20.10.2025

Eduskunta
Liikenne- ja viestintävaliokunta

Viite: VNS 6/2025 vp

Lausunto: Valtioneuvoston selonteko sisäisestä turvallisuudesta

Kiitämme mahdollisuudesta lausua asiasta. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa. Teknologiateollisuuden jäsenet vastaavat puolesta Suomen viennistä, tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista.

Tiivistelmä

Selonteossa kuvataan sisäisen turvallisuuden toimintaympäristöä ja sen muutosta sekä määritellään keskeisimmät sisäisen turvallisuuden politiikan painopisteet ja tavoitteet. Selonteko määrittää yhdessä eduskunnan siitä antaman mietinnön kanssa Suomen sisäisen turvallisuuden politiikkaa koskevat keskeiset linjaukset tuleville vuosille. Selonteko muodostaa yhdessä ulko- ja turvallisuuspoliittisen ja puolustuspoliittisen selonteon kanssa kolmen turvallisuusselonteon kokonaisuuden.

Katsomme, että selonteko täydentää asianmukaisesti ulko- ja turvallisuuspoliittista sekä puolustuspoliittista selontekoa. Vaikka Suomessa on useita etuja ja ansioita sisäisen turvallisuuden alueella ja myös erinomaisia tavoitteita, ollaan niiden toteutumisesta edelleen varsin kaukana. Selonteko kuvastaa valitettavan hyvin sitä, että valmistelun aikana on kuultu ainoastaan työryhmän käsityksen mukaisia tärkeimpiä sidosryhmiä, eikä niistäkään ole annettu tarkempaa selvitystä. Otamme alla kuitenkin kantaa ainoastaan toimialamme ja elinkeinoelämän kannalta keskeisiin seikkoihin (selonteon otsikkojakoa mukaillen). Keskeiset havainnot:

- Vaikka sisäisen turvallisuuden ylläpitäminen on valtion tärkeimpiä tehtäviä myös Suomen n. 600 000 yritykselle, tämä osa-alue jää selonteossa lähes huomiotta, ml. omaisuus- ja elinkeinorikoksien osalta
- Ylivoimainen osa teknologiaan liittyvästä kehitystyöstä tehdään yritysten toimesta ja yksityisen ja julkisen sektorin kumppanuudet ovat luoneet vaikuttavia ratkaisuja
- Turvallisuusviranomaisten toimivaltuuksien kehittämisen tai käytön ei tule heikentää yritysten kilpailukykyä tai toimintamahdollisuuksia
- Vaikka yhteiskuntaan kohdistuu vakavia tietoturvaloukkauksia ja kansalaiset, yritykset ja yhteisöt ovat hyvin huolestuneita, selonteossa ei esitetä täsmällisiä kehitysehdotuksia
- Rikostiedustelun sijaan ratkaisevat menestystekijät perustuvat tehostettuihin esitutkinta- ja syytetoimiin kansainvälinen viranomaisyhteistyö mukaan luettuna
- Yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten suojaamisen sekä huoltovarmuuden turvaamisen näkökulma on puutteellinen
- Vihamielisen informaation torjunta on puutteellinen tehokkaiden keinojen strategisen käytön ja resurssien ohjaamistavoitteiden osalta
- Kyberturvallisuuden suhteen selonteko on puutteellinen yksityisen sektorin roolin ja vaikutusmahdollisuuksien arvioinnissa ja suosituksissa
- Selonteossa ei käsitellä lainkaan Naton puolustusmenotavoitteeseen (5 % BKT:stä) liittyviä maanpuolustusta tukevia investointeja (1,5 % BKT:stä)
- Selonteko sisältää useita kehitysehdotuksia, jotka ovat ristiriidassa Suomen taloudellisen hyvinvoinnin, elinkeinoelämän sekä perusoikeuksien näkökulmista

Eteläranta 10, PL 10, 00131 Helsinki

Sisäinen turvallisuus muuttuvassa toimintaympäristössä

Selonteossa todetaan, että *kansakunnan taloudellisella hyvinvoinnilla on tärkeä ja monialainen vaikutus sisäiseen turvallisuuteen*. Näkemys on vähintäänkin epätarkka, ellei jopa vähättelevä. Ensinnäkin Suomi elää yritysten harjoittamasta viennistä ja ulkomaankaupasta. Lähes yhtä tärkeä havainto on, että myös demokraattinen hallintomallimme sekä julkinen taloutemme nojaavat taloudelliseen hyvinvointiin. Rikollisuus, yhteiskunnallinen epävakaus, poliittinen tyytymättömyys sekä turvattomuus ovat korkealla tasolla, kun yhteiskunnan taloudellinen hyvinvointi on matala. Selonteossa ei oteta juurikaan kantaa, mikä merkitys sisäisen turvallisuuden toiminnalla on yrityksiin ja yhteisöihin sekä toisin päin.

