FiCom ry | Asko Metsola
4.3.2024

FiComin lausunto CER-direktiivin täytäntöönpanosta

Sisäministeriö on pyytänyt lausuntoja luonnoksesta hallituksen esitykseksi eduskunnalle kriittisen infrastruktuurin direktiivin (CER-direktiivi) täytäntöönpanemiseksi. FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- Suomen vallitseva varautumis- ja huoltovarmuusjärjestelmä tulee ottaa paremmin huomioon, kun CER-direktiivi pannaan kansallisesti täytäntöön.
- NIS2-direktiivin velvoitteet ovat digitaalisen infrastruktuurin osalta riittävät, ja esitysluonnoksen soveltamisalan rajauksia koskeva muotoilu pääosin kannatettava.
- Turvallisuusselvityksiä koskeva 28 § tulee ulottaa koskemaan myös digitaalista infrastruktuuria.
- Uuden lain 6 §:n 2 mom 8 kohtaan ehdotettu teknologiaan liittyvän kansallisen turvallisuuden uhan käsittely kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskevassa kansallisessa riskiarvioinnissa tulee poistaa, tai vaihtoehtoisesti digitaalisen infrastruktuurin kriittiset toimijat tulee rajata jo voimassa olevan sääntelyn vuoksi kansallisen riskiarvioinnin ulkopuolelle.
- Kansallinen strategia ja riskiarviointi tulee valmistella laajapohjaisessa yhteistyössä eri ministeriöiden ja muiden viranomaisten sekä yksityisen sektorin kanssa esimerkiksi pysyvässä yhteistyöryhmässä.

Yleiset huomiot CER-direktiivin kansallisesta toteuttamistavasta, kuten esimerkiksi viranomaistoiminnan järjestämisestä ja valvontamallista

Esitysluonnoksessa ehdotettavan uuden, yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annettavan lain 7 §:n mukaan toiminnan yleinen ohjaus, seuranta, yhteensovittaminen ja kehittäminen kuuluisivat sisäministeriölle. Sisäministeriö toimisi CER-direktiivin 9 artiklan 1 kohdan mukaisena toimivaltaisena viranomaisena ja vastaisi direktiivin säännösten asianmukaisesta soveltamisesta ja kansallisesta toimeenpanosta. Esitysluonnoksen mukaan muut ministeriöt vastaisivat toimialoistaan yleisen ohjauksen puitteissa, ja käytännössä sisäministeriö käsittelisi yhteiskunnan kriittisen infrastruktuurin suojaamiseen ja häiriönsietokyvyn parantamiseen liittyviä asioita yhteistyössä toimialoistaan vastaavien valtioneuvoston ministeriöiden ja viranomaisten sekä muiden relevanttien tahojen kanssa.

Kuten esitysluonnoksessakin todetaan, lakiehdotus on lähtökohdiltaan ja periaatteeltaan erilainen kuin Suomen varautumis- tai huoltovarmuusjärjestelmä (esitysluonnoksen s. 72). Kun **CER-direktiivi pannaan kansallisesti täytäntöön, tulee FiComin mielestä nykyluonnosta vahvemmin ottaa huomioon huoltovarmuuskriittisten toimijoiden jatkuvuudenhallinta, jo olemassa olevat varautumisjärjestelyt sekä tukitoimet kriittisiksi määriteltäville toimijoille.**

Huoltovarmuuskeskuksen mukaan CER-direktiivin toimeenpano tulisi rakentaa osaksi nykyistä huoltovarmuusjärjestelmää, jotta Suomeen ei synny päällekkäisiä varautumisjärjestelmiä. Suomen huoltovarmuusjärjestelmä on toiminut yhtenä mallina CER-direktiiville ja vahvistuvalle EU:n yhteiselle

varautumiselle. Erityistä Suomen järjestelmässä on yksityisten yritysten ja viranomaisten pitkäaikaiselle, keskinäiselle luottamukselle rakentuva yhteistyö, jota käytännössä tehdään Huoltovarmuusorganisaation kautta. Huoltovarmuuskeskus on yhdessä eri toimialojen kanssa tunnistanut kriittisiä kohteita ja varmistaa jo nyt yritysten ja muiden viranomaisten kanssa niiden suojaamisen. Uusien velvoitteiden tulisi tukea ja tarpeellisilta osin täydentää yritysten olemassa olevaa, liiketoimintaan kuuluvaa jatkuvuussuunnittelua ja riskienhallintaa. **FiCom yhtyy HVK:n näkemyksiin CER-direktiivin kansallisesta toteuttamistavasta.**

