LIIKENNE- JA VIESTINTÄVALIOKUNNAN LAUSUNTO 7/2013 vp

Valtioneuvoston selvitys (UTP) valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuus-strategiasta

Suomen kyberturvallisuusstrategia

Ulkoasiainvaliokunnalle

JOHDANTO

Vireilletulo

Ulkoasiainvaliokunta on 8 päivänä helmikuuta 2013 lähettänyt valtioneuvoston selvityksen valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiasta (UTP 2/2013 vp) liikenne- ja viestintävaliokunnalle mahdollisia toimenpiteitä varten.

Liikenne- ja viestintävaliokunta on 19 päivänä helmikuuta 2013 päättänyt käsitellä omana asianaan Suomen kyberturvallisuusstrategiaa (LIO 3/2013 vp).

Asiantuntijat

Valiokunnassa ovat olleet kuultavina

- pääsihteeri, eversti Aapo Cederberg, turvallisuus- ja puolustusasiain komitean sihteeristö TPAK
- lainsäädäntöneuvos Laura Vilkkonen, liikenne- ja viestintäministeriö
- lainsäädäntöneuvos Tiina Ferm, sisäasiainministeriö
- erityisasiantuntija Yrjö Benson, valtiovarainministeriö
- apulaisjohtaja Erka Koivunen ja yksikön päällikkö Kirsi Karlamaa, Viestintävirasto
- tietosuojavaltuutettu Reijo Aarnio, Tietosuojavaltuutetun toimisto, OM
- tutkija, ST Martti Lehto, Jyväskylän yliopisto
- tutkimusjohtaja Tatu Koljonen, Valtion teknillinen tutkimuskeskus VTT
- yliasiamies Mikko Kosonen, Suomen itsenäisyyden juhlarahasto Sitra
- tutkimus- ja kehittämisjohtaja Jyrki Kasvi, Tietoyhteiskunnan kehittämiskeskus TIEKE ry
- Chief Research Officer Mikko H. Hyppönen, F-Secure Oyj
- tietoyhteiskuntasuhteiden johtaja Max Mickelsson, Microsoft Oy
- Director of Cyber Security Jarno Limnell, Stonesoft Corporation
- toimitusjohtaja Timo Lehtimäki, Suomen Erillisverkot Oy
- Principal Sales Consultant Markku A. Suistola, Symantec
- yritysturvallisuustoimiston päällikkö Jyrki Hollmén, Elinkeinoelämän keskusliitto EK
- varapuheenjohtaja Ville Oksanen, Electronic Frontier Finland ry EFFI
- varautumispäällikkö Kari Wirman, FiCom
- puheenjohtaja Jorma Mellin, Ficix ry.

VALIOKUNNAN KANNANOTOT

Perustelut

Yleistä

Nyky-yhteiskunta on lähes kaikilta keskeisiltä ja elintärkeiltä toiminnoiltaan riippuvainen tietojärjestelmien ja viestintäverkkojen toiminnasta. Tieto- ja viestintäjärjestelmien toimivuus on käytännössä myös elinehto nykyaikaisten yritysten liiketoiminnalle. Tämän riippuvuuden vuoksi viestintäverkot ja -palvelut ovat myös entistä houkuttelevampi erilaisten kyberhyökkäysten kohde, ja kriisitilanteissa sähköisen viestinnän merkitys vain kasvaa entisestään. Valiokunta pitää saamansa selvityksen perusteella todennäköisenä, että yhteiskunnan riippuvuus kyberympäristöstä syvenee tulevaisuudessa edelleen nykytilanteeseen verrattuna.

Tietojärjestelmien ja viestintäverkkojen hyödyntäminen tarjoaa kokonaisuutena huomattavia tehokkuus-, kustannus- yms. etuja. Niiden käyttöön liittyy kuitenkin myös kybertoimintaympäristöön kuuluvia uhkia, jotka tulee osata tunnistaa, varautua niihin ja reagoida niihin oikea-aikaisesti ja tehokkaasti. Kyberturvallisuudella pyritään tavoitetilaan, jossa tähän ympäristöön voidaan luottaa ja jossa voidaan varmistaa kyberympäristöstä riippuvaisten toimintojen jatkuminen. Valiokunta toteaa, että yhtenä keskeisenä tavoitteena kyberympäristössä tulee toimintojen jatkumisen lisäksi olla myös kansalaisille ja yrityksille kuuluvien oikeuksien toteutuminen.

