Sisäministeriö
Inrikesministeriet

Hallintovaliokunnalle 3.3.2026

Asia: Lisäselvitys valtioneuvoston selonteko sisäisestä turvallisuudesta VNS 6/2025 vp.

Eduskunnan hallintovaliokunta on pyytänyt sisäministeriöltä kirjallista lisäselvitystä siitä, mitkä ovat keskeisimmät lainsäädännön muutostarpeet, jotka liittyvät valtioneuvoston sisäisen turvallisuuden selonteon kyberuhkia koskevien tavoitteiden toteuttamiseksi? Lisäksi valiokunta pyytää selvitystä siitä, millä lainsäädännöllisillä toimenpiteillä voidaan vaikuttaa siihen, että esim. Valtorin tietomurron kaltaiset teot voidaan jatkossa nykyistä tehokkaammin estää ja teoista aiheutuvat vahingot minimoida? Sisäministeriö toteaa asiasta seuraavaa:

Panostetaan kyberuhkien havaitsemiseen ja torjuntaan sekä niihin liittyvään tiedonvaihtoon turvallisuusviranomaisten välillä

Sisäministeriön ja puolustusministeriön asettaman yhteisen työryhmän selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa (Valtioneuvoston julkaisuja 2023:31) suositteli annettavaksi uudelleen rauennut liikenne- ja viestintäministeriön johdolla valmisteltu hallituksen esitys (HE 243/2022 p) viranomaisten yhteistoiminnan edistämiseksi yhteiskunnan toiminnan kannalta vakavissa tietoturvaloukkaustilanteissa.

Lainsäädännön valmistelun tavoitteena oli kehittää kyberturvallisuuden viranomaisten tiedonvaihtoa. Olennaisena seikkana nostettiin esiin ainakin se, että poliisi, liikenne- ja viestintävirasto, suojelupoliisi ja puolustusvoimat voisivat vaihtaa viranomaisten kesken tietoa tahallisista ja haitallisista kybertapahtumista tieturvaloukkauksen tai sen uhkan selvittämiseksi tai ennalta estämiseksi. Tiedon luovuttamisen yhteydessä viranomaiset olisivat voineet asettaa tiedon käytölle rajoituksia, jolla voitaisiin varmistaa tiedon luottauksellinen käsittely viranomaisissa. Sisäministeriön näkemyksen mukaan vastaavan tyyppinen lainsäädäntö olisi edelleen tarpeellinen. Lisäksi sisäministeriön näkemyksen mukaan lakia sähköisen viestinnän palveluista (917/2014) tulisi muuttaa siltä osin, että siinä huomioitaisiin poliisi yhtenä tiedon saavana viranomaisena, jolle tietoa voidaan luovuttaa em. kybertapahtumista.

Eduskunnan käsiteltävänä on parasta aikaa hallituksen esitys (HE 182/2025 vp) eduskunnalle laiksi poliisilain muuttamisesta ja siihen liittyviksi laeiksi. Esityksen mukaan poliisilaissa ja henkilötietojen käsittelystä poliisitoimessa annetussa laissa säädettyjä tiedonsaanti- ja tietojen luovutussäännöksiä muutettaisiin siten, että ne mahdollistaisivat nykyistä paremmin poliisin tietojenvaihdon muiden viranomaisten kanssa muun muassa rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi. Laeissa säädettäisiin poliisin oikeudesta luovuttaa tietoja salassapitosäänteln estämättä sekä pyynnöstä että oma-aloitteisesti. Poliisilaissa säädettäisiin poliisin oikeudesta luovuttaa

tietoja tilanteissa, joissa se olisi tarpeen poliisille tai muulle viranomaiselle tai julkista tehtävää hoitavalle kuuluvan tehtävän vuoksi tai välttämätöntä tärkeän yleisen tai yksityisen edun vuoksi. Tietoja voitaisiin luovuttaa viranomaisten ja julkista tehtävää hoitavan yhteisön lisäksi myös yksityisille tahoille laissa säädetyin edellytyksin. Poliisilakiin lisättäisiin myös nimenomainen säännös tietojen luovuttamisesta kriittiseen infrastruktuuriin liittyville toimijoille.

