikäytön torjunnan tehostamiseksi, COM(2020) 607.

osoittanut rikollisuuden muuttumisen sosiaaliset seuraukset. Hiljattain tehty tutkimus osoitti, että suurin osa EU:n kansalaisista (55 %) on huolissaan siitä, että rikolliset ja huijarit pääsevät käsiksi heidän tietoihinsa.[13]

Myös **globaali ympäristö** korostaa näitä uhkia. Kolmansien maiden tiukka teollisuuspolitiikka ja jatkuvat teollis- ja tekijänoikeuksien varkaudet verkossa muuttavat strategista paradigmaa kohti Euroopan etujen suojelemista ja edistämistä. Tätä korostaa kaksikäyttösovellusten yleistyminen, minkä vuoksi vahva siviiliteknologiasektori on voimavara myös puolustus- ja turvallisuusvalmiuksille. Teollisuusvakoilu vaikuttaa merkittävästi EU:n talouteen, työllisyyteen ja kasvuun: Liikesalaisuuksien kybervarkauksien arvioidaan aiheuttavan EU:lle 60 miljardin euron kustannukset.[14] Tämä vaatii perusteellista pohdintaa siitä, miten riippuvuussuhteet ja lisääntynyt altistuminen kyberuhkille vaikuttavat EU:n kykyyn suojella ihmisiä ja yrityksiä.

Covid-19-kriisi on nostanut esiin myös sen, miten sosiaaliset jakolinjat ja epävarmuustekijät luovat haavoittuvuuksia turvallisuuteen. Tämä lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia tehdä kehittyneempiä **hybridihyökkäyksiä**, joissa haavoittuvuuksia hyödynnetään erilaisten kyberhyökkäysten, kriittisen infrastruktuurin vahingoittamisen[15], disinformaatiokampanjoiden ja poliittisen narratiivin radikalisoitumisen avulla.[16]

Samalla pidempään jatkuneet uhat kehittyvät edelleen. **Terrori-iskut** vähenivät EU:ssa vuonna 2019. Daeshin ja al-Qaidan sekä niiden liittolaisten suorittamien tai inspiroimien jihadistihyökkäysten uhka EU:n kansalaisia kohtaan on kuitenkin edelleen suuri.[17] Samaan aikaan väkivaltaisten äärioikeiston muodostama uhka on kasvussa.[18] Rasismin innoittamat hyökkäykset ovat vakava huolenaihe: Kuolonuhreja vaatineet juutalaisvastaiset terrori-iskut Hallessa muistuttivat tarpeesta tehostaa toimia vuonna 2018 annetun neuvoston julkilausuman[19] mukaisesti. Joka viides ihminen EU:ssa on erittäin huolissaan mahdollisesta terrori-iskusta seuraavien 12 kuukauden aikana.[20] Valtaosa viimeaikaisista terrori-iskuista on ollut ns. matalan teknologian iskuja, joissa yksin toimivat henkilöt ovat valinneet kohteekseen ihmisiä julkisissa tiloissa. Terroristien verkossa levittämä propaganda muuttui merkittävästi Christchurchin hyökkäysten suoran verkkolähetyksen myötä.[21] Radikalisoituneiden henkilöiden aiheuttama uhka on edelleen suuri, ja takaisin palaavat

---

13 Euroopan unionin perusoikeusvirasto (2020), ”Your rights matter: Security concerns and experiences”, perusoikeusviraston tutkimus, Luxemburg, julkaisutoimisto.

14 The scale and impact of industrial espionage and theft of trade secrets through cyber, 2018.

15 Elintärkeät infrastruktuurit ovat keskeisiä yhteiskunnan välttämättömien toimintojen, terveydenhuollon, turvallisuuden, turvatoimien sekä taloudellisen ja sosiaalisen hyvinvoinnin ylläpitämiseksi, ja niiden vahingoittumisella tai tuhoutumisella olisi merkittävä vaikutus (neuvoston direktiivi 2008/114/EY).

16 EU:n kansalaisista 97 prosenttia on joutunut tekemisiin valeuutisten kanssa, 38 prosenttia päivittäin. Ks. JOIN(2020) 8 (final).

17 EU:n jäsenvaltioista 13 ilmoitti yhteensä 119:stä toteutetusta, epäonnistuneesta tai estetystä terrori-iskusta, joissa kuoli 10 ja loukkaantui 27 ihmistä (Europol, TE-SAT-selvitys, 2020).

18 Vuonna 2019 tehtiin kuusi äärioikeistolaista terrori-iskua (yksi toteutui, yksi epäonnistui ja neljä estettiin kolmessa jäsenvaltiossa), kun vuonna 2018 vastaava luku oli vain yksi. Lisäksi äärioikeiston toiminta aiheutti kuolemantapauksia, joiden syyksi ei luokiteltu terrorismia (Europol, 2020).

19 Ks. myös neuvoston julkilausuma antisemitismin torjunnasta ja yhteisen turvallisuustoimintamallin kehittämisestä Euroopan juutalaisyhteisöjen ja - instituutioiden suojelemisen parantamiseksi.

20 EU:n perusoikeusvirasto: ”Your rights matter: Security concerns and experiences”, 2020.

21 Europol löysi ajanjaksolla heinäkuusta 2015 vuoden 2019 loppuun terroristista sisältöä 361 eri alustalta (Europol, 2020).

terrorismiin syyllistyvät vierastaistelijat ja vankilasta vapautetut ääriajattelijat saattavat pahentaa sitä.[22]

Kriisi on myös osoittanut, miten olemassa olevat uhat voivat kehittyä uusissa olosuhteissa. **Rikollisjärjestöt** ovat hyödyntäneet eri tuotteiden pulaa, mikä on avannut uusia laittomia markkinoita. Laittomien huumeiden kauppa on edelleen EU:n suurin rikollisen liiketoiminnan ala. Sen vähittäismyyntiarvon arvioidaan olevan EU:ssa vähintään 30 miljardia euroa vuodessa.[23] Ihmiskauppa jatkuu edelleen: kaikenlaisen hyväksikäytön vuosituotto on maailmanlaajuisesti arviolta lähes 30 miljardia euroa.[24] Lääkeväärennösten kansainvälisen kaupan arvo nousi 38,9 miljardiin euroon.[25] Samaan aikaan rikolliset voivat takavarikointien vähäisen määrän ansiosta laajentaa rikollista toimintaansa edelleen ja soluttautua lailliseen talouteen.[26] Rikollisten ja terroristien on entistä helpompi hankkia ampuma-aseita verkossa toimivilta markkinapaikoilta ja uuden teknologian (esimerkiksi 3D-tulostuksen) avulla.[27] Tekoälyn, uuden teknologian ja robotiikan käyttö lisää entisestään sitä riskiä, että rikolliset hyödyntävät innovoinnin etuja vihamielisiin tarkoituksiin.[28]

Nämä uhat ovat monimuotoisia ja kohdistuvat eri tavoin yhteiskunnan eri osiin. Yhdessä ne kaikki ovat merkittävä uhka sekä ihmisille että yrityksille ja edellyttävät kattavia ja johdonmukaisia toimia EU:n tasolla. Kun jopa pienet verkkoon yhteydessä olevat kodinkoneet (esimerkiksi jääkaappi ja kahvinkeitin) voivat aiheuttaa tietoturvariskin, emme voi enää luottaa pelkästään perinteisiin valtiollisiin toimijoihin turvallisuutemme takaamiseksi. Talouden toimijoiden on otettava suurempi vastuu markkinoille saattamiensa tuotteiden ja palvelujen kyberturvallisuudesta. Myös tavallisten kansalaisten pitäisi tuntea edes perusasiat kyberturvallisuudesta, jotta he voisivat suojautua näiltä uhilta.

III. Koko yhteiskunnan kattava EU:n tason koordinoitu reagointi

EU on jo osoittanut kykynsä tuottaa todellista lisäarvoa. Turvallisuusunioni on vuodesta 2015 lähtien luonut uusia kytköksiä turvallisuuspolitiikan käsittelyyn EU:n tasolla. Tarvitaan kuitenkin lisää toimia, jotta koko yhteiskunta saadaan mukaan – hallitukset kaikilla tasoilla, yritykset kaikilta aloilta ja ihmiset kaikista jäsenvaltioista. Kasvava tietoisuus riippuvuusriskeistä[29] ja vahvan eurooppalaisen teollisuusstrategian[30] tarve viittaavat siihen, että EU on saavuttanut kriittisen massan teollisuudessa, teknologian tuotannossa ja toimitusketjujen häiriönsietokyvyssä. Vahvuuteen kuuluu myös perusoikeuksien ja EU:n arvojen täysimääräinen kunnioittaminen: ne ovat oikeutetun, tehokkaan ja kestävän turvallisuuspolitiikan perusedellytys. Turvallisuusunionistrategiassa

[22] Europol: ”A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism”, 2019.

[23] EMCDDA:n ja Europolin EU:n huumausainemarkkinoita koskeva raportti vuodelta 2019.

[24] Europol: ”Report on Trafficking in Human Beings, Financial Business Model”, 2015.

[25] Euroopan unionin teollisoikeuksien viraston ja OECD:n raportti lääkeväärennösten kaupasta.

[26] Varojen takaisinhankinta ja menetetyksi tuomitseminen: takeet sille, että rikos ei kannata, COM(2020) 217.

[27] Vuonna 2017 ampuma-aseita käytettiin 41 prosentissa kaikista terrori-iskuista (Europol, 2018).

[28] Heinäkuussa 2020 Ranskan ja Alankomaiden lainvalvonta- ja oikeusviranomaiset ilmoittivat Europolin ja Eurojustin kanssa yhteisestä tutkinnasta EncroChatin sulkemiseksi. EncroChat on salattu puhelinverkko, jota käyttävät väkivaltaisista hyökkäyksistä, korruptiosta, murhayrityksistä ja laajamittaisista huumekuljetuksista epäillyt rikollisverkostot.

[29] Riippuvuuteen ulkomaista liittyy riskejä lisääntyneestä altistumisesta mahdollisille uhkille. Näitä ovat esimerkiksi kriittisiä infrastruktuureja (esim. energia, liikenne, pankkitoiminta ja terveydenhuolto) tukevien tietotekniikkainfrastruktuurien haavoittuvuuksien hyödyntäminen, teollisuuden hallintajärjestelmien haltuunotto ja tietovarkauksien tai vakoilun lisääntyminen.

[30] Komission tiedonanto – Euroopan uusi teollisuusstrategia, COM(2020) 102.

esitetään konkreettisia toimintalinjoja. Strategia rakentuu seuraavien yhteisten tavoitteiden ympärille:

- ***Voimavarojen ja valmiuksien kehittäminen kriisien varhaista havaitsemista, ennaltaehkäisyä ja nopeaa reagointia varten:*** Euroopan on pystyttävä nykyistä paremmin ehkäisemään tulevia häiriöitä, suojautumaan niiltä sekä selviytymään niistä. Meidän on kehitettävä voimavaroja ja valmiuksia turvallisuuskriisien varhaista havaitsemisesta ja nopeaa reagointia varten yhdennetyllä ja koordinoidulla toimintamallilla sekä maailmanlaajuisesti että toimialakohtaisten aloitteiden kautta (kuten rahoituksen, energian, oikeuslaitoksen, lainvalvonnan, terveydenhuollon, merenkulun ja liikenteen aloilla) ja olemassa olevien välineiden ja hankkeiden pohjalta.[31] Lisäksi komissio esittää ehdotuksia laaja-alaisesta EU:n kriisinhallintajärjestelmästä, joka myös voi olla merkittävä turvallisuuden kannalta.
- ***Tuloksiin keskittyminen***: Tuloslähtöisen strategian on perustuttava huolelliseen uhkien ja riskien arviointiin, jotta toimet voidaan kohdentaa mahdollisimman tehokkaasti. Strategiassa on määriteltävä oikeat säännöt ja välineet sekä niiden soveltaminen. Tämä edellyttää luotettavaa strategista tiedustelutietoa EU:n turvallisuuspolitiikan perustaksi. Tarvittaessa EU:n lainsäädäntöä on muutettava, jotta strategia voidaan panna täysimääräisesti täytäntöön hajanaisuuden ja haavoittuvuuksien välttämiseksi. Strategian tehokas täytäntöönpano riippuu myös asianmukaisen rahoituksen varmistamisesta seuraavalla ohjelmakaudella 2021–2027, myös asiaan kuuluville EU:n virastoille.
- ***Kaikkien julkisen ja yksityisen sektorin toimijoiden osallistuminen yhteisiin toimiin:*** Keskeiset toimijat sekä julkisella että yksityisellä sektorilla ovat olleet haluttomia jakamaan turvallisuuden kannalta keskeisiä tietoja siksi, että ne pelkäävät kansallisen turvallisuuden tai kilpailukykynsä vaarantuvan.[32] Olemme kuitenkin tehokkaimmillamme silloin, kun kaikki osapuolet on valjastettu tukemaan toisiaan. Tämä tarkoittaa ensinnäkin tiiviimpää jäsenvaltioiden välistä yhteistyötä, johon osallistuvat lainvalvonta- ja oikeusviranomaiset sekä muut viranomaiset yhdessä EU:n toimielinten ja virastojen kanssa. Tällä rakennetaan yhteisiä ratkaisuja varten tarvittavaa yhteisymmärrystä ja tietojenvaihtoa. Yhteistyö yksityisen sektorin kanssa on myös avainasemassa, varsinkin kun otetaan huomioon, että teollisuus omistaa merkittävän osan siitä digitaalisesta ja muusta infrastruktuurista, joka on keskeinen rikollisuuden ja terrorismin torjunnan kannalta. Lisäksi yksittäiset ihmiset voivat osallistua esimerkiksi kehittämällä kyberrikollisuuden ja disinformaation torjumiseen tarvittavia taitoja ja tietoisuutta. Yhteistyön on ulotuttava rajojemme ulkopuolelle, ja meidän on tiivistettävä suhteitamme samanmielisiin kumppaneihin.

IV. Kaikille turvallinen EU: Turvallisuusunionin strategiset painopisteet

EU:lla on erityisen hyvät edellytykset vastata uusiin maailmanlaajuisiin uhkiin ja haasteisiin. Edellä esitetty uhka-analyysi osoittaa, että EU:n tasolla on vietävä eteenpäin neljä toisistaan riippuvaista strategista painopistettä, perusoikeuksia täysimääräisesti kunnioittaen: (i)

[31] Esimerkiksi poliittisen kriisitoiminnan integroidut järjestelyt (IPCR), EU:n hätäavun koordinointikeskus, komission suositus koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (C(2017) 6100), EU:n operatiivinen protokolla hybridiuhkien torjumiseksi SWD(2016) 227.

[32] Yhteinen tiedonanto: "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle", JOIN(2017) 450.

tulevaisuudenkestävä turvallisuusympäristö, (ii) muuttuvien uhkien torjuminen, (iii) eurooppalaisten suojeleminen terrorismilta ja järjestäytyneeltä rikollisuudelta, (iv) vahva eurooppalainen turvallisuusekosysteemi.

1. Tulevaisuudenkestävä turvallisuusympäristö

Kriittisen infrastruktuurin suojaaminen ja häiriönsietokyky

Ihmiset turvautuvat jokapäiväisessä elämässään keskeisiin infrastruktuureihin matkustaessaan, työskennellessään ja käyttäessään keskeisiä julkisia palveluja, kuten terveydenhuoltoa, joukkoliikennettä ja energiahuoltoa, sekä käyttäessään demokraattisia oikeuksiaan. Jos nämä infrastruktuurit eivät ole riittävän suojattuja ja kestäviä, hyökkäykset voivat aiheuttaa valtavia häiriöitä – fyysisiä tai digitaalisia – sekä yksittäisissä jäsenvaltioissa että mahdollisesti koko EU:ssa.