Osin vastaavaa kapeakatseisuutta osoittaa selonteon lyhyt pohdinta teknologisesta murroksesta, jossa tosiasioista poiketen esitetään, että *teknologiaan liittyvät ratkaisut synnytetään usein viranomaisyhteistyön tuloksena*. On yleisesti tiedossa, että ylivoimainen osa teknologiaan liittyvästä kehitystyöstä tehdään yritysten toimesta ja että nimenomaan yksityisen ja julkisen sektorin kumppanuudet ovat luoneet tehokkaita ja vaikuttavia ratkaisuja viranomaisten tunnistamiin haasteisiin ja kehitystarpeisiin. Tähän liittyen Suomen tulisi aiempaa systemaattisemmin hyödyntää kansallista ja kansainvälistä tutkimus-, kehittämis- ja innovaatiorahoitusta (TKI) sekä -yhteistyötä sisäisen turvallisuuden vahvistamiseksi. Tätä tavoitetta ei voi saavuttaa ilman, että Sisäministeriö priorisoi ko. tavoitetta ja ohjaa siihen tarvittavat henkilö- ja taloudelliset resurssit. Moni muu hallinnonala on ryhtynyt jo toimeen vastaavalla tavalla.

Selonteossa nostetaan ansiokkaasti esiin eri rikoslajien suuruusluokka, mutta vaikka omaisuusrikokset muodostavat lähes puolet kaikista rikoksista, huomiota ei ole lainkaan osoitettu sille, ketkä ovat näiden rikosten asianomistajia eli uhreja. On huomattavaa merkitystä myös toimenpidesuositusten näkökulmasta, miltä osin uhrit ovat yrityksiä ja yhteisöjä ja miltä osin yksityisiä henkilöitä.

Turvallisuusviranomaisten toimivaltuuksien kehittämisen tai käytön ei tule heikentää yritysten kilpailukykyä tai toimintamahdollisuuksia, vaan niiden tulee olla sopusoinnussa elinkeinopoliittisten kysymysten kanssa. Elinkeinotoiminta, panostukset tutkimukseen, tuotekehitykseen ja innovaatiotoimintaan luovat edellytykset tulevaisuuden kasvulle ja vauraudelle. Suomen houkuttelevuus investointien kohteena on kaukana jäljessä kansainvälisistä verrokkimaista ja asettamistamme tavoitteista, eikä viranomaistoiminnan, eritoten pitkälle menevän salaisen tiedonhankinnan tule vaarantaa tätä tavoitetta. Suomessa ei tule yleisesti myöskään antaa EU-säädöksiä täydentävää sääntelyä, joka lisää hallinnollista takkaa tai vaikuttaa kielteisesti yritysten toimintaedellytyksiin kilpailijamaihin verrattuna.

Sisäisen turvallisuuden painopisteet ja tavoitteet, vieraiden valtioiden vakoilutoiminnan sekä järjestäytyneen ja vakavan rikollisuuden torjunta (oikeus- ja yhteiskuntajärjestyksen turvaamiseksi)

Tietoverkkoavusteisen rikollisuuden ja erityisesti omaisuus- ja petosrikollisuuden todetaan kasvaneen merkittävästi ja toiminnan kehittyvän nopeasti. Lisäksi korostetaan *merkittäviä rikollisia taloushyötyjä, sekä tarvetta nopeaa reagointikykyyn rikosvahinkojen minimoimiseksi myös kansainvälisen yhteistyön osalta*. Ilmiön laajamittaisuutta ja yhteiskunnallista vaikutusta korostaa mm. se, että tuoreen Digiturvabarometri 2025 (DVV) mukaan n. 60 % kansalaisista on huolissaan yhteiskuntaan kohdistuvista kyberhyökkäyksistä ja digihuijauksista, ja lähes 40 % kokee luottamuksensa digiturvaan heikentyneen. Vastaavasti Elisa Oyj:n suomalaisille suuryrityksille tänä vuonna suunnatun selvityksen mukaan yli 90 % vastaajista kokee kyberuhkien lisääntyneen viime vuosina. Suomessa viranomaisten tietoon tulee n. 150 vakavaa

tietoturvallisuusloukkaustapausta vuosittain. Tämä tarkoittaa sitä, että käytännössä joka toinen päivä tapahtuu yhteiskuntaan vaikuttavia vakavia tapahtumia. Yllä mainituista huomioista huolimatta selonteossa ei esitetä mitään täsmällisiä ongelmaan kohdistuvia kehitysehdotuksia.