Kyberturvallisuuslaissa (124/2025) 25 §:ssä säädetään CSIRT-yksikölle vapaaehtoisesti luovutettavan tiedon käyttämisen kiellosta tiedon luovuttajaan kohdistuvassa rikostutkinnassa. Vastaavan sisältöistä lainsäädäntöä on esitetty EU:n kyberturvallisuussäädöksen toimeenpanon yhteydessä laiksi eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista (HE 179/2025 vp) 8 §:ssä. Lainsäädäntöön rakennettavat kiellot tiedon hyödyntämiselle rikosten selvittämisessä eivät ole tyypillisesti ole olleet osa Suomen lainsäädäntöä ja sisäministeriön näkemyksen mukaan tällainen lainsäädäntö ei palvele rikosten estämistä, paljastamista ja selvittämistä.

Lisäksi sisäministeriö pitää tärkeänä, että valtionhallinnon kyberresilienssiä edelleen kehitetään muun muassa siten, että kriittisin tieto velvoitettaisiin säilyttämään kansallisissa järjestelmissä, joita on mahdollista suojata kansallisilla havainto- ja valvontajärjestelmillä, eikä sitä siirrettäisi ulkomaisiin pilvipalveluihin.

Arvioidaan ja toteutetaan poliisin esitutkintavelvoitteen mahdolliset lainsäädännölliset muutostarpeet paremman tiedonsaannin mahdollistamiseksi kyberuhkien osalta

Tietoverkkorikollisuutta koskevan kokonaiskuvan kannalta olisi tärkeää, että tietoverkkorikosten uhreiksi joutuneet tahot tekisivät nykyistä useammin poliisille rikosilmoituksen. Oikea ja ajantasainen tilannekuva ja -tietoisuus on edellytys tietojohtoiselle poliisitoiminnalle.

Tiedonsaannin haasteeksi on tunnistettu yritysten ja julkishallinnon organisaatioiden osalta se, että ne eivät ilmoita tapahtumista poliisille, koska tiedot tapahtumasta tulevat ainakin pääosin julkisiksi poliisi toimittaman esitutkinnan jälkeen ja mahdollisen rikosprosessin aikana. Tietojen julkituleminen saatetaan nähdä mainehaittana tai esitutkintapöytäkirjan tietojen uskotaan sisältävän liikesalaisuuksia tai yritysturvallisuuteen liittyviä tietoja. Poliisin toimintaa tietojen julkisuuden osalta säätelee ainakin laki viranomaisten toiminnan julkisuudesta (621/1999) ja esitutkintalaki (805/2011). Mikäli tutkittavana ollut rikos etenee tuomioistuimen käsiteltäväksi, niin asiakirjajulkisuudesta säädetään laissa oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa (370/2007). Vaikka poliisi päättäisi salata esitutkinta-aineistosta osan esimerkiksi yrityssalaisuuteen liittyen, niin tuomioistuin voi päättää itsenäisesti, että ko. osa ei ole salassa pidettävä.

Poliisille on tullut tutkittavaksi viime vuosina yhä enemmän hyvin laajoja tietoverkkorikoskokonaisuuksia (esim. Vastaamo), joissa saattaa olla jopa

kymmeniätuhansia asianomistajia tai jotka ovat pitäneet sisällään ennennäkemättömän määrän käsiteltävää, analysoitavaa ja tutkittavaa dataa, joka liittyy useisiin eri maihin. Tällaisten juttujen rikosprosessin läpivieminen on ollut haastavaa. Poliisin rikostorjunnan resurssit suurimmissa kaupungeissa olivat esimerkiksi hetkellisesti sidottuja pelkästään siihen, että Vastaamo-tapauksen rikosilmoitukset saatiin kirjattua poliisin järjestelmiin. Tapaus aiheutti ja aiheuttaa yhteiskunnalle merkittäviä kuluja muun muassa rikosprosessin myötä. Ennustettavissa myös on, että niin sanottujen ylisuurten rikostapausten määrä lisääntyy tulevaisuudessa.

Hallitusohjelmassa on monia tavoitteita, joiden pyrkimyksenä on tehostaa rikostorjuntaa, keventää esitutkintaviranomaisen velvoitteita ja parantaa poliisin rikostorjunnan edellytyksiä. Esimerkiksi laajojen massarikoskokonaisuuksien tutkintaa sujuvoitetaan ja laajennetaan tutkinnan rajoittamisedellytysten käyttöalaa helpottamalla niiden käyttöä. Rikosprosessia ja esitutkintaviranomaisten toimintaa koskevaa lainsäädäntöä tulee kuitenkin edelleen kehittää siten, että viranomaisten resurssit voidaan kohdentaa vaikuttavalla ja tarkoituksenmukaisella tavalla.

