TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

Teleyritysten varautuminen normaaliolojen häiriötilanteiden ja poikkeusolojen varalle

Kotimaisen lainsäädännön näkökulma

Kriisi- ja valmiuslainsäädäntö
ON-työ/Tutkielma

Laatija:
Veikka Paasikoski

29.4.2024

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

Tiivistelmäsivu

ON-työ / Tutkielma

Oppiaine: Oikeustiede, Kriisi- ja valmiuslainsäädännön erikoistumisjakso
Tekijä: Veikka Paasikoski
Otsikko: Teleyritysten varautuminen normaaliolojen häiriötilanteiden ja poikkeusolojen varalle: Kotimaisen lainsäädännön näkökulma
Ohjaaja: Jaakko Ossa
Sivumäärä: IV + 25 sivua
Päivämäärä: 29.4.2024

Teleyrityksillä on informaation välittämisen mahdollistajina merkittävä rooli yhteiskunnan toiminnan jatkuvuuden mahdollistamisessa myös erilaisissa häiriötilanteissa ja poikkeusoloissa. Viime vuosina kiristyneen maailmanpolitiikan seurauksena ja Venäjän harjoittaman aggressiivisen ulkopolitiikan myötä riski teleyritysten hallinnoimiin viestintäverkkoihin ja niiden tarjoamiin viestintäpalveluihin kohdistuvista hyökkäyksistä on kohonnut.

Tämän ON-opinnäytetyön pääasiallinen tutkimuskysymys on selvittää, miten teleyritykset velvoitetaan lainsäädännössämme varautumaan normaaliolojen häiriötilanteiden sekä poikkeusolojen varalle. Pääasiasilliseen tutkimuskysymykseen liittyen tutkimuksessa tarkastellaan myös teleyritysten vapaaehtoisuuteen perustuvaa varautumista osana huoltovarmuustoimintaa.

Opinnäytetyön tavoitteena on lainopillisin metodein systematisoida voimassa oleva relevantti varautumissääntely helposti hahmotettavaksi ja päivitetyksi kokonaisuudeksi. Tutkimuksen keskiössä on sähköisen viestinnän palveluista annettu laki, jossa teleyritysten varautumisvelvollisuudesta säädetään. Sen sisällön tulkitsemisen ja systematisoinnin ohella tutkimuksessa otetaan kantaa sääntelyn nykytilaan sekä tarjotaan siihen muutosehdotuksia.

Tutkimuksen perusteella voidaan todeta, että teleyritysten varautuminen normaaliolojen häiriötilanteiden sekä poikkeusolojen varalle varmistetaan kokonaisuutena tarkastellen kattavan ja toimivan laintasoisen sääntelyn avulla. Varautumista tukee myös teleyritysten vapaaehtoisuuteen perustuva yhteistyö etenkin huoltovarmuustoimintaan kuuluvassa Digipoolissa, jossa kehitetään muun muassa alan toimijoiden kyberturvallisuutta. Sähköisen viestinnän palveluista annettuun lakiin sisältyvää teleyritysten velvollisuutta varautumissuunnitteluun voisi kuitenkin joiltain osin päivittää. Varautumissuunnittelun sisällöstä voisi olla paikallaan säätää nykyistä tarkemmin, jotta teleyrityksillä olisi mahdollisimman yhtenevät toimintamallit erilaisten kriisien varalle. Lisäksi varautumissuunnitelmien laintasoista viranomaiskontrollia tulisi lisätä, jotta laadukas varautuminen pystytään mahdollisimman kattavasti turvaamaan.

Avainsanat: teleyritykset, teletoiminta, varautuminen, sähköisen viestinnän palveluista annettu laki, huoltovarmuus, kriittinen infrastruktuuri

Sisällys

Lähteet

Kirjallisuus

Aine, Antti - Nurmi, Veli-Pekka - Ossa, Jaakko - Penttilä, Teemu - Salmi, Ilkka - Virtanen, Vesa, Moderni kriisilainsäädäntö. WSOYpro 2011.

Kolehmainen, Antti, Tutkimusongelma ja -metodi lainopillisessa työssä. Edilex-sarja 2015/29, Asiantuntija-artikkeli 2015.

Liikenne- ja viestintävirasto Traficom. Perustelumuistio 54 C/2021 M liittyen määräykseen viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Traficom 2021.

Mäenpää, Olli, Hallinto-oikeus. 3., uudistettu painos. Alma Talent Oy 2023.

Siltala, Raimo, Oikeustieteen tieteenteoria. Suomalaisen Lakimiesyhdistyksen julkaisuja: A-sarja 2003.

Turvallisuuskomitea. Yhteiskunnan turvallisuusstrategia, valtioneuvoston periaatepäätös. Turvallisuuskomitea 2017.

Virallislähteet

539/2008. Valtioneuvoston päätös huoltovarmuuden tavoitteista.

1048/2018. Valtioneuvoston päätös huoltovarmuuden tavoitteista.

HE 20/2013 vp. Hallituksen esitys eduskunnalle sähkö- ja maakaasumarkkinoita koskevaksi lainsäädännöksi.

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

HE 112/2002 vp. Hallituksen esitys eduskunnalle viestintämarkkinoita koskevan lainsäädännön muuttamisesta.

LiVM 10/2014 vp. Liikenne – ja viestintävaliokunnan mietintö hallituksen esitykseen HE 221/2013.

Sisäministeriö, Kansallisen turvallisuuden yksikkö. Luonnos hallituksen esitykseksi eduskunnalle laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriösietokyvyn parantamisesta ja eräiksi muiksi laeiksi. Sisäministeriö 2024.

TRAFICOM/54045/03.04.05.00/2020. Traficomin määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista.

Viranomaislähteet

Huoltovarmuuskeskus. Ajankohtaisia kysymyksiä ja vastauksia kriittisestä infrastruktuurista ja varautumisesta. Huoltovarmuuskeskus päivitetty, 2.11.2023. https://www.huoltovarmuuskeskus.fi/a/ajankohtaisia-kysymyksia-ja-vastauksia-kriittisesta-infrastruktuurista-ja-varautumisesta (Viitattu 17.2.2024).

Huoltovarmuuskeskus. Huoltovarmuus Suomessa. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/huoltovarmuus-suomessa (Viitattu 17.2.2024). (Huoltovarmuuskeskus a)

Huoltovarmuuskeskus. Huoltovarmuusorganisaatio. https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio (Viitattu 20.2.2024). (Huoltovarmuuskeskus b)

Huoltovarmuuskeskus. HVK on kehottanut kriittisen infrastruktuurin yrityksiä nostamaan varautumistasoa. Huoltovarmuuskeskus 11.10.2023. https://www.huoltovarmuuskeskus.fi/a/hvk-on-kehottanut-kriittisen-infrastruktuurin-yrityksia-nostamaan-varautumistasoa (Viitattu 19.2.2024).

Huoltovarmuuskeskus. Julkisen ja yksityisen sektorin kumppanuus. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/julkisen-ja-yksityisen-sektorin-kumppanuus (Viitattu 17.2.2024). (Huoltovarmuuskeskus c)

Huoltovarmuuskeskus. Poolit: Digipooli. https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta/poolit (Viitattu 18.2.2024). (Huoltovarmuuskeskus d)

Huoltovarmuuskeskus. Sektorit ja poolit. https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit (Viitattu 17.2.2024). (Huoltovarmuuskeskus e)

Sisäministeriö. Kyberturvallisuus osana kansallista turvallisuutta. https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus (Viitattu 28.2.2024). (Sisäministeriö a)

Sisäministeriö. Lainsäädäntöhanke: Kriittisen infrastruktuurin tunnistaminen ja kriisinkestävyyden parantaminen. https://intermin.fi/hankkeet/hankesivu?tunnus=SM047:00/2022 (Viitattu 7.3.2024). (Sisäministeriö b)

Traficom. Mikä on teletoimintaa? Päivitetty 23.9.2023. https://www.traficom.fi/fi/viestinta/viestintaverkot/mika-teletoimintaa (Viitattu 18.2.2024).

Turvallisuuskomitea. Mikä on yhteiskunnan turvallisuusstrategia 2017? https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/ (Viitattu 15.2.2024).

Työ- ja elinkeinoministeriö. Huoltovarmuus ja elintärkeiden toimintojen turvaaminen työ- ja elinkeinoministeriön hallinnonalalla. https://tem.fi/elintarkeiden-toimintojen-turvaaminen (Viitattu 18.2.2024).

Muut lähteet

Ficom. Digipooli – mitä, miksi ja kenelle? Ficom 22.10.2019. https://ficom.fi/ajankohtaista/uutiset/digipooli-mita-miksi-ja-kenelle/ (Viitattu 1.3.2024).

Laukkanen, Jonna. ”Ruotsalaisasiantuntija: Venäjä voi ottaa Itämeren datakaapelit kohteekseen: ”Uhka on suuri”. Ilta-Sanomat 6.3.2024. https://www.is.fi/ulkomaat/art-2000010272930.html (Luettu 7.3.2024).

Pekki, Jaakko, Huoltovarmuuskeskuksen operatiivisen osaston johtaja. Kriisi- ja valmiuslainsäädäntö-kurssilla pidetty luento 29.1.2024. Turun yliopisto.

