FiCom ry | Asko Metsola
9.8.2024

FiComin lausunto Suomen kyberturvallisuusstrategiasta

Liikenne- ja viestintäministeriö on pyytänyt FiComilta lausuntoa valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiasta 2024–2035. FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- Tilanteessa, jossa EU:n lisääntyvä sääntely vaikuttaa kyberturvallisuuden kehittämisen mahdollisuuksiin tulevaisuudessa, Suomeen ei tarvita kansallista lisäsääntelyä.
- Kyberturvallisuuden roolia tulee kyberturvallisuusstrategiassa ehdotetun mukaisesti vahvistaa kasvatuksessa, koulutuksessa ja opetuksessa sekä laajasti yhteiskunnan ja työelämän kaikilla tasoilla.
- Kyberturvallisuuden tietopääoma on aidosti suojattava.
- Luottamusta ei rakenneta tietojen luovutusten lisävelvoitteilla.
- Kyberyhteistyössä on säilytettävä vakaus.

Ei kansallista lisäsääntelyä

FiComin mielestä on hyvä, että Suomen kyberturvallisuusstrategiaa päivitetään, kun otetaan huomioon jo pelkästään verkko- ja tietoturvadirektiivin päivityksen eli ns. NIS2-direktiivin myötä tulevat uudet vaatimukset. On myös hyvä, että toimialoja on osallistettu strategiaan jo sen laatimisvaiheessa.

Kuten kyberturvallisuusstrategiassakin todetaan, viime vuosina merkittävästi kehittyneen, kyberturvallisuuteen vaikuttavan EU-sääntelyn kansallinen täytäntöönpano ja organisaatioiden toiminnan mukauttaminen sen mukaisesti haastavat tulevina vuosina niin viranomaisia kuin elinkeinoelämääkin (s. 13). EU:n lisääntyvä sääntely vaikuttaa kyberturvallisuuden kehittämisen mahdollisuuksiin tulevaisuudessa (s. 15), ja EU-sääntelyn myötä lisääntyneet viranomaistehtävät ja velvoitteet edellyttävät riittäviä resursseja (s. 42).

EU:sta on tullut ja tuloillaan pelkästään kyberturvallisuuteen liittyviä velvoitteita mm. NIS2-direktiivin sekä sitä kansallisesti toimeenpanevan kyberturvallisuuslain, kriittistä infrastruktuuria koskevan CER-direktiivin sekä sitä kansallisesti toimeenpanevan yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain, kyberkestävyyssäädöksen, kyberturvallisuusasetuksen, ns. DORA-asetuksen ja kybersolidaarisuusasetuksen muodossa. Lisäksi yrityksiin kohdistuvaa uutta sääntelyä on tullut tai tuloillaan myös mm. datasäädöksestä, tekoälysäädöksestä ja digipalvelusäädöksestä.

Kyberturvallisuusstrategiassa tunnistetaan, kuinka elinkeinoelämä omistaa merkittävän osan Suomen kriittisestä infrastruktuurista ja vastaa sen kyberturvallisuuden varmistamisesta. Kyberturvallisuusstrategiassa esitetyn varovaisen arvion mukaan elinkeinoelämän panostukset kyberturvallisuuteen ovat vähintään kymmenkertaisia verrattuna valtionhallinnon osoittamaan

rahoitukseen. Myös huoltovarmuuden näkökulmasta yritysten käyttämät resurssit kyberturvallisuuteen ovat yhä tärkeämpiä, ja kyberturvallisuuteen investoidaan myös välillisesti (s. 41).