EU:n nykyinen kriittisen infrastruktuurin suojaamista ja häiriönsietokykyä koskeva kehys[33] ei ole pysynyt muuttuvien riskien tahdissa. Keskinäisten riippuvuussuhteiden lisääntyminen merkitsee sitä, että yhdellä alalla esiintyvät häiriöt voivat vaikuttaa välittömästi muiden alojen toimintaan: sähköntuotantoon kohdistuva hyökkäys voisi lamauttaa televiestinnän, sairaalat, pankit tai lentoasemat, kun taas digitaaliseen infrastruktuuriin kohdistuva hyökkäys voisi johtaa häiriöihin sähkö- tai rahoitusverkoissa. Kun taloutemme ja yhteiskuntamme siirtyy yhä enemmän verkkoon, tällaiset riskit lisääntyvät entisestään. Nämä keskinäiset kytkökset ja riippuvuussuhteet on otettava huomioon lainsäädäntökehyksessä toteuttamalla vankkoja kriittisen infrastruktuurin suojausta ja häiriönsietokykyä parantavia toimenpiteitä sekä kyber- että fyysisen turvallisuuden osa-alueilla. Keskeiset palvelut, myös avaruusinfrastruktuuriin perustuvat palvelut, on suojattava asianmukaisesti nykyisiltä ja odotettavissa olevilta uhkilta, mutta niiden on myös oltava kestäviä. Tämä edellyttää järjestelmältä kykyä valmistautua haittatapahtumiin, laatia suunnitelmia niiden varalta, kestää niitä, toipua niistä ja mukautua niihin paremmin.

Samalla jäsenvaltiot ovat käyttäneet harkintavaltaansa ja panneet voimassa olevan lainsäädännön täytäntöön eri tavoin. Tästä seurauksena oleva hajanaisuus voi heikentää sisämarkkinoita ja vaikeuttaa rajatylittävää koordinointia erityisesti raja-alueilla. Keskeisiä palveluja eri jäsenvaltioissa tarjoavien toimijoiden on noudatettava erilaisia raportointijärjestelmiä. Komissio selvittää, voitaisiinko **uudella sekä fyysistä että digitaalista infrastruktuuria koskevalla kehyksellä** luoda johdonmukaisempi ja yhtenäisempi lähestymistapa keskeisten palvelujen luotettavan tarjonnan varmistamiseksi. Tätä kehystä on täydennettävä **toimialakohtaisilla aloitteilla**, joilla puututaan elintärkeisiin infrastruktuureihin kohdistuviin erityisriskeihin. Näihin infrastruktuureihin kuuluvat esimerkiksi liikenne, avaruus, energia, rahoitus ja terveydenhuolto[34]. Ottaen huomioon rahoitusalan suuri riippuvuus tietotekniikkapalveluista ja sen suuri haavoittuvuus kyberhyökkäyksille, ensimmäinen askel on rahoitusalan digitaalista häiriönsietokykyä koskeva aloite. Energiajärjestelmän erityisherkkyyksien ja merkityksen vuoksi tarvitaan erityinen aloite, jolla parannetaan kriittisen energiainfrastruktuurin sietokykyä fyysisiä,

[33] Direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, EUVL L 194, 19.7.2016; neuvoston direktiivi 2008/114/EY Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista.

[34] Koska terveydenhuoltoalaan on kohdistunut paineita erityisesti covid-19-kriisin aikana, komissio harkitsee myös aloitteita, joilla vahvistetaan EU:n terveysturvallisuutta koskevaa kehystä ja asiasta vastaavia EU:n virastoja, jotta ne voivat reagoida vakaviin rajat ylittäviin terveysuhkiin.

kyber- ja hybridiuhkia vastaan ja varmistetaan tasapuoliset toimintaedellytykset energia-alan toimijoille yli rajojen.

Lisäksi EU:n jäsenvaltiot ja komissio arvioivat ulkomaisten suorien sijoitusten seurantaan tarkoitettujen uusien eurooppalaisten puitteiden mukaisesti sellaisten ulkomaisten suorien sijoitusten turvallisuuden kannalta merkityksellisiä vaikutuksia, jotka todennäköisesti vaikuttavat kriittisiin infrastruktuureihin tai teknologioihin.[35]

EU voi myös kehittää uusia välineitä elintärkeän infrastruktuurin häiriönsietokyvyn parantamiseksi. Maailmanlaajuisesti internet on tähän mennessä osoittanut suurta häiriönsietokykyä erityisesti kyvyssään tukea kasvaneita liikennemääriä. Meidän on kuitenkin valmistauduttava mahdollisiin tuleviin kriiseihin, jotka uhkaavat internetin turvallisuutta, vakautta ja häiriönsietokykyä. Internetin toimintakuntoisuuden varmistaminen edellyttää, että kyberturvallisuuden häiriötilanteita ja vihamielistä verkkotoimintaa torjutaan tehokkaasti ja että riippuvuutta Euroopan ulkopuolella sijaitsevasta infrastruktuurista ja palveluista rajoitetaan. Verkko- ja tietojärjestelmien turvallisuuden yhtenäisen korkean tason varmistaminen EU:ssa edellyttää uutta lainsäädäntöä ja nykyisten sääntöjen tarkistamista, lisäinvestointeja tutkimukseen ja innovaatioon sekä keskeisten internet-infrastruktuurien ja -resurssien (erityisesti verkkotunnusjärjestelmän[36]) käyttöönottoa tai vahvistamista.

EU:n ja kansallisen tason keskeisten digitaalisten voimavarojen turvaamiseksi on ensiarvoisen tärkeää tarjota elintärkeälle infrastruktuurille suojattu viestintäkanava. Komissio tekee yhteistyötä jäsenvaltioiden kanssa luodakseen sertifioidun, koko käyttöketjultaan tietoturvallisen maan päälle ja avaruuteen sijoitettavan kvanttiviestintäinfrastruktuurin yhdessä avaruusohjelmaa koskevassa asetuksessa[37] säädetyn suojatun valtiollisen satelliittiviestintäjärjestelmän kanssa.

Kyberturvallisuus

Kyberhyökkäysten määrä on edelleen kasvussa.[38] Hyökkäykset ovat kehittyneempiä kuin koskaan, ne ovat peräisin useista eri lähteistä EU:ssa ja sen ulkopuolella, ja niitä kohdistetaan erityisen haavoittuviin alueisiin. Niiden taustalla on usein valtioita tai valtion tukemia toimijoita, jotka valitsevat kohteikseen keskeisiä digitaalisia infrastruktuureja, kuten suuria pilvipalvelujen tarjoajia.[39] Kyberriskeistä on tullut merkittävä uhka myös rahoitusjärjestelmälle. Kansainvälinen valuuttarahasto on arvioinut, että kyberhyökkäysten aiheuttamat vuotuiset tappiot ovat 9 prosenttia pankkien maailmanlaajuisista nettotuloista, eli noin 100 miljardia dollaria.[40] Siirtyminen verkkoon liitettyihin laitteisiin tuo suuria etuja

---

[35] Unioniin tulevien ulkomaisten suorien sijoitusten seurantaan tarkoitettujen puitteiden perustamisesta 19 päivänä maaliskuuta 2019 annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2019/452 aletaan soveltaa täysimääräisesti 11. lokakuuta 2020. Se antaa EU:n käyttöön uuden yhteistyömekanismin, joka koskee sellaisia EU:n ulkopuolelta tulevia suoria sijoituksia, jotka todennäköisesti vaikuttavat turvallisuuteen tai yleiseen järjestykseen. Asetuksen nojalla jäsenvaltiot ja komissio arvioivat tällaisiin suoriin ulkomaisiin sijoituksiin liittyviä mahdollisia riskejä ja ehdottavat tarvittaessa asianmukaisia keinoja riskien lieventämiseksi, jos ne koskevat useampaa kuin yhtä jäsenvaltiota.

[36] Verkkotunnusjärjestelmä (DNS) on hierarkkinen ja hajautettu nimijärjestelmä internetiin tai yksityisverkkoon yhdistetyille tietokoneille, palveluille tai muille resursseille. Se muuntaa verkkotunnukset IP-osoitteiksi, joiden avulla tietokonepalvelut ja -laitteet voidaan paikantaa ja tunnistaa.

[37] Ehdotus asetukseksi unionin avaruusohjelman ja Euroopan unionin avaruusohjelmaviraston perustamisesta, COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Hajautetut palvelunestohyökkäykset ovat edelleen pysyvä uhka: Suurten palveluntarjoajien oli torjuttava massiivisia hajautettuja palvelunestohyökkäyksiä (esim. Amazonin verkkopalveluja vastaan helmikuussa 2020 tehty hyökkäys).

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

käyttäjille, mutta kun dataa säilytetään ja käsitellään vähemmän datakeskuksissa ja lähempänä käyttäjää ”verkon reunalla”[41], kyberturvallisuudessa ei voida enää keskittyä keskuspisteiden suojaamiseen.[42]

EU esitti vuonna 2017 kyberturvallisuutta koskevan lähestymistavan, joka perustuu häiriönsietokykyyn, nopeaan reagointiin ja tehokkaaseen pelotevaikutukseen.[43] Nyt EU:n on huolehdittava siitä, että sen kyberturvallisuusvalmiudet pysyvät tilanteen tasalla, jotta sekä häiriönsietokyky että reagointi pystytään takaamaan. Tämä edellyttää todellista koko yhteiskunnan kattavaa lähestymistapaa, jossa EU:n toimielimet, virastot ja elimet, jäsenvaltiot, teollisuus, tiedemaailma ja yksityishenkilöt asettavat kyberturvallisuuden etusijalle.[44] Tätä horisontaalista lähestymistapaa on edelleen täydennettävä toimialakohtaisilla kyberturvallisuutta koskevilla toimintamalleilla esimerkiksi energian, rahoituspalvelujen, liikenteen ja terveydenhuollon aloilla. EU:n toimien seuraava vaihe olisi esitettävä Euroopan tarkistetussa kyberturvallisuusstrategiassa.

Tiedustelupalvelujen, EU:n tiedusteluanalyysikeskuksen ja muiden turvallisuusalan organisaatioiden välisten uusien ja tehostettujen yhteistyömuotojen selvittäminen olisi otettava osaksi pyrkimyksiä parantaa kyberturvallisuutta sekä torjua terrorismia, ääriliikkeitä, radikalismia ja hybridiuhkia.

5G-infrastruktuuria ollaan ottamassa käyttöön eri puolilla EU:ta, ja monet kriittiset palvelut ovat potentiaalisesti riippuvaisia 5G-verkoista, joten systeemisillä ja laajoilla häiriöillä olisi erityisen vakavia seurauksia. 5G-verkkojen kyberturvallisuudesta vuonna 2019 annetulla komission suosituksella[45] käyttöön otettu prosessi on nyt johtanut jäsenvaltioiden suorittamiin erityistoimiin 5G-välineistössä[46] esitettyjen keskeisten toimenpiteiden osalta.

Yksi tärkeimmistä pitkän aikavälin tarpeista on **sisäänrakennetun kyberturvallisuuden** kulttuurin kehittäminen siten, että turvallisuus sisällytetään tuotteisiin ja palveluihin alusta alkaen. Tässä auttaa merkittävästi kyberturvallisuusasetuksen mukainen uusi kyberturvallisuuden sertifiointikehys[47]. Kehystä laaditaan jo, kahta sertifiointijärjestelmää valmistellaan nyt, ja jatkotoimien painopisteet määritellään myöhemmin tänä vuonna. EU:n kyberturvallisuusviraston (ENISA), tietosuojaviranomaisten ja Euroopan tietosuojaneuvoston[48] välinen yhteistyö on avainasemassa tällä osa-alueella.

Komissio on jo todennut, että jäsenneltyä ja koordinoitua operatiivista yhteistyötä varten tarvitaan **yhteinen kyberturvallisuusyksikkö**. Siihen voisi sisältyä keskinäisen avunannon

---

[41] Reunalaskenta käyttää hajautettua avointa IT-arkkitehtuuria, jossa prosessointiteho on hajautettu, mikä mahdollistaa mobiilitietotekniikkaan ja esineiden internetiin liittyvän teknologian. Reunalaskennassa tiedot käsitellään itse laitteessa tai paikallisella tietokoneella tai palvelimella sen sijaan, että ne siirrettäisiin datakeskukseen.

[42] Tiedonanto Euroopan datastrategiasta, COM(2020) 66 final.

[43] Yhteinen tiedonanto: ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle”, JOIN(2017) 450.

[44] Yhteisen tutkimuskeskuksen raportissa ”Cybersecurity – our digital Anchor” esitetään moniulotteisia näkemyksiä kyberturvallisuuden kasvusta viimeisten 40 vuoden aikana.

[45] Komission 5G-verkkojen kyberturvallisuutta koskeva suositus, COM(2019) 2335 final. Suosituksen mukaan sitä tarkastellaan uudelleen vuoden 2020 viimeisellä neljänneksellä.

[46] Ks. verkko- ja tietoturva-alan yhteistyöryhmän 24. heinäkuuta 2020 antama raportti välineistön täytäntöönpanosta.

[47] Asetus (EU) 2019/881 Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (kyberturvallisuusasetus).

[48] Tiedonanto tietosuojasäännöistä kansalaisten vaikutusmahdollisuuksien ja EU:n digitaalisen muutoksen edistäjänä – yleistä tietosuoja-asetusta sovellettu kaksi vuotta, COM(2020) 264.

mekanismi kriisiaikoina EU:n tasolla. Yhteinen kyberturvallisuusyksikkö voisi suunnitelmasuosituksen[49] täytäntöönpanon pohjalta rakentaa luottamusta Euroopan kyberturvallisuusekosysteemin eri toimijoiden välille ja tarjota tätä keskeistä palvelua jäsenvaltioille. Komissio käynnistää keskustelut asianomaisten sidosryhmien kanssa (alkaen jäsenvaltioista) ja esittää selkeän etenemissuunnitelman, välitavoitteet ja aikataulun vuoden 2020 loppuun mennessä.

Myös yhteiset tietoturvallisuutta ja kyberturvallisuutta koskevat säännöt kaikille EU:n toimielimille, elimille ja virastoille ovat tärkeitä. Olisi luotava velvoittavat ja tiukat yhteiset säännöt, jotka koskevat suojattua tietojenvaihtoa ja digitaalisten infrastruktuurien ja järjestelmien turvallisuutta kaikissa EU:n toimielimissä, elimissä ja virastoissa. Tämän uuden säännöstön olisi tuettava vahvaa ja tehokasta operatiivista yhteistyötä kyberturvallisuuden alalla kaikissa EU:n toimielimissä, elimissä ja virastoissa ja keskityttävä EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) rooliin.

