



Sisäministeriö Inrikesministeriet

Viranomaisten toimintaedellytyksiä on tarve parantaa kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa ja kyberpuolustuksessa

Suomen kyberturvallisuusympäristö on merkittävästi muuttunut viime vuosina ja Suomeen kohdistuu joka päivä niin kybervaikuttamista ja kybervakoilua kuin kyberrikollisten tietomurtoja ja kiristyshaittaohjelmahyökkäyksiä. Vaikka Suomen valtionhallinnossa tietoturvallisuus ja varautuminen kyberuhkiin on hyvällä tasolla, vaatii kybertoimintaympäristön ja sen uhkien kehittyminen kyberturvallisuuden jatkuvaa parantamista ja lainsäädännön ajantasaistamista vastaamaan kybertoimintaympäristön uhkiin.

Sisäministeriön ja puolustusministeriön yhteisessä laajapohjaisessa selvityshankkeessa (3/2022-3/2023) viranomaisten toimintaedellytysten selvittämiseksi ja kehittämisehdotusten laatimiseksi kansallisen kyberturvallisuuden varmistamiseksi, vakavan kyberrikollisuuden torjumiseksi ja kyberpuolustuksen kehittämiseksi tunnistettiin lukuisia toimenpidetarpeita. Näistä keskeisimmät kehittämistarpeet ovat:

1. Kyberturvallisuusstrategia tulee uudistaa kansallinen tavoitetilan määrittelemiseksi huomioiden sekä muutokset turvallisuusympäristössä että EU-lainsäädännön ja Nato-jäsenyyden vaatimukset.
2. Annetaan uudelleen edellisellä vaalikaudella rauennut hallituksen esitys (HE243/2022 p) viranomaisten yhteistoiminnan edistämiseksi.
3. Viranomaisten yhteistoimintaa ja tilannekuva tulee parantaa luomalla pysyvä viranomaisyhteistyörakenne valtioneuvostotason ja teknisen asiantuntijatason väliselle virastotasolle.
4. Kansallisen kyberturvallisuuden suojaamista on parannettava kehittämällä lainsäädäntöä mahdollistamaan tehokkaampi tiedonvaihto poliisin, suojelupoliisin ja Liikenne- ja viestintäviraston sekä Puolustusvoimien välillä.
5. Poliisin toimintaedellytyksiä kybertoimintaympäristössä on parannettava lainsäädäntömuutoksilla liittyen sekä poliisin toimivaltuuksiin, tiedonvaihtoon ja tietojen luovutukseen. Lisäksi poliisille tulee olla resurssien käytön tehostamiseksi mahdollista rajata esitutkinnan toimittamisvelvollisuutta erityisesti silloin, kun vihamielisen kybertoiminnan taustalla on valtiollinen toimija, jota tästä johtuen ei voida saattaa rikosoikeudelliseen vastuuseen Suomessa.
6. Tehokkaamman tiedonhankinnan mahdollistamiseksi kyberuhista tulisi tiedusteluviranomaisten toimintaedellytyksiä kybertoimintaympäristössä kehittää luomalla edellytykset tiedustelumenetelmien kohdistamiseksi yksittäisten laitteiden sijasta virtuaalisten järjestelmien muodostamiin kokonaisuuksiin ja kehittämällä palomuurisääntelyä mahdollistamaan riittävä tiedon luovuttaminen rikostorjuntaviranomaisille kansallisen turvallisuuden suojaamiseksi.
7. Viranomaisille tulee luoda lainsäädännön mahdollistamat edellytykset avustaa laajemmin yhteiskunnan toiminnan ja huoltovarmuuden kannalta kriittisiä yrityksiä kyberuhkiin varautumisessa ja kyberhyökkäyksistä toipumisessa.
8. Viranomaisverkkojen suojausta tulee edelleen parantaa kehittämällä lainsäädäntö siten, että se mahdollistaa relevanttien viranomaisten osallistumisen viranomaisverkkojen kybersuojaukseen.
9. Puolustusvoimille tulee laatia kyberpuolustustehtävät mahdollistava lainsäädäntö mukaan lukien riittävät toimivaltuudet sekä tiedonvaihdon ja tietojen luovutuksen edellytykset.

Yhteyshenkilö: Ylijohtaja **Petri Knape**, p. +358 295 488 235, petri.knape@gov.fi

Kirkkokatu 12, Helsinki

PL 26, 00023 Valtioneuvosto

Vaihe 0295 480 171 | kirjaamo.sm@gov.fi | www.intermin.fi