Sen sijaan selonteossa esitetään jo kertaalleen selvitettyä ja Eduskunnan käsittelemää (Poliisin rikostiedustelulainsäädännön kehittämistarpeet, SM:n julkaisuja 2023:19) tarvetta viranomaisten ”paremmalle” tiedonhankinnalle eli kattavammalle rikostiedustelulle. Viittaamme aiempaan kantaamme rikostiedustelun toimivaltuuksien laajentamisesta ”sisäisen turvallisuuden vaarantumisen” perusteena:

> *Mikäli sisäisen turvallisuuden suojaamista käytettäisiin itsenäisenä tiedonhankintatoimivaltuuksien käytön tai henkilötietojen käsittelyn perusteena, sisäisen turvallisuuden uhat olisi kyettävä määrittelemään riittävän täsmällisesti ja tarkkarajaisesti niin sisällöllisesti, henkilöllisesti kuin ajallisestikin. Esimerkiksi tietoverkkoja hyväksi käyttävä rikollisuus kattaa varsin huomattavan määrän rikoksia petoksista vakoiluun. Samalla eri rikoslajien vakavuus vaihtelee jokseenkin alhaisen rangaistusasteen asianomistajarikoksista ylitörkeisiin. Lisäksi laajamittaisuuden osalta voidaan todeta, että todellisuudessa merkittävä osa suomalaisista joutuu vuosittain jonkin tietoverkkorikoksen (yrityksen) kohteeksi esim. huijaus-, haittaohjelma- tai kalasteluviestien muodossa. Ilmiö on niin laaja ja yleinen, että yhteiskuntamme ei edes enää tunnista rikosilmiön laajuutta. Toisin sanoen rikosoikeudellisesti katsoen teot ovat moitittavuudeltaan hyvin eri tasoisia, josta syystä niitä ei voitane oikeudellisesti kestävällä tavalla käsitellä toisilleen rinnasteisina toimivallan perustavina uhkailmiönä.*

Katsomme, että ratkaisevat menestystekijät perustuvat rikosvastuun toteuttamiseen tähtäävät tehostetut esitutkinta- ja syytetoimet kansainvälinen ja eritoten eurooppalainen viranomaisyhteistyö mukaan luettuna. Sisäiseen turvallisuuteen ja eritoten Suomen taloudelliseen turvallisuuteen liittyy olennaisesti yritysvakoilun torjunta (verkko- ja henkilövakoilu) ja rinnasteiset elinkeinorikokset, jotka yhdessä rapauttavat Suomessa toimivaa teollisuutta (tutkimus, tuote- ja tuotantomenetelmien kehitys). Lisäksi teollisuuden toimintaedellytyksiä ja kannattavuutta haittaavat vahingonteko- ja yleisvaaralliset rikokset, jotka vaikuttavat suorien vahinkojen lisäksi myös epäsuorasti suomalaisten käyttäytymiseen huolestuneisuuden sekä kulutus- ja investointihaluttomuuden lisääntymisenä. Katsomme aiemman kantamme mukaan edelleen, että empiirisen tiedon ja kokemuksen perusteella voidaan sanoa, että terroristinen toiminta ei Suomessa kykene perustuslaillisen oikeus- ja yhteiskuntajärjestyksemme murtamiseen eikä merkittävästi heikentämään yritysten kilpailukykyä tai toimintamahdollisuuksia. Tätä seikkaa vasten väkivaltaisten ääriliikkeiden ja terrorismin uhkan hallintaan on ohjattu merkittäviä ja kasvavia resursseja, eritoten Suojelupoliisille saatavien yhteiskunnallisten hyötyjen punnintaa ja priorisointia. Selonteko jää ilmeisen puutteelliseksi yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten suojaamisen sekä huoltovarmuuden turvaamisen näkökulmista.