Varmistetaan lainvalvontaviranomaisten pääsy tietoon kybertoimintaympäristössä ja kehitetään toimivaltuuksia ja työvälineitä verkossa tapahtuvien rikosten torjuntaan

Sisäministeriö viittaa eduskunnan käsiteltävänä olevaan valtioneuvoston E-selvitykseen: Etenemissuunnitelma – lainvalvontaviranomaisten laillinen ja tosiasiallinen pääsy dataan, tiedonanto (E 99/2025 vp) ja siinä nostettuihin Suomen kantoihin.

Rikollisryhmät hyödyntävät yhä laajemmin tietoverkkoja, valmiita ohjelmistoja tai teknistä infrastruktuuria rikosten toteuttamisessa tai toiminnan tukena. Tietoverkkoavusteisten petosten määrä kasvaa ja toteutustavat kehittyvät edelleen. Tekoäly, pimeä verkkoja päästä päähän salattujen viestintäsovellusten käyttö ja kryptovaluutat mahdollistavat rikollisen toiminnan. Kehitys yhdistettynä uusiin teknologioihin ja kansainvälisiin yhteyksiin haastaa merkittävästi rikostorjuntaa ja muuttaa jatkuvasti poliisin tehtäväkenttää. Teknologinen kehitys ja kansainvälisen kyberrikollisuuden kasvu vaativat poliisilta uudenlaista osaamista. Samalla tekoäly, valvontateknologiat ja data-analytiikka voivat tukea poliisin työtä.

Mahdollistetaan Suomen viranomaisille oikeus puuttua sellaisten ulkomailla olevien tietoverkkolaitteiden ja ohjelmistojen toimintaan, joita käytetään Suomen kansallista turvallisuutta vakavasti vaarantavaan kybervakoiluun tai -vaikuttamiseen.

Sisäministeriössä on käynnissä siviilitiedustelua koskevan lainsäädännön uudistaminen

Lakihankkeen tavoitteena on parantaa suomalaisen yhteiskunnan mahdollisuuksia suojautua kansalliseen turvallisuuteen kohdistuvilta vakavilta uhilta. Sisäministeriössä on käynnissä siviilitiedustelua koskeva

lainsäädäntöhanke, jossa siviilitiedustelu koskeva lainsäädäntö uudistetaan vastaamaan muuttuneen turvallisuus- ja kybertoimintaympäristön vaatimuksiin. Hankkeessa on tarkoitus ehdottaa poliisilain 5 a lukuun uudet asiaa koskevat säännökset (39 a ja 39 b §:t).

Siviilitiedustelulakihankkeessa on tarkoitus ehdottaa säädettäväksi myös valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta, jossa hallitusohjelman mukaisesti mahdollistettaisiin muun muassa tiedustelu laite- ja järjestelmäketjuihin.

Millä lainsäädännöllisillä toimenpiteillä voidaan vaikuttaa siihen, että esim. Valtorin tietomurron kaltaiset teot voidaan jatkossa nykyistä tehokkaammin estää ja teoista aiheutuvat vahingot minimoida?

Valtorin tietomurtoa koskevaa tapausta on käsitelty muun muassa valtiovarainministeriön johdolla valtioneuvoston kyberkoordinaatioryhmän puitteissa. Tapauksen selvittäminen on vielä kesken, joten mahdollisia lainsäädännön kehittämistä edellyttävien toimia ei ole vielä identifioitu. Kyberturvallisuutta vakavasti vaarantavissa tilanteissa toimivaltaisten viranomaisten tehtävät on määritelty pääsääntöisesti riittävällä tavalla viranomaisia koskevassa lainsäädännössä. Siltä osin kuin haitalliset ja tahalliset kyberturvallisuuteen vaikuttavat tapahtumat liittyvät valtiolliseen vaikuttamiseen on tärkeää, että viranomaisille on säädetty mahdollisuus vaihtaa hallussaan olevaa tietoa muiden viranomaisten kanssa tapahtuman selvittämiseksi ja uusien vahinkojen torjumiseksi. Tältä osin viitataan edellä tietojenvaihtoa käsittelevään kohtaan.

Valtorin tietomurron estämiseen ja selvittämiseen liittyvästä tapauksen tutkinnasta tiedottaa tapaukselle määrätty tutkinnanjohtaja.