Ehdotettu tehtävä olisi sisäministeriölle kokonaan uusi, kun taas HVK:lla on jo valmiina tarvittava horisontaalinen osaaminen ja verkostot kriittisten sektoreiden varautumisen tukemiseen ja toimijoiden häiriönsietokyvyn vahvistamiseen. Vastaavien toimintojen pystyttäminen uutena kokonaisuutena jonkin toisen organisaation rakenteisiin olisi sekä kustannuksiltaan että työmäärältään suurempi tehtävä. Samalla täytyy kuitenkin ottaa huomioon HVK:n tärkeä rooli yritysten huoltovarmuustyön tukemisessa. Se mm. rahoittaa tarvittavia huoltovarmuusinvestointeja. Tämän takia on äärimmäisen tärkeää varmistaa HVK:n riippumattomuus, eikä HVK:lle saa tulla esimerkiksi vaatimusten ja varautumisen toteutuksen valvontaan liittyviä tehtäviä, koska ne ovat selvästi ristiriidassa investointitukien myöntämiseen liittyvien tehtävien kanssa.

Soveltamisalaa koskevat huomiot, kuten esimerkiksi kriittisen toimijan määrittäminen ja kriteeristön kattavuus

Digitaalinen infrastruktuuri, jota FiComin jäsenyritykset rakentavat ja ylläpitävät, on CER-direktiivissä poikkeussektori. Digitaalisen infrastruktuurin kriittisiin toimijoihin, kuten myös pankki- ja finanssisektorin kriittisiin toimijoihin, kohdistuisi direktiivin 8 artiklan ja johdantokappaleen 20 mukaisesti muihin CER-direktiivin sektoreihin verrattuna rajoitetusti säännöksiä. Nämä säännökset olisivat kriittisten toimijoiden resilienssistrategia (art. 4), riskienarvioinnit (art. 5) ja tukimekanismit (art. 10).

Digitaalisen infrastruktuurin sektorin toimijoiden verkko- ja tietojärjestelmien turvallisuussääntelyä on muun muassa NIS2-direktiivissä, jossa säädetään kattavasti esimerkiksi digitaalisen infrastruktuurin alaan kuuluvien toimijoiden verkko- ja tietojärjestelmien turvallisuuteen kohdistuvista riskienhallintatoimenpiteistä sekä merkittävän poikkeaman raportointivelvoitteista. NIS2-direktiivissä säädettyjen turvallisuusvaatimusten on katsottu olevan vaikutukseltaan vähintään vastaavia kuin CER-direktiivissä säädetyt velvoitteet, ja näitä sovelletaan ensisijaisesti suhteessa CER-direktiiviin. CER-direktiivin 8 artiklan mukaan direktiivin jäsenvaltioiden välistä yhteistyötä koskevaa 11 artiklaa sekä direktiivin kriittisten toimijoiden häiriönsietokykyä koskevaa III lukua, Euroopan kannalta erityisen merkittävä kriittistä toimijaa koskevaa IV lukua ja valvontaa ja täytäntöönpanon valvontaa koskevaa VI lukua ei sovellettaisi niihin digitaalisen infrastruktuurin toimijoihin, jotka on määritelty CER-direktiivin 6 artiklan mukaisesti kriittisiksi. Tämä pitäisi sisällään myös CER-direktiivissä mainitut datakeskuspalvelujen tarjoajat ja sisällönjakeluverkkojen tarjoajat.