Suomalaista luottamusyhteiskuntaa suojataan vihamieliseltä informaatiovaikuttamiselta

Selonteossa todetaan, että *yksittäiset disinformaatiokampanjat eivät ole merkittävin ongelma, vaan että tehokas informaatiovaikuttaminen on pitkäkestoista ja toistaa kertomuksia ja maailmankuvia, jotka vaikuttavat alitajuisesti ihmisten mieliin. Tarkoituksena on heikentää yhteiskunnan toimijoiden toimintakykyä ja päätöksentekoa. Lisäksi todetaan, että kansalaisten luottamus demokratiaan, yhteiskunnan instituutioihin ja muihin ihmisiin suojaa yhteiskuntaa haavoittuvuuksilta ja ylläpitää henkistä kriisinkestävyyttä*.

Eräänlaiseksi ratkaisuksi esitetään, että ”avoimella, aktiivisella ja strategisella viranomaisviestinnällä on keskeinen rooli informaatiovaikuttamisen torjunnassa”. Tämä on nähdäksemme avoimen demokraattisen yhteiskunnan perusedellytys eikä sitä voida pitää selonteossa tavoiteltuna kehityskeinona. Sen sijaan informaatiovaikuttamisen hallinnan ja torjunnan keskeisimmät keinot liittyvät tehokkaaseen viestintäalustojen (some yms.) lainvalvontaan ja vastuun toteuttamiseen. Lakivaatimukset ovat yhteiseurooppalaisia, kuten EU:n digipalvelusasetus, yleinen tietosuoja-asetus, digimarkkina-asetus, eIDAS sekä CoC/CoP disinformaation torjunnasta. Lainvalvonta ja muut keinot kuten EU:n diplomaattisen työkalupakin valikoima on jaettu EU:n instituutioiden, että jäsenvaltioiden välille. Selonteko jää ilmeisen puutteelliseksi näiden keinojen strategisen käytön ja resurssien ohjaamistavoitteiden osalta.

Suomi suojaa kriittistä infrastruktuuriaan

Selonteossa todetaan, *että kyberturvallisuutta vakavasti vaarantavassa tilanteessa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa. Sääntelyn ja tehtävien hajautuminen, erilaiset toimintamallit ja soveltuvien yhteisten tietojärjestelmien puute edellyttävät yhteistoimintaa, jonka perusteet on kuvattu vuoden 2024 kyberturvallisuusstrategiassa ja yhteiskunnan turvallisuusstrategiassa. Kyberuhkien havaitsemista ja torjuntaa tulee jatkossa parantaa muun muassa varmistamalla keskeisten toimijoiden välisen tiedonvaihdon sujuvuus sekä viranomaisten riittävät toimivaltuudet*.

Suomessa lähes kaikki kriittinen infrastruktuuri on kiinnittynyt tietojärjestelmiin. Kyberturvallisuuden riskienhallintatoimenpiteiden keskeinen vastuu on yrityksillä ja yhteisöillä, sillä ne muodostavat suurimman osan yhteiskunnan toiminnallisesta ja taloudellisesta rakenteesta sekä omaavat juridis-hallinnollis-teknologiset kyvyt niiden toteuttamiseen. Yritykset ja yhteisöt tunnistavat tieto- ja viestintäjärjestelmiinsä kohdistuvat poikkeamat, selvittävät niiden syyt ja vaikutukset sekä poistavat kielteiset vaikutukset. Kyberturvallisuus on siis päivittäishyödyke, joka syntyy datan haltijoiden toimesta valtaosin siellä, missä taltioitu tieto-omaisuus (data) ja tietojärjestelmät ovat. Yritysten ja yhteisöjen hallinnassa olevien tietojärjestelmien toimintavarmuus ja luotettavuus ei pelkästään varmista organisaatioiden omaa toimintaa, vaan johtaa myös kollektiiviseen luotettavuuteen ja häiriöttömyyteen ulkoisvaikutusten kautta. Olennaista ovat ihmisiin, prosesseihin sekä teknologiaan liittyvien uhkien systemaattinen hallinta. Kyse ei siis ole pääosin valtioille ja viranomaisille kohdistetuista odotuksista ”hallita, torjua ja puolustaa” kyberturvallisuutta. Selonteko jää ilmeisen puutteelliseksi yksityisen sektorin roolin ja vaikutusmahdollisuuksien arvioinnissa ja suosituksissa.

Siviiliväestöä suojataan tehokkaasti laajoissa häiriötilanteissa ja poikkeusoloissa

Selonteossa todetaan, että *uudetkin turvallisuusuhat kuuluvat pääasiallisesti sisäisen turvallisuuden kansallisten toimijoiden vastuulle, ja ne ovat avainasemassa yhteiskunnan häiriöttömän toiminnan varmistajina, hybridiuhkiin vastaamisessa, kriittisen infrastruktuurin suojaamisessa sekä väestönsuojelussa*.