1 Johdanto

Viime vuosina kiristynyt maailmanpolitiikan tilanne on johtanut siihen, että Suomessa on alettu keskustelemaan entistä enemmän erilaisiin yhteiskuntaan kohdistuviin uhkiin varautumisesta. Termit kuten hybridivaikuttaminen, kyberhyökkäys ja kriittisen infrastruktuurin suojaaminen ovat tulleet uutisia seuraaville tutuiksi. Erilaisiin kriiseihin ja häiriötilanteisiin varautuminen onkin tällä hetkellä ajankohtaisempaa kuin pitkään aikaan esimerkiksi Venäjän Ukrainaan aloittaman hyökkäyssodan ja Suomen Nato-jäsenyyden myötä. Yhteiskunnallisen varautumisen kannalta keskeisessä asemassa on myös kriittisen infrastruktuurin, kuten viestintäverkojen ja -palvelujen suojaaminen erilaisten häiriötilanteiden varalle. Viime lokakuussa uutisoitiin Balticconnector-kaasuputkessa havaitusta vuodosta ja sen yhteydessä havaitusta Suomen ja Viron välillä kulkevan tietoliikennekaapelin vauriosta. Huoltovarmuuskeskuksen raportin mukaan kaapelin vaurioituminen ei vaikuttanut Suomen kannalta kriittisiin tietoliikenneyhteyksiin ja raportissa korostettiin, että Suomessa kriittiset yhteydet on varmistettu usean järjestelyn kautta.[1]

Tapahtuma kuitenkin herättää kysymyksen siitä, kenen vastuulla kriittiseen infrastruktuuriin kuuluvien erilaisten verkkoyhteyksien ja -palveluiden suojaaminen yhteiskunnassa on. Vaikka arkielämässä asiaa ei tule useinkaan ajatelleeksi, on itse asiassa yrityksillä merkittävä rooli erilaisiin häiriötilanteisiin ja kriiseihin varautumisessa.

Koska yritysten rooli kriisinhallinnassa on merkittävä, tässä tutkielmassa perehdytään siihen, miten yritykset, tarkemmin teleyritykset, velvoitetaan lainsäädännössämme varautumaan erilaisten häiriötilanteiden ja poikkeusolojen varalle. Lisäksi tarkastellaan teleyritysten vapaaehtoisuuteen perustuvaa varautumista. Näkökulma on tilan rajallisuuden, mutta myös aiheen ajankohtaisuuden vuoksi rajattu juuri teleyrityksiin. Tämän vuoksi on hyvä jo aluksi määritellä, minkälaisia yrityksiä teleyrityksillä tarkoitetaan.

Teleyrityksen juridinen määritelmä löytyy sähköisen viestinnän palveluista annetusta laista (LSVP, 917/2014). Sen 1 luvun 3 §:n 2 momentin 27 kohdassa teleyritykseksi määritellään yritys, ”joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa teletoimintaa”. Verkkopalvelulla tarkoitetaan saman momentin 34 kohdan mukaan palvelua, ”jossa teleyrityksen omistamaa tai hallinnoimaa viestintäverkkoa

[1] Huoltovarmuuskeskus 2.11.2023

tarjotaan käytettäväksi viestien siirtoon tai jakeluun”. Viestintäpalvelulla puolestaan tarkoitetaan 2 momentin 37 kohdan mukaan palvelua, ”joka muodostuu kokonaan tai pääosin viestien siirtämisestä viestintäverkossa sekä siirto- ja lähetyspalvelua joukkoviestintäverkossa ja henkilöiden välisen viestinnän palvelua”. Tällaisia verkko- ja viestintäpalveluita tarjoavia teleyrityksiä ovat Suomessa esimerkiksi Telia Finland Oyj, Dna Oyj ja Elisa Oyj.

Jotta teleyrityksiä koskeva lainsäädäntö soveltuisi yritykseen, tulee sen siis harjoittaa yleistä teletoimintaa. Tämä poissulkee säännösten soveltamisalasta muun muassa yritykset, jotka tarjoavat verkko- ja viestintäpalveluita yrityksensä sisäiseen käyttöön sekä koulut, jotka tarjoavat palveluita opiskelijoilleen. Tällaisissa tapauksissa palveluiden kohteena on ennalta rajattu käyttäjäpiiri. Lisäksi on huomattava, että viestinnän sisältö ei ole teletoimintaa. Näin ollen esimerkiksi videoiden tarjoaminen nettisivuilla tai keskustelupalstojen ylläpito ei ole teletoimintaa. ICT-palvelut, kuten laitteiden tai ohjelmistojen tarjoaminen, eivät nekään kuulu teletoiminnan alaan. [2]

Pelkistäen voisikin sanoa, että teleyritykset mahdollistavat informaation kulun yhteiskunnassa. Tämä korostaa niiden merkitystä yhteiskunnan varautumisessa erilaisiin häiriötilanteisiin ja poikkeusoloihin, joiden aikana on vielä normaalioloja tärkeämpää varmistaa tiedonkulku yhteiskunnassa.

[2] Traficom 23.9.2023

2 Tutkielman tutkimuskysymykset ja -metodit sekä tiedonintressi

Tutkielman pääasiallinen tutkimuskysymys on se, miten teleyritykset velvoitetaan lain ja viranomaisten määräysten nojalla varautumaan normaaliolojen häiriötilanteiden ja poikkeusolojen varalle. Tähän liittyvänä alakysymyksenä tutkielmassa selvitetään myös yleisellä tasolla, miten teleyritykset osallistuvat varautumiseen sopimusten ja vapaaehtoisuuden nojalla. Tiedonintressinä on sekä systematisoida että tulkita tutkimuskysymyksen osalta relevanttia oikeutta. Lisäksi tutkielmassa otetaan paikoin kantaa siihen, miten onnistunutta teleyrityksiä velvoittava varautumissääntely ja annetaan mahdollisia muutosehdotuksia.

Teleyritysten varautumisvelvollisuuksia lainopillisesta näkökulmasta käsittelevää tutkimusta on tällä hetkellä hyvin niukasti. Aihetta sivuavat julkaisut, kuten Puolustustaloudellisen suunnittelukunnan ohjeet ”Tietotekniikan turvallisuus ja toiminnan varmistaminen” (2002) ja ”Viestintäverkkojen ja viestintäpalveluiden varmistaminen” (2005) ovat jo varsin vanhoja. Tutkielman tavoitteena onkin systematisoida voimassa oleva relevantti varautumissääntely helposti hahmotettavaksi ja päivitetyksi kokonaisuudeksi. Lisäksi relevantien normien tulkinnalla pyritään tutkielmassa avaamaan sitä, mihin eri normit käytännössä teleyrityksiä velvoittavat.

Metodina tutkielmassa käytetään lainoppia. Lainopilla tarkoitetaan lyhyesti voimassa olevan oikeuden sisällön tulkintaa ja systematisointia sekä eri oikeusperiaatteiden punnintaa.[3] Oikeusnormien tulkintaan käytetään tutkielmassa lainoppiin kuuluvaa oikeuslähdeoppia, tarkemmin staattista oikeuslähdeoppia, jossa eri oikeuslähteiden velvoittavuuden asteet ovat ennalta vakioidut. Staattisessa oikeuslähdeopissa eri oikeuslähteet jaotellaan vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin.[4]

Vahvasti velvoittavista oikeuslähteistä tutkielmassa keskitytään voimassa olevaan lainsäädäntöön. Tutkimuskysymyksiin haetaan vastauksia kotimaisesta näkökulmasta keskittyen kotimaisen lainsäädännön tutkimiseen. Heikosti velvoittavista oikeuslähteistä paneudutaan tutkielmassa ainoastaan lainvalmisteluaineistoon, erityisesti relevantteihin hallitusten esityksiin. Tutkimuskysymysten kannalta relevanttia, heikosti velvoittaviin oikeuslähteisiin myös kuuluvaa korkeimman oikeuden oikeuskäytäntöä ei ole, joten siihen ei

[3] Siltala 2003, s. 67
[4] Kolehmainen 2015, s. 10

tutkimuskysymyksiin vastatessa voida tukeutua. Sallituista oikeuslähteistä paneudutaan jonkin verran relevanttiin oikeuskirjallisuuteen sekä aihetta käsitteleviin viranomaislähteisiin.[5] Teleyrityksien varautumiseen liittyvää kirjallisuutta ei juurikaan ole, mutta tutkielmassa hyödynnetään eräiltä osin yleistä hallinto-oikeudellista kirjallisuutta teleyrityksiä koskevan lainsäädännön tulkinnan helpottamiseksi.

Lisäksi tutkielmassa pyritään avaamaan kriiseihin varautumisen isoa kuvaa, jonka pohjalta tutkimuskysymysten osalta relevantteja lakeja ja määräyksiä on annettu. Tässä yhteydessä perehdytään erityisesti erilaisiin viranomaislähteisiin, kuten Huoltovarmuuskeskuksen ja Turvallisuuskomitean raportteihin ja artikkeleihin.

[5] Eri oikeuslähteiden velvoittavuudesta ks. Kolehmainen 2015 s. 10–11

3 Huoltovarmuus ja kriittisen infrastruktuurin suojaaminen

3.1 Huoltovarmuuden turvaaminen Suomessa

Ennen teleyrityksiä velvoittavan lainsäädännön tutkimista, on syytä tarkastella sääntelyn lähtökohtia sekä pakollisen varautumisen ohella tärkeää vapaaehtoista varautumista. Normaalioloissa yhteiskunnallisen varautumisen lähtökohtana on valtioneuvoston periaatepäätös ”Yhteiskunnan turvallisuusstrategia 2017 (YTS 2017)”. Olennainen osa turvallisuusstrategiaa on siinä esitetty yhteistoimintamalli, jonka pohjalta Suomessa varaudutaan ja toimitaan erilaisissa häiriötilanteissa. Suomalaista kokonaisturvallisuuden toimintamallia voi pitää kansainvälisestä näkökulmasta uniikkina, sillä se perustuu laaja-alaiseen yhteistyöhön viranomaisten, elinkeinoelämän, kansalaisten ja kansalaisjärjestöjen välillä. Turvallisuusstrategian pohjalta varaudutaan normaaliolojen häiriötilanteiden lisäksi myös poikkeusoloihin.[6]

Strategiassa korostetaan yhteiskunnan eri toimijoiden, kuten valtion, kuntien ja elinkeinoelämän yhteistyötä erilaisiin uhkiin varautumisessa.[7] Lisäksi siinä on kuvattu ”yhteiskunnan toimivuuden kannalta välttämättömät, kaikissa tilanteissa ylläpidettävät toimintokokonaisuudet”.[8] Näistä tutkielman keskiössä olevien teleyritysten toimintaan vaikuttavat erityisesti talouden, infrastruktuurin ja huoltovarmuuden turvaamista koskeva osa-alue.