Esitysluonnoksessa ehdotettavan uuden, yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annettavan lain soveltamisalan rajauksia koskevan 2 §:n 3 momentin mukaan lain 7 §:n 3 momenttia ja 15–18, 20–23 ja 28 §:iä ei sovellettaisi kriittiseen toimijaan, joka olisi määritetty pankkialan, rahoitusmarkkinoiden infrastruktuurin ja digitaalisen infrastruktuurin toimialoilla. **Ehdotettu vastaa CER-direktiivin 8 artiklaa ja on pääosin kannatettava, lukuun ottamatta lain 6 §:n 2**

momentin 8 kohtaa ja turvallisuusselvitystä koskevaa 28 §:ää myöhemmin lausunnossa tarkennettavista syistä.

Vaikutustenarviointia koskevat huomiot, kuten esimerkiksi yhteiskunnalliset vaikutukset, taloudelliset vaikutukset yrityksille, hallinnollinen taakka ja muut kustannukset sekä vaikutukset yritysten toimintaan

Esitysluonnoksessa ei ole arvioitu ehdotuksen taloudellisia vaikutuksia yrityksille käytännössä lainkaan. Siinä on kuitenkin todettu, että esityksen mukaisten velvoitteiden täytäntöönpano voi lisätä kriittisiksi toimijoiksi määriteltyjen toimijoiden kustannuksia velvoitteiden noudattamisen takia.

Koska sääntely kohdistuu kriittisiksi määriteltäviin, valtaosin yksityisiin toimijoihin, tulisi varautumista koskevan sääntelyn, kuten CER- ja NIS2-direktiivien, yhteisvaikutukset yrityksille tunnistaa ja niiden vaikutukset arvioida tarkkaan. Mikäli sääntelystä aiheutuvat kustannukset siirtyvät merkittävältä osin elinkeinoelämän toimijoiden maksettavaksi, heikentää tämä suomalaisten yritysten kilpailukykyä.

Valvontaa koskevat huomiot

Digitaalinen infrastruktuuri on CER-direktiiviehdotuksessa poikkeussektori, eikä direktiivistä siten aiheudu toimialalle uusia valvontatehtäviä. Esitysluonnoksessa on siksi arvioitu, että CER-direktiivin vaikutukset nykyisten viranomaisten ohjaus- ja valvontatoimintaan olisivat rajalliset. Liikenne- ja viestintävirasto on kuitenkin viime vuosina saanut lukuisia uusia tehtäviä, jotka ovat tuoneet virastolle merkittävästi lisätyötä ja edellyttäneet uutta osaamista ja lisäresursseja. **Liikenne- ja viestintäviraston riittävistä resursseista tulee huolehtia, jotta sekä uudet valvontatehtävät että jo olemassa olevat viraston tehtävät voidaan hoitaa.**

Miten arvioitte turvallisuusselvityslakia koskevan esityksen tarpeellisuutta ja muotoilua? Millaisia turvallisuusvaikutuksia esityksellä olisi?

Esitysluonnoksen 2. lakiesityksessä ehdotetaan turvallisuusselvityslakiin muutosta, joka koskee pääsyä välttämätöntä infrastruktuuria koskeviin tietoihin. Perusmuotoisen henkilöturvallisuusselvityksen piiriin kuuluvia tehtäviä koskevaa turvallisuusselvityslain 19 §:n 1 momentin 4 kohtaa laajennettaisiin siten, että siinä erikseen mainitaan tehtävät, joissa selvityksen kohdehenkilö voi saamiensa salassa pidettävien tietojen oikeudettomalla käytöllä merkittävällä tavalla vaarantaa valtion turvallisuutta tai muuta merkittävää yleistä etua.