Valiokunta pitää kyberturvallisuusstrategian laatimista erittäin tärkeänä ja tarpeellisena. Strategian tehokkaalla ja riittävän koordinoidulla toimeenpanolla voi lähivuosina olla olennainen merkitys Suomen kokonaisturvallisuuden ja kybertoimintaympäristöä kohtaan tunnettavan luottamuksen kannalta.

Strategiassa on pyritty määrittelemään kyberturvallisuuden visio, yleiset toimintamallit ja strategiset linjaukset, joilla pystytään vastaamaan kybertoimintaympäristön haasteisiin. Valiokunta toteaa, että strategiassa on kuitenkin käsitelty asioita varsin yleisellä tasolla, mikä korostaa jatkossa huomattavasti strategian konkreettisen toimeenpano-ohjelman suunnittelun ja toteuttamisen merkitystä.

Strategian mukaan elintärkeitä toimintoja ovat valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentulo sekä henkinen kriisinkestävyys. Yhteiskunnan turvallisuusstrategiassa (YTS 2010) on määritelty eri yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta keskeiset strategiset tehtävät ja kunkin strategisen tehtävän kehittämisestä ensisijaisesti vastuussa oleva ministeriö. Liikenne- ja viestintäministeriön tehtäväksi on määritelty sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistaminen, varoitus- ja hälytysjärjestelmien rakentamisen ja ylläpidon tukeminen sekä kuljetusten jatkuvuuden turvaaminen.

Myös liikenne- ja viestintävaliokunnan toimiala ja näkökulma painottuu kyberturvallisuuden kannalta sähköisen tieto- ja viestintäjärjestelmäinfrastruktuurin toimivuuteen ja sen varmistamiseen. Kyberstrategiakokonaisuudessa valiokunnan toimialaan kuuluu mm. avointen viestintäverkkojen ja verkkopalveluiden tietoturvallisuus, viestintäpalveluiden tietoturvallisuus, teleyritysten tietoturvallisuus ja varautuminen, sähköisen viestinnän luottamuksellisuutta ja tietosuojaa koskeva sääntely, Viestintäviraston tehtävät myös perustettavan Kyberturvallisuuskeskuksen osalta sekä mm. kyberympäristön vaikutukset liikennesektoriin. Valiokunta ei tässä lausunnossaan käsittele sille kuulumattomina asioina turvallisuusviranomaisten, kuten puolustusvoimien tai poliisin, roolia eikä valtionhallinnon omien verkkojen tai tietojärjestelmien tietoturvallisuutta.

Liikenne- ja viestintävaliokunta on käsitellyt samaa tämän lausunnon kohteena olevaa Suomen kyberturvallisuusstrategiaa myös omana asianaan LIO 3/2013 vp. Valiokunta on päättänyt yhdistää näiden kahden asian käsittelyt.

Kybertoimintaympäristön piirteitä

Kaikkiin toimintaympäristöihin kuuluu uhkia ja riskejä. Kyberympäristön jonkinasteiset uhat ja häiriöt ovat arkipäivää niille tietojärjestelmille ja viestintäverkoille, joista kyberympäristö rakentuu. Toiminnan ja varautumisen lähtökohdaksi on käytännössä välttämätöntä asettaa, että myös vakavampia häiriöitä tulee esiintymään.

Kaikki internetliikenne kulkee, saapuu Suomeen ja lähtee Suomesta, käytännössä teleyritysten hallinnoimien avointen viestintäverkkojen kautta. Viestintäverkot ovat myös se pääasiallinen reitti, jonka kautta mahdolliset kyberhyökkäykset useimmiten tehdään ja jonka kautta kyberympäristön ongelmat leviävät. Teleyrityksillä, teleyritysten toteuttamilla toimenpiteillä ja niitä koskevalla sääntelyllä on siten aivan keskeinen merkitys kyberympäristön turvallisuuden kannalta.