Huoltovarmuudella tarkoitetaan Huoltovarmuuskeskuksen mukaan ”varautumista mahdollisiin kriiseihin ja häiriötilanteisiin sekä jatkuvuudenhallintaa turvaamalla elintärkeät toiminnot, jotta yhteiskunta ja elinkeinoelämä toimivat ja ihmiset voivat turvallisesti elää arkeaan”.[9] Huoltovarmuuden turvaaminen toteutetaan yksityisen ja julkisen sektorin sekä erilaisten järjestöjen yhteistyönä. Näin ollen yhteiskunnan turvallisuusstrategiassa korostettu yhteistyö eri yhteiskunnan toimijoiden välillä konkretisoituu käytännön tasolla huoltovarmuuden turvaamisessa. Työ- ja elinkeinoministeriön alaisuudessa toimivan Huoltovarmuuskeskuksen tehtävänä työ- ja elinkeinoministeriön mukaan on yhteensovittaa

[6] Turvallisuuskomitea 2023
[7] Turvallisuuskomitea 2017, s. 7–8
[8] Turvallisuuskomitea 2017, s. 14
[9] Huoltovarmuuskeskus a

viranomaisten ja elinkeinoelämän välistä yhteistyötä varautumisessa sekä vastata valtion varmuus- ja turvavarastojen hoidosta.[10]

Huoltovarmuustoiminta jakautuu eri sektoreihin, joita ovat muun muassa energiahuolto, elintarvikehuolto sekä tietoyhteiskunnan turvaaminen. Huoltovarmuuden turvaamisella on myös lainsäädännöllinen perusta. Sitä sääntelee huoltovarmuuden turvaamisesta annettu laki (1390/1992). Laissa säädetään huoltovarmuuden turvaamisesta yleisellä tasolla määrittämällä esimerkiksi huoltovarmuudesta vastuussa olevat viranomaiset, niiden tehtävät sekä säätämällä yleisesti huoltovarmuuteen liittyvästä yhteistyöstä eri toimijoiden välillä. Käytännön huoltovarmuustyön ja siihen liittyvän yhteistyön järjestäminen jää kuitenkin viranomaisten ja erilaisten verkostojen, kuten Huoltovarmuuskeskuksen ja Huoltovarmuusorganisaation varaan. Lisäksi ministeriöt kehittävät huoltovarmuuden turvaamisesta annetun lain mukaan huoltovarmuutta omailla toimialaloillaan.

3.2 Julkisen ja yksityisen sektorin sopimusperusteinen yhteistyö varautumisessa

Huoltovarmuustyön edellyttämä yhteistyö julkisen ja yksityisen sektorin välillä toteutetaan sekä huoltovarmuussektoreilla että huoltovarmuuspooleissa.[11] Huoltovarmuussektorit, -poolit sekä -toimikunnat ovat osa Huoltovarmuusorganisaatiota. Huoltovarmuusorganisaatio, johon kuuluvat myös Huoltovarmuuskeskus, sen hallitus sekä huoltovarmuusneuvosto, mahdollistaa huoltovarmuuden kannalta tärkeän yhteistyön toteuttamisen.[12] Sektoreilla, jotka on jaettu eri huoltovarmuuden painopisteiden mukaan, toimialan merkittävimmät yritykset ja viranomaiset yhdessä ohjaavat ja koordinoivat oman alansa varautumista sekä asettavat tavoitteet oman alansa pooleille.[13]

Huoltovarmuuspoolit ovat hyvä esimerkki yritysten kriiseihin ja häiriötilanteisiin varautumisen vapaaehtoisesta ulottuvuudesta. Poolien perustaminen tapahtuu nimittäin yritysten ja niiden etujärjestöjen kanssa tehtävillä vapaaehtoisilla sopimuksilla.[14] Toimialakohtaisesti muodostetuissa pooleissa suurin vetovastuu on elinkeinoelämällä, ja niissä huolehditaan toimialan operatiivisesta varautumisesta sekä määritellään kyseisellä

[10] Työ- ja elinkeinoministeriö
[11] Huoltovarmuuskeskus c
[12] Huoltovarmuuskeskus b
[13] Huoltovarmuuskeskus c
[14] Aine ym. 2011, s. 114

toimialalla huoltovarmuuden turvaamisen kannalta kriittiset yritykset. Pooleissa korostuu tiivis yhteistyö toimialalla toimivien yritysten kesken.[15]

Teleyritykset kuuluvat digipooliin, joka Huoltovarmuuskeskuksen mukaan on ”tietotekniikka- ja tietoverkkoalan sekä viranomaisten välinen verkosto”. Kyseiseen pooliin kuuluu tele- ja muiden yritysten lisäksi myös viranomaisista Liikenne ja viestintävirasto Traficom, Puolustusvoimat ja Huoltovarmuuskeskus. Digipoolin tehtäviin kuuluu muun muassa tilannekuvan muodostaminen oman toimialan huoltovarmuudesta. Lisäksi se tuottaa ja jakaa kyberturvallisuuden tilannekuvaa yhdessä yritysten ja viranomaisten kanssa sekä ohjaa ja seuraa oman alansa yritysten varautumista.[16] Oleellista teleyritysten kannalta on myös se, että digipoolissa määritellään, mitkä teleyritykset ovat huoltovarmuustoiminnan kannalta kriittisiä.

Digipoolin merkitystä teleyritysten varautumisessa korostaa se, että sen sisällä kehitetään myös yritysten kyberturvallisuutta ja jatkuvuudenhallintaa.[17] Kyberturvallisuuden kehittämisen taustalla on sisäministeriön mukaan tarve suojata yhteiskuntaa tai yhteiskunnan toimintakykyä vihamieliseltä kybervaikuttamiselta ja tietoverkkotiedustelulta.[18] Kyberturvallisuuteen panostaminen on teleyritysten toiminnan kannalta keskeistä, sillä kyberuhat kohdistuvat teleyritysten hallinnoimiin ja omistamiin tietoverkkoihin. Vapaaehtoisuuteen ja sopimuksiin perustuva varautuminen on siis lainsäädännön ohella tärkeässä roolissa teleyritysten häiriötilanteisiin ja poikkeusoloihin liittyvässä varautumisessa.

3.3 Kriittisen infrastruktuurin suojaaminen

Huoltovarmuuden turvaamisen kannalta keskeistä on myös yhteiskunnan kriittisen infrastruktuurin suojaaminen. Kriittinen infrastruktuuri on huoltovarmuuden tavoitteista annetussa valtioneuvoston päätöksessä 1048/2018 määritelty ”perusrakenteiksi, palveluiksi sekä niihin liittyviksi toiminnoiksi, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi”.[19] Kriittistä infrastruktuuria eivät siis ole ainoastaan perinteisemmät fyysiset laitokset ja kriittiset rakenteet, vaan etenkin tietoyhteiskunnassa korostuvat digitaaliset palvelut ja toiminnot, kuten tieto- ja viestintäjärjestelmät. Huoltovarmuuskeskuksen julkaisemassa tiedotteessa ”Ajankohtaisia kysymyksiä ja vastauksia kriittisestä infrastruktuurista ja varautumisesta” korostetaan sitä, että kriittisten yritysten,

[15] Huoltovarmuuskeskus e
[16] Huoltovarmuuskeskus d
[17] Ficom 22.10.2019
[18] Sisäministeriö a
[19] 1048/2018, s. 4

kuten teleyritysten, tulee itse vastata omistamansa tai hallinnoimansa kriittisen infrastruktuurin suojaamisesta.[20] Tämä ei sulje pois sitä, että tällaiset yritykset voivat ulkoistaa kriittisen infrastruktuurin suojaamisen tai sen ylläpitämiseen liittyvät palvelut. Vastuu suojaamisesta on silti sillä yrityksellä, joka omistaa kriittisen infrastruktuurin.[21] Yksityisille yrityksille asetettu vastuu kriittisen infrastruktuurin suojaamisesta on luonnollista ottaen huomioon, että suurin osa kriittisestä infrastruktuurista on yksityisen sektorin omistuksessa.[22]

Kriittiseen infrastruktuuriin kuuluvien verkko- ja viestintäpalveluiden omistajina ja hallinnoijina teleyrityksillä on siis vastuu niiden suojaamisesta. Suomen kaltaisessa tietoyhteiskunnassa verkko- ja viestintäpalvelut mahdollistavat informaation kulun yhteiskunnassa. Mikäli niiden toiminta vakavasti häiriintyisi, vaikuttaisi se monen kriittisen toimialan toimintaan ja vaarantaisi näin koko yhteiskunnan normaalin toiminnan jatkumisen. Lisäksi yhteiskuntaan kohdistuvien uhkien ehkäisyssä ja selvittämisessä informaation nopea kulkeminen viranomaisten ja muiden tärkeiden toimijoiden välillä on tärkeää. Samasta syystä myös poikkeusolojen, kuten sodan tai pandemian aikana, verkko- ja viestintäpalvelujen merkitys korostuu.