Esitysluonnoksen mukaan säännös ei koske pääsyä mihin tahansa välttämättömään infrastruktuuriin liittyviin tietoihin, vaan tietojen käyttämisestä olisi seurattava riski valtion turvallisuuden tai muun merkittävän yleisen edun vaarantumisesta. Säännöksessä tarkoitettua merkitystä voi esitysluonnoksen mukaan olla esimerkiksi ulkomaanliikenteen sataman turvatoimia koskevilla tiedoilla sekä vastaavilla sähkö- ja energiahuoltoa, rahoitus- ja maksuliikennettä sekä keskeistä kuljetuslogistiikkaa koskevilla tiedoilla.

Viitaten myös seuraavaan, CER-yleislain 28 §:ää koskevaan lausuntoon, **myös viestintäverkkoja koskevat tiedot tulee katsoa säännöksessä tarkoitetuksi tiedoiksi, joiden oikeudettomalla käytöllä voi merkittävällä tavalla vaarantaa valtion turvallisuutta tai muuta merkittävää yleistä etua.**

Viestintäverkot ovat kriittistä infrastruktuuria, ja siksi niille on eri säädöksissä ja määräyksissä asetettu lukuisia turvallisuus- ja laatuvaatimuksia. Myös turvallisuusselvityslain esitöissä (HE 57/2013 vp, s. 38) viitataan valtioneuvoston vuonna 2010 tehtyyn yhteiskunnan turvallisuusstrategiaa koskevaan periaatepäätökseen, jonka mukaan kriittiseen infrastruktuuriin ja tuotantoon voidaan lukea muun muassa tietoliikenne- ja tietojärjestelmät. Pääministeri Petteri Orpon hallitusohjelmassa tavoitteeksi on asetettu, että yhteiskunnan toimintakyvyn kannalta kriittisen infrastruktuurin suojaamista parannetaan. Lisäksi arvioidaan turvallisuusselvityksen käyttöalan laajentamista kattamaan erityisesti kriittisen infrastruktuurin ja teknologian parissa työskentely (hallitusohjelman s. 178).

Venäjän 24.2.2022 Ukrainassa aloittaman laittoman hyökkäyssodan myötä Suomen turvallisuustilanne on muuttunut ratkaisevasti. Esimerkiksi Suomen ja Viron välisessä tietoliikenneyhteyksiä varmentavassa merikaapelissa havaittiin häiriö 7.–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 keinovalikoimassa. Merikaapelit ovat otollisia kohteita, koska ne kulkevat väistämättä aluevesiemme ulkopuolella, jolloin viranomaisillamme on rajoittuneet toimivaltuudet.

CER-yleislain 28 §:ään liittyen, miten arvioitte säännösehdotuksia, jotka koskevat muiden EU-jäsenvaltioiden rikosrekisteritietojen käyttämistä kriittisen toimijan työntekijästä tehtävässä turvallisuusselvityksessä?

Esitysluonnoksen mukaan uuden, yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annettavan lain turvallisuusselvitystä koskevassa 28 §:ssä säädettäisiin muiden EU:n jäsenvaltioiden rikosrekistereihin sisältyvien tietojen pyytämisestä tilanteessa, jossa turvallisuusselvityslaissa tarkoitettu henkilöturvallisuusselvitys laaditaan kriittisen toimijan palveluksessa työskentelevästä tai palvelukseen otettavasta henkilöstä. Pykälällä pantaisiin täytäntöön taustatarkistuksia koskeva CER-direktiivin 14 artikla, jonka mukaan kriittisten toimijoiden tulee voida asianmukaisesti perustelluissa tapauksissa esittää taustan tarkistusta koskevia pyyntöjä artiklassa tarkemmin määritellyistä palveluksessaan olevista tai palvelukseen otettavista henkilöistä. **Ehdotettu muotoilu vastaa direktiiviä ja on erittäin kannatettava.**

Esitysluonnoksessa ehdotettavan uuden lain soveltamisalan rajauksia koskevan 2 §:n 3 momentin mukaan lain 28 §:iä ei sovellettaisi kriittiseen toimijaan, joka olisi määritetty pankkialan, rahoitusmarkkinoiden infrastruktuurin ja digitaalisen infrastruktuurin toimialoilla. Ehdotettu vastaa CER-direktiivin 8 artiklaa, mutta **FiComin ja sen digitaalisen infrastruktuurin alalla toimivien jäsenyritysten mielestä uuden lain turvallisuusselvitystä koskeva 28 § tulisi ulottaa koskemaan myös digitaalisen infrastruktuurin toimialan kriittisiä toimijoita.**