Kybertoimintaympäristön toimintaan ja käyttöön liittyvä tekniikka kehittyy nopeasti, ja sen kehittymissuuntaa on hyvin vaikeaa arvioida useita vuosia eteenpäin. Mahdollisiin hyökkäyksiin käytettävät menetelmät seuraavat ja pyrkivät ennakoimaan tekniikan kehittymistä. Haavoittuvuudet voivat liittyä teknologian ominaisuuksiin ja puutteisiin, henkilöiden toimintatapoihin tai esimerkiksi organisaatiossa käytössä oleviin prosesseihin.

Kyberympäristössä periaatteessa jokin pienilläkin resursseilla varustettu yksittäinen, mutta hyvin osaava toimija saattaa pystyä halutessaan aiheuttamaan huomattavaakin vahinkoa. Verkkoympäristössä myös erilaisten epäasiallisten tai rikollisten toimenpiteiden kynnys saattaa olla matalampi kuin reaalimaailmassa. Kyberympäristössä ongelmia aiheuttavat toimijat toimivat tänä päivänä usein myös ammattimaisesti, mikä asettaa uusia haasteita uhkien torjumiselle. Toiminnan ammattimaisuudesta kertoo, jos hyökkäys on räätälöity tarkasti tiettyyn kohteeseen siten, että hyökkääjällä on täytynyt olla huomattavan paljon yksityiskohtaistakin tietoa hyökkäyksen kohteesta. Myös joidenkin valtiollisten toimijoiden arvioidaan aiheuttavan potentiaalisia uhkia yritysten ja yhteiskunnan toiminnalle kyberympäristössä.

Kyberympäristön ongelmat voivat olla tahallisesti aiheutettuja, mutta toimintaympäristön häiriö voi syntyä myös esimerkiksi teknisestä viasta johtuen. Tarkoituksellisen kyberhyökkäyksen vaikuttimina voi olla esimerkiksi taloudellisen hyödyn tavoittelu, teollisuusvakoilu taikka vakavimmillaan tavoite häiritä tai peräti lamauttaa yhteiskunnan kriittisiä toimintoja. Valiokunnan saaman selvityksen mukaan esimerkiksi valtaosa nykyisistä haittaohjelmatapauksista voidaan luokitella taloudellista hyötyä tavoitteleviksi. Vaikuttimena voi kuitenkin olla myös aktivismi tai jopa valtiollinen intressi. Konkreettisena pyrkimyksenä voi olla esimerkiksi tietojen anastaminen ja väärinkäyttäminen, tietojärjestelmään sisältyvien tietojen vääristäminen tai esimerkiksi jonkin toiminnan keskeyttäminen. Yksilöön kohdistuvina riskeinä tavanomaisia ovat petostarkoituksessa tehdyt identiteettivarkaudet, esimerkiksi henkilötietojen tai luottokorttitietojen anastaminen. Mahdollisilla hyökkäyksillä voi kuitenkin olla vaikutuksia myös kokonaan muihin toimintoihin kuin mitä vastaan ne oli tarkoitettu.

Toimintaympäristön monimutkaisen luonteen vuoksi häiriöiden aiheuttajia, häiriön kokonaisvaikutuksia tai edes häiriöiden aiheuttamisen syitä voi kuitenkin olla vaikeaa arvioida. Erityisen haasteellista on arvioida eri sektoreiden välisiä riippuvuussuhteita sekä häiriöiden vaikutuksia eri sektoreihin ja yhteiskunnan kokonaisturvallisuuteen. Kyberympäristön häiriöiden vaikutusten arvioiminen edellyttänee väistämättä myös hyökkäysmenetelmien teknistä analysointia. Valiokunta toteaa saamansa selvityksen perusteella, että hyökkäysmenetelmiä koskevalla tietämyksellä saattaa jossain tapauksissa olla myös ennalta ehkäiseviä vaikutuksia kyberympäristön häiriöiden syntymisen kannalta.