Verkko- ja viestintäpalveluiden merkittävä rooli yhteiskunnan toiminnan jatkumisen turvaamisessa on varmasti keskeinen syy sille, että lainsäätäjä on katsonut tarpeelliseksi varmistaa teleyritysten riittävän varautumisen lailla ja antanut viranomaisille toimivallan tarkentaa varautumisvelvollisuuksien sisältöä määräyksien avulla. Huoltovarmuuden turvaamiseen ja sen osana kriittisen infrastruktuurin suojaamiseen liittyvät tavoitteet ovatkin huomattavissa teleyrityksiä koskevassa varautumissääntelyssä.

[20] Huoltovarmuuskeskus 2.11.2023
[21] Huoltovarmuuskeskus 2.11.2023
[22] Huoltovarmuuskeskus 11.10.2023

4 Teleyritysten laintasoiset varautumisvelvollisuudet

4.1 Varautumisen lähtökohdat

Vaikka kriiseihin ja häiriötilanteisiin varautumisessa julkisen ja yksityisen sektorin yhteistyöhön ja sopimuksiin perustuva varautuminen on tärkeää, on varautumisvelvollisuuksista kriittisillä aloilla toimiville yrityksille säädetty myös lailla. Tällaisista varautumisvelvollisuuksista säädetään useissa toimialakohtaisissa erityislaeissa, kuten sähkömarkkinalaissa (588/2013), vesihuoltolaissa (119/2001) sekä liikenteen palveluista annetussa laissa (liikennepalvelulaki, 320/2017).[23] Tämän tutkielman kannalta relevantein laki on sähköisen viestinnän palveluista annettu laki (LSVP, 917/2014). Kyseinen laki velvoittaa teleyrityksiä varautumaan sekä normaaliolojen häiriötilanteiden että valmiuslain tarkoittamien poikkeusolojen varalle.

Häiriötilanteiden ja poikkeusolojen määritelmät löytyvät edellä mainitusta Yhteiskunnan turvallisuusstrategia 2017 -periaatepäätöksestä. Sen mukaan häiriötilanteilla tarkoitetaan ”uhkaa tai tapahtumaa, joka vaarantaa yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää”.[24] Yhteiskunnan elintärkeät toiminnot on samaisessa periaatepäätöksessä määritelty ”yhteiskunnan toimivuuden kannalta välttämättömiksi, kaikissa tilanteissa ylläpidettäviksi toimintakokonaisuuksiksi”.[25] Tällaisia toimintakokonaisuuksia ovat esimerkiksi yhteiskunnan puolustuskyky, sisäinen turvallisuus sekä talous, infrastruktuuri ja huoltovarmuus. Näitä vaarantavia uhkia ja tapahtumia voivat olla esimerkiksi vakavat luonnon onnettomuudet, mutta myös terrori-iskujen tai kyberhyökkäysten kaltaiset ihmisten aiheuttamat häiriötilanteet. Häiriötilanteet eivät välttämättä kohdistu koko yhteiskuntaan, vaan ne voivat olla myös paikallisia tai alueellisia, kuten vain tietylle alueelle kohdistuvat myrskytuhot.[26]

Poikkeusoloilla tarkoitetaan yhteiskunnan turvallisuusstrategian mukaan puolestaan valmiuslaissa tarkoitettua yhteiskunnan tilaa, ”jossa on niin paljon tai niin vakavia häiriöitä tai uhkia, että on tarpeen mahdollistaa viranomaisten tavanomaisesta poikkeava toimivaltuuksien

[23] Pekki, Jaakko 29.1.2024
[24]Turvallisuuskomitea 2017, s. 97
[25] Turvallisuuskomitea 2017, s. 14
[26] Turvallisuuskomitea 2017, s. 97

käyttö”.[27] Toisin sanoen normaaliolojen tai normaalioloissa esiintyvien häiriötilanteiden hoitamiseen annetut toimivaltuudet eivät enää poikkeusoloissa ole riittäviä yhteiskunnan toiminnan turvaamisen takaamiseen. Tämän vuoksi poikkeusoloiksi voidaan lukea vain hyvin vakavat erityistilanteet, jotka on kuvattu valmiuslaissa ja puolustustilalaissa.[28]

4.2 Teleyritysten yleinen varautumisvelvollisuus sekä velvollisuus varautumissuunnitteluun

Sähköisen viestinnän palveluista annetun lain 35 luvun 281 §:n ensimmäinen momentin mukaan ”Teleyrityksen on huolehdittava siitä, että sen toiminta jatkuu mahdollisimman häiriöttömästi myös normaaliolojen häiriötilanteissa sekä valmiuslaissa tarkoitetuissa poikkeusoloissa”. Kyseistä momenttia voidaan pitää ikään kuin teleyritysten yleisenä varautumisvelvollisuutena.

Varautumisvelvollisuuden tarkempaa sisältöä tulkittaessa on syytä perehtyä tarkastelevan lain esitöihin, sillä teleyritysten varautumisvelvollisuutta koskevaa oikeuskäytäntöä ei ole. LSVP:n esitöihin kuuluvan hallituksen esityksen HE 221/2013 281 §:ää koskevissa perusteluissa todetaan, että pykälän tarkoituksena on ”myös jo normaalioloissa varmistaa se, että sähköisen viestinnän kannalta keskeiset toiminnot jatkuvat erilaisissa häiriö- ja kriisitilanteissa”.[29] Tämä osuus perusteluista liittyy kriisi- ja valmiuslainsäädännön kantaviin teemoihin, eli yhteiskunnan toiminnan turvaamiseen kaikenlaisissa tilanteissa. Teleyritysten vastuu jo normaalioloissa varmistaa toimintojensa jatkuminen erilaisissa häiriö- ja kriisitilanteissa on luontevaa, sillä normaalioloissa tehtävistä vastuussa olevilla tahoilla on alansa ammattilaisina paras tietämys siitä, mitä tehtävien hoitaminen erilaisissa erityistilanteissa vaatii. Täten normaalioloissa verkko- ja viestintäpalveluiden toiminnasta vastaavilla teleyrityksillä on velvollisuus huolehtia, että kyseiset palvelut toimivat myös häiriötilanteiden ja poikkeusolojen aikana. Eduskunnan liikenne- ja viestintävaliokunta hyväksyi edellä mainitun hallituksen esityksen varautumista koskevien pykälien osalta vain pienin muutoksin, mikä vahvistaa esityksen painoarvoa tulkittaessa teleyritysten varautumisvelvollisuuden tarkempaa sisältöä.[30]

---

[27] Turvallisuuskomitea 2017, s.97
[28] Aine ym. 2011 s. 17
[29] HE 221/2013 vp, s. 203
[30] LiVM 10/2014 vp, s. 42-43

Konkreettisemmin varautumisvelvollisuudella tarkoitetaan esityksen perusteella sitä, että laissa tarkoitetut teleyritykset ovat velvollisia huolehtimaan tarvittavilla etukäteisvalmisteluilla, toimenpiteillä ja suunnitelmilla siitä, että ne pystyvät jatkamaan toimintaansa häiriöttömästi erilaisissa olosuhteissa.[31] Varautumisvelvollisuus konkretisoituu esimerkiksi riskiarvioon perustuvassa varautumissuunnittelussa, josta säädetään LSVP:n 35 luvun 282 §:n ensimmäisessä momentissa. Sen mukaan varautumisvelvollisen on arvioitava riskit, jotka voivat vaarantaa toiminnan jatkuvuuden, ja sen on niiden perusteella suunniteltava, miten sen toiminta jatkuu normaaliolojen häiriötilanteissa ja valmiuslain 9 luvun mukaisia toimivaltuuksia käytettäessä. Varautumissuunnittelun tarkoituksena on, että teleyritykset arvioivat viestintäverkkojensa ja -palveluidensa toimintavarmuutta erilaisissa häiriötilanteissa sekä poikkeusoloissa.[32] Kun verkkojen ja palveluiden toimintavarmuutta arvioidaan jo normaalioloissa, antaa se luonnollisesti teleyrityksille paremman käsityksen siitä, mitä järjestelyitä sen tarjoamien palveluiden järjestäminen vaatii häiriötilanteiden ja poikkeusolojen aikana.

Varautumissuunnittelu perustuu riskiarvioon, jossa teleyritykset arvioivat toimialalleen ja toimintaympäristölleen mahdollisia uhkia ja häiriöitä sekä tekevät suunnitelmia niiden varalle. Eri teleyritysten toimintaa vaarantavat uhat saattavat olla hyvin erilaisia teleyrityksen maantieteellisestä toiminta-alueesta ja toimialasta riippuen. Keskeistä onkin, että teleyrityksien suorittamissa riskiarvioissa otetaan huomioon juuri heidän toiminta-alueelleen ja -ympäristölleen keskeiset uhkatekijät ja riittävällä suunnitelmallisuudella varaudutaan näiden torjumiseen.[33] Lisäksi suunnittelussa olisi HE 221/2013:n perusteella hyvä ottaa huomioon teleyrityksen omistamien tai hallinnoimien viestintä- ja verkkopalveluiden vaikutukset niitä käyttävien, huoltovarmuuden kannalta tärkeiden sektoreiden, kuten energiahuollon-, kuljetus- ja terveydenhuoltosektorin hyödykkeiden tuottajien toimintaan.[34] Tästä huomataan, että varautumisvelvollisuuden säätämisen taustalla ovat olleet selkeästi myös huoltovarmuuden turvaamisesta kumpuavat tavoitteet. Vapaaehtoisen varautumisen ohella lainsäätäjä on halunnut varmistaa huoltovarmuuden turvaamisen kannalta oleellisen varautumisen myös lainsäädännöllisen keinoin.