Tästä vasten on huomionarvoista, että normaaliolojen merkittäviin poikkeamiin ja poikkeusoloihin varautumisen suhteen selonteossa ei käsitellä lainkaan Naton puolustusmenotavoitteeseen (5 % BKT:stä) liittyviä maanpuolustusta tukevia investointeja (1,5 % BKT:stä). Erityisesti tulisi huomioida yritysten ja yhteisöjen rooli ja niiden tukeminen modernien kyberturvallisuuden riskienhallintakeinojen käyttöönotossa, eritoten yhteiskunnan toiminnan kannalta keskeisten sektorien osalta. Näiden sektorien kyberturvallisuuden investointivaje Suomessa on 1–1,5 mrd€, jonka lisäksi on muita kustannuksia kuten,

väestönsuojankustannukset ja huoltovarmuusmaksut sekä hallinnonalojen turvallisuusmenot. Lisäksi on selvää, että elinkeinoelämä on yksi tärkeimmistä toimijajoukoista varautumisessa ja valmiussuunnittelussa ja yritykset tulisikin huomioida selkeämmin selonteossa.

Selonteossa todetaan, että *Suomen tulisi vaikuttaa aktiivisesti EU:ssa yhteisen varautumispolitiikan ja siihen liittyvien toimien valmisteluun sekä toimeenpanoon*. Yhtenä konkreettisena ehdotuksena EU:n varautumispolitiikassa on yksityisen ja julkisen sektorin yhteistyö. Eurooppalainen politiikka kaipaa ratkaisuja ja Suomella on niitä esittää. Huoltovarmuusajattelua ja -toimintaa ei ole vaivatonta tuoda EU-tasolle. Uutena lähestymistapana EU:ssa voitaisiin pitää suomalaista yksityisen ja julkisen sektorin yhteistä resilienssitoimintaa.

Selonteossa todetaan, että *Suomen tulisi edistää EU:n ja Naton yhteistyötä yhteiskuntien kriisinkestävyyden vahvistamiseksi ja osallistua aktiivisesti Naton resilienssi-, tiedustelu- ja turvallisuusyhteistyöhön sekä kehittää NATOn siviilisuunnittelun järjestelyjä yhteistyössä puolustushallinnon ja muiden viranomaisten kanssa*. Olennainen keino tavoitteen edistämiseksi on luoda tukielementtejä suomalaisille toimijoille, jotta ne voivat paremmin osallistua NATOn resilienssiyhteistyöhön. Esimerkiksi erilaisten NATO-kriteerien täyttäminen on aiheena yhä uusi suomalaiselle elinkeinoelämälle.

Toimenpiteistä ja linjauksista

Torjutaan vakavaa rikollisuutta ja hybridivaikuttamista sekä kehitetään tiedustelua vastaamaan muuttuneen turvallisuus- ja kybertoimintaympäristön vaatimuksia:

- Kannatamme rikostiedustelua ja niihin liittyviä toimivaltuuksia koskevan sääntelyn kehittämistä vain hyvin harkitusti ja rajallisesti yllä esitettyjen huomioiden mukaisesti.
- Emme kannata lainvalvontaviranomaisten pääsyä tietoon kybertoimintaympäristössä yleisesti, mutta kannatamme välttämätöntä pääsyä digitaaliseen todistusaineistoon esitutkinnan turvaamiseksi. Katsomme, että tätä tavoitta tulee edistää ainoastaan niin, että teknologisten ratkaisujen, jotka mahdollistavat lainvalvontaviranomaisten pääsyn salattuihin tietoihin laillisesti, on suojattava myös kyberturvallisuutta ja perusoikeuksia.
- Kannatamme poliisin esitutkintavelvoitteeseen liittyvien lainsäädännöllisten muutostarpeiden arvioimista paremman tiedonsaannin mahdollistamiseksi kyberuhkien osalta, mutta asiassa on välttämätöntä ottaa huomioon yleiset asiaan vaikuttavat jo käynnissä olevat kehitystoimet, kuten luonnos hallituksen esitykseksi laeiksi esitutkintalain, oikeudenkäynnistä rikosasioissa annetun lain ja oikeudenkäymiskaaren 11 luvun 3 b §:n muuttamisesta (VN/22303/2023).
- Kannatamme harkitusti ja rajallista kehittämistä Suomen viranomaisten oikeuteen puuttua ulkomailla olevien tietoverkkolaitteiden ja ohjelmistojen toimintaan, joita käytetään Suomen kansallista turvallisuutta vakavasti vaarantavaan kybervakoiluun tai -vaikuttamiseen. Katsomme, että mahdollinen oikeus tulisi normaaliaikoina olla ainoastaan osana rikosperusteista toimivaltakokonaisuutta ja perustua rikostorjunnan keinovalikoimaan.
- Kannatamme poikkihallinnollisen informaatiovaikuttamisen torjuntakyvyn vahvistamista, mutta emme selonteossa esitettyä lainkaan riittävänä. Viittaamme yllä esittämiimme keskeisempiin ja tehokkaampiin keinoihin.

Kehitetään rikosprosessia ja torjutaan nuoriso-, jengi- ja järjestäytynyttä rikollisuutta:

- Kannatamme rikosprosessin ja esitutkintaviranomaisten toimintaa koskevan lainsäädännön edelleen kehittämistä siten, että viranomaisten resurssit voidaan

kohdentaa vaikuttavalla ja tarkoituksenmukaisella tavalla. Katsomme, että asiassa on välttämätöntä huomioida jo käynnissä olevat kehittämistoimet, kuten luonnos hallituksen esitykseksi laeiksi esitutkintalain, oikeudenkäynnistä rikosasioissa annetun lain ja oikeudenkäymiskaaren 11 luvun 3 b §:n muuttamisesta (VN/22303/2023).

- Kannatamme rajatuilta osin järjestäytyneen rikollisuuden torjunnan lainsäädännön kehittämistä, joka mahdollistaa entistä tehokkaamman tietojenvaihdon ja hallinnollisen torjunnan. Asiassa on tärkeää huomioida mm. yritysten toimintaan ja yrityssalaisuuksiin liittyvät seikat. Tässä yhteydessä on harkittava myös yksityisille toimijoille annettavat tiedot rikosten torjumiseksi.

Suojataan Suomelle kriittistä infrastruktuuria

- Kannatamme turvallisuusselvityslain uudistamista. Asiassa on tärkeä huomioida mm. käsittelyaikojen lyhentäminen (nyt prosessi kestää usein kuukausia), mutta ei lisäresursoinnilla, vaan muuttamalla henkilöturvallisuusselvitys henkilöön ja voimassaoloaikaan perustuvaksi. Selvitysmenettelyyn hyväksytyillä yrityksillä tulisi olla mahdollisuus pystyä havaitsemaan turvallisuusselvitysrekisteristä onko henkilöllä jo voimassa oleva turvallisuusselvitys hallinnoinnin helpottamiseksi. Lisäksi tulisi harkita merkityksellisten tietojen luovuttamista myös kohdehenkilön työnantajalle tilanteessa, jossa jokin toinen organisaatio, esim. asiakkaana toimiva viranomainen on toiminut selvityksen hakijana.
- Kannatamme kriittisen infrastruktuurin kohteiden suojaamista CER-direktiivin toimeenpanon edellyttämällä tasolla, mutta emme pidä tätä riittävänä toimena. Asiassa tulisi huomioida luonnos hallituksen esitykseksi poliisilain ja siihen liittyvien lakien muuttamisesta (VN/27065/2023) esittämämme seikat, tärkeimpänä tietojen luovuttaminen kriittiseen infrastruktuuriin liittyville toimijoille kyberturvallisuuslain soveltamisalan mukaisesti.
- Kannatamme suojelupoliisin strategisen suorituskyvyn kehittämistä rajatusti ja harkiten, rajoittuen pääosin turvallisuusselvitysmenettelyn sekä yritysvakoilun torjunnan kehittämiseen.
- Emme kannata Poliisin suorituskyvyn kehittämistä operatiivisen henkilöstön määrän perusteella, vaan poliisin vaikuttamistavoitteiden ja tulosten kautta. Poliisia tulee ohjata niin, että sillä on mahdollisuus kehittää tietojärjestelmiään ja teknologisia kykyjään sekä henkilöstöään niin, että yhteiskunnan asettamat tavoitteet on mahdollista saavuttaa.

Kyberala ry
Peter Sund
Toimitusjohtaja

Lisätiedot:

Peter Sund, 050 565 0621
peter.sund@teknlogiateollisuus.fi