Vahvojen **kansainvälisten kumppanuuksien** luominen ja ylläpitäminen on niiden globaalin luonteen vuoksi olennaisen tärkeää kyberhyökkäysten ehkäisemisessä ja niihin reagoimisessa. EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevissa puitteissa (kyberdiplomatian välineistö)[50] vahvistetaan yhteisen ulko- ja turvallisuuspolitiikan mukaiset toimenpiteet, kuten rajoittavat toimenpiteet (pakotteet), joilla voidaan vastata toimintaan, joka vahingoittaa unionin poliittisia, turvallisuuteen liittyviä ja taloudellisia etuja. EU:n olisi myös tehostettava kehitys- ja yhteistyörahastojen käyttöä valmiuksien kehittämiseen kumppanimaiden tukemiseksi niiden digitaalisten ekosysteemien vahvistamisessa, kansallisen lainsäädännön uudistamisessa ja kansainvälisten normien noudattamisessa. Näin lisätään yhteisön häiriönsietokykyä kokonaisuudessaan sekä sen kykyä torjua kyberuhkia ja reagoida niihin tehokkaasti. Tähän sisältyy erityistoimia, joilla edistetään EU:n normeja ja asiaankuuluvaa lainsäädäntöä lähialueen kumppanimaiden kyberturvallisuuden parantamiseksi.[51]

Julkisten tilojen suojeleminen

Viimeaikaiset terrori-iskut ovat kohdistuneet **julkisiin tiloihin**, kuten uskonnonharjoittamispaikkoihin ja liikenteen solmukohtiin. Iskuissa on hyödynnetty paikkojen avoimuutta. Poliittisen tai ideologisesti motivoituneen ääriliikehdinnän aiheuttama terrorismin lisääntyminen on lisännyt tätä uhkaa entisestään. Tämä edellyttää sekä näiden paikkojen parempaa fyysistä suojelua että asianmukaisia havaitsemisjärjestelmiä ilman, että kansalaisten vapauksia kuitenkaan heikennetään.[52] Komissio tehostaa julkisen ja yksityisen sektorin yhteistyötä julkisten tilojen suojelemiseksi myöntämällä rahoitusta, vaihtamalla kokemuksia ja hyviä käytäntöjä sekä antamalla erityisohjeita[53] ja suosituksia.[54] Tähän toimintamalliin kuuluu myös tietoisuuden lisääminen,

---

[49] Komission suositus (EU) 2017/1584 koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/fi/pdf

[51] Ks. neuvoston päätelmissä 26. kesäkuuta 2018 hyväksytyt EU:n ulkoisten kybervalmiuksien kehittämistä koskevat suuntaviivat.

[52] Biometrisiin etätunnistusjärjestelmiin on kiinnitettävä erityistä huomiota. Komission alustavat näkemykset esitetään komission 19. helmikuuta 2020 antamassa tekoälyä koskevassa valkoisessa kirjassa, COM(2020) 65.

[53] Esimerkiksi ohjeet asianmukaisten turvaesteratkaisujen valitsemiseen julkisten tilojen suojelemiseksi (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Hyviä käytäntöjä koskevia ohjeita annetaan asiakirjassa SWD(2019) 140, joka sisältää julkisen ja yksityisen sektorin yhteistyötä käsittelevän osion. ISF:n poliisiyhteistyön rahoituksessa keskitytään erityisesti julkisen ja yksityisen sektorin yhteistyön tehostamiseen.

havainnointilaitteiden suorituskykyvaatimukset ja testaus sekä parannetut taustaselvitykset sisäpiiriuhkien torjumiseksi. Eräs tärkeä huomioitava näkökohta on se, että vaikutukset saattavat kohdistua suhteettomasti vähemmistöihin ja haavoittuvassa asemassa oleviin henkilöihin, kuten uskontonsa tai sukupuolensa vuoksi iskujen kohteeksi joutuneisiin ihmisiin, minkä vuoksi niihin on kiinnitettävä erityistä huomiota. Alue- ja paikallisviranomaisilla on tärkeä rooli julkisten tilojen turvallisuuden parantamisessa. Komissio tukee myös kaupunkeja julkisten tilojen turvallisuuteen tähtäävässä innovoinnissa.[55] Marraskuussa 2018 käynnistetty uusi EU:n kaupunkiagendaan[56] sisältyvä julkisten tilojen turvallisuutta koskeva kumppanuus on osoitus siitä, että jäsenvaltiot, komissio ja kaupungit ovat sitoutuneet vastaamaan paremmin kaupunkialueiden turvallisuusuhkiin.

Drooneja markkinoidaan yhä laajemmin, ja niillä on monia hyödyllisiä ja laillisia käyttötarkoituksia. Rikolliset ja terroristit voivat kuitenkin käyttää niitä myös väärin, ja erityisesti julkiset tilat ovat uhattuina. Kohteita voivat olla yksittäiset ihmiset, ihmisjoukot, kriittinen infrastruktuuri, lainvalvontaviranomaiset, rajat tai julkiset tilat. Tietämystä droonien käytöstä konflikteissa saattaa tulla Eurooppaan joko suoraan (palaavien terrorismiin syyllistyvien vierastaistelijoiden mukana) tai verkon välityksellä. Euroopan lentoturvallisuusviraston jo laatimat säännöt ovat tärkeä ensimmäinen askel esimerkiksi droonien pakollisen etätunnistuksen ja käyttäjien rekisteröinnin osalta. Lisätoimia tarvitaan droonien parantuneen saatavuuden ja suorituskyvyn sekä hintojen laskun myötä. Näitä voisivat olla tietojen, ohjeistuksen ja hyvien käytäntöjen jakaminen kaikille, myös lainvalvontaviranomaisille, sekä drooneihin kohdistuvien vastatoimien testaamisen[57] lisääminen. Lisäksi olisi analysoitava ja käsiteltävä tarkemmin droonien käytön vaikutuksia yksityisyyteen ja tietosuojaan julkisissa tiloissa.

Keskeiset toimet
• Kriittisen infrastruktuurin suojaamista ja häiriönsietokykyä koskeva lainsäädäntö • Verkko- ja tietoturvadirektiivin tarkistaminen • Rahoitusalan toiminnallisen häiriönsietokyvyn kehittämisaloite • Kriittisen energiainfrastruktuurin suojaaminen ja kyberturvallisuus sekä kyberturvallisuutta rajat ylittävissä sähkövirroissa koskeva verkkosääntö • Euroopan kyberturvallisuusstrategia • Seuraavat vaiheet yhteisen kyberyksikön perustamiseksi • Yhteiset tietoturvallisuutta ja kyberturvallisuutta koskevat säännöt EU:n toimielimille, elimille ja virastoille • Tehostettu yhteistyö julkisten tilojen (mukaan lukien uskonnonharjoituspaikat) suojelemiseksi • Droonien väärinkäytön torjuntaa koskevien parhaiden käytäntöjen jakaminen

[55] Kolme kaupunkia (Pireus Kreikassa, Tampere Suomessa ja Torino Italiassa) testaavat uusia ratkaisuja osana kaupunkialueiden innovatiivisia toimia, jotka yhteisrahoitetaan Euroopan aluekehitysrahastosta (EAKR).

[56] EU:n kaupunkiagenda edustaa uutta monitasoista työskentelytapaa, joka edistää yhteistyötä jäsenvaltioiden, kaupunkien, Euroopan komission ja muiden sidosryhmien välillä. Yhteistyön tavoitteena on tukea kasvua, asuinkelpoisuutta ja innovointia Euroopan kaupungeissa sekä tunnistaa sosiaalisia haasteita ja pyrkiä ratkaisemaan ne.

[57] Hiljattain perustettiin monivuotinen testausohjelma, jolla autetaan jäsenvaltioita kehittämään yhteinen menetelmä ja testausalusta tätä tarkoitusta varten.

2. Reagointi muuttuviin uhkiin

Kyberrikollisuus

Teknologia luo yhteiskunnalle uusia mahdollisuuksia. Se myös tarjoaa uusia välineitä oikeuslaitoksen ja lainvalvonnan käyttöön. Samalla se kuitenkin avaa ovia rikollisille. Haittaohjelmat, henkilö- tai yritystietojen varastaminen hakkeroimalla ja digitaalisen toiminnan katkaiseminen aiheuttavat taloudellista vahinkoa tai tahraavat mainetta. Vahvan kyberturvallisuuden tarjoama selviytymiskykyinen ympäristö on paras puolustus näitä vastaan. Lainvalvontaviranomaiset tarvitsevat selkeät säännöt digitaalisen tutkinnan alalle rikostutkintaa ja syytteeseenpanoa varten sekä riittävän suojelun tarjoamiseksi rikosten uhreille. Niiden olisi pohjauduttava Europolin yhteisen tietoverkkorikollisuutta käsittelevän toimintaryhmän työhön ja EU:n lainvalvonnan hätäaputoimien protokollaan, joka laadittiin koordinoimaan laajamittaisiin kyberhyökkäyksiin reagoimista. Avainasemassa ovat myös tehokkaat mekanismit, jotka mahdollistavat julkisen ja yksityisen sektorin kumppanuudet ja yhteistyön.

Samalla kyberrikollisuuden torjunnasta pitäisi tehdä strategisen viestinnän prioriteetti kaikkialla EU:ssa, jotta eurooppalaiset olisivat tietoisia riskeistä ja ennalta ehkäisevistä toimenpiteistä, joihin he voisivat ryhtyä. Tämän olisi oltava osa ennakoivaa lähestymistapaa. Myös nykyisen oikeudellisen kehyksen[58] täysimääräinen täytäntöönpano on olennainen askel: komissio on tarvittaessa valmis käyttämään rikkomusmenettelyjä ja tarkistamaan tätä kehystä varmistaakseen, että se pysyy tarkoituksenmukaisena. Komissio selvittää myös yhdessä Europolin ja EU:n kyberturvallisuusviraston ENISAn kanssa mahdollisuutta toteuttaa kyberrikollisuuteen liittyvä EU:n tason nopea hälytysjärjestelmä, jolla voitaisiin varmistaa tiedonkulku ja nopea reagointi kyberrikosaaltojen aikana.

Kyberrikollisuus on maailmanlaajuinen haaste, joka edellyttää tehokasta kansainvälistä yhteistyötä. EU tukee Euroopan neuvostossa tehtyä kyberrikollisuutta koskevaa Budapestin yleissopimusta. Se on toimiva ja vakiintunut kehys, jonka avulla kaikki maat voivat selvittää, mitä järjestelmiä ja viestintäkanavia niiden on otettava käyttöön voidakseen työskennellä tehokkaasti toistensa kanssa.

Lähes puolet EU:n kansalaisista on huolissaan tietojen väärinkäytöstä[59] ja **identiteettivarkauksista**.[60] Henkilöllisyyden vilpillinen käyttö taloudellisen hyödyn saamiseksi ei ole ainoa ongelma. Identiteettivarkaudella voi olla myös huomattavia henkilökohtaisia ja psykologisia vaikutuksia, sillä varkaan tekemät laittomat julkaisut voivat jäädä verkkoon vuosikausiksi. Komissio selvittää mahdollisia käytännön toimenpiteitä uhrien suojelemiseksi kaikenlaisilta identiteettivarkauksilta ja ottaa huomioon tulevan eurooppalaista digitaalista identiteettiä[61] koskevan aloitteen.

Kyberrikollisuuden torjunta edellyttää katseen pitämistä tulevaisuudessa. Kun yhteiskunta käyttää uutta teknologiaa talouden ja yhteiskunnan vahvistamiseen, myös rikolliset voivat pyrkiä hyödyntämään samoja välineitä haitallisiin tarkoituksiin. Rikolliset voivat

---

58 Direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä.

59 46 % (Eurobarometri-tutkimus eurooppalaisten asenteista kyberturvallisuuteen, tammikuu 2020).

60 Vuonna 2018 tehtyyn Eurobarometri-tutkimukseen ”eurooppalaisten asenteet internetin turvallisuuteen” valtaosa vastaajista (95 %) piti identiteettivarkauksia vakavina rikoksina ja seitsemän kymmenestä piti niitä erittäin vakavina. Tammikuussa 2020 julkaistu Eurobarometri-tutkimus vahvisti osaltaan huolet tietoverkkorikollisuudesta, verkkopetoksista ja identiteettivarkauksista: kaksi kolmasosaa vastaajista oli huolissaan pankkipetoksista (67 %) tai identiteettivarkauksista (66 %).

61 Komission 19. helmikuuta 2020 antama tiedonanto ”Euroopan digitaalista tulevaisuutta rakentamassa”, COM(2020) 67.

esimerkiksi käyttää tekoälyä havaitsemaan ja tunnistamaan salasanoja, helpottamaan haittaohjelmien luomista tai hyödyntämään kuva- ja äänimateriaalia identiteettivarkauksissa tai -petoksissa.

Moderni lainvalvonta

Lainvalvonta- ja oikeusalalla työskentelevien on mukauduttava uuteen teknologiaan. Teknologian kehitys ja uudet uhat edellyttävät, että lainvalvontaviranomaiset saavat käyttöönsä uusia välineitä, hankkivat uusia taitoja ja kehittävät vaihtoehtoisia tutkintamenetelmiä. Täydentääkseen lainsäädäntötoimia sähköisen todistusaineiston rajatylittävän saatavuuden parantamiseksi rikostutkimuksissa EU voi auttaa lainvalvontaviranomaisia kehittämään tarvittavia valmiuksia tunnistaa, suojata ja lukea rikosten tutkinnassa tarvittavia tietoja ja käyttämään niitä todisteina tuomioistuimessa. Komissio kartoittaa toimenpiteitä **lainvalvontavalmiuksien parantamiseksi digitaalisissa tutkintatoimissa** ja määrittää, miten tutkimusta ja kehitystä voidaan hyödyntää parhaiten uusien välineiden tarjoamiseksi lainvalvonnan käyttöön ja miten koulutuksella voidaan tarjota oikeanlaisia taitoja lainvalvonta- ja oikeusalan työhön. Tämä sisältää myös tiukkoja tieteellisiä arviointeja ja testausmenetelmiä, joista vastaa komission Yhteinen tutkimuskeskus.

Yhteisillä toimintamalleilla voidaan myös varmistaa, että **tekoäly, avaruusvoimavarat, massadata** ja **suurteholaskenta sisällytetään** turvallisuuspolitiikkaan tavalla, joka on tehokas sekä rikosten torjunnassa että perusoikeuksien kunnioittamisen varmistamisessa. Tekoäly voi olla tehokas väline rikollisuuden torjunnassa. Kyky analysoida suuria määriä tietoja ja tunnistaa malleja ja poikkeamia lisää tutkintavalmiuksia valtavasti.[62] Tekoäly voi myös tarjota konkreettisia välineitä, joiden avulla pystytään tunnistamaan terroristista verkkosisältöä, havaitsemaan epäilyttäviä liiketoimia vaarallisten tuotteiden markkinoilla tai tarjoamaan hätätilanteissa apua kansalaisille. Tämän potentiaalin hyödyntämiseksi tutkimus, innovointi ja tekoälyn käyttäjät on saatettava yhteen oikeanlaiseen hallintorakenteeseen ja tekniseen infrastruktuuriin sekä otettava yksityinen sektori ja tiedeyhteisö aktiivisesti mukaan. Lisäksi on varmistettava perusoikeuksien kunnioittaminen korkeimmalla mahdollisella tasolla samalla varmistaen kansalaisten tehokas suojelu. Varsinkin yksilöihin vaikuttavissa päätöksissä tarvitaan ihmisten suorittamaan arviointia. Kyseisten päätösten on lisäksi noudatettava asianmukaista EU:n lainsäädäntöä.[63]

Sähköistä tietoa ja todistusaineistoa tarvitaan noin 85 prosentissa vakavien rikosten tutkimuksista, ja 65 prosenttia kaikista pyynnöistä osoitetaan toisen lainkäyttöalueen palveluntarjoajille.[64]. Perinteiset fyysiset jäljet ovat siirtyneet verkkoon, mikä lisää entisestään kuilua lainvalvonnan ja rikollisten toimintavalmiuksien välillä. On olennaisen tärkeää ottaa käyttöön selkeät säännöt sähköisen todistusaineiston saatavuudesta rajatylittävässä rikostutkinnassa. Tämän vuoksi Euroopan parlamentin ja neuvoston on hyväksyttävä nopeasti sähköistä todistusaineistoa koskevat ehdotukset, jotta rikostutkijat saisivat käyttöönsä tehokkaan välineen. Sähköisen todistusaineiston rajatylittävä saatavuus

[62] Esimerkiksi talousrikoksissa.

[63] Tämä tarkoittaa voimassa olevaa lainsäädännön noudattamista, mukaan lukien yleinen tietosuoja-asetus (EU) 2016/679 sekä direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.