[31] HE 221/2013 vp, s. 201
[32] HE 221/2013 vp, s. 201
[33] HE 221/2013 vp, s. 203
[34] HE 221/2013 vp, s. 204

HE 221/2013:n mukaan riskien arviointiin sisältyy keskeisesti myös kriittisten viestintäjärjestelmien määritteleminen. Esitys sitoo kriittisten viestintäjärjestelmien määrittelyn tärkeyden valtioneuvoston päätökseen huoltovarmuuden turvaamisesta (539/2008).[35] Sen mukaan ”kriittisimmät ja keskeisimmät tietotekniikan varassa olevat yhteiskunnan toiminnot tulee tunnistaa ja niihin liittyvät tietojärjestelmäratkaisut ja -palvelut tulee varmistaa erilaisia vakavia häiriöitä ja poikkeusoloja kestävillä järjestelyillä”.[36]

Teleyrityksillä on velvollisuus arvioida, mitkä niiden omistuksessa olevat viestintäjärjestelmät ovat kriittisiä niiden tarjoamien viestintäpalveluiden toimivuuden turvaamiseksi. Viestintäjärjestelemän kriittisyyden arviointiin vaikuttavat esimerkiksi järjestelmän maantieteellinen alue, käyttäjämäärä sekä sen merkitys käyttäjille. Lisäksi viestintäjärjestelmän kriittisyyttä lisää se, jos se on merkittävä viranomaisten toiminnan turvaamiseksi.[37]

Siihen, kuinka kattavia teleyritysten laatimien varautumissuunnitelmien tulee olla, vaikuttaa hallituksen esityksen perusteella se, kuinka merkityksellistä kyseisen teleyrityksen ”toiminta on yhteiskunnan turvallisuuden tai johtamisen varmistamisen kannalta”. Lisäksi varautumissuunnittelun kattavuuteen vaikuttaa se, mikä merkitys teleyrityksen toiminnalla on elinkeinoelämän toimintakyvyn varmistamisessa. Tässä arvioinnissa voidaan käyttää samoja kriteerejä kuin kriittisten viestinjärjestelmien arvioinnissakin eli palvelujen käyttäjämäärää, maantieteellistä aluetta ja yleistä merkitystä käyttäjille.[38]

Edellä esitetyn perusteella selvää onkin, että joiltain teleyrityksiltä vaaditaan laajempaa varautumissuunnittelua kuin toisilta. Kyse on yrityskohtaisesta harkinnasta ja eri teleyritysten varautumissuunnittelussa voivat korostua erilaiset tekijät. Joidenkin teleyritysten tarjoamat palvelut saattavat olla kriittisiä esimerkiksi puolustusvoimien toiminnan turvaamiseksi ja joidenkin taas rahoitusalan toiminnan turvaamiseksi.

4.3 Viestintäverkon kriittisen järjestelmän palauttaminen Suomeen ja tarkempien määräysten antaminen varautumisesta

Edellisessä luvussa todettiin, että teleyrityksen tulee osana varautumissuunnittelua arvioida, mitkä sen omistamat viestintäjärjestelmät ovat sen tarjoamien viestintäpalveluiden toiminnan

[35] HE 221/2013 vp, s. 204
[36] 539/2008, s. 1
[37] HE 221/2013 vp, s. 204
[38] HE 221/2013 vp, s. 203

kannalta kriittisiä. LSVP:n 35 luvun 283 § liittyy tähän kiinteästi, sillä siinä velvoitetaan teleyrityksiä huolehtimaan, että sen tarjoamien palveluiden kannalta kriittinen viestintäjärjestelmä sekä sen ohjaus, ylläpito ja hallinta voidaan poikkeusolojen vallitessa valmiuslain 60 § 1 momentin 8 kohdan mukaisella toimivaltuudella palauttaa Suomeen. Sääntely on loogista, sillä valmiuslain 60 § 1 momentin 8 kohdan nojalla liikenne- ja viestintäministeriö voi poikkeusoloissa velvoittaa teleyrityksen ylläpitämään järjestelmiä ja palveluita tietyistä paikoista. Tämän toimivaltuuden käyttö ei olisi mahdollista, mikäli kriittisten viestintäjärjestelmien palauttaminen Suomeen ei onnistuisi.

Toimivaltuus tarkempien määräysten antamisesta teleyritysten varaurautumiseen on LSVP:n 35 luvun 284:ssä annettu Liikenne- ja viestintävirasto Traficomille. Tällaiset määräykset voivat liittyä varautumissuunnitteluun ja niiden tarkempaan sisältöön taikka teknisiin toimenpiteisiin, jotka ovat tarpeellisia tietoturvaloukkausten vahingollisten vaikutusten minimoimiseksi. Traficom ei ole toimivallastaan huolimatta kuitenkaan antanut sellaisia teleyritysten varautumista koskevia määräyksiä, jotka olisi annettu 284 §:n nojalla. Sen sijaan LSVP:n 29 luvussa säädettyihin viestinverkon ja viestintäpalvelun laatuvaatimuksien sisältöä Traficom on määräyksellään tarkentanut.[39] Laatuvaatimukset kytkeytyvät läheisesti varautumisvelvollisuuteen.

4.4 Viestintäverkkojen ja viestintäpalveluiden laatuvaatimukset

Edellä mainittuja teleyritysten laintasoisia varautumisnormeja ja niiden esitöitä tutkimalla saadaan yleiskuva siitä, mihin varautumisella pyritään ja mitä siinä tulee ottaa huomioon. Teleyritysten varautumisen kannalta konkreettisista toimenpiteistä ei pelkästään niitä tutkimalla kuitenkaan saa kattavaa kuvaa. Sen sijaan sähköisen viestinnän palveluista annetun lain viestintäverkon ja viestintäpalveluiden laatuvaatimuksia käsittelevässä 29 luvussa on selkeästi tarkempia teleyrityksiä koskettavia velvollisuuksia. Laatuvaatimukset liittyvä kiinteästi varautumisvelvollisuuksiin. Ne velvoittavat teleyrityksiä ottamaan mahdolliset häiriöt ja uhat huomioon jo viestintäverkkojen ja -palveluiden suunnittelu- ja rakentamisvaiheessa. Näin ollen, mikäli laatuvaatimuksia noudetaan asianmukaisesti, helpottaa se varautumista ja siihen kuuluvaa varautumissuunnittelua myös jatkossa.

LSVP:n 29 luvun pykälistä keskitytään tässä tutkielmassa niiden havainnollistavuuden, mutta myös tilan rajallisuuden vuoksi viestintäverkon ja viestintäpalvelun laatuvaatimuksia yleisesti

[39] ks. TRAFICOM/54045/03.04.05.00/2020

sääntelevään 243 §:ään sekä viestintäverkkoja ja -palveluita koskevia määräyksiä käsittelevään 244 §:ään. 243 §:ssä on lueteltu tyhjentävä 16-kohtainen lista seikoista, jotka tulee ottaa huomioon yleisiä viestintäverkkoja ja -palveluita sekä niihin liitettäviä viestintäverkkoja ja -palveluita suunniteltaessa, rakennettaessa sekä ylläpidettäessä. Huomioon tulee 243 §:n nojalla ottaa muun muassa se, että viestintäverkot ja -palvelut ”kestävät normaalit odotettavissa olevat ilmastolliset, mekaaniset, sähkömagneettiset ja muut ulkoiset häiriöt sekä tietoturvauhat” ja että ”niihin kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat sekä niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita.” Lisäksi tämän tutkielman teeman osalta merkittävä vaatimus on sen varmistaminen, että viestintäverkot ja -palvelut toimivat mahdollisimman luotettavasti myös häiriötilanteissa ja poikkeusoloissa. Näihin seikkoihin tulee kiinnittää huomiota siis jo viestinverkkojen ja -palveluiden suunnittelu- ja rakentamisvaiheessa.

Kuten huomataan, laatuvaatimuksia säädettäessä on otettu huomioon erilaiset häiriötilanteet ja poikkeusolot sekä niiden varalta suojautuminen. Käytännön toimenpiteet, joilla 243 §:ssä mainitut seikat otetaan huomioon, konkretisoituvat Liikenne- ja viestinvirasto Traficomin antamilla määräyksillä. Traficomin toimivallasta tarkempien määräysten antamiseen säädetään LSVP:n 244 §:ssä. Määräyksiä voidaan sen nojalla antaa viestintäverkkojen ja -palveluiden laadusta, tietoturvallisuudesta ja yhteensopivuudesta. Niiden sisältönä on 244 §:n perusteella käytännössä viestintäverkoille ja -palveluille asetettavat tekniset vaatimukset, kuten viestintäverkon ja siihen kuuluvan laitetilan sähköiseen ja fyysiseen suojaamiseen liittyvät vaatimukset sekä vaatimukset noudatettavista standardeista.

Laatuvaatimuksia voi pitää sisällöltään konkreettisempina ja yksityiskohtaisempina kuin LSVP:n teleyritysten varautumista yleisellä tasolla käsitteleviä 35 luvun säännöksiä. Siihen, miten viestinverkot ja -palvelut toimivat erilaisissa häiriötilanteissa ja poikkeusoloissa, vaikuttaa keskeisesti se, miten ne on suunniteltu ja rakennettu. Esimerkiksi erilaisten tietoliikennekaapeleiden rakennusvaiheessa voidaan riittävin varmistuksin ja suojauksin parantaa niiden toimintakykyä tilanteissa, joissa niitä koitetaan tuhoa osana sodankäyntiä tai joissa niiden sijaitsemalla alueella vallitsee luonnonkatastrofi. Laatuvaatimusten tärkeydestä osoituksena on se, että toisin kuin varautumisvelvollisuuksien osalta, Traficom on päättänyt käyttää tarkentavien määräysten antamisen toimivaltaansa laatuvaatimusten osalta.