Pykälämuutoksen taustalla olevaa CER-direktiivin taustatarkistuksia koskevaa 14 artiklaa ei kriittisten toimijoiden häiriönsietokykyä koskevan III luvun säännöksenä sovelleta digitaalisen infrastruktuurin kriittisiin toimijoihin. Kuten turvallisuusselvityslakiin ehdotetun muutoksen osalta on lausuttu, viestintäverkot ovat

kuitenkin kriittistä infrastruktuuria, ja digitaalisen infrastruktuurin kriittisten toimijoiden palveluksessa on lukuisia direktiivin 14 artiklassa tarkoitettuja henkilöitä, joilla on erityisesti kriittisen toimijan häiriönsietokyvyn kannalta arkaluonteinen rooli tai valtuudet päästä suoraan tai etäyhteydellä sen tiloihin, tietoihin tai valvontajärjestelmiin.

Pankkitoiminnan, finanssimarkkinoiden infrastruktuurin ja digitaalisen infrastruktuurin kriittisiä toimijoita koskevan CER-direktiivin 8 artiklan mukaan jäsenvaltiot voivat hyväksyä kansallisen lainsäädännön säännöksiä saavuttaakseen korkeamman häiriönsietokyvyn tason kyseisten kriittisten toimijoiden osalta edellyttäen, että kyseiset säännökset ovat sovellettavan unionin oikeuden mukaisia. Ehdotettu säännös vastaa unionin oikeutta muilla aloilla toimivien kriittisten toimijoiden osalta. Direktiivi ei siis estä sitä, että ehdotettu 28 §:n sääntely ulotetaan koskemaan myös digitaalisen infrastruktuurin kriittisiä toimijoita, jotta saavutetaan korkeampi häiriönsietokyky.

Muut huomiot

Ehdotetun lain 6 §:n 2 mom 8 kohdan mukaan kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskevassa kansallisessa riskiarvioinnissa on käsiteltävä merkityksellisiä muita uhkia, kuten teknologiaan liittyviä kansallisen turvallisuuden uhkia tai paikkatiedon väärinkäytön uhkaa. Teknologiaan liittyviä kansallisen turvallisuuden uhkia ei ole mainittu asetuksen jäsenvaltioiden suorittamaa riskinarviointia koskevassa 5 artiklassa tai asetuksen johdantokappaleissa. Säännöksen laajennusta ei esitysluonnoksessa ole perusteltu muuten kuin toteamalla, että teknologiaan liittyy kansallisen turvallisuuden uhkia ja teknologiaa liittyviä asioita on suojattava.

Vaikka digitaalinen infrastruktuuri on CER-direktiivissä poikkeussektori, ja sen alalla toimiviin kriittisiin toimijoihin kohdistuisi direktiivin 8 artiklan ja johdantokappaleen 20 mukaisesti muihin CER-direktiivin sektoreihin verrattuna rajoitetusti säännöksiä, direktiivin 5 artiklassa tarkoitettu jäsenvaltion suorittama riskinarviointi otettaisiin esitysluonnoksen mukaan huomioon (esitysluonnoksen s. 19). Koska direktiivin ja sen täytäntöönpanon valvontaa koskevaa VI lukua - ja siten myöskään esitysluonnoksessa ehdotettavan uuden lain valvontaa koskevaa 5 lukua tai sen 20–23 §:iä - ei sovellettaisi digitaalisen infrastruktuurin alan kriittisiin toimijoihin, jää epäselväksi, miten kansallisessa riskinarvioinnissa käsiteltävällä teknologiaan liittyvällä kansallisen turvallisuuden uhalla on tarkoitus vaikuttaa digitaalisen infrastruktuurin kriittisiin toimijoihin. Lisäksi ehdotetun lain 6 §:n 2 mom. 8 kohta on digitaalisen infrastruktuurin kriittisiä toimijoita koskevilta osin päällekkäinen voimassa olevan sähköisen viestinnän palveluista annetun lain sääntelyn kanssa.