[64] Komission yksiköiden valmisteluasiakirja SWD(2018) 118 final.

monenvälisten ja kahdenvälisten kansainvälisten neuvottelujen kautta on myös ensiarvoisen tärkeää, jotta voidaan vahvistaa kansainvälisesti yhteensopivat säännöt.[65]

Digitaalisen todistusaineiston saatavuus riippuu myös tiedon saatavuudesta. Jos tiedot poistetaan liian nopeasti, tärkeää todistusaineistoa saattaa kadota, jolloin epäiltyjen ja rikollisverkostojen (sekä uhrien) tunnistaminen ja paikantaminen ei ole enää mahdollista. Toisaalta tietojen säilytysjärjestelmät herättävät kysymyksiä yksityisyyden suojasta. Unionin tuomioistuimessa vireillä olevien asioiden lopputuloksesta riippuen komissio arvioi, miten tietojen säilyttämisen suhteen olisi edettävä.

Pääsy internetin verkkotunnusten rekisteröintitietoihin (jäljempänä 'WHOIS-tiedot')[66] on tärkeää rikostutkinnan, kyberturvallisuuden ja kuluttajansuojan kannalta. Näiden tietojen saanti on kuitenkin vaikeutumassa, kun Internet Corporation for Assigned Names and Numbers (ICANN) hyväksyy uudet WHOIS-käytännöt. Komissio jatkaa yhteistyötä ICANNin ja monisidosryhmäisen yhteisön kanssa sen varmistamiseksi, että oikeutetut käyttöoikeuksien hakijat, myös lainvalvontaviranomaiset, voivat saada WHOIS-tiedot tehokkaasti käyttöönsä EU:n ja kansainvälisiä tietosuojasäännöksiä noudattaen. Tähän kuuluu mahdollisten ratkaisujen arviointi, mukaan lukien se, edellyttääkö tietojen saantia koskevien sääntöjen selkeyttäminen lainsäädäntöä.

Lainvalvonta- ja oikeusviranomaisilla on oltava välineet tarvittavien tietojen ja todisteiden hankkimiseksi myös sen jälkeen, kun **matkaviestinnän 5G-arkkitehtuuri** on otettu täysimääräisesti käyttöön EU:ssa, kuitenkin viestinnän luottamuksellisuutta kunnioittaen. Komissio tukee tehostettua ja koordinoitua lähestymistapaa laadittaessa kansainvälisiä normeja sekä määriteltäessä parhaita käytäntöjä, prosesseja ja teknistä yhteentoimivuutta tekoälyn, esineiden internetin tai lohkoketjuteknologian kaltaisilla keskeisillä teknologian aloilla.

Nykyisin huomattavaan osaan kaikkea rikollisuuden ja terrorismin vastaista tutkimustyötä liittyy **salattua tietoa**. Salaus on olennaisen tärkeää digitaalimaailmassa, sillä se turvaa digitaaliset järjestelmät ja sähköiset maksutapahtumat sekä suojaa myös useita perusoikeuksia, kuten sananvapautta, yksityisyyttä ja tietosuojaa. Jos sitä kuitenkin käytetään rikollisiin tarkoituksiin, se voi myös salata rikollisten henkilöllisyyden ja piilottaa heidän viestiensä sisällön. Komissio kartoittaa ja tukee tasapainoisia teknisiä, operatiivisia ja oikeudellisia ratkaisuja näihin haasteisiin ja kannattaa lähestymistapaa, jossa tehokas salaus säilytetään viestinnän yksityisyyden ja turvallisuuden suojaamiseksi mutta joka kuitenkin torjuu tehokkaasti rikollisuutta ja terrorismia.

Laittoman verkkosisällön torjunta

Verkkoympäristön ja fyysisen ympäristön turvallisuuden yhdenmukaistaminen edellyttää jatkuvia toimia **laittoman verkkosisällön torjumiseksi**. Kansalaisiin kohdistuvat keskeiset uhat, kuten terrorismi, ääriliikkeet ja lasten seksuaalinen hyväksikäyttö, ovat yhä enemmän riippuvaisia digitaalisesta ympäristöstä. Tämä vaatii konkreettisia toimia ja säännöstön, jolla varmistetaan perusoikeuksien kunnioittaminen. Tärkeä ensimmäinen askel on saattaa nopeasti päätökseen neuvottelut terroristista verkkosisältöä koskevasta lainsäädäntöehdotuksesta[67] ja varmistaa sen täytäntöönpano. Lainvalvontaviranomaisten ja

[65] Erityisesti Euroopan neuvoston tietoverkkorikollisuutta koskevan Budapestin yleissopimuksen toinen lisäpöytäkirja sekä EU:n ja Yhdysvaltojen välinen sopimus sähköisen todistusaineiston rajatylittävästä saatavuudesta.

[66] Tallennettu tietokantoihin, joita ylläpitää 2 500 rekisteriä ja rekisterinpitäjää eri puolilla maailmaa.

[67] Ehdotus verkossa tapahtuvan terroristisen sisällön levittämisen estämisestä, COM(2018) 640, 12. syyskuuta 2018.

yksityisen sektorin välisen vapaaehtoisen yhteistyön vahvistaminen **EU:n internetfoorumissa** on myös avainasemassa torjuttaessa terroristien, väkivaltaisten ääriliikkeiden ja rikollisten harjoittamaa internetin väärinkäyttöä. Europolissa toimivalla internetsisältöä koskevia ilmoituksia tekevällä EU:n yksiköllä on edelleen keskeinen rooli terroristiryhmien verkkotoiminnan ja alustojen toiminnan seurannassa[68] sekä **EU:n kriisisäännöstön**[69] kehittämisessä. Lisäksi komissio jatkaa yhteistyötä kansainvälisten kumppaneiden kanssa muun muassa osallistumalla **terrorismintorjunnan maailmanlaajuiseen internetfoorumiin** vastatakseen näihin haasteisiin maailmanlaajuisesti. Työtä vaihtoehtoisten ja vastakkaisten narratiivien kehittämiseksi jatketaan kansalaisyhteiskunnan vaikutusmahdollisuuksia parantavan ohjelman[70] kautta.

Ehkäistäkseen ja torjuakseen laittoman vihapuheen leviämistä verkossa komissio laati vuonna 2016 käytännesäännöt verkossa esiintyvän laittoman vihapuheen torjumiseksi, ja verkkoalustat sitoutuivat poistamaan vihapuhesisällön vapaaehtoisesti. Viimeisimmän arvioinnin mukaan yritykset arvioivat 90 prosenttia ilmoitetusta sisällöstä 24 tunnin kuluessa ja poistavat 71 prosenttia laittomaksi vihapuheeksi katsotusta sisällöstä. Alustojen on kuitenkin lisättävä läpinäkyvyyttä sekä käyttäjille annettavaa palautetta ja varmistettava, että ilmoitettu sisältö arvioidaan johdonmukaisesti.[71]

EU:n internetfoorumi helpottaa myös tietojenvaihtoa nykyisestä ja kehitteillä olevasta teknologiasta, jolla voidaan vastata verkossa tapahtuvaan lasten seksuaaliseen hyväksikäyttöön liittyviin haasteisiin. Lasten seksuaalisen hyväksikäytön torjuminen verkossa on keskeisessä asemassa uudessa strategiassa, jolla tehostetaan **lasten seksuaalisen hyväksikäytön torjuntaa**[72] ja pyritään maksimoimaan EU:n tasolla käytettävissä olevien välineiden käyttö näiden rikosten torjumisessa. Yritysten on pystyttävä jatkamaan työtään verkossa olevan lasten seksuaalista hyväksikäyttöä kuvaavan materiaalin havaitsemiseksi ja poistamiseksi, ja tällaisen materiaalin vahingoittavuus edellyttää säännöstöä, jossa määritellään selkeät ja pysyvät velvoitteet ongelman ratkaisemiseksi. Strategiassa ilmoitetaan myös, että komissio alkaa valmistella alakohtaista lainsäädäntöä verkossa tapahtuvan lasten seksuaalisen hyväksikäytön tehokkaammaksi torjumiseksi perusoikeuksia täysimääräisesti kunnioittaen.

Yleisemmällä tasolla tulevassa digitaalisia palveluja koskevassa säädöksessä lisäksi selkeytetään ja parannetaan digitaalisten palvelujen vastuu- ja turvallisuussääntöjä ja poistetaan pidätteleviä tekijöitä, jotka estävät laittomiin sisältöihin, tavaroihin tai palveluihin kohdistuvia toimia.

Lisäksi komissio jatkaa yhteistyötä kansainvälisten kumppaneiden kanssa ja **terrorismintorjunnan maailmanlaajuisessa internetfoorumissa** muun muassa riippumattoman neuvoa-antavan komitean kautta ja keskustelee siitä, miten näihin haasteisiin voidaan vastata maailmanlaajuisesti samalla EU:n arvot ja perusoikeudet säilyttäen. Lisäksi olisi käsiteltävä algoritmien ja verkkopelien kaltaisia uusia aiheita.[73]

Hybridiuhat

---

68 Europol, marraskuu 2019.

69 Eurooppa, joka suojelee – EU:n kriisisäännöstö:reagointi terroristiseen verkkosisältöön, lokakuu 2019.

70 Liittyy radikalisoitumisen torjuntaverkoston työhön, ks. kohta IV.3 jäljempänä.

71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

72 EU:n strategia lasten seksuaalisen hyväksikäytön torjunnan tehostamiseksi, COM(2020) 607.

73 Terroristit käyttävät yhä enemmän pelialustojen viestijärjestelmiä yhteydenpitoon. Lisäksi nuoret terroristit toistavat väkivaltaisia iskuja videopeleissä.

Tämän päivän hybridiuhat ovat ennennäkemättömän laajoja ja moninaisia. Tämän osoittaa muun muassa se, kuinka covid-19-kriisin aikaan valtiolliset ja valtiosta riippumattomat toimijat pyrkivät hyödyntämään pandemiaa etenkin manipuloimalla tietoympäristöä ja haastamalla keskeisiä infrastruktuureja. Tämä uhkaa heikentää sosiaalista yhteenkuuluvuutta ja horjuttaa luottamusta EU:n toimielimiin ja jäsenvaltioiden hallituksiin.

EU:n lähestymistapa hybridiuhkiin vahvistetaan vuoden 2016 yhteisessä kehyksessä[74] ja vuonna 2018 annetussa hybridiuhkiin valmistautumista koskevassa yhteisessä tiedonannossa[75]. EU:n tason toimia tuetaan mittavalla välineistöllä, joka kattaa sisäisen ja ulkoisen turvallisuuden yhteyden ja joka perustuu koko yhteiskunnan kattavaan lähestymistapaan ja tiiviiseen yhteistyöhön strategisten kumppanien, erityisesti Naton ja G7-maiden, kanssa. Kertomus hybridiuhkien torjumista koskevan EU:n lähestymistavan täytäntöönpanosta[76] julkaistaan yhdessä tämän strategian kanssa. Komission yksiköt ja Euroopan ulkosuhdehallinto luovat yhdessä tämän strategian kanssa esitetyn kartoituksen[77] pohjalta **rajoitetun verkkoalustan**, jolta jäsenvaltiot saavat tietoa hybridiuhkien torjuntaan liittyvistä EU:n tason välineistä ja toimenpiteistä.

Vastuu hybridiuhkien torjunnasta on ensisijaisesti jäsenvaltioilla, koska se kytkeytyy vahvasti kansallisiin turvallisuus- ja puolustuspolitiikkoihin. Jotkin haavoittuvuudet ovat kuitenkin yhteisiä kaikille jäsenvaltioille ja jotkin uhat ulottuvat rajojen yli, kuten rajat ylittäviin verkkoihin tai infrastruktuuriin. Komissio ja korkea edustaja laativat hybridiuhkia koskevan EU:n lähestymistavan, jossa ulkoinen ja sisäinen ulottuvuus integroidaan saumattomasti toisiinsa ja kansalliset ja EU:n laajuiset näkökohdat tuodaan yhteen. Sen on katettava kaikki toimet varhaisesta havaitsemisesta, analysoinnista, tietoisuudesta, selviytymiskyvyn kehittämisestä ja ennaltaehkäisystä kriisitoimintaan ja seurausten hallintaan.

Koska hybridiuhat muuttuvat jatkuvasti, täytäntöönpanon tehostamisen lisäksi kiinnitetään erityistä huomiota **hybridinäkökohtien sisällyttämiseen poliittiseen päätöksentekoon**, dynaamisessa kehityksessä mukana pysymiseen ja sen varmistamiseen, ettei mitään mahdollisesti merkityksellisiä aloitteita jätetä huomiotta. Uusien aloitteiden vaikutuksia arvioidaan myös hybridiuhkien valossa, mukaan lukien aloitteet aloilla, jotka eivät ole tähän mennessä kuuluneet hybridiuhkien torjuntaa koskevan kehyksen soveltamisalaan, kuten koulutus, teknologia ja tutkimus. Tässä lähestymistavassa olisi hyötyä hybridiuhkien käsitteellistämiseksi tehdystä työstä, joka tarjoaa kattavan kuvan vastustajien käytössä mahdollisesti olevista eri välineistä.[78] Olisi pyrittävä varmistamaan, että päätöksentekoprosessia tuetaan säännöllisellä ja kattavalla tiedustelutietoon perustuvalla raportoinnilla hybridiuhkien kehityksestä. Tämä edellyttää jäsenvaltioilta saatavia tiedustelutietoja ja jäsenvaltioiden toimivaltaisten yksiköiden kanssa tehtävän tiedusteluyhteistyön tehostamista EU:n tiedusteluanalyysikeskuksen avulla.

Komission yksiköt ja Euroopan ulkosuhdehallinto tarkastelevat **tilannetietoisuuden** parantamiseksi mahdollisuuksia virtaviivaistaa tiedonkulkua eri lähteistä, mukaan lukien

[74] Yhteinen kehys hybridiuhkien torjumiseksi: Euroopan unionin toimet, JOIN(2016) 18.

[75] Selviytymiskyvyn ja valmiuksien kehittäminen hybridiuhkien varalta, JOIN(2018) 16.

[76] Kertomus vuonna 2016 hyväksytyn hybridiuhkien torjumista koskevan yhteisen kehyksen täytäntöönpanosta (SWD(2020) 153) ja vuonna 2018 annettu yhteinen tiedonanto selviytymiskyvyn ja valmiuksien kehittämisestä hybridiuhkien varalta.

[77] ”Mapping of the measures related to enhancing resilience and countering hybrid threats” (resilienssin parantamiseen ja hybridiuhkien torjuntaan liittyvien toimien kartoitus), SWD(2020) 152.

[78] Yhteisen tutkimuskeskuksen ja hybridiosaamiskeskuksen raportti hybridiuhkiin liittyvästä käsitemallista:”The Landscape of Hybrid Threats: A conceptual Model”, JRC117280.

jäsenvaltioista ja EU:n virastoista, kuten ENISAsta, Europolista ja Frontexista. EU:n hybridianalyysikeskus pysyy unionin hybridiuhkien arvioinnin keskuspisteenä. **Häiriönsietokyvyn kehittäminen** on keskeistä hybridiuhkien ehkäisemisessä ja niiltä suojautumisessa. Sen vuoksi on ratkaisevan tärkeää seurata järjestelmällisesti ja mitata puolueettomasti siinä saavutettua edistystä. Ensimmäiseksi on määritettävä alakohtaiset perusvaatimukset hybridiuhkista selviytymiseksi jäsenvaltioissa ja EU:n toimielimissä ja elimissä. Jotta **hybridikriiseihin varautumista** voitaisiin parantaa, nykyisiä menettelyjä olisi tarkasteltava uudelleen, kuten vuoden 2016 EU:n operatiivisessa protokollassa hybridiuhkien torjumiseksi[79] on määritelty, ottaen huomioon parhaillaan käsiteltävänä olevan EU:n kriisitoimintajärjestelmän laajempi tarkistaminen ja vahvistaminen.[80] Tavoitteena on maksimoida EU:n toimien vaikutus kokoamalla nopeasti yhteen alakohtaiset ratkaisut ja varmistamalla saumaton yhteistyö kumppaneiden, ensi sijassa Naton, kanssa.