4.5 Laatuvaatimusten tarkentaminen Liikenne- ja viestintävirasto Traficomin määräyksin

Liikenne- ja viestintävirasto Traficom on LSVP:n 29 luvun 244 §:ssä sille säädetyn toimivallan nojalla antanut vuonna 2021 määräyksen viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Määräyksen perustelumuistiossa tiivistetään hyvin se, miksi häiriötilanteisiin tulee varautua jo viestintäverkkojen suunnittelu- ja rakentamisvaiheessa. Se kytkeytyy havaintoon siitä, että häiriön sattuessa ei yleensä enää ole aikaa tehdä riittäviä varmistuksia verkkoihin ja palveluihin, jotta häiriön vaikutukset viestiliikenteeseen voitaisiin estää. Näin ollen varmistusten rakentaminen viestintäverkkoihin ja -palveluihin tulee tehdä etukäteen normaalioloissa.[40]

Traficomin perustelumuistiossa avataan myös LSVP:tä ja sen esitöitä tarkemmin sitä, minkälaisia viestinverkkoihin tai -palveluihin kohdistuvat häiriöt yleensä ovat. Niitä ovat esimerkiksi yleisen sähköverkon sähkökatkot, viestintäverkon tai palvelun komponenttien laiterikot sekä komponenttien välisten yhteyksien kaapelikatkot. [41] Komponentilla tarkoitetaan määräyksessä viestintäverkkojen tai -palveluiden komponenttia. Vielä tarkemmin sillä tarkoitetaan ”verkkoelementtiä, laitetta tai tietojärjestelmää, joista viestintäverkko tai -palvelu muodostuu tai jota se hyödyntää.”[42]

Viestintäverkkojen ja -palvelujen toiminta häiriötilanteissa pyritään turvaamaan määräyksessä esitetyillä vaatimuksilla, joilla viestintäverkkoihin vaaditaan rakentamaan erilaisia varmistusmekanismeja. Näin ollen mahdollisten häiriöiden ilmaantuessa, viestintäverkoissa on jo valmiina häiriöiltä suojaavia mekanismeja.[43] Määräyksessä esitetyt varmistusmekanismit ovat moninaisia. Siinä ohjeistetaan esimerkiksi, kuinka teleyrityksen tulee luokitella viestintäverkkojensa ja -palveluidensa komponentit tärkeysjärjestykseen komponenttien palvelevien maantieteellisten sijaintien ja käyttäjämäärien perusteella.[44] Lisäksi siinä asetetaan velvoitteita esimerkiksi laitteisto- ja reittivarmistuksiin. Määräys on pitkä, hyvin tekninen ja yksityiskohtainen.[45] Sen yksityiskohtainen avaaminen tässä yhteydessä ei palvele tutkielman tavoitetta. On kuitenkin tärkeää ymmärtää sen merkitys teleyritysten varautumisen osalta, sillä se antaa laintasoisia varautumisnormeja ja

[40] Traficom 54 C/2021 M, s. 12
[41] Traficom 54 C/2021 M, s. 11
[42] Traficom 54 C/2021 M, s. 16
[43] Traficom 54 C/2021 M, s. 12
[44] Traficom 54 C/2021 M, s. 21
[45] ks. TRAFICOM/54045/03.04.05.00/2020

laatuvaatimuksia tarkempia ja konkreettisempia velvoitteita varautumiseen. Lisäksi Traficomin määräys on hyvä esimerkki siitä, miten viranomaisen päätöksellä voidaan tarkentaa laintasoisia varautumisvelvollisuuksia.

4.6 Sähköisen viestinnän palveluista annetun lain varautumissääntelyn arviointi suhteessa sähkömarkkinalain sääntelyyn

LSVP:ssä säädetyn teleyritysten varautumista koskevan sääntelyn kokonaisuusuudessa on sekä yhtäläisyyksiä että eroja muiden toimialakohtaisissa erityislaeissa säädettyjen varautumisvelvollisuuksien kanssa. Kun tarkastellaan LSVP:n varautumissääntelyä esimerkiksi suhteessa sähkömarkkinalakiin tai liikennepalvelulakiin, huomataan, että kaikissa näissä velvoitetaan alan toimijoita varautumaan sekä häiriötilanteiden että poikkeusolojen varalle. Esimerkiksi sähkömarkkinalain 28 §:ssä säädetään verkonhaltijan velvollisuudesta varautumissuunnitteluun häiriötilanteiden ja poikkeusolojen varalle. Liikennepalvelulaissa puolestaan eri liikennepalveluiden harjoittajien varautumisvelvollisuuksista on säädetty erikseen toimialakohtaisissa luvuissa. Esimerkiksi kaupunkiraideliikenteen harjoittajan varautumisvelvollisuudesta häiriötilanteiden ja valmiuslain tarkoittamien poikkeusolojen varalle säädetään lain 7 luvussa ja rautatieliikenteen harjoittajan vastaavasta velvollisuudesta puolestaan lain 6 luvussa. Toisaalta varautumissuunnitteluun liittyvässä sääntelyssä on kyseisissä laeissa myös eroavaisuuksia LSVP:n sääntelyyn verrattuna.

Koska sähkömarkkinalain sääntelyn alaiset verkonhaltijat ovat toimialaltaan esimerkiksi rautatieliikenteenharjoittajia lähempänä teleyrityksiä, jotka hallinnoivat viestintäverkkoja, vertaillaan seuraavaksi LSVP:n ja sähkömarkkinalain varautumissääntelyä. Tarkoituksena on vertailun avulla selvittää, olisiko sähkömarkkinalain varautumissääntelystä omaksuttavissa jotain LSVP:n varautumissääntelyyn.

Sähkömarkkinalain 28 §:ssä asetetaan verkonhaltijalle velvollisuus varautumissuunnitteluun. Merkille pantavaa on, että varautumissuunnitteluun velvoittava 28 § on ainoa verkonhaltijoiden varautumista sääntelevä pykälä sähkömarkkinalaissa. LSVP:n teleyrityksiä varautumiseen velvoittava sääntely on puolestaan jaettu neljään pykälään, joista vain yksi velvoittaa nimenomaisesti varautumissuunnitteluun. Varautumissuunnittelusta on sähkömarkkinalaissa säädetty myös LSVP:tä kattavammin. Sähkömarkkinalain 28 § velvoittaa erilaisiin häiriötilanteiseen ja poikkeusoloihin varautumisen ohella sähköverkonhaltijoita myös laatimaan konkreettisen varautumissuunnitelman, joka tulee

toimittaa Energiavirastolle. Varautumissuunnitelman laatimista ei puolestaan LSVP:n sääntelyssä suoraan edellytetä, vaikka sen laatimiseen viitataankin lain esitöissä.[46] Lisäksi sähkömarkkinalain esitöihin kuuluvassa hallituksen esityksessä HE 20/2013 syvennytään LSVP:n esitöitä tarkemmin siihen, mitä varautumissuunnittelussa ja varautumissuunnitelman laatimisessa tulee ottaa huomioon.

Esityksen perusteella sähköverkonhaltijan pitäisi sisällyttää varautumissuunnitelmaansa muun muassa suunnitelmat siitä, miten riittävä asiakastiedon antaminen erilaisissa häiriötilanteissa ja poikkeusoloissa varmistetaan sekä siitä, miten toimiva yhteys toiminta-alueen infrastruktuurin haltijoihin, kuten poliisiin, pelastusviranomaisiin ja teleyrityksiin järjestetään kaikissa olosuhteissa. Lisäksi valmiussuunnitelmasta tulisi ilmetä, millä tavalla ja missä järjestyksessä sähköt palautettaisiin asiakkaille mahdollisten häiriötilanteiden aikana.[47]

Kuten edellä teleyritysten varautumissuunnittelua käsiteltäessä todettiin, LSVP:n ja sen esitöiden nojalla teleyritysten varautumissuunnittelussa tuli ottaa huomioon heidän omalle toiminta-alueelleen ja -ympäristölleen keskeiset uhkatekijät ja riittävällä suunnitelmallisuudella varautua näiden torjumiseen. Näin ollen harkintavaltaa on enemmän kuin sähkömarkkinalain sääntelyssä, jossa annetaan tarkempia ohjeita siitä, mitä varautumissuunnitelman tulee pitää sisällään. Suurempi harkintavalta varautumissuunnittelussa antaa teleyrityksille mahdollisuuden tehdä yksilöllisempiä varautumissuunnitelmia, joissa varaudutaan juuri heidän toimintansa kannalta relevantteihin riskeihin. Kääntöpuolena on, että teleyritysten varautumissuunnitelmat saattavat poiketa merkittävästi toisistaan. Yhteneväisemmät varautumissuunnitelmat toimialan eri toimijoiden välillä helpottavat kriisien valtakunnallista johtamista erityistilanteissa. LSVP:n sääntelyä voisikin olla paikallaan tarkentaa sen osalta, mitä varautumissuunnittelussa tulee ottaa huomioon. Toisaalta harkintavaltaa on teleyrityksille vielä hyvä jättää jatkossakin jonkin verran, sillä teleyritysten joukko on erilaisten verkko- ja viestintäpalveluiden tarjoajina verrattain moninainen. Samoin täytyy muistaa, että digipoolissa teleyritykset kommunikoivat vapaaehtoisesti eri tahojen kanssa varautumisesta, mikä voi osaltaan vähentää varautumissuunnittelun hajanaisuutta teleyritysten keskuudessa.