Sähköisen viestinnän palveluista annetun lain 244 a §:ssä on erikseen säännelty viestintäverkon kriittisissä osissa käytettävistä laitteista. Pykälän mukaan viestintäverkkolaitetta ei saa käyttää yleisen viestintäverkon kriittisissä osissa, jos on painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta siten, että käytöllä mahdollistettaisiin ulkomainen tiedustelutoiminta tai toiminta, jolla häirittäisiin, lamautettaisiin tai muuten vahingollisella tavalla vaikutettaisiin Suomen tärkeisiin etuihin, yhteiskunnan perustoimintoihin tai kansanvaltaiseen yhteiskuntajärjestykseen. Liikenne- ja viestintävirasto antaa tarkempia määräyksiä viestintäverkkojen, erityisesti niiden kriittisten osien, teknisestä määrittelystä 244 b §:ssä tarkoitetun verkkoturvallisuuden neuvottelukunnan suositukset huomioiden.

Sisäasiainhallinto on yhdessä liikenne- ja viestintäministeriön, puolustushallinnon, ulkoasiainhallinnon, työ- ja elinkeinoministeriön sekä muiden viestintäverkkojen turvallisuuden kannalta keskeisten hallinnonalojen kanssa edustettuna verkkoturvallisuuden neuvottelukunnassa, joten digitaalisen infrastruktuurin kriittisten toimijoiden osalta teknologiaan liittyvät mahdolliset kansallisen turvallisuuden uhat on huomioitu jo voimassa olevassa lainsäädännössä. Tämän vuoksi esitykseen tulee lisätä maininta siitä, että olemassa olevan työn tulokset täytyy ottaa huomioon kansallisessa riskinarvioinnissa.

Uuden lain 6 §:n 2 mom 8 kohtaan ehdotettu teknologiaan liittyvän kansallisen turvallisuuden uhan käsittely kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskevassa kansallisessa riskiarvioinnissa tulee joko poistaa tai vaihtoehtoisesti digitaalisen infrastruktuurin kriittiset toimijat tulee rajata jo voimassa olevan sääntelyn vuoksi kansallisen riskiarvioinnin ulkopuolelle.

Hallituksen esityksessä ei myöskään ole kuvattu kovin selvästi, miten kansallinen strategia (uuden lain 5 §) ja riskiarviointi (6 §) valmistellaan. **Esitykseen on lisättävä, että nämä tulee käsitellä laajapohjaisessa yhteistyössä eri ministeriöiden ja muiden viranomaisten sekä yksityisen sektorin kanssa.** Eri kriittisiä toimialoja koskeva osaaminen on eri ministeriöissä ja niiden alaisissa virastoissa, esimerkiksi teletoimialan osalta liikenne- ja viestintäministeriössä ja Liikenne- ja viestintävirasto Traficomissa. Lisäksi yksityinen sektori vastaa valtaosin kriittisestä infrastruktuurista, minkä vuoksi on tärkeää, että myös sen tietämys ja osaaminen otetaan huomioon em. dokumenttien valmistelussa. Esimerkiksi juuri lausunnoilla olleessa valmiuslain varautumisvelvollisuutta koskevassa muistiossa (VN/5137/2022) yksityisen sektorin kasvanut rooli ja merkitys tunnistetaan ja tunnustetaan.

Parasta olisi, että kansallinen strategia ja riskinarviointi valmisteltaisiin laajapohjaisesti pysyvässä yhteistyöryhmässä. Aihealueiden osaaminen on levittäytynyt yhteiskunnan eri sektoreille, joten valmistelu edellyttää sekä julkisen että yksityisen sektorin toimijoiden kattavaa osallistamista.