Keskeiset toimet
• Varmistetaan kyberrikollisuutta koskevan lainsäädännön täytäntöönpano ja tarkoituksenmukaisuus. • Laaditaan strategia lasten seksuaalisen hyväksikäytön torjunnan tehostamiseksi. • Esitetään ehdotuksia lasten seksuaaliseen hyväksikäyttöön liittyvän materiaalin havaitsemiseksi ja poistamiseksi. • Laaditaan EU:n lähestymistapa hybridiuhkien torjumiseen. • Tarkistetaan EU:n operatiivista protokollaa hybridiuhkien torjumiseksi. • Arvioidaan tapoja parantaa lainvalvontavalmiuksia digitaalisissa tutkintatoimissa.

3. Eurooppalaisten suojeleminen terrorismilta ja järjestäytyneeltä rikollisuudelta

Terrorismi ja radikalisoituminen

Terrorismin uhka on EU:ssa edelleen suuri. Vaikka iskujen määrä on kaiken kaikkiaan vähentynyt, niillä voi silti olla tuhoisia vaikutuksia. Lisäksi radikalisoituminen voi luoda laajempaa vastakkainasettelua ja horjuttaa sosiaalista yhteenkuuluvuutta. Vastuu terrorismin ja radikalisoitumisen torjunnasta kuuluu edelleen ensisijaisesti jäsenvaltioille. Uhkan ulottuminen rajojen yli ja eri aloille yhä suuremmissa määrin edellyttää kuitenkin lisää yhteistyötä ja koordinointia EU:n tasolla. EU:n terrorisminvastaisen lainsäädännön tehokas täytäntöönpano, rajoittavat toimenpiteet[81] mukaan luettuina, on ensisijaisen tärkeää. Tavoitteena on yhä laajentaa Euroopan syyttäjänviraston toimivaltuuksia rajatylittäviin terrorismirikoksiin.

Terrorismin torjunta alkaa perimmäisiin syihin puuttumisella. Yhteiskunnan polarisoituminen, todellinen tai havaittu syrjintä ja muut psykologiset ja sosiologiset tekijät voivat lisätä ihmisten altistumista radikalismille. **Radikalisoitumisen** torjunta liittyy näin ollen tiiviisti sosiaalisen yhteenkuuluvuuden edistämiseen paikallisella, kansallisella ja

[79] ”EU operational protocol for countering hybrid threats, ’EU Playbook’”, SWD(2016) 227.

[80] Eurooppa-neuvoston jäsenet hyväksyivät 26. maaliskuuta 2020 pidetyn videoneuvottelun jälkeen julkilausuman EU:n toimista, jotka liittyvät covid-19-pandemiaan, ja kehottivat komissiota esittämään ehdotuksia kunnianhimoisemmasta ja laaja-alaisemmasta EU:n kriisinhallintajärjestelmästä.

[81] Neuvosto hyväksyi ISILiä (Daesh) ja al-Qaidaa koskevia rajoittavia toimenpiteitä sekä tiettyihin henkilöihin ja yhteisöihin kohdistuvia erityisiä rajoittavia toimenpiteitä terrorismin torjumiseksi. Yleiskatsaus kaikista rajoittavista toimenpiteistä esitetään EU:n pakotekartassa (https://www.sanctionsmap.eu/#/main).

Euroopan tasolla. Viime vuosikymmenen aikana on laadittu useita vaikuttavia aloitteita ja toimintalinjoja erityisesti radikalisoitumisen torjuntaverkoston ja ”EU:n kaupungit radikalisoitumista vastaan” -aloitteen[82] kautta. Nyt on aika harkita toimia, joilla voidaan yhdenmukaistaa EU:n politiikkoja, aloitteita ja varoja radikalisoitumisen torjumiseksi. Toimilla voitaisiin tukea valmiuksien ja taitojen kehittämistä, tehostaa yhteistyötä, vahvistaa näyttöpohjaa ja arvioida edistymistä ottamalla mukaan kaikki asiaankuuluvat sidosryhmät, mukaan lukien kenttätyöntekijät, poliittiset päättäjät ja tiedemaailma.[83] Pehmeillä politiikoilla, kuten koulutukseen, kulttuuriin, nuorisoon ja urheiluun liittyvillä toimilla, voitaisiin edistää radikalisoitumisen torjumista, tarjota mahdollisuuksia riskiryhmään kuuluville nuorille ja parantaa unionin yhtenäisyyttä.[84] Painopisteinä ovat muun muassa varhainen havaitseminen ja riskinhallinta, häiriönsietokyvyn kehittäminen ja osallistumattomuuteen puuttuminen sekä kuntoutus ja yhteiskuntaan sopeuttaminen.

Terroristit ovat pyrkineet hankkimaan **kemiallisia, biologisia, säteily- ja ydinmateriaaleja** (CBRN)[85] käyttääkseen niitä aseina sekä kehittämään tietämystä ja valmiuksia niiden käyttämiseksi.[86] CBRN-iskujen mahdollisuus on näkyvästi esillä terroristisessa propagandassa. Koska ne voivat aiheuttaa suurta vahinkoa, asiaan on kiinnitettävä erityistä huomiota. Komissio tarkastelee räjähteiden lähtöaineiden saatavuuden sääntelyyn sovellettavan lähestymistavan pohjalta tiettyjen sellaisten vaarallisten kemikaalien saatavuuden rajoittamista, joita voitaisiin käyttää iskujen tekemiseen. Keskeistä on myös CBRN-alaan liittyvien EU:n pelastuspalvelutoimien (rescEU) kehittäminen. Yhteistyö kolmansien maiden kanssa on myös tärkeää, jotta voidaan edistää CBRN-materiaaleihin liittyvää yhteistä turvallisuuskulttuuria. Tässä voidaan hyödyntää täysimääräisesti EU:n maailmanlaajuisia CBRN-osaamiskeskuksia. Tähän yhteistyöhön kuuluu kansallisten puutteiden ja riskien arviointi, kansallisten ja alueellisten CBRN-toimintasuunnitelmien tukeminen, hyvien käytäntöjen vaihto ja CBRN-valmiuksien kehittäminen.

EU:n lainsäädäntö on maailman edistynein niiltä osin, joilla sillä rajoitetaan **räjähteiden lähtöaineiden**[87] saatavuutta ja havaitaan epäilyttäviä liiketoimia, joiden tarkoituksena on omatekoisten räjähteiden valmistaminen. Omatekoisten räjähteiden aiheuttama uhka on kuitenkin edelleen suuri, ja niitä on käytetty useissa iskuissa eri puolilla unionia.[88] Ensimmäiseksi on pantava täytäntöön säännöt ja varmistettava, että verkkoympäristö ei mahdollista valvonnan ohittamista.

Terroristien, mukaan lukien tällä hetkellä Syyriassa ja Irakissa olevien **terrorismiin syyllistyvien vierastaistelijoiden**, tehokas syytteeseenpano on myös tärkeä osa terrorisminvastaista politiikkaa. Vaikka näitä asioita käsitellään pääasiassa jäsenvaltioiden tasolla, EU:n koordinointi ja tuki voivat auttaa jäsenvaltioita vastaamaan yhteisiin

[82] Pilottihankkeen ”EU:n kaupungit radikalisoitumista vastaan” tavoitteina on edistää asiantuntemuksen vaihtoa EU:n kaupunkien välillä ja kerätä palautetta siitä, miten paikallisyhteisöjä voidaan parhaiten tukea EU:n tasolla.

[83] Rahoitus esimerkiksi Euroopan turvallisuusrahastosta ja kansalaisuusohjelmasta.

[84] EU:n toimet kuten Erasmus+ Virtual Exchange -aloite ja eTwinning-hanke.

[85] Esimerkiksi kahden viime vuoden aikana sekä Euroopassa (Ranskassa, Saksassa ja Italiassa) että muualla maailmassa (Tunisiassa ja Indonesiassa) on ollut useita tapauksia, joissa on käytetty biologisia materiaaleja (yleensä kasviperäisiä toksiineja).

[86] Neuvosto hyväksyi rajoittavia toimenpiteitä kemiallisten aseiden leviämisen ja käytön torjumiseksi.

[87] Kemikaalit, joita voidaan käyttää väärin kotitekoisten räjähteiden valmistamiseen. Niistä säädetään räjähteiden lähtöaineiden markkinoille saattamisesta ja käytöstä annetussa asetuksessa (EU) 2019/1148.

[88] Esimerkkejä tällaisista tuhoisista iskuista ovat Oslossa (2011), Pariisissa (2015), Brysselissä (2016) ja Manchesterissa (2017) tehdyt iskut. Kotitekoisella räjähteellä toteutettu isku Lyonissa haavoitti 13:a ihmistä vuonna 2019.

haasteisiin. Toteutettavat toimet, joilla pannaan täysimääräisesti täytäntöön rajaturvallisuutta koskeva lainsäädäntö[89] ja hyödynnetään täysimääräisesti kaikkia asiaankuuluvia EU:n tietokantoja tietojen jakamiseksi tiedossa olevista epäillyistä, ovat tärkeä askel. Suuririskisten henkilöiden tunnistamisen lisäksi tarvitaan sopeuttamis- ja kuntoutuspolitiikkaa. Monialainen yhteistyö, myös vankila- ja ehdonalaishenkilöstön kanssa, vahvistaa oikeudellista ymmärtämystä väkivaltaisten ääriliikkeiden ja radikalisoitumisen prosesseista ja oikeuslaitoksen lähestymistavasta tuomitsemiseen ja vangitsemisen vaihtoehtoihin.

Terrorismiin syyllistyvien vierastaistelijoiden aiheuttamille haasteille on tunnusomaista sisäisen ja **ulkoisen turvallisuuden** yhteys. Yhteistyö terrorismin torjunnassa sekä radikalisoitumisen ja väkivaltaisen ääriliikehdinnän ehkäisemisessä ja torjunnassa on keskeistä EU:n sisäisen turvallisuuden kannalta.[90] Lisätoimia tarvitaan terrorisminvastaisten kumppanuuksien ja yhteistyön kehittämiseksi naapuruusmaiden ja kauempana sijaitsevien maiden kanssa EU:n terrorismintorjunnan ja turvallisuusasiantuntijoiden verkoston asiantuntemuksen pohjalta. Länsi-Balkanin yhteinen terrorisminvastainen toimintasuunnitelma on hyvä viitepohja tällaiselle kohdennetulle yhteistyölle. Erityisesti olisi pyrittävä tukemaan kumppanimaiden valmiuksia tunnistaa ja paikantaa terrorismiin syyllistyviä vierastaistelijoita. EU jatkaa myös monenvälisen yhteistyön edistämistä ja tekee yhteistyötä alan johtavien globaalien toimijoiden, kuten Yhdistyneiden kansakuntien, Naton, Euroopan neuvoston, Interpolin ja Etyjin, kanssa. Se tekee yhteistyötä myös maailmanlaajuisen terrorisminvastaisen foorumin ja Daeshin vastaisen maailmanlaajuisen liittoutuman sekä asiaankuuluvien kansalaisyhteiskunnan toimijoiden kanssa. Unionin ulkopolitiikan välineet, kuten kehitykseen ja yhteistyöhön liittyvät toimet, ovat myös tärkeässä asemassa työskenneltäessä kolmansien maiden kanssa terrorismin ja merirosvouden torjumiseksi. Lisäksi kansainvälinen yhteistyö on olennaisen tärkeää kaikkien **terrorismin rahoituslähteiden** tukkimiseksi esimerkiksi rahanpesunvastaisen toimintaryhmän kautta.

Järjestäytynyt rikollisuus

Järjestäytynyt rikollisuus aiheuttaa valtavia taloudellisia kustannuksia ja suurta inhimillistä kärsimystä. Järjestäytyneestä rikollisuudesta ja korruptiosta aiheutuvien taloudellisten menetysten arvioidaan olevan vuositasolla 218–282 miljardia euroa.[91] Euroopassa oli vuonna 2017 tutkinnan kohteena yli 5 000 järjestäytynyttä rikollisryhmää, mikä on 50 prosenttia enemmän kuin vuonna 2013.[92] Järjestäytynyt rikollisuus toimii yhä enemmän rajojen yli, myös EU:n lähinaapurustosta käsin, mikä edellyttää tehostettua operatiivista yhteistyötä ja tietojenvaihtoa naapurialueiden kumppaneiden kanssa.

Esiin on nousemassa uusia verkkorikollisuuteen liittyviä haasteita: covid-19-pandemian aikaan haavoittuviin ryhmiin kohdistuvat verkkohuijaukset lisääntyivät merkittävästi ja varkauksia ja murtoja kohdistettiin terveys- ja hygieniatuotteisiin.[93] EU:n on tehostettava järjestäytyneen rikollisuuden vastaisia toimiaan, myös kansainvälisellä tasolla, ottamalla

[89] Mukaan lukien Euroopan raja- ja merivartioviraston (Frontex) uusi toimeksianto.

[90] Neuvoston 16. kesäkuuta 2020 antamissa päätelmissä korostettiin tarvetta suojella EU:n kansalaisia terrorismilta ja väkivaltaisilta ääriliikkeiltä niiden kaikissa muodoissa ja niiden alkuperästä riippumatta sekä tarvetta vahvistaa edelleen EU:n ulkoista terrorisminvastaista yhteistyötä ja toimintaa tietyillä ensisijaisilla maantieteellisillä ja temaattisilla aloilla.

[91] Suhteessa bruttokansantuotteeseen (BKT); Europolin selvitys: ”Does crime still pay? – Criminal asset recovery in the EU”, 2016.

[92] Europolin laatimat vakavaa ja järjestäytynyttä rikollisuutta koskevat uhkakuva-arviot (SOCTA), 2013 ja 2017.

[93] Europol, 2020.

käyttöön lisää välineitä järjestäytyneen rikollisuuden toimintamallin hajottamiseksi. Järjestäytyneen rikollisuuden torjunta edellyttää myös tiivistä yhteistyötä paikallis- ja alueviranomaisten sekä kansalaisyhteiskunnan kanssa, sillä ne ovat keskeisiä kumppaneita rikosten ehkäisemisessä ja uhrien auttamisessa ja tukemisessa. Erityisesti yhteistyö raja-alueiden viranomaisten kanssa on tarpeen. Tähän liittyvät toimet kootaan yhteen **järjestäytyneen rikollisuuden torjuntaa koskevaksi toimintasuunnitelmaksi**.

Yli kolmannes EU:ssa toimivista järjestäytyneistä rikollisryhmistä on mukana huumausaineiden tuotannossa, kaupassa tai jakelussa. Huumeriippuvuus aiheutti EU:ssa yli kahdeksan tuhatta yliannostuskuolemaa vuonna 2019. Valtaosa **huumekaupasta** tapahtuu rajojen yli, ja iso osa voitoista ohjautuu lailliseen talouteen.[94] Uudella EU:n huumeiden vastaisella ohjelmalla[95] vahvistetaan EU:n ja jäsenvaltioiden toimia huumeiden kysynnän ja tarjonnan vähentämiseksi, määritellään yhteisiä toimia yhteisen ongelman ratkaisemiseksi ja vahvistetaan EU:n ja ulkoisten kumppaneiden välistä vuoropuhelua ja yhteistyötä huumausainekysymyksissä. Komissio arvioi Euroopan huumausaineiden ja niiden väärinkäytön seurantakeskuksen arvioinnin perusteella, onko sen toimeksiantoa päivitettävä uusiin haasteisiin vastaamiseksi.

