

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Keskusrikospoliisin lausunto

Keskusrikospoliisi näkee tärkeänä uuden Suomen kyberturvallisuusstrategian 2024–2035 ja kiittää mahdollisuudesta lausua. Suomen kyberturvallisuusstrategia on ajankohtainen ja laadukas, siinä on huomioitu laajasti yhteiskunnan elintärkeät toiminnot ja suojaamistarpeet.

Keskusrikospoliisi lausuu pyynnössä esitetyn mukaisesti seuraavaa;

Poliisin toimivalta ja ajantasainen tilannetietous

Poliisi on sisäisen turvallisuuden toimivaltainen viranomaisen normaalioloissa. Poliisin päätöksenteon ja johtamisen tulee perustua tietoon, joten uhkatilanteissa poliisilla tulee olla ajantasaisen tiedon lisäksi kyvykkyys ja toimivaltuus toimia, sekä mahdollisuus antaa tilanteen kannalta olennaista tietoa toiselle viranomaiselle tai hallinnolliselle toimijalle.

Keskusrikospoliisi näkee, että viranomaisille on turvattava riittävät kyvykkyudet rikosvahinkojen estämiseksi. Keskeistä on viranomaisten sujuva tiedonvaihto ja päivittyvä yhteinen tilannekuva oikea-aikaisen päätöksenteon ja tiedolla johtamisen tukena. Toimintaympäristön muutoksen ja uhkien monimuotoistumisen myötä, viranomaisten yhteistyö myös menetelmien ja kyvykkyyksien tehokkaan yhteiskäytön osalta, on merkittävässä ja jatkuvasti kasvavassa roolissa.

Keskusrikospoliisin näkökulmasta strategiassa tulisi nykyistä selkeämmin kiinnittää huomiota sisäisen ja ulkoisen turvallisuuden viranomaisten toimivaltuuksiin ja tehtävien jakoon poikkeusolojen ulkopuolella. Kuten parhaillaan vireillä olevan rikostiedustelulainsäädäntöuudistuksen valmisteluvaiheessa on juridisten asiantuntijoiden näkökulmasta todettu, nämä vastuujaot ovat

perinteisesti olleet selkeät ja toimivat. Saman periaatteen tulisi heijastua myös strategia-asiakirjassa, niin liittyen viranomaisyhteistyöhön, toimivaltuuksiin kuin myös tiedonvaihtoon.

Turvallisuusympäristön muutos ja toimivalta

Verkottuneessa yhteiskunnassa kyberympäristön osuus ja näin ollen mahdollinen hyökkäyspinta-ala kasvaa eksponentiaalisesti. Kybertoimintaympäristön tapahtumat voivat olla monikerroksisia kokonaisuuksia, jotka voivat samaan aikaan täyttää rikoksen tunnusmerkistön ja olla riski kansalliselle turvallisuudelle. Moniulotteisuus haastaa toiminnan tunnistamista, resurssien kohdentamista ja vaikeuttaa vastatoimia. On myös syytä huomioida toimintaympäristön monimutkaistuesssa yksittäiset rikosilmiöt ja niiden monimutkaisuus, joka edellyttää tehokkaampaa ja tiiviimpää yhteistyötä yhteiskunnan eri toimijoiden välillä.

Keskusrikospoliisi pitää tärkeänä, että yhteiskunnan toimintaan laaja-alaisesti vaikuttava tietoverkkorikollisuuden merkittävä kasvu huomioidaan monipuolisesti. Kyberrikollisuuden määrä on kasvanut merkittävästi. Tietoverkot mahdollistavat laajamittaisen rikollisuuden perusrikostenkin tekemiseen ja siten aiheuttavat haittaa paitsi rikosten uhreille myös palveluiden käytettävyydelle ja kehittämiselle. Perusrikollisuudella ilman valtiollista kytkentääkin on merkittävä vaikutus koko yhteiskuntaan.

Esitutkinta- ja lainvalvontaviranomaisten roolia lainsäädännön ja tiedonvaihdon näkökulmasta käsitellään Keskusrikospoliisin näkemyksen mukaan strategia-asiakirjassa yleisellä tasolla asianmukaisesti. On kuitenkin syytä ottaa huomioon – erityisesti strategia-asiakirjan ennakoivuutta silmälläpitäen, että parhaillaan vireillä olevan rikostiedustelulainsäädännön uudistaminen jää asiakirjan käsittelyssä puutteelliseksi. Siten Keskusrikospoliisin näkökulmasta olisi tarpeellista huomioida tämä kehityslinja selkeällä viittauksella myös strategia-asiakirjassa, sillä rikostiedustelulainsäädäntöuudistuksen siirryttyä toimeenpanovaiheeseen on Suomen viranomaiskentässä myös juridisesta näkökulmasta viranomaisia, jotka tekevät rikostiedustelua osana lakisäätteisiä tehtäviään.