[46] HE 221/2013 vp, s. 203
[47] HE 20/2013 vp s. 85

Mielenkiintoinen eroavaisuus LSVP:n sääntelyyn verrattuna on myös sähkömarkkinalain 28 §:n 3 momentissa asetettu velvollisuus toimittaa varautumissuunnitelma ja siihen tehtävät muutokset Energiavirastolle sekä Energiavirastolle annettu toimivalta kuuden kuukauden kuluessa suunnitelman jättämisestä vaatia siihen tehtäväksi muutoksia, mikäli se ei täytä varautumissuunnitelmalle asetettuja vaatimuksia. Samanlaista toimivaltuutta viranomaisille ei LSVP:ssä ole säädetty. Sen 282 §:n 3 momentin mukaan ”Varautumisvelvollisen on Liikenne- ja viestintäviraston pyynnöstä yksittäistapauksissa ilmoitettava, miten se varautuu yksittäiseen häiriötilanteeseen tai sellaisen uhkaan ja mihin varautumissuunnittelunsa mukaisiin toimiin se on tilanteen johdosta ryhtynyt tai aikoo ryhtyä”.

Liikenne- ja viestinvirastolle LSVP:n 28 §:n nojalla annettu toimivalta koskettaa siis ainoastaan yksitäistapauksia eikä kyse ole järjestelmällisestä varautumissuunnitelmien tarkistamisesta sähkömarkkinalain sääntelyn tapaan. Viranomaiskontrollia voisikin lisätä myös teleyrityksiä koskevaan varautumissääntelyyn. Tällä hetkellä LSVP:n sääntely ei vaadi edes varautumissuunnitelmien toimittamista viranomaiselle puhumattakaan niiden järjestelmällisestä viranomaistason tarkistamisesta. Kun otetaan huomioon varautumissuunnittelun keskeinen rooli häiriötilanteiden ja poikkeusolojen varalle varautumisessa, olisi sähkömarkkinalaissa tarkoitettu viranomaiskontrolli aiheellista omaksua myös LSVP:n varautumissääntelyyn. Tällöin teleyritysten varautumissuunnittelun riittävä taso voitaisiin taata järjestelmällisesti viranomaiskeinoin ja tällaisella kontrollilla olisi vahva lainsäädännöllinen perusta.

Varautumissääntelyn logiikka on kuitenkin sähköisen viestinnän palvelusta annetusta laissa ja muita kriittisiä toimialoja säätelevissä erityislaeissa samankaltainen. Kriittisillä aloilla toimivien yritysten varautuminen erilaisiin häiriötilanteisiin ja poikkeusoloihin on haluttu varmistaa laintasoisin normein. Eri aloilla toiminnan jatkumista vaarantavat riskit ovat erilaisia ja täten varautumissuunnittelussa huomioon otettavat vaihtelevat toimialoittain.

5 Varautumisen kustannukset ja valvonta

5.1 Varautumistoimenpiteistä aiheutuneiden kustannusten hyvittäminen

Sähköisen viestinnän palveluista annettua lakia säädettäessä on tunnistettu, että 35 luvun mukaisista varautumistoimenpiteistä saattaa koitua kustannuksia teleyrityksille. Lain 37 luvun 298 §:n perusteella teleyrityksillä on tietyissä tapauksissa oikeus saada korvaus tällaisista kustannuksista huoltovarmuuden turvaamisesta annetussa laissa tarkoitetusta huoltovarmuusrahastosta. Kustannusten korvaaminen edellyttää kyseisen pykälän mukaan sitä, että kustannukset ovat teleyrityksen toiminnan luonne ja laajuus huomioon ottaen huomattavia. Kyseinen lainkohta on tarpeellinen, sille ei olisi reilua, että teleyritysten tekemistä, mahdollisesti koko yhteiskunnan kriisinsietokykyä parantavista varautumistoimenpiteistä aiheutuvat huomattavat kustannukset jäisivät pelkästään teleyritysten maksettaviksi. Huoltovarmuuskeskus päättää kustannusten korvaamisesta pyydettyään ensin korvaushakemusta koskevan lausunnon liikenne- ja viestintäministeriöltä.

LSVP:n esitöissä ei käsitellä sitä, mitkä tekijät tulee ottaa huomioon kustannusten huomattavuutta arvioitaessa. HE 221/2013:sa todetaan, että tarkasteltavan pykälän sisältö pysyy pääosin samansisältöisenä kuin LSVP:n edeltäjän, viestintämarkkinalain korvauksia käsittelevä 94 §.[48] Esityksessä on viitattu viestintämarkkinalain esitöihin, tarkemmin hallituksen esitykseen HE 112/2002. Siinä kerrotaan varautumistoimenpiteistä aiheutuneiden kustannusten huomattavuuden arvioinnin sijasta kustannusten kohtuullisuuden arvioinnista.[49] Tästä voi mielestäni tehdä päätelmän, että korvaukset, jotka kohtuullisuusarvioinnin perusteella katsotaan kohtuullisiksi, eivät ole huomattavia, eikä tällaisia kustannuksia tällöin korvattaisi. HE 112/2002 perusteella aiheutuneiden kustannusten kohtuullisuuden arvioinnissa kustannukset tulisi suhteuttaa esimerkiksi teleyrityksen liikevaihtoon, sen harjoittaman toiminnan luonteeseen sekä sen kilpailutilanteeseen markkinoilla.[50] Näin ollen samankaltaisista varautumistoimenpiteistä aiheutuneet samaa suuruusluokkaa olevat kustannukset saatetaan joissain tapauksissa korvata ja joissakin tapauksissa taas jättää korvaamatta.

---

[48] HE 221/2013 vp, s. 213
[49] HE 112/2002 vp, s. 172
[50] HE 112/2002 vp, s. 172

5.2 Valvontapäätökset ja pakkokeinot varautumisvelvollisuuksien tehostajina

Jotta laissa säädettyjä velvollisuuksia noudetaan myös käytännössä, on niiden rikkomisesta tärkeää seurata sanktioita tai muita viranomaistoimenpiteitä. Sähköisen viestinnän palveluista annetussa laissa säädettyjä viranomaisten keinoja reagoida varautumisvelvollisuuksien rikkomiseen ovat valvontapäätös, väliaikainen päätös sekä uhkasakko, keskeyttämisuhka ja teettämisuhka. Lisäksi äärimmäisen keinona on käytettävissä teletoiminnan kieltäminen. Näistä säädetään LSVP:n 42 luvussa.

Laissa määritelty yleinen valvontaviranomainen on Liikenne- ja viestintävirasto Traficom. Sillä on LSVP:n 42 luvun 330 §:n 1 momentin perusteella annettu toimivalta antaa huomautuksia sille, ”joka rikkoo tätä lakia taikka sen nojalla annettuja säännöksiä, määräyksiä, päätöksiä ja lupaehtoja”. Lisäksi saman momentin mukaan Traficom voi ”velvoittaa tämän korjaamaan virheensä tai laiminlyöntinsä kohtuullisessa määräajassa”. Jälkimmäisessä tapauksessa kyse on valvontapäätöksen antamisesta.

Jos teleyritys siis rikkoo laintasoisia varautumisnormeja, esimerkiksi laiminlyö edellä mainittua velvollisuutta varautumissuunnitteluun, Traficomilla on oikeus velvoittaa kyseinen yritys täyttämään varautumisvelvollisuutensa. Samanlainen oikeus Traficomilla on esimerkiksi silloin, jos teleyrityksen omistamat viestintäverkot tai palvelut eivät täytä 29 luvun 243 §:n mukaisia laatuvaatimuksia. Tällaisissa tapauksissa teleyritykselle voidaan ensin antaa huomautus, mutta HE 221/2013 perusteella sen antaminen ennen valvontapäätöksen antamista ei ole välttämätöntä.[51]

Valvontapäätöksen perusteella sen kohteena olevan teleyrityksen tulee korjata päätöksessä mainittu virhe tai laiminlyönti kohtuullisessa määräajassa. Kohtuullisen ajan määrittämisessä tulee kiinnittää huomiota hallintolakiin sekä hyvän hallinnon periaatteisiin.[52] Valvontapäätöksen tehostamiseksi on Traficomille LSVP:n 42 luvun 332 §:n nojalla annettu toimivalta asettaa uhkasakko tai ”uhka siitä, että toiminta keskeytetään taikka että tekemättä jätetty toimenpide teetetään laiminlyöjän kustannuksella” eli keskeyttämis- tai teettämisuhka.

Uhkasakko, keskeyttämisuhka ja teettämistaakka ovat yleisiä hallinto-oikeudellisia keinoja viranomaisten antamien velvoitteiden, kieltojen tai vaatimusten tehostamiseen. Niistä säädetään uhkasakkolaissa. Olli Mäenpää on kuvannut kyseisten keinojen käyttämistä

[51] HE 221/2013 vp, s. 232
[52] HE 221/2013 vp, s. 232

teoksessaan ”Hallinto-oikeus” (2023). Hänen mukaansa keinoista tärkein ja yleisin on uhkasakon asettaminen.[53] Uhkasakon avulla esimerkiksi Traficom voi asettaa teleyritykselle velvollisuuden korjata laatuvaatimuksiin liittyvä laiminlyöntinsä maksuvelvollisuuden eli uhkasakon uhalla. Uhkasakko asetetaan joko kiinteänä tai juoksevana euromääränä, jolloin maksettavan sakon määrä kasvaa päävelvoitteen noudattamisen viivästyessä.[54] Mikäli teleyritys ei uhkasakosta huolimatta toteuta tarvittavia toimenpiteitä virheensä tai laiminlyöntinsä korjaamiseksi, Traficom voi määrätä uhkasakon maksettavaksi.