Järjestäytyneet rikollisryhmät ja terroristit ovat myös keskeisiä toimijoita **laittomien ampuma-aseiden** kaupassa. Vuosina 2009–2018 Euroopassa tapahtui 23 joukkoammuskelua, joissa kuoli yli 340 ihmistä.[96] Ampuma-aseita kaupataan EU:hun usein sen lähinaapurustosta.[97] Tämän vuoksi on tarpeen vahvistaa koordinointia ja yhteistyötä sekä unionin sisällä että kansainvälisten kumppaneiden, erityisesti Interpolin, kanssa ampuma-aseiden takavarikointeja koskevien tietojen keruun ja raportoinnin yhdenmukaistamiseksi. On myös olennaisen tärkeää parantaa aseiden jäljitettävyyttä, myös verkossa, ja varmistaa tietojen vaihdon sujuvuus lupa- ja lainvalvontaviranomaisten välillä. Komissio esittää uutta **EU:n toimintasuunnitelmaa ampuma-aseiden laittoman kaupan torjumiseksi**[98] ja arvioi myös, ovatko ampuma-aseiden vientilupia sekä tuonti- ja kauttakuljetusmenettelyjä koskevat säännöt[99] edelleen tarkoituksenmukaisia.

Rikollisjärjestöt kohtelevat maahanmuuttajia ja kansainvälisen suojelun tarpeessa olevia ihmisiä kauppatavarana. EU:hun saapuvista laittomista maahanmuuttajista 90:tä prosenttia auttaa jokin rikollisverkosto.[100] Siirtolaisten salakuljetus kytkeytyy usein myös muihin järjestäytyneen rikollisuuden muotoihin, erityisesti ihmiskauppaan.[101] Sen lisäksi, että ihmiskauppa aiheuttaa valtavia inhimillisiä menetyksiä, Europol arvioi, että kaikkien siihen liittyvien hyväksikäytön muotojen vuotuinen tuotto nousee 29,4 miljardiin euroon. Ihmiskauppa on rajatylittävää rikollisuutta, joka saa voimansa unionin sisä- ja ulkopuolelta tulevasta laittomasta kysynnästä ja koskee kaikkia EU:n jäsenvaltiota. Koska näiden rikosten tunnistaminen, syytteeseenpano ja tuomitseminen on ollut heikkoa, toimia on tehostettava uudella lähestymistavalla. Toimintatavat kootaan yhteen uudessa **ihmiskaupan torjuntaa**

---

94 EMCDDA:n ja Europolin EU:n huumausainemarkkinoita koskeva raportti, marraskuu 2019.

95 EU:n huumeidenvastainen ohjelma ja toimintasuunnitelma 2021–2025, COM (2020) 606.

96 Flemish Peace Institute, ”Armed to kill”, lokakuu 2019.

97 EU on rahoittanut pienaseiden ja kevyiden aseiden leviämisen ja kaupan torjuntaa alueella vuodesta 2002. Erityisesti se on rahoittanut Kaakkois-Euroopan ampuma-aseasiantuntijoiden verkostoa (SEEFEN). Länsi-Balkanin kumppanit ovat vuodesta 2019 lähtien osallistuneet täysimääräisesti Euroopan monialaisen rikosuhkien torjuntafoorumin (EMPACT) ampuma-aseita koskevaan prioriteettiin.

98 COM(2020) 608.

99 Asetus (EU) N:o 258/2012 Yhdistyneiden kansakuntien ampuma-aseiden laittoman valmistuksen ja laittoman kaupan torjuntaa koskevan lisäpöytäkirjan 10 artiklan täytäntöönpanosta.

100 Lähde: Europol.

101 Europol, ihmisten salakuljetusta tutkiva eurooppalainen keskus (EMSC), 4. vuosikertomus.

koskevassa kokonaisvaltaisessa lähestymistavassa. Lisäksi komissio aikoo esittää **uuden siirtolaisten salakuljetuksen vastaisen EU:n toimintasuunnitelman** vuosiksi 2021–2025. Näissä kummassakin keskitytään rikollisverkostojen torjuntaan, yhteistyön parantamiseen ja lainvalvontatyön tukemiseen.

Järjestäytyneet rikollisryhmät sekä terroristit etsivät mahdollisuuksia myös muilta aloilta, erityisesti sellaisilta, jotka tuottavat suuria voittoja ja joilla kiinnijäämisen riski on pieni, kuten **ympäristörikollisuus**. Luonnonvaraisten eläinten ja kasvien laittomasta metsästyksestä ja kaupasta, laittomasta kaivostoiminnasta ja puunkorjuusta sekä jätteiden laittomasta hävittämisestä ja siirrosta on tullut maailman neljänneksi suurin rikollisen toiminnan ala.[102] Myös päästökauppa- ja energiatodistusjärjestelmiä on käytetty rikollisesti hyväksi ja ympäristökestävyyteen ja kestävään kehitykseen osoitettuja varoja on käytetty väärin. Sen lisäksi, että komissio edistää EU:n, jäsenvaltioiden ja kansainvälisen yhteisön toimia ympäristörikollisuuden[103] torjunnan tehostamiseksi, se arvioi, onko ympäristörikosdirektiivi[104] edelleen tarkoituksenmukainen. Myös **kulttuuriesineiden laittomasta kaupasta** on tullut yksi tuottoisimmista rikollisista toimista ja tulonlähde terroristeille ja järjestäytyneelle rikollisuudelle. Olisikin tutkittava toimia, joilla parannetaan kulttuuriesineiden jäljitettävyyttä sisämarkkinoilla, niin verkossa kuin sen ulkopuolella, ja yhteistyötä niiden kolmansien maiden kanssa, joissa kulttuuriesineitä ryöstetään. Lisäksi olisi tuettava aktiivisesti lainvalvontaviranomaisia ja tiedeyhteisöä.

Talousrikokset ovat hyvin monimutkaisia, ja ne vaikuttavat vuosittain miljooniin kansalaisiin ja tuhansiin yrityksiin EU:ssa. Petosten torjunta on ratkaisevan tärkeää ja edellyttää EU:n tason toimia. Europol tukee yhdessä Eurojustin, Euroopan syyttäjänviraston ja Euroopan petostentorjuntaviraston kanssa jäsenvaltioita ja EU:ta talous- ja finanssimarkkinoiden ja EU:n veronmaksajien rahojen suojaamisessa. Euroopan syyttäjänvirasto tulee olemaan täysin toimintavalmis vuoden 2020 lopulla. Se tutkii EU:n talousarvioon kohdistuvia rikoksia, kuten petoksia, korruptiota ja rahanpesua, ja asettaa niiden tekijät syytteeseen ja tuomittaviksi. Se käsittelee myös rajatylittäviä arvonlisäveropetoksia, jotka aiheuttavat veronmaksajille vähintään 50 miljardin euron vuotuiset kustannukset.

Komissio tukee myös kehittyviin riskeihin, kuten kryptovaroihin ja uusiin maksujärjestelmiin, liittyvän asiantuntemuksen kehittämistä ja lainsäädäntökehyksen laatimista. Komissio aikoo erityisesti tarkastella kryptovarojen, kuten bitcoinin, käyttöönottoa ja sitä, miten nämä uudet teknologiat vaikuttavat rahoitusvarojen liikkeeseenlaskuun, vaihtamiseen, jakamiseen ja hyödyntämiseen.

Euroopan unionissa olisi sovellettava nollatoleranssia laittomaan rahaan. EU on kolmenkymmenen vuoden aikana luonut vankan sääntelykehyksen **rahanpesun** ja terrorismin rahoituksen ehkäisemiseksi ja torjumiseksi ja ottanut siinä täysimääräisesti huomioon henkilötietojen suojan tarpeen. Enenevässä määrin ollaan kuitenkin sitä mieltä, että nykyisen kehyksen täytäntöönpanoa on parannettava huomattavasti. Suuret erot sen soveltamisessa ja vakavat puutteet sääntöjen täytäntöönpanossa on korjattava. Kuten toukokuussa 2020 annetussa toimintasuunnitelmassa[105] esitetään, parhaillaan arvioidaan vaihtoehtoja rahanpesun ja terrorismin rahoituksen torjuntaa koskevan EU:n kehyksen parantamiseksi. Muihin tarkasteltaviin aiheisiin kuuluu kansallisten keskitettyjen

[102] UNEPin ja Interpolin laatima nopean toiminnan arvio ”The Rise of Environmental Crime”, kesäkuu 2016.
[103] Ks. Euroopan vihreän kehityksen ohjelma, COM (2019) 640 final.
[104] Direktiivi 2008/99/EY ympäristönsuojelusta rikosoikeudellisin keinoin.
[105] Rahanpesun ja terrorismin rahoituksen torjuntaa koskeva toimintasuunnitelma, COM(2020) 2800.

pankkitilirekisterien yhteenliittäminen, millä voitaisiin merkittävästi nopeuttaa rahanpesun selvittelykeskusten ja lainvalvontaviranomaisten pääsyä rahoitustietoihin.

Järjestäytyneiden rikollisryhmien voittojen arvioidaan olevan EU:ssa vuositasolla 110 miljardia euroa. Tähän pyritään puuttumaan yhdenmukaistamalla menetetyksi tuomitsemista ja varojen takaisinperintää[106] koskevaa lainsäädäntöä, jotta voidaan parantaa rikoksella saatujen varojen jäädyttämistä ja menetetyksi tuomitsemista unionissa ja edistää jäsenvaltioiden keskinäistä luottamusta ja tehokasta rajatylittävää yhteistyötä. Kuitenkin vain noin prosentti näistä voitoista takavarikoidaan[107], ja näin ollen järjestäytyneet rikollisryhmät voivat investoida rikollisen toimintansa laajentamiseen ja soluttautua lailliseen talouteen. Erityisesti pienet ja keskisuuret yritykset, joiden luotonsaanti on heikkoa, ovat rahanpesun avainkohteena. Komissio aikoo tarkastella lainsäädännön[108] täytäntöönpanoa ja mahdollista tarvetta antaa uusia yhteisiä sääntöjä muun muassa tuomioon perustumattomasta menetetyksi tuomitsemisesta. Lisäksi varallisuuden takaisin hankinnasta vastaaville toimistoille[109], jotka ovat keskeisiä toimijoita varallisuuden takaisin hankinnassa, voitaisiin antaa paremmat välineet varojen tunnistamiseksi ja jäljittämiseksi nopeammin kaikkialla EU:ssa ja näin tehostaa menetetyksi tuomitsemista.

Järjestäytyneen rikollisuuden ja **korruption** välillä on vahva yhteys. On arvioitu, että pelkästään korruptio maksaa EU:n taloudelle 120 miljardia euroa vuodessa.[110] Korruption ehkäisyä ja torjuntaa seurataan edelleen säännöllisesti oikeusvaltiomekanismin ja eurooppalaisen ohjausjakson puitteissa. Eurooppalaisen ohjausjakson yhteydessä on arvioitu korruption torjuntaan liittyviä haasteita, kuten julkisia hankintoja, julkishallintoa, liiketoimintaympäristöä ja terveydenhuoltoa. Korruption torjuntaa käsitellään myös komission uudessa oikeusvaltiota koskevassa vuosikertomuksessa, jonka avulla voidaan käydä ennaltaehkäisevää vuoropuhelua kansallisten viranomaisten ja asianomaisten sidosryhmien kanssa EU:n ja kansallisella tasolla. Myös kansalaisyhteiskunnan organisaatiot voivat olla keskeisessä asemassa edistettäessä viranomaisten toimintaa järjestäytyneen rikollisuuden ja korruption ehkäisemisessä ja torjunnassa, ja nämä ryhmät voitaisiin koota yhteen yhteiselle foorumille. Koska järjestäytynyt rikollisuus ja korruptio ovat luonteeltaan rajatylittäviä, keskeisenä osa-alueena on myös EU:n naapurialueiden kanssa tehtävä yhteistyö ja avunanto.

Keskeiset toimet
• EU:n terrorismin vastainen ohjelma, mukaan lukien uudet radikalisoitumisen vastaiset toimet EU:ssa • Uusi terrorismin vastainen yhteistyö keskeisten kolmansien maiden ja kansainvälisten organisaatioiden kanssa

[106] EU:n lainsäädännössä edellytetään, että varallisuuden takaisin hankinnasta vastaavia toimistoja on kaikissa jäsenvaltioissa.

[107] Varojen takaisinhankinta ja menetetyksi tuomitseminen: takeet sille, että rikos ei kannata, COM(2020) 217 final.

[108] Direktiivi 2014/42/EU rikoksentekovälineiden ja rikoshyödyn jäädyttämisestä ja menetetyksi tuomitsemisesta Euroopan unionissa.

[109] Neuvoston päätös 2007/845/YOS varallisuuden takaisin hankinnasta vastaavien jäsenvaltioiden toimistojen yhteistyöstä rikoksen tuottaman hyödyn tai muun rikokseen liittyvän omaisuuden jäljittämisessä ja tunnistamisessa.

[110] Korruption taloudellisten kokonaiskustannusten arvioiminen on vaikeaa, vaikkakin Kansainvälisen kauppakamarin, Transparency Internationalin, YK:n Global Compactin ja Maailman talousfoorumin kaltaiset elimet ovat tehneet niistä laskelmia. Niiden tekemien arvioiden mukaan korruption osuus on viisi prosenttia maailmanlaajuisesta BKT:sta.

- Toimintasuunnitelma järjestäytyneen rikollisuuden ja ihmiskaupan torjumiseksi
- EU:n huumeidenvastainen ohjelma ja toimintasuunnitelma 2021–2025
- Euroopan huumausaineiden ja niiden väärinkäytön seurantakeskuksen arviointi
- Ampuma-aseiden laitonta kauppaa koskeva EU:n toimintasuunnitelma vuosiksi 2020–2025
- Varojen jäädyttämistä ja menetetyksi tuomitsemista sekä varallisuuden takaisin hankinnasta vastaavia toimistoja koskevan lainsäädännön tarkistaminen
- Ympäristörikosdirektiivin arviointi
- Siirtolaisten salakuljetuksen vastainen EU:n toimintasuunnitelma (2021–2025)

4. Vahva eurooppalainen turvallisuusekosysteemi

Yhteiskunnan kaikkien osien on pyrittävä yhdessä kohti toimivaa ja todellista turvallisuusunionia. Hallitusten, lainvalvontaviranomaisten, yksityisen sektorin, koulutusalan ja kansalaisten itsensä on oltava sitoutuneita ja valmiita ja yhteydessä toisiinsa, jotta voidaan kehittää kaikkien, erityisesti heikoimmassa asemassa olevien, uhrien ja todistajien, valmiuksia ja selviytymiskykyä.

Turvallisuuden on oltava osa kaikkia politiikkoja, ja EU voi edistää sitä kaikilla tasoilla. Yksi unionin vakavimmista turvallisuusriskeistä on perheväkivalta: EU:ssa 22 prosenttia naisista on kokenut väkivaltaa lähisuhteessaan.[111] EU:n liittyminen naisiin kohdistuvan väkivallan ja perheväkivallan ehkäisemisestä ja torjumisesta tehtyyn Istanbulin yleissopimukseen on edelleen yksi ensisijaisista tavoitteista. Jos neuvottelut eivät etene, komissio aikoo toteuttaa muita toimenpiteitä sopimuksen tavoitteiden saavuttamiseksi, kuten ehdottaa, että naisiin kohdistuva väkivalta lisätään luetteloon EU:n perussopimuksessa määritellyistä rikoksista.