Digitalisaation ja teknologisen kehityksen vaikutukset ulottuvat myös vakavaan ja järjestäytyneeseen rikollisuuteen, jota käytetään ajoittain myös valtiollisten intressien ajamiseksi. Valtiollinen vaikuttaminen voidaan nähdä myös osana järjestäytyntä ja vakavaa rikollisuutta. On kuitenkin huomioitava, ettei kaikki kyberrikollisuus pidä sisällään valtiollista tai välillisesti valtiollista vaikuttamista. Kyberrikollisuus itsessään on usein vaikutuksiltaan vakavaa, huolimatta rikollisen toiminnan luonteesta.

Keskusrikospoliisi toteaa, että nuorten tekemä kyberrikollisuus tulee ottaa vakavasti sekä nuoren että yhteiskunnallisten vaikutusten kannalta. Kyberrikoksiin syyllistyvät ensikertalaiset ovat usein hyvin nuoria, kyberrikoksissa käytettäviä työkaluja ja ohjeita on helposti kaikkien saatavilla verkossa,

eikä kyberrikoksen tekemiseen vaadita mittavaa teknistä osaamista. Nuoret eivät myöskään välttämättä ymmärrä tekojensa vakavuutta, ja saattavat kiusantekomielessä syyllistyä kyberrikoksiin, joista aiheutuu vakavaa vahinkoa yhteiskunnalle. Nuoria voidaan myös käyttää välineenä järjestäytyneen tai valtiollisen rikollisuuden toiminnassa.

Valtiollisen tason toiminta täyttää usein myös jonkin Rikoslaisissa määritellyn rikoksen tunnusmerkistön. Esitutkintatoimenpiteillä meneillä olevaan rikokseen voidaan vaikuttaa asianmukaisin vastatoimin hyödyntämällä poliisille annettuja esitutkintaan kuuluvia toimivaltuuksia. Asian käsittely esitutkinnassa on merkityksellistä erityisesti attribuution ja toiminnan aiheuttaman vaaran ja vakavuuden arvioimiseksi. Lisäksi tulee muistaa, että poliisilla on esitutkintavelvollisuus, joka velvoittaa selvittämään asiaa ja tekemään asian osalta siihen liittyviä toimenpiteitä. Siltä osin onkin pohdittava, olisiko turvallisuusviranomaisilla mahdollisuutta tehdä asiassa yhteistyötä esimerkiksi jakamalla asiaan liittyviä tietoja.

Kasvava kyberrikollisuus ja turvallisuusympäristön muutokset

Uudet teknologiat haastavat myös sisäisestä turvallisuudesta vastaavia lainvalvontaviranomaisia kehitysnopeutensa ja muuntautumiskykynsä vuoksi. Tekoälyn kehittyminen on mahdollistanut uudenlaisten rikosten syntymistä. Uusiin teknologioihin liittyvien kehityskulkujen ennakointi on äärimmäisen tärkeää, jotta ymmärretään, millaisiin uhkiin on syytä varautua tulevaisuudessa. Pitkän aikavälin suunnitelmallinen seuranta ja uusien ilmiöiden, teknologioiden ja rikostrendien sekä hiljaisten signaalien seuranta korostuu varautumisessa.

Avoimena oikeusvaltiona Suomen lainsäädännön kehittäminen ja muutokset ovat yleensä pitkän aikavälin prosesseja. Turvallisuusympäristön muutokset ovat kuitenkin pakottaneet nopeampaan reagointiin ja kehittämiseen. Mahdollisuudet lainsäädännön ennakoivaan kehittämiseen nopealla aikataululla ovat kuitenkin rajalliset. Murrosteknologioiden asteittainen yleistyminen ja kypsyminen vaikeuttavat toimintaympäristön muutosten ennakointia myös lainsäädännön kehittämisen näkökulmasta.

Keskusrikospoliisi näkee, että yhteiskunnan kokonaisturvallisuuden kannalta on tarpeen huomioida keskeiset toimintaympäristöön laajasti vaikuttavat muutostekijät ja niiden keskinäiset sidonnaisuudet. Tästä näkökulmasta Keskusrikospoliisi toteaa strategia-asiakirjan tärkeäksi askeleeksi laajoihin muutoksiin varautumiseksi.

Ruotsalainen Heidi
Keskusrikospoliisi