Keskeyttämis- ja teettämisuhka ovat uhkasakolle vaihtoehtoisia keinoja viranomaisen antaman velvoitteen tehostamiseksi. Keskeyttämisuhan nojalla teleyritys voidaan velvoittaa Traficomin määräämiin toimiin sillä uhalla, että jos se ei annetussa määräajassa ryhdy tarvittaviin toimenpiteisiin, sen toiminta voidaan keskeyttää. Teettämisuhan perusteella taas Traficom voi tehostaa teleyrityksille asettamiaan velvoitteita sillä uhalla, että määräajan kuluessa umpeen, laiminlyöty toimenpide toteutettaisiin teleyrityksen kustannuksella.[55]

Sellaisissa tapauksissa, joissa edellä mainituista virheistä laiminlyönneistä voi aiheutua välitöntä ja vakavaa vaaraa esimerkiksi yleiselle järjestykselle tai turvallisuudelle taikka vakavaa taloudellista vaaraa tai toiminnallista haittaa muille yrityksille, tilaajille tai käyttäjille taikka viestintäverkkojen tai -palveluiden toiminnalle, Traficom voi 42 luvun 331 §:n 1 momentin nojalla päättää viipymättä tarvittavista väliaikaisista toimista säädetystä 330 §:ssä säädetystä kohtuullisesta määräajasta välittämättä. Tällaisena väliaikaisena toimena Traficom voi esimerkiksi keskeyttää teleyrityksen vaaraa tai vakavaa haittaa aiheuttavan toiminnan. Väliaikainen päätös on 331 §:n mukaan voimassa enintään kolme kuukautta, mutta sitä voidaan jatkaa sen jälkeen kolmella kuukaudella, mikäli teleyritys ei ole tässä ajassa virhettään tai laiminlyöntiään korjannut. Tämä ja muut edellä esitetyt hallintopäätökset ovat valituskelpoisia, joten teleyritys voi hakea niihin muutosta viime kädessä hallinto-oikeudesta ja korkeimmasta hallinto-oikeudesta.

Viranomaisille annetut toimivaltuudet puuttua teleyritysten varautumisvelvollisuuksien laiminlyöntiin ovat tärkeitä, jotta yritykset suhtautuvat varautumiseen vakavasti. Esimerkiksi uhkasakkojen suuruudet voivat olla yrityksen koosta riippuen huomattaviakin, joten viimeistään niiden avulla varautumisvelvollinen saadaan ymmärtämään varautumisen tärkeys.

---

[53] Mäenpää 2023, s. 583
[54] Mäenpää 2023, s. 583
[55] Mäenpää 2023, s. 583

Vaikka hallinnollisille sanktioille olisikin käytännössä harvoin käyttöä, on niillä pelotevaikuttimena tärkeä merkitys.

6 Yhteenveto ja teleyritysten varautumisvelvollisuuteen liittyvät tulevaisuuden näkymät

Kuten huomataan, teleyritysten varautuminen on sekä vapaaehtoista ja sopimuksiin perustuvaa että lailla säänneltyä. Lakiin perustuvat velvollisuudet velvoittavat laatuvaatimusten muodossa teleyrityksiä huomiomaan erilaiset häiriötilanteet ja poikkeusolot jo viestintäverkkojen ja -palvelujen suunnittelu- ja rakennusvaiheessa. Laatuvaatimusten täyttämisen lisäksi teleyritysten tulee jo normaalioloissa arvioida tarjoamiinsa palveluihin kohdistuvia riskejä ja uhkia sekä laatia niiden perusteella riittäviä varautumissuunnitelmia. Näiden suunnitelmien pohjalta niiden tulee tehdä tarvittavia etukäteisvalmisteluita ja toimenpiteitä, joilla riskit minimoidaan. Lisäksi lain säännösten ohella teleyritysten tulee noudattaa Liikenne- ja viestintävirasto Traficomin antamia määräyksiä varautumiseen liittyvien velvollisuuksien tarkemmasta sisällöstä. Traficomille on myös annettu toimivalta valvoa teleyritysten varautumisvelvollisuuksien täyttämistä ja puuttua tarvittaessa laiminlyönteihin esimerkiksi valvontapäätöksien avulla.

Teleyrityksiä velvoittavaa LSVP:n sisältämää varautumiseen liittyvää sääntelyä voidaankin pitää kokonaisuudessa kattavana ja toimivana. 35 luvun yleinen varautumissääntely yhdessä 29 luvun mukaisten laatuvaatimusten kanssa muodostavat toimivan kokonaisuuden, jossa teleyritykset velvoitetaan toisaalta arvioimaan toimintaansa vaarantavia riskejä jo viestintäverkkojen ja -palveluiden suunnittelu- ja rakennusvaiheessa ja toisaalta sen jälkeenkin ottamaan toiminnassaan huomioon riittävällä tavalla mahdolliset toiminnan jatkumisen vaarantavat uhkatekijät. Lisäksi varautumista tehostavat viranomaisten toimivaltuudet valvontapäätösten ja esimerkiksi uhkasakkojen asettamiseen niissä tilanteissa, joissa varautumisvelvollisuuksia laiminlyödään. Jotkin muutokset LSVP:n sääntelyyn voisivat kuitenkin olla paikallaan. Ensinnäkin varautumissuunnittelun sisältöä voitaisiin aiemmin kohdassa 4.6 mainituin tavoin tarkentaa. Lisäksi suunnittelun kontrollia voisi olla paikallaan lisätä, jotta varautumissuunnitelmien laatu voitaisiin viranomaiskontrollin keinoin taata.

Rinnakkain sähköisen viestinnän palveluista annetun lain kanssa, teleyritysten varautumiseen vaikuttaa merkittävästi myös sopimuksiin ja vapaaehtoiseen yhteistyöhön perustuva varautuminen. Merkittävässä roolissa on etenkin Huoltovarmuusorganisaatioon kuuluvassa Digipoolissa teleyritysten muiden yritysten sekä toimialalla toimivien järjestöjen ja viranomaisten kanssa tekemä yhteistyö. Tämän yhteistyön osana kehitetään kyberturvallisuutta, jonka merkitys on etenkin viime vuosina kiristyneen maailmanpoliittisen

tilanteen myötä kasvanut. Kyberturvallisuuden tärkeydestä ja ajankohtaisuudesta hyvä osoitus on Ilta-Sanomien uutinen ”Ruotsalaisasiantuntija: Venäjä voi ottaa Itämeren datakaapelit kohteekseen: ”Uhka on suuri”, joka on julkaistu 6.3.2024. Siinä kerrotaan, että juuri Natoon hyväksytyssä Ruotsissa esiintyy pelkoa siitä, että Venäjä saattaa kostaa Natoon liittymisen Ruotsille esimerkiksi sabotoimalla meren pohjassa kulkevia sähkö- ja datakaapeleita.[56] Meren pohjassa kulkeviin kaapeleihin kohdistuvien iskujen mahdollisuus tulee Suomessakin ottaa vakavasti. Kriittiseen infrastruktuuriin kuuluvien datakaapelien suojaamiseen tulee kiinnittää jatkossakin huomiota, jopa nykyistä enemmän.

Teleyritysten varautumiseen liittyvän sääntelyn kannalta tulee vielä mainita, että sisäministeriössä on tällä hetkellä käynnissä lainsäädäntöhanke ”Kriittisen infrastruktuurin tunnistaminen ja kriisinkestävyyden parantaminen”. Hankkeen tarkoituksena on panna täytäntöön niin sanottu CER-direktiivi, tarkemmin Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557 kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta.[57]

Tässä kohtaa on vielä liian aikaista arvioida, miten kyseinen lainsäädäntöhanke tulee lopulta vaikuttamaan teleyrityksien varautumista koskevaan lainsäädäntöön. Toisaalta muutosten ei voida olettaa olevan kovin merkittäviä ainakaan lainsäädäntöhankkeen pohjalta syntyneen luonnoksen ”Hallituksen esitys laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi” perusteella. Sen mukaan nimittäin digitaalinen infrastruktuuri, jonka alaan teleyritysten omistamat ja hallinnoimat viestintäverkot- ja palvelutkin kuuluvat, ”on CER-direktiivissä poikkeussektori. Täten siihen ”kohdistuisi muihin CER-direktiivin sektoreihin verrattuna rajoitetusti säännöksiä.”[58]

Toisaalta kyseinen lainsäädäntöhanke on vielä kesken ja luonnokseen perustuva lausuntokierroskin päättyi vasta 4.3.2024.[59] Voi siis olla, että lausuntojen pohjalta ja hankkeen edetessä, esitys tulee vielä muuttumaan ja hankkeen pohjalta valmistuvaan lainsäädäntöön tulee myös teleyritysten varautumiseen liittyviä muutoksia. Joka tapauksessa on hyvä, että tässä maailmanpoliittisessa tilanteessa kriittisen infrastruktuuriin suojaamista koskevaa lainsäädäntöä tarkistetaan ja mahdollisesti päivitetään vastaamaan nykytilanteessa relevantteja uhkakuvia. Selvää on se, että teleyritysten varautuminen erilaisten

[56] Laukkanen 6.3.2024
[57] Sisäministeriö b
[58] Sisäministeriö, Kansallisen turvallisuuden yksikkö 2024, s. 62
[59] Sisäministeriö b

häiriötilanteiden sekä poikkeusolojen varalle tulee olemaan tulevaisuudessa vähintään yhtä tärkeää, ellei tärkeämpääkin kuin nykyään.