Yhteistyö ja tietojen vaihto

Yksi tärkeimmistä toimista, joita EU voi toteuttaa kansalaisten suojelemiseksi, on edistää turvallisuudesta vastaavien yhteistyötä. Yhteistyö ja tietojen vaihto ovat tehokkaimpia välineitä rikollisuuden ja terrorismin torjunnassa ja oikeuden tavoittelussa. Jotta ne olisivat tuloksellisia, ne on kohdennettava ja ajoitettava oikein, ja jotta niihin voidaan luottaa, niihin on sovellettava yhteisiä suojatoimia ja valvontaa.

Jäsenvaltioiden välisen **operatiivisen lainvalvontayhteistyön** kehittämiseksi on otettu käyttöön useita EU:n välineitä ja alakohtaisia strategioita[112]. Yksi tärkeimmistä EU:n välineistä jäsenvaltioiden välisen lainvalvontayhteistyön tukemiseksi on Schengenin tietojärjestelmä, jolla vaihdetaan reaaliaikaisesti tietoja etsityistä ja kadonneista henkilöistä ja esineistä. Sen ansiosta on voitu pidättää rikollisia, takavarikoida huumeita ja pelastaa mahdollisia uhreja.[113] Yhteistyön tasoa voitaisiin kuitenkin vielä parantaa yhdenmukaistamalla ja parantamalla käytettävissä olevia välineitä. Suurin osa operatiivisen lainvalvontayhteistyön taustalla olevasta EU:n oikeudellisesta kehyksestä laadittiin 30 vuotta sitten. Jäsenvaltioiden kahdenvälisten sopimusten, joista monet ovat vanhentuneita tai vähän käytettyjä, monitahoinen vyyhti uhkaa purkautua. Pienemmissä maissa tai sisämaavaltioissa rajojen yli toimivien lainvalvontaviranomaisten on toteutettava

[111] Tasa-arvon unioni: sukupuolten tasa-arvostrategia 2020–2025, COM(2020) 152.

[112] Esimerkiksi EU:n merellisen turvallisuuden strategian toimintasuunnitelma, jonka ansiosta saavutettiin merkittävää edistystä rannikkovartiostojen tehtävien alan yhteistyössä asianomaisten EU:n virastojen välillä.

[113] Järjestäytyneen rikollisuuden torjunta EU:ssa vuonna 2019 (neuvosto, 2020).

operatiivisia toimia noudattaen jopa seitsemää eri sääntökokonaisuutta: tästä seuraa, että joitakin operaatioita, kuten epäiltyjen takaa-ajoja sisärajojen yli, ei yksinkertaisesti toteuteta. EU:n nykyinen kehys ei myöskään kata uusia teknologioita, kuten drooneja, koskevaa operatiivista yhteistyötä.

Operatiivista tehokkuutta voidaan tukea erityisellä lainvalvontayhteistyöllä. Sen avulla voidaan tukea myös muita poliittisia tavoitteita, kuten tuoda turvallisuusnäkökulma mukaan ulkomaisten suorien sijoitusten uuteen arviointiin. Komissio aikoo tarkastella, miten tätä voitaisiin tukea poliisiyhteistyösäännöstöllä. Jäsenvaltioiden lainvalvontaviranomaiset ovat hyödyntäneet EU:n tason tukea ja asiantuntemusta enenevässä määrin. EU:n tiedusteluanalyysikeskus on puolestaan ollut keskeisessä asemassa edistämässä strategisten tiedustelutietojen vaihtoa jäsenvaltioiden tiedustelu- ja turvallisuuspalvelujen välillä ja toimittanut tiedusteluun perustuvia tilannetietoja EU:n toimielimille.[114] **Europolilla** voi myös olla keskeinen rooli laajennettaessa yhteistyötä kolmansien maiden kanssa rikollisuuden ja terrorismin torjumiseksi johdonmukaisesti EU:n muiden ulkoisten politiikkojen ja välineiden kanssa. Europolin toimintaa kuitenkin rajoittavat nykyisin useat tekijät etenkin siltä osin, joka koskee henkilötietojen suoraa vaihtoa yksityisten osapuolten kanssa. Rajoitusten vuoksi se ei voi tukea tehokkaasti jäsenvaltioita terrorismin ja rikollisuuden torjunnassa. Europolin toimeksiantoa arvioidaan parhaillaan tarkoituksena parantaa sitä ja varmistaa, että virasto voi hoitaa tehtävänsä täysimääräisesti. Asiaan liittyvien EU:n tason viranomaisten (kuten OLAFin, Europolin, Eurojustin ja Euroopan syyttäjänviraston) olisi myös tehtävä tiiviimpää yhteistyötä ja parannettava tiedonvaihtoa.

Tämän lisäksi olisi kehitettävä myös **Eurojustia**, niin että voidaan maksimoida lainvalvontayhteistyön ja oikeudellisen yhteistyön väliset synergiaedut. EU hyötyisi myös strategisemmasta johdonmukaisuudesta: **EMPACT**[115] on järjestäytynyttä ja vakavaa kansainvälistä rikollisuutta koskeva EU:n toimintapoliittinen sykli. Se tarjoaa viranomaisille rikostiedusteluun perustuvan menetelmän, jolla ne voivat yhdessä käsitellä vakavimpia rikollisuuden EU:lle aiheuttamia uhkia. Se on tuottanut merkittäviä operatiivisia tuloksia[116] viimeksi kuluneella vuosikymmenellä. Alan toimijoiden kokemusten perusteella nykyistä mekanismia olisi tehostettava ja yksinkertaistettava, jotta kiireellisimpiin ja muuttuviin rikosuhkiin voidaan puuttua paremmin uudessa toimintapoliittisessa syklissä 2022–2025.

Oikea-aikaiset ja merkitykselliset **tiedot** ovat ratkaisevan tärkeitä päivittäisessä rikostenselvitystyössä. Vaikka turvallisuutta ja rajaturvallisuutta varten on kehitetty uusia EU:n tason tietokantoja, tietoa on edelleen paljon kansallisissa tietokannoissa tai sitä vaihdetaan EU:n välineiden ulkopuolella. Tämä lisää merkittävästi työmäärää, viiveitä ja riskiä siitä, että keskeisiä tietoja jää huomaamatta. Parempiin tuloksiin päästäisiin paremmilla, nopeammilla ja yksinkertaisemmilla prosesseilla, joihin koko turvallisuusyhteisö osallistuu. Oikeat välineet ovat välttämättömiä, jotta tietojenvaihdon mahdollisuuksia voidaan hyödyntää rikosten tehokkaassa selvittämisessä, ottaen huomioon tarvittavat suojatoimet niin, että tietojenvaihdossa noudatetaan tietosuojalainsäädäntöä ja perusoikeuksia. EU voisi teknologian, rikosteknisen tutkimuksen ja tietosuojan kehityksen sekä muuttuneiden operatiivisten tarpeiden vuoksi tarkastella tarvetta nykyaikaistaa välineitä, kuten **vuoden 2008 Prüm-päätöksiä**. Päätöksillä otettiin käyttöön DNA-tunnisteiden, sormenjälkitietojen ja ajoneuvorekisteritietojen automaattinen vaihto, jotta

[114] EU:n tiedusteluanalyysikeskus on ainoa kanava, jonka kautta jäsenvaltioiden tiedustelu- ja turvallisuuspalvelut voivat toimittaa tiedusteluun perustuvia tilannetietoja EU:lle.

[115] EMPACT-lyhenne tulee sanoista European Multidisciplinary Platform Against Criminal Threats (Euroopan monialainen rikosuhkien torjuntafoorumi).

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

jäsenvaltioiden rikos- tai muissa tietokannoissa jo saatavilla olevia tietoluokkia voidaan vaihtaa automaattisesti rikostutkintaa varten. Lisäksi komissio tarkastelee mahdollisuutta vaihtaa rikosrekisteritietoja sen selvittämiseksi, onko henkilöstä merkintää jonkin toisen jäsenvaltion rikosrekisterissä, ja helpottaa näiden rekisteritietojen saatavuutta ottaen huomioon tarvittavat suojatoimet.

Matkustajia koskevat tiedot ovat auttaneet parantamaan rajatarkastuksia, vähentämään laitonta muuttoliikettä ja tunnistamaan turvallisuusriskin aiheuttavia henkilöitä. Ennalta annettavat matkustajatiedot ovat matkustajien henkilötietoja, joita lentoliikenteen harjoittajat keräävät lähtöselvityksen aikana ja lähettävät etukäteen rajavalvontaviranomaisille määränpäässä. Oikeudellisen kehyksen[117] tarkistaminen mahdollistaisi tietojen tehokkaamman käytön samalla kun varmistettaisiin tietosuojalainsäädännön noudattaminen ja helpotettaisiin matkustajavirtojen kulkua. Matkustajarekisteritiedot (PNR) ovat tietoja, joita matkustajat antavat lentoja varatessaan. PNR-direktiivin[118] täytäntöönpano on avainasemassa, ja komissio aikoo jatkossakin tukea ja valvoa sitä. Lisäksi komissio aloittaa **matkustajarekisteritietojen siirtoa kolmansiin maihin** koskevan nykyisen lähestymistavan väliarvioinnin.

Oikeudellista yhteistyötä tarvitaan täydentämään poliisin toimia rajatylittävän rikollisuuden torjumiseksi. Oikeudellinen yhteistyö on muuttunut perusteellisesti 20 viime vuoden aikana. **Euroopan syyttäjänviraston** ja **Eurojustin** kaltaisilla elimillä on oltava täydet toimintamahdollisuudet tai niitä on vahvistettava. Oikeusalan toimijoiden välistä yhteistyötä voitaisiin myös tehostaa oikeudellisten päätösten vastavuoroiseen tunnustamiseen, oikeusalan koulutukseen ja tietojenvaihtoon liittyvillä lisätoimilla. Tavoitteena olisi oltava tuomareiden ja syyttäjien keskinäisen luottamuksen lisääminen, sillä se olisi keskeistä rajatylittävien menettelyjen sujuvuuden kannalta. Oikeusjärjestelmien tehokkuutta voidaan parantaa myös **digitaaliteknologian** avulla. Parhaillaan ollaan perustamassa uutta digitaalista tietojenvaihtojärjestelmää eurooppalaisten tutkintamääräysten, keskinäistä oikeusapua koskevien pyyntöjen ja asiaan liittyvän viestinnän välittämiseksi jäsenvaltioiden välillä Eurojustin tuella. Komissio tekee yhteistyötä jäsenvaltioiden kanssa nopeuttaakseen tarvittavien tietotekniikkajärjestelmien käyttöönottoa kansallisella tasolla.

Myös kansainvälinen yhteistyö on keskeistä tehokkaan lainvalvontayhteistyön ja oikeudellisen yhteistyön kannalta. Keskeisten kumppanien kanssa tehtävillä kahdenvälisillä sopimuksilla on keskeinen rooli EU:n ulkopuolelta saapuvien tietojen ja todisteiden suojaamisessa. **Interpolilla**, joka on yksi suurimmista kansainvälisistä rikospoliisijärjestöistä, on tärkeä rooli. Komissio tarkastelee mahdollisia tapoja vahvistaa yhteistyötä sen kanssa. Tarkastelun kohteina ovat muun muassa pääsy Interpolin tietokantoihin ja operatiivisen ja strategisen yhteistyön vahvistaminen. EU:n lainvalvontaviranomaiset luottavat myös siihen, että keskeiset kumppanimaat havaitsevat ja tutkivat rikollisia ja terroristeja. **EU:n ja kolmansien maiden välisiä turvallisuusalan kumppanuuksia** voitaisiin tehostaa, jotta voitaisiin lisätä yhteistyötä yhteisten uhkien, kuten terrorismin, järjestäytyneen rikollisuuden, kyberrikollisuuden, lasten seksuaalisen hyväksikäytön ja ihmiskaupan, torjumiseksi. Tällainen lähestymistapa perustuisi yhteisiin turvallisuusetuihin, vakiintuneeseen yhteistyöhön ja turvallisuusalan vuoropuheluihin.

[117] Neuvoston direktiivi 2004/82/EY liikenteenharjoittajien velvollisuudesta toimittaa tietoja matkustajista.

[118] Direktiivi (EU) 2016/681 matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten.

Tietojenvaihdon lisäksi asiantuntemuksen vaihto voi olla erityisen hyödyllistä lainvalvontaviranomaisten valmiuden parantamiseksi **muita kuin perinteisiä uhkia** vastaan. Sen lisäksi, että komissio kannustaa parhaiden käytäntöjen vaihtoon, se tarkastelee **EU:n tason koordinointimekanismin perustamista poliisivoimille** ylivoimaisten esteiden, kuten pandemioiden, varalle. Pandemia on myös osoittanut, että poliisitoiminta digitaalisessa yhteisössä yhdessä verkkopoliisitoimintaa helpottavien oikeudellisten kehysten kanssa on olennaisen tärkeää rikollisuuden ja terrorismin torjunnassa. Poliisin ja yhteisöjen väliset kumppanuudet verkossa ja sen ulkopuolella voivat ehkäistä rikollisuutta ja lieventää järjestäytyneen rikollisuuden, radikalisoitumisen ja terroritoiminnan vaikutuksia. Yhteys paikallisten, alueellisten, kansallisten ja EU:n poliisitoimien välillä on keskeinen menestystekijä koko EU:n turvallisuusunionin kannalta.

Vahvojen ulkorajojen merkitys

Ulkorajojen nykyaikainen ja tehokas valvonta auttaa sekä Schengenin yhtenäisyyden säilyttämisessä että kansalaisten turvallisuuden takaamisessa. Se että kaikki asiaankuuluvat toimijat saadaan mukaan edistämään mahdollisimman tehokkaasti rajaturvallisuutta, voi todella auttaa rajatylittävän rikollisuuden ja terrorismin ehkäisemisessä. Äskettäin vahvistetun eurooppalaisen raja- ja merivartioston[119] yhteisillä operatiivisilla toimilla edistetään rajatylittävän rikollisuuden ehkäisemistä ja havaitsemista **ulkorajoilla** ja EU:n ulkopuolella. Tullitoimet, joilla havaitaan tavaroiden turvallisuusriskit ennen niiden saapumista unioniin ja valvotaan tavaroita niiden saapuessa, ovat olennaisen tärkeitä rajatylittävän rikollisuuden ja terrorismin torjunnassa. Tulevalla tulliliittoa koskevalla toimintasuunnitelmalla otettaan käyttöön toimia, joilla vahvistetaan riskinhallintaa ja parannetaan sisäistä turvallisuutta, mukaan lukien etenkin arvioimalla asiaankuuluvien tietojärjestelmien välisen yhteyden toteutettavuutta turvallisuusriskianalyysiä varten.

Toukokuussa 2019 hyväksyttiin kehys **EU:n tietojärjestelmien yhteentoimivuudelle** oikeus- ja sisäasioiden alalla. Uudella rakenteella pyritään parantamaan uusien tai parannettujen tietojärjestelmien tehokkuutta ja vaikuttavuutta.[120] Sen avulla lainvalvontaviranomaisia, rajavartijoita ja maahanmuuttoviranomaisia voidaan tiedottaa entistä nopeammin ja järjestelmällisemmin. Lisäksi se helpottaa henkilöiden asianmukaista tunnistamista ja henkilöllisyyspetosten torjumista. Tämän mahdollistamiseksi yhteentoimivuuden toteuttaminen sekä poliittisella että teknisellä tasolla olisi otettava ensisijaiseksi tavoitteeksi. EU:n virastojen ja kaikkien jäsenvaltioiden tiivis yhteistyö on ensiarvoisen tärkeää, jotta täysi yhteentoimivuus saavutetaan vuoteen 2023 mennessä.

Matkustusasiakirjoihin liittyviä petoksia pidetään yhtenä yleisimmistä rikoksista. Ne helpottavat rikollisten ja terroristien laitonta liikkumista, ja niillä on keskeinen rooli ihmiskaupassa ja huumekaupassa.[121] Komissio tutkii, miten EU:n oleskelu- ja matkustusasiakirjojen turvavaatimuksia koskevaa nykyistä työtä voitaisiin laajentaa muun muassa digitalisaatiota hyödyntäen. Jäsenvaltiot alkavat myöntää elokuusta 2021 alkaen yhdenmukaiset turvavaatimukset täyttäviä henkilökortteja ja oleskelulupia. Asiakirjoissa on oltava muun muassa biometrisiä tunnisteita sisältävä siru, jonka kaikki EU:n

[119] Eurooppalainen raja- ja merivartiosto koostuu Euroopan raja- ja merivartiovirastosta (Frontex) sekä jäsenvaltioiden rajavalvontaviranomaisista ja rannikkovartioviranomaisista.

[120] Rajanylitystietojärjestelmä (EES), EU:n matkustustieto- ja -lupajärjestelmä (ETIAS), laajennettu eurooppalainen rikosrekisteritietojärjestelmä (ECRIS-TCN), Schengenin tietojärjestelmä, viisumitietojärjestelmä ja tuleva päivitetty Eurodac.

[121] Asiakirjaväärennösten ja ihmiskaupan välistä yhteyttä käsitellään asiakirjassa ”Toinen kertomus edistymisestä ihmiskaupan torjunnassa” (COM (2018) 777) ja siihen liittyvässä asiakirjassa SWD (2018) 473 sekä Europolin tilannekatsauksessa ”Trafficking in human beings in the EU” (2016).

rajaviranomaiset voivat tarkistaa. Komissio seuraa näiden uusien sääntöjen täytäntöönpanoa, mukaan lukien tällä hetkellä käytössä olevien asiakirjojen asteittaista korvaamista.

Turvallisuutta koskevan tutkimuksen ja innovoinnin vahvistaminen

Työ kyberturvallisuuden varmistamiseksi ja järjestäytyneen rikollisuuden, kyberrikollisuuden ja terrorismin torjumiseksi perustuu vahvasti välineiden kehittämiseen tulevaisuutta varten. Tavoitteena on laatia turvallisempaa ja suojatumpaa uutta teknologiaa ja vastata teknologian mukanaan tuomiin haasteisiin sekä tukea lainvalvontatyötä yksityisten kumppaneiden ja eri toimialojen tuella.

Innovointi olisi nähtävä strategisena välineenä, jolla voidaan torjua nykyisiä uhkia ja ennakoida sekä tulevia riskejä että mahdollisuuksia. Innovatiiviset teknologiat voivat tarjota uusia välineitä lainvalvonnan ja muiden turvallisuusalan toimijoiden tueksi. Tekoälyssä ja massadata-analyysissä voitaisiin hyödyntää suurteholaskentaa ja siten tehostaa havaitsemista ja tuottaa nopeita, kattavia analyysejä.[122] Luotettavan teknologian kehittämisen keskeisenä edellytyksenä ovat korkealaatuiset data-aineistot, joiden avulla toimivaltaiset viranomaiset voivat kouluttaa, testata ja validoida algoritmeja.[123] Yleisesti ottaen teknologiariippuvuuden riski on tällä hetkellä suuri: EU on esimerkiksi kyberturvallisuustuotteiden ja -palvelujen nettotuoja, millä on vaikutuksia talouteen ja kriittisiin infrastruktuureihin. Euroopan on oltava mukana asianomaisten arvoketjujen kriittisissä osissa ja sillä on oltavat tarvittavat valmiudet, jotta teknologiaa voidaan hallita ja tarjonnan jatkuvuus taata myös epäsuotuisien tapahtumien ja kriisien yhteydessä.

EU:n **tutkimus, innovointi ja teknologian kehittäminen** mahdollistavat sen, että turvallisuusulottuvuus otetaan huomioon näitä teknologioita ja niiden soveltamista kehitettäessä. Seuraavan sukupolven EU-rahoitusehdotukset voivat toimia merkittävänä kannustimena.[124] Eurooppalaisia data-avaruuksia ja pilvi-infrastruktuureja koskevissa aloitteissa turvallisuus on otettu alusta alkaen huomioon. Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus ja kansallisten koordinointikeskusten verkosto aikovat luoda tehokkaan ja toimivan rakenteen, joka kokoaa ja jakaa kyberturvallisuusalan tutkimusvalmiuksia ja tuloksia.[125] EU:n avaruusohjelma puolestaan tuottaa palveluja, joilla tuetaan EU:n, sen jäsenvaltioiden ja yksittäisten henkilöiden turvallisuutta.[126]

EU:n rahoittama turvallisuustutkimus on keskeinen väline turvallisuusratkaisuja tukevan teknologian ja tietämyksen edistämisessä: vuodesta 2007 lähtien on käynnistetty yli 600 alan hanketta, joiden kokonaisarvo on lähes kolme miljardia euroa. Komissio tarkastelee osana Europolin toimeksiannon arviointia **eurooppalaisen sisäisen turvallisuuden innovaatiokeskuksen**[127] perustamista. Keskuksen tarkoituksena olisi laatia sellaisia yhteisiä

[122] Tässä olisi hyödynnettävä komission tekoälyästrategiaa.

[123] Euroopan datastrategia, COM(2020) 66 final.

[124] Horisontti Eurooppa -puiteohjelmaa, sisäisen turvallisuuden rahastoa, yhdennetyn rajaturvallisuuden rahastoa, InvestEU-ohjelmaa, Euroopan aluekehitysrahastoa ja Digitaalinen Eurooppa -ohjelmaa koskevilla komission ehdotuksilla tuetaan innovatiivisten turvallisuusteknologioiden ja -ratkaisujen kehittämistä ja käyttöönottoa turvallisuusalan arvoketjussa.

[125] Komission 12 päivänä syyskuuta 2018 antama ehdotus Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta, COM(2018) 630.

[126] Esimerkiksi Copernicus-ohjelman tuottamien palveluiden avulla voidaan valvoa EU:n ulkorajoja ja merialueita ja siten torjua merirosvousta ja salakuljetusta ja tukea elintärkeitä infrastruktuureja. Ohjelma tulee olemaan keskeinen tekijä siviili- ja sotilasoperaatioissa, kun se on saatu kaikilta osin toimintaan.

[127] Keskus toimisi myös Frontexin, CEPOLin, eu-LISAn ja yhteisen tutkimuskeskuksen kanssa.

ratkaisuja yhteisiin turvallisuushaasteisiin ja -mahdollisuuksiin, joita jäsenvaltiot eivät ehkä pysty hyödyntämään yksin. Yhteistyö on olennaisen tärkeää, jotta investoinnit voidaan kohdentaa mahdollisimman tehokkaasti ja voidaan kehittää innovatiivisia teknologioita, joista on hyötyä sekä turvallisuuden että talouden kannalta.

Taitojen kehittäminen ja tietoisuuden lisääminen

Tietoisuus turvallisuuskysymyksistä ja taitojen hankkiminen mahdollisten uhkien käsittelemiseksi ovat olennaisen tärkeitä, jotta voidaan parantaa yhteiskunnan selviytymiskykyä ja lisätä yritysten, viranomaisten ja yksilöiden valmiuksia. Tietotekniseen infrastruktuuriin ja sähköisiin järjestelmiin liittyvät haasteet ovat osoittaneet, että kyberturvallisuuteen liittyviä valmiuksia ja toimia koskevaa osaamista on kehitettävä. Pandemia toi myös esiin digitalisoinnin merkityksen kaikilla EU:n talouden ja yhteiskunnan aloilla.

Jopa **perustietämyksellä turvallisuusuhkista** ja niiden torjunnasta voi olla todellista vaikutusta yhteiskunnan selviytymiskyvyn kannalta. Tietoisuus kyberrikollisuuden riskeistä ja tarpeesta suojautua niiltä voivat yhdessä palveluntarjoajien tarjoaman suojan kanssa auttaa torjumaan kyberhyökkäyksiä. Huumekaupan vaaroista ja riskeistä tiedottaminen voi vaikeuttaa rikollisten menestymistä. EU voi edistää parhaiden käytäntöjen levittämistä esimerkiksi Safer Internet -keskusten verkoston[128] kautta ja varmistaa, että tällaiset tavoitteet otetaan huomioon sen omissa ohjelmissa.

Tulevaan digitaalisen koulutuksen toimintasuunnitelmaan olisi sisällytettävä kohdennettuja toimenpiteitä, joilla kehitetään koko väestön tietoteknisiä turvallisuustaitoja. Äskettäin hyväksytyllä osaamisohjelmalla[129] tuetaan osaamisen kehittämistä läpi elämän. Se sisältää toimia, joilla pyritään lisäämään kyberturvallisuuden kaltaisilla kehityksen kärjessä olevilla aloilla tarvittavien luonnontieteiden, teknologian, insinööritieteiden, taiteen ja matematiikan alan loppututkinnon suorittaneiden määrää. Digitaalinen Eurooppa -ohjelmasta rahoitetuilla muilla toimilla tuetaan sitä, että turvallisuusalan ammattilaiset pysyvät ajan tasalla turvallisuustilanteen muutoksista. Samalla paikataan EU:hun työmarkkinoilla esiintyviä puutteita. Näiden toimien ansiosta ihmiset voivat hankkia taitoja turvallisuusuhkien käsittelemiseksi ja yritykset saada tarvitsemiaan alan ammattilaisia. Luonnontieteiden, teknologian, insinööritieteiden, taiteen ja matematiikan alan työmahdollisuuksia edistetään myös tulevilla eurooppalaisella tutkimusalueella ja eurooppalaisella koulutusalueella.

On myös tärkeää, että **uhrit** voivat käyttää oikeuksiaan. Heidän on saatava tilanteensa edellyttämää apua ja tukea. Erityistä huomiota on kiinnitettävä vähemmistöihin ja haavoittuvimmassa asemassa oleviin uhreihin, kuten seksuaalista hyväksikäyttöä varten käytävän ihmiskaupan uhreiksi joutuneisiin tai perheväkivallalle altistuviin naisiin ja lapsiin.[130]

Lainvalvontaviranomaisten taitojen parantaminen on erityisen tärkeää. Nykyiset ja uudet teknologiset uhat edellyttävät lisäinvestointeja lainvalvontaviranomaisten taitojen parantamiseen mahdollisimman varhaisessa vaiheessa ja koko heidän uransa ajan. CEPOL on keskeinen kumppani, joka auttaa jäsenvaltioita tässä tehtävässä. Rasismiin ja

[128] Ks. www.betterinternetforkids.eu: keskusportaalia ja kansallisia Safer Internet -keskuksia rahoitetaan tällä hetkellä Verkkojen Eurooppa -välineen televiestintäohjelmasta, ja tulevaa rahoitusta on ehdotettu Digitaalinen Eurooppa -ohjelmasta.

[129] Euroopan osaamisohjelma kestävän kilpailukyvyn, sosiaalisen oikeudenmukaisuuden ja mukautumisvalmiuksien edistämiseksi, COM(2020) 274 final.

[130] Ks. sukupuolten tasa-arvostrategia, COM(2020) 152; uhrien oikeuksia koskeva strategia, COM(2020) 258; ja eurooppalainen strategia internetin parantamiseksi lasten näkökulmasta, COM(2012) 196.

muukalaisvihaan sekä yleisemmin kansalaisten oikeuksiin liittyvän lainvalvontakoulutuksen on oltava olennainen osa EU:n turvallisuuskulttuuria. Myös kansallisilla oikeusjärjestelmillä ja oikeusalan toimijoilla on oltava valmiudet sopeutua ja vastata ennennäkemättömiin haasteisiin. Yhteistyövälineiden tuloksellisuus perustuu siihen, että jäsenvaltioiden lainvalvontaviranomaiset osaavat käyttää niitä. Lisäksi olisi kaikin tavoin pyrittävä edistämään sukupuolten tasa-arvon valtavirtaistamista ja naisten osallistumista lainvalvontatyöhön.

Keskeiset toimet
• Europolin toimeksiannon vahvistaminen • EU:n poliisiyhteistyösäännöstön ja poliisitoiminnan kriisiajan koordinoinnin tarkastelu • Eurojustin vahvistaminen oikeus- ja lainvalvontaviranomaisten välisen yhteyden muodostamiseksi • Matkustajien ennakkotietoja koskevan direktiivin tarkistaminen • Tiedonanto matkustajarekisteritietojen ulkoisesta ulottuvuudesta • EU:n ja Interpolin välisen yhteistyön vahvistaminen • Kehys keskeisten kolmansien maiden kanssa käytäville neuvotteluille tietojen jakamisesta • Matkustusasiakirjojen turvavaatimusten parantaminen • Eurooppalaisen sisäisen turvallisuuden innovaatiokeskuksen tarkastelu

V. Päätelmät

Euroopan unionia pidetään edelleen yleisesti yhtenä turvallisimmista paikoista maailmassa, joka käy yhä epävakaammaksi. Unionin turvallisuutta ei kuitenkaan voida pitää itsestäänselvyytenä.

Uudessa turvallisuusunionistrategiassa luodaan perusta koko eurooppalaisen yhteiskunnan kattavalle turvallisuusekosysteemille. Turvallisuus on yhteisesti kaikkien vastuulla. Se on asia, joka koskee kaikkia. Kaikkien hallintoelinten, yritysten, yhteiskunnallisten organisaatioiden, laitosten ja kansalaisten on täytettävä velvollisuutensa yhteiskunnan turvallisuuden parantamiseksi.

Turvallisuuskysymyksiä on nyt tarkasteltava entistä paljon laajemmasta näkökulmasta, ja fyysisen ja digitaalisen turvallisuuden virheellisestä erottelusta on luovuttava. EU:n turvallisuusunionistrategiassa kootaan yhteen kaikki turvallisuustarpeet ja keskitytään tulevina vuosina EU:n turvallisuuden kannalta kriittisimpiin aloihin. Siinä myös otetaan huomioon, että turvallisuusuhat eivät noudata maantieteellisiä rajoja, ja tuodaan esiin sisäisen ja ulkoisen turvallisuuden yhä kiinteämpi yhteys.[131] EU:n on tärkeää tehdä yhteistyötä kansainvälisten kumppaneiden kanssa, jotta se voi suojella EU:n kansalaisia ja koordinoida tämän strategian täytäntöönpanoa tiiviisti EU:n ulkoisen toiminnan kanssa.

Turvallisuus kytkeytyy perusarvoihimme. Kaikki tässä strategiassa ehdotetut toimet ja aloitteet ovat täysin perusoikeuksien ja eurooppalaisten arvojen mukaisia. Nämä ovat eurooppalaisen elämäntavan perusta, ja niiden on pysyttävä kaiken työmme ytimessä.

Komissio tiedostaa täysin, että pelkkä politiikka tai toimi ei riitä. Tarvitaan myös sen täytäntöönpanoa. Sen vuoksi nykyisen ja tulevan lainsäädännön asianmukaista täytäntöönpanoa ja sen valvontaa on painotettava tinkimättä. Tätä seurataan säännöllisten

[131] Ks. EU:n globaalistrategia

turvallisuusunionia koskevien kertomusten avulla, ja komissio pitää Euroopan parlamentin, neuvoston ja sidosryhmät ajan tasalla ja mukana kaikissa asiaankuuluvissa toimissa. Komissio on valmis osallistumaan turvallisuusunionistrategiasta käytäviin yhteisiin keskusteluihin ja järjestämään niitä toimielinten kanssa arvioidakseen yhdessä saavutettua edistystä ja tarkastellakseen tulevia haasteita.

Komissio pyytää Euroopan parlamenttia ja neuvostoa hyväksymään turvallisuusunionistrategian turvallisuutta koskevan yhteistyön ja yhteisen toiminnan perustaksi seuraaviksi viideksi vuodeksi.