Paljon palstatilaa viime vuosina saaneiden palvelunestohyökkäysten takana on todennäköisesti ollut useissa tapauksissa aktivismin kaltaisia vaikuttimia. Palvelunestohyökkäykset eivät kuitenkaan pääsääntöisesti uhkaa esimerkiksi yhteiskunnan elintärkeitä toimintoja. Sen sijaan potentiaalinen uhka yhteiskunnan kriittisille toi-

minnoille olisi, jos joku pääsisi murtautumaan tai asentamaan esimerkiksi haittaohjelman niihin tietojärjestelmiin, joista kyseinen toiminto on riippuvainen. Valiokunnan saaman selvityksen mukaan keskeistä on pitää esimerkiksi rahaliikenteen, energiayhtiöiden, terveydenhuollon, teollisuuden ja logistiikan tieto-, tuotanto- ja ohjausjärjestelmät mahdollisuuksien mukaan erillään yleisistä viestintäverkoista. Avointen viestintäverkkojen kautta saatavilla olevat sähköisen asioinnin palvelut tai muut vastaavat verkon kautta tarjottavat pankki- yms. palvelut sen sijaan ovat periaatteessa haavoittuvia palvelunestohyökkäyksille, mihin tulee kiinnittää huomiota riittävin suojauskeinoin.

Valiokunta kiinnittää huomiota siihen, että kovaa vauhtia yleistyvillä erilaisten toimintojen toteutusta hajauttavilla pilvipalveluilla on asiantuntijakuulemisen perusteella sekä turvallisuushyötyjä että kyberympäristön uhkia lisääviä piirteitä. Valiokunta toteaa, että vuonna 2013 toimintansa todennäköisesti aloittavan Pilvipalveluiden kehittämislaboratorion olisi hyvä keskittyä toiminnassaan myös näiden kysymysten arviointiin.

Kriittisten suojattavien kohteiden priorisointi on rajallisten resurssien vuoksi välttämätöntä. Valiokunnan käsityksen mukaan priorisoinnissa on keskeistä arvioida, millä toiminnoilla on eniten kokonaisvaikutuksia yhteiskunnan elintärkeisiin ja kriittisiin toimintoihin. Tietojärjestelmiä toisiinsa yhdistävillä avoimilla viestintäverkoilla on avainasema kyberturvallisuuden saavuttamisessa. Näiden verkkojen toiminnan vakavilla häiriöillä olisi hyvin laajoja ja vakavia vaikutuksia koko muuhun kyberympäristöön ja siitä riippuvaisiin toimintoihin. Viestintäverkoilla ja joukkoviestinnän toimivuudella on olennainen merkitys myös erilaisten häiriötilanteiden vaatiman tiedottamisen ja varoitusten välittämisen kannalta.

Valiokunta korostaa, että kyberturvallisuuden selkäranka on tietoturvallisuus ja ennen kaikkea se, että kaikki keskeiset toimijat toteuttavat omalta osaltaan kyberturvallisuuden tavoitetilan saavuttamisen vaatimat tietoturvallisuusmenettelyt. Toimenpiteiden laiminlyönti jonkun toimijan osalta lisää kyberympäristökokonaisuuden turvattomuutta myös muiden toimijoiden kannalta, joten kaikkien keskeisten kotimaisten toimijoiden tulisi kantaa oma vastuunsa yhteisen toimintaympäristön turvallisuuden varmistamiseksi.

Strategian visio

Kyberturvallisuusstrategian visiona on esitetty, että Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan. Lisäksi kansalaisilla, viranomaisilla ja yrityksillä tulee olla mahdollisuus hyödyntää tehokkaasti turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.

Valiokunta näkee kansalaisten kannalta tärkeänä avoimen, vapaan ja luotettavan kyberympäristön luomisen ja ylläpitämisen. Elinkeinoelämän näkökulmasta kyberympäristön taas tulee olla turvallinen liiketoimintaympäristö. Koko yhteiskunnan toiminnan näkökulmasta kyse on näiden tavoitteiden lisäksi keskeisesti elintärkeiden toimintojen turvaamisesta. Valiokunta pitää strategian vision mukaisesti tärkeänä, että kaikilla toimijoilla on mahdollisuus hyödyntää turvallista kyberympäristöä mm. kasvun, kilpailukyvyn ja innovaatioiden tukemiseksi. Tämän tavoitteen kannalta keskeistä on