Tätä taustaa vasten on kummallista, että kyberturvallisuusstrategian strategisissa kehittämisehdotuksissa ehdotetaan säädöspohjaa, normeja ja ohjeita muutettavaksi strategian kehittämistoimien edellyttämällä tavalla (s. 44). Tämä tarkoittaa siis käytännössä uutta kansallista lisäsääntelyä. Uutta lainsäädäntöä toivotaan muun muassa murrosteknologioiden sisäänrakennetun turvallisuuden periaatteen varmistamiseksi (s. 24) sekä kyberrikosten ennalta estämiseen, jotta tiedon jakaminen viranomaisten ja yritysten kesken mahdollistuisi (s. 28). Jälkimmäisen osalta on sinänsä kannatettavaa, että nykyisiä laintulkintoja yhdenmukaistettaisiin ja tarkennettaisiin (s. 33), mutta lainsäädäntöön kirjattujen, selkeiden edellytyksien ja osallistuvien tahojen määrittelyn sekä toisaalta nykyisten rajoitteiden perusteiden arvioinnin tiedonvaihdon laajentamiseksi ei saa johtaa kansalliseen lisäsääntelyyn. Liitteessä 1 (s. 46) viitataan valmiuslaista tuleviin velvoitteisiin, mutta kyberturvallisuusstrategiassa tulee paremmin huomioida parhaillaan vireillä oleva valmiuslain kokonaisuudistus, josta on myös odotettavissa uutta kansallista sääntelyä.

Suomen tulee vaikuttaa kyberturvallisuutta, kyberrikollisuutta ja kyberpuolustusta koskevaan päätöksentekoon niin YK:ssa, EU:ssa, Natossa kuin muissakin keskeisissä kansainvälisissä järjestöissä ja verkostoissa (s. 31), mutta pidättäytyä kyberturvallisuuden kehittämisen mahdollisuuksia vaikeuttavasta kansallisesta lisäsääntelystä.

On hyvä, että eri toimintojen ja toimijoiden välinen keskinäisriippuvuus esimerkiksi toimitusketjujen osalta sekä julkisen ja yksityisen sektorin yhteistyön tärkeys on tunnistettu strategiassa. On kuitenkin huomattava, että yritykset tekevät yhteistyötä julkisen sektorin ohella myös laajasti yksityisen sektorin eri toimijoiden kanssa. Esimerkiksi sääntelyyn tai turvallisuusselvitysmenettelyihin liittyvät käytännön esteet voivat kuitenkin heikentää mahdollisuuksia yhteistyöhön, vaikka rajat ylittävä yhteistyö niin julkisen kuin yksityisen sektorin toimijoiden kesken on tärkeää, jotta kyberturvallisuuden parantamiseksi saadaan paras tieto ja osaaminen. Turvallisuusselvitysprosessien yhdenmukaistamista Pohjoismaiden kesken tulisi arvioida siten, että tavoitteena on rajat ylittävä yhteistyö sekä julkisella että yksityisellä sektorilla. Yhdenmukaistetut turvallisuusselvitysprosessit Pohjoismaissa helpottaisivat sekä yksityisen että julkisen sektorin henkilöstön mahdollisuuksia jakaa tietoa ja parhaita käytänteitä, mikä parantaisi myös verkkoturvallisuutta yli rajojen

Panostus osaamiseen kannattaa aina

Vaikka kyberkoulutukseen ja -tutkimukseen sijoitettu euro näkyy kyberturvallisuuden vahvistumisessa usein vasta myöhemmin (s. 41), kyberturvallisuus mahdollistaa liiketoiminnan kasvun (s. 15). Siksi on ehdottoman kannatettavaa, että kyberosaamiseen panostettaisiin Suomessa kaikilla koulutusasteilla ja erilaisissa tutkimushankkeissa (s. 41). Kyberturvallisuuden roolia tulee kyberturvallisuusstrategiassa ehdotetun mukaisesti vahvistaa laajasti kasvatuksessa, koulutuksessa ja opetuksessa sekä yhteiskunnan ja työelämän kaikilla tasoilla (s. 23).

Kyberturvallisuuden roolin vahvistamisessa täytyy kuitenkin keskittyä resurssien tehokkaaseen käyttöön. Kyberturvallisuusstrategiassa puhutaan eri julkisen sektorin toimijoiden tarjoamista keskitetyistä kyberturvallisuuspalveluista (s. 35), joita ei kuitenkaan avata sen tarkemmin. On aiheellista kysyä, miten

tällaiset keskitetyt palvelut vaikuttavat suomalaisten yritysten kilpailukykyyn ja onko niiden kehittäminen tehokasta resurssien käyttöä?

Kyberturvallisuuden tietopääoma on aidosti suojattava

Kyberturvallisuusstrategiassa todetaan, kuinka Suomeen kohdistuvan vihamielisen kybertoiminnan lisääntyessä oman toimintaympäristön, tietojärjestelmien ja etenkin näiden välisten keskinäisriippuvuuksien tuntemus on entistä tärkeämpää (s. 11). Onkin tärkeää, että julkisen ja yksityisen sektorin kriittinen tietopääoma tunnistetaan ja suojataan yhteiskunnan toimivuuden varmistamiseksi (s. 25). Kyberturvallisuuden tietopääomaan lukeutuvat esimerkiksi palvelut, tietojärjestelmät, osaaminen, prosessit, patentit, tavaramerkit ja kumppanuudet.

Tällä hetkellä kansallinen trendi on kuitenkin ollut päinvastainen. Esimerkiksi Liikenne- ja viestintävirasto Traficom on tarpeettomasti kokoamassa tarkat tiedot eri verkkojen fyysisestä infrastruktuurista yhteen paikkaan keskitettyyn Sijaintitietopalveluun. Energiatehokkuuslakia ollaan muuttamassa siten, että datakeskusten tulisi asettaa tiettyjä tietoja julkisesti saataville, eikä julkisuuslain ajantasaistamisenkaan yhteydessä ole haluttu sisällyttää kriittistä infrastruktuuria tai sen turvajärjestelyä ja niiden toteuttamista koskevaa tietoa salassa pidettävien tietojen määritelmään.

Viimeistään Venäjän Ukrainassa aloittaman hyökkäyssodan jälkeen maailma on muuttunut, eikä kaikkea tietoa kannata enää jakaa avoimesti. Traficom sulki merialueiden syvyystietoja julkaisevan palvelunsa ja myöhemmin myös merikaapeleiden ja muun vedenalaisen infran tiedot poistettiin avoimesta Oskari-tietopalvelusta. Silti esimerkiksi Suomen ja Viron välisessä tietoliikenneyhteyksiä varmentavassa merikaapelissa havaittiin häiriö 7. ja 8.10.2023 välisenä yönä, ja valtionjohto sekä viranomaiset ovat kertoneet, että kaapelia on vahingoitettu tarkoituksella. Liikenne- ja viestintäministeri Lulu Ranne on todennut FiComin verkkosivuille laatimassaan kirjoituksessa, kuinka merikaapelien ja laajemmin merenalaisen infrastruktuurin vahingoittamista käytetään todennäköisesti jatkossakin hybridivaikuttamisen keinona. Merikaapelit ovat otollisia kohteita, koska ne kulkevat väistämättä aluevesiemme ulkopuolella, jolloin viranomaisillamme on rajoittuneet toimivaltuudet.

Pääministeri Petteri Orpon hallitusohjelman mukaan hallitus määrittelee ja tunnistaa yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja varmistaa näiden toimintavarmuuden sekä turvallisuuden (s. 114). Lisäksi hallitusohjelman mukaan kriittisen infrastruktuurin tietojen avoin jakaminen arvioidaan uudelleen huomioiden kansallinen turvallisuus (s. 167), edistäen myös EU:n ja Naton välistä resilienssi- ja varautumisyhteistyötä erityisesti kriittisen infrastruktuurin suojaamiseksi (s. 173). Hallitusohjelman mukaan kyberturvallisuutta vahvistetaan tiiviissä yhteistyössä yritysten, elinkeinoelämän ja kolmannen sektorin kanssa huomioiden se, että iso osa kriittisestä infrastruktuurista on yksityisessä omistuksessa (s. 168). Tavoitteeksi on asetettu, että yhteiskunnan toimintakyvyn kannalta kriittisen infrastruktuurin suojaamista parannetaan, ja lisäksi arvioidaan turvallisuusselvityksen käyttöalan laajentamista kattamaan erityisesti kriittisen infrastruktuurin ja teknologian parissa työskentely (hallitusohjelman s. 178). Kriittisten toimijoiden häiriönsietokyvystä annetun ns. CER-direktiivin kansallisen täytäntöönpanon myötä myös turvallisuusselvityslakiin ehdotetaan muutosta, joka koskee pääsyä välttämätöntä infrastruktuuria koskeviin tietoihin.

Viestintäverkot ovat yhteiskunnan toiminnan kannalta olennaisia, ja siksi niille on eri säädöksissä ja määräyksissä asetettu lukuisia turvallisuus- ja laatuvaatimuksia. Kriittisten infratietojen keskittäminen samanmuotoisena yhteen pisteeseen, tietojen jatkuva siirtely ja ylläpitotoimet kasvattavat tietoturvariskiä. Teleyritykset luovuttavat tietoja lakisääteisesti ja vapaaehtoisesti viranomaisille, mutta myös viranomaisten on osaltaan huolehdittava yhteiskunnan toiminnan kannalta kriittisten tietojen salassa pitämisestä, vaikka ne eivät olisikaan kaikilta osin liikesalaisuuksia. Kriittisen infran tietojen avoin jakaminen on arvioitava uudelleen.

Fyysiseen turvallisuuteen ja kyberpuolustukseen panostettava

Yksi kyberturvallisuuden merkittävä ulottuvuus on fyysisessä maailmassa, mutta fyysinen turvallisuus on kyberturvallisuusstrategiassa kokonaan sivuutettu, vaikka esimerkiksi viestintäverkkojen fyysisestä turvallisuudesta säädetään muun muassa sähköisen viestinnän palveluista annetun lain 243 ja 244 §:ssä ja Traficomin määräyksessä viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Fyysisen verkkoinfrastruktuurin suojaaminen on olennainen osa yhteiskunnan toiminnan kannalta olennaisten digitaalisten palveluiden jatkuvuuden turvaamista kyberuhilta.

Kuten kyberturvallisuusstrategiassakin useassa kohtaa todetaan, kyberuhat kuten sabotaasi, tiedonhankinta, vaikuttaminen ja hyökkäykselliset kyberoperaatiot ovat yhä useammin vihamielisten valtioiden organisoimia tai rahoittamia ja kohdistuvat erityisesti kansallisesti tärkeään infrastruktuuriin kuten viestintäverkkoihin ja -palveluihin. Valtiollisten tahojen kohdistamissa kyberoperaatioissa tulisi myös puolustuksen ja iskujen ennaltaehkäisyn olla valtiolähtöistä, mikä edellyttää riittävää resursointia esimerkiksi poliisille ja Puolustusvoimille.

Vaikka kyberturvallisuusstrategiassa on hyvin tunnistettu riippuvuuksien ymmärtämisen tärkeys ja yhteistyön ja tiedonvaihdon puutteet viranomaisten kesken, tulee siinä sanoa suoremmin, että Suomeen on saatava uskottava kyberpuolustus valtiolliselta tasolta. Suomi tarvitsee puolustuksen kyberrintamalle samaan tapaan kuin muillakin puolustuksen aloilla. Tällä hetkellä puolustus on hyvin pitkälti yritysten vastuulla.

Luottamusta ei rakenneta lisävelvoitteilla

Suuri osa yhteiskunnan toiminnan kannalta kriittisestä infrastruktuurista on yksityisen sektorin omistuksessa. Viranomaisten ja yksityisen sektorin välinen yhteistyö perustuu Suomessa sääntelyn, sopimusten ja palveluiden lisäksi luottamukseen ja vapaaehtoisuuteen, mikä on omiaan helpottamaan tiedonvaihtoa esimerkiksi erilaisista uhkista ja häiriöistä (s. 14). Kansalliset toimialakohtaiset tiedonvaihtoverkostot ovat elinvoimaisia, ja näissä verkostoissa samalla sektorilla kilpailevat yritykset vaihtavat aktiivisesti kyberturvallisuuteen liittyvää tietoa sekä keskenään että julkisen sektorin kanssa (s. 16). Yhteiskunnan eri toimijoiden keskinäinen luottamus sekä luottamus julkisiin instituutioihin ja niiden palveluihin rakentavat vahvaa kansallista resilienssiä. Luottamus on myös onnistuneen kansallisen kyberturvallisuustyön, varautumisen, yhteisesti jaetun tilanneymmärryksen ja oikea-aikaisen reagoinnin edellytys (s. 28).

Kyberturvallisuusstrategian mukaan toimintaympäristön muutoksen vuoksi tiedonvaihto ja siihen käytettävät välineet sekä tilanneymmärryksen muodostaminen eivät kuitenkaan nykyisellään ole riittäviä, ja

lainsäädännön, viranomaisten toimivaltuuksien ja yhteistyörakenteiden ja -verkostojen kehittäminen on välttämätöntä (s. 14). Viranomaisten keskenään koordinoimassa ja analysoimassa tilannekuvassa ja tilanneymmärryksessä on kyberturvallisuusstrategian mukaan kehitettävää, eikä myöskään julkisten palveluiden kyberturvallisuustietoja jaeta nykytilassa riittävästi strategia-, normi-, resurssi- ja informaatio-ohjauksen näkökulmista kaikkien julkisen hallinnon ja elinkeinoelämän toimijoiden välillä (s. 19). Lisäksi tilannetietoja vakavista kyberuhkista olisi voitava jakaa entistä tehokkaammin huoltovarmuuskriittisille yrityksille, kunnille, kuntaomisteisille palveluntarjoajille sekä hyvinvointialueille (s. 34).

Luottamusta ei kuitenkaan rakenneta lisävelvoitteilla. Kyberturvallisuusstrategiassakin todetaan, kuinka tiedonvaihdon tulee olla riittävää, luottamusta ylläpitävää, tasapainoista ja käyttötarkoitussidonnaista perustuen tiedon luovuttamisen ja saamisen oikeuteen sekä intressiin ja oikeuteen jakaa tietoa sitä tarvitsevien kesken (s. 33). Yrityksille on asetettu laajoja velvollisuuksia antaa tietoja viranomaisille. Nykyään yritykset kuitenkin luovuttavat viranomaisille enemmän tietoa kuin mihin niillä on lakisääteinen velvollisuus, koska viranomaisten ja yritysten suhde on luottamuksellinen. Mikäli viranomaiset voisivat helpommin luovuttaa tietoja toisilleen tai esimerkiksi ulkomaisille kollegoilleen, olisi yhteiskunnan etu, että vastavuoroisuuden nimissä myös viranomaiset kertoisivat yrityksille, mitä niiden tietoja on luovutettu ja kenelle. Jos tietoja annetaan ulkomaisille viranomaisille, luovutuksen edellytysten on oltava samat kuin kotimaassa. Yrityksiä kiinnostaa myös viranomaisille luovuttamiensa tietojen turvallisuus ja luovutuksesta mahdolliset aiheutuvat uhat.

Esimerkiksi EU:n verkko- ja tietoturvadirektiivin päivittävää niin sanottua NIS2-direktiiviä kansallisesti täytäntöönpanevaa kyberturvallisuuslakia koskevassa hallituksen esityksessä (HE 57/2024 vp) tarkennettiin Liikenne- ja viestintävirastossa toimivalle CSIRT-yksikölle vapaaehtoisesti luovutettavia tietoja koskevaa 25 §:ää siten, että CSIRT-yksikölle tämän lain mukaisten tehtävien hoitamiseksi vapaaehtoisesti luovutettua tietoa ei saa ilman tiedon luovuttaneen suostumusta käyttää tiedon luovuttajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa. Näin varmistettiin vapaaehtoinen tietojen luovutus CSIRT-yksikön tietoturvaloukkauksiin reagoimista ja niiden tutkimista varten, vaikka samassa virastossa on myös toimijoita koskevaa valvontaa.

Jos tietojen luovutusvelvollisuuksia säädetään lisää, lisääntyy myös sääntelyn epäselvyys ja yritysten hallinnollinen taakka. Pelkästään sähköisen viestinnän palvelulaissa on useita velvollisuuksia, jotka koskevat tietojen luovutusta eri viranomaisille. Lisäksi laissa on runsaasti tietojen käsittelyä eri viranomaisissa koskevia säännöksiä. Luovutus- ja käsittelysäännösten edellytykset poikkeavat toisistaan useissa kohdin, sillä säännöksiä on lisätty ja muutettu vuosien saatossa, eikä kokonaisuus ole enää selkeä. FiComin mielestä Suomessa tulisikin velvollisuuksien lisäämisen sijaan tehdä kokonaisarviointi käsittely- ja luovutusedellytyksistä.

Kuten kyberturvallisuusstrategiassakin sivutaan, kyberturvallisuuden varmistamisen kannalta olennaista on tilanne- ja uhkatiedonjakamisen sujuvoittaminen yritysten ja eri viranomaisten kesken. Uhkatiedon ja tilannekuvan vaihto on pystyttävä varmistamaan kaikissa tilanteissa. Sääntely ei nykyisellään estä tiedonvaihtoa, eikä lisäsääntelylle ole tarvetta. Sen sijaan pirstaleista kansallista sääntelyä olisi syytä selkeyttää, jotta viranomaistahojen ymmärrys ja tulkinta olisi yhteneväistä. Lisäksi tarvitaan turvallisia tiedonvaihtokanavia ja työkaluja, jotta tiedonvaihto viranomaisten ja huoltovarmuuskriittisten toimijoiden

välillä on käytännössä mahdollista. Toimiva tiedonvaihto edellyttää luottamusta, ja sen tulee perustua vapaaehtoisuuteen, mutta on myös hyvä korostaa tiedonvaihdon vastavuoroisuutta ja molemminpuolisuutta. Torjuakseen kyberuhkia myös elinkeinoelämä tarvitsee käyttöönsä viranomaisten keräämää ajantasaista ja kattavaa tilannekuvaa.

Kyberturvallisuuskeskuksen rooli ja sijainti säilytettävä

Kyberturvallisuusstrategiassa kyberhäiriöiden ja -uhkatilanteiden johtamismallia ehdotetaan kehitettäväksi siten, että oikea-aikaisen reagoinnin ja vastatoimien tueksi muodostetaan virastotason yhteistyörakenteessa operatiivisten viranomaisten yhteinen analysoitu tilannekuva. Yhteistyörakenteella ja siihen kuuluvilla viranomaisilla olisi oltava riittävät tiedon luovutus- ja saantioikeudet, jotta toiminnan koordinointi pystytään toteuttamaan. Kansallisen kyberturvallisuuden ja sen edellyttämän viranomaisten tiedonhankinnan, tiedonsaantioikeuden ja tiedonvaihdon painopiste olisi oltava yhteiskunnan elintärkeisiin toimintoihin, kansalliseen turvallisuuteen, maanpuolustukseen ja huoltovarmuuteen kohdistuvien vakavien kyberuhkien ja -rikollisuuden ehkäisyssä ja torjunnassa kaikilla hallinnon tasoilla (s. 37).

Kuten kyberturvallisuusstrategiassakin todetaan, kybertoimintaympäristön turvallisuutta vaarantava tapahtuma voi olla samanaikaisesti tietoturvauhka, rikos sekä kansallista turvallisuutta ja maanpuolustusta vaarantava uhka, jolla on ulko- ja turvallisuuspoliittisia vaikutuksia. Siksi tapahtuman selvitys on useimmiten samanaikaisesti usean viranomaisen vastuulla. Suomessa ei kyberturvallisuusstrategian mukaan kuitenkaan ole riittävässä laajuudessa säädetty viranomaisten välisestä koordinaatiosta ja yhteistoiminnasta kybertoimintaympäristössä, eikä säännöksissä ole otettu riittävästi huomioon kybertoimintaympäristön erityispiirteitä kyberuhkiin vastaamisessa ja tiedonvaihdossa (s. 19).

Viranomaiset, yritykset ja yhteisöt tuottavat nykytilassa tehtäviensä hoitamiseksi tilannekuvia eri tasoilla, eri käyttötarkoituksiin ja erilaisella sisällöllä. Hallinnonalat tuottavat omaa tilannekuvaansa myös valtionjohdon tarpeisiin. Kansallisen kyberturvallisuuden tilannekuvan ylläpidosta ja analysoinnista vastaa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus yhteistyötahojen kanssa, Strategisella tasolla toimivan Kyberturvallisuuden koordinaatioryhmän tavoitteena on varmistaa, että ministeriöillä ja kyberturvallisuusviranomaisilla on yhdenmukainen yleistilannekuva yhteiskunnan kyberturvallisuuden tilasta. Valtion kyberturvallisuusjohtaja toimii valtionjohdon neuvonantajana kyberturvallisuuteen liittyvissä asioissa (s. 19).

Kyberturvallisuusstrategian strategisissa kehittämisehdotuksissa ehdotetaan, että viranomaisten yhteistoimintaa ja yhteistä tilanneymmärrystä kehitetään luomalla tarvittavat yhteistyörakenteet ja koordinointimallit, selkeyttämällä roolit ja vastuut sekä varmistamalla tiedonvaihdon ja tiedonsaannin edellytykset (s. 44).

Yritysten kannalta tärkeintä on, että asiat hoituvat mutkattomasti ja nopeasti. Tällöin hallintorakenteiden vastuut, myös poliittinen vastuu, tulee olla selkeästi jaotellut. Toimialalla pitää kaikilla olla avoimesti viestitty kokonaiskuva asiasta. On yhteinen etu, että mahdollisen kriisin keskellä kaikki tietävät, miten asiat hoidetaan.

On hyvä, että kyberturvallisuusstrategian liitteessä 1 kuvattu hajautettu kyberturvallisuuden kansallinen yhteistoimintamalli Suomessa on strategian lähtökohtana. Jokainen toimija vastaa itse omasta kyberturvallisuudestaan, ja toisaalta jokainen viranomainen vastaa oman sektorinsa osalta kyberturvallisuudesta.

Liikenne- ja viestintäviraston yhteydessä toimiva Kyberturvallisuuskeskus tekee arvokasta työtä kiinteässä yhteistyössä yritysten kanssa. Suomessa viranomaisten ja yritysmaailman luottamuksellinen suhde on keskeistä, sillä maamme kyberturvallisuuden takaavat yritykset. KTK:n tehtävistä valtaosa on lakisääteisiä, nimenomaan televiestinnän sääntelyyn liittyviä. Vaikka toimenkuvaa on viime vuosina laajennettu, selkeä KTK:n ydintehtävä on edelleen teletoimialan ja teleoperaattoreiden kanssa tehtävä yhteistyö.

Tietoliikenneverkot ovat digitaalisen yhteiskuntamme perusta, ja viranomaisista niiden asiantuntemus on Liikenne- ja viestintävirastossa. Kyberturvallisuuskeskuksen siirtämisestä valtioneuvoston kanslian alaisuuteen on aika ajoin keskusteltu, mutta siirto loisi vakavan epävarmuustekijän turvallisuuspoliittisesti herkällä hetkellä. Kansainvälisestikin arvioiden Kyberturvallisuuskeskuksen dynaaminen rooli yritysten tukena ja luotettavana viranomaisena on poikkeuksellinen – siitä kannattaa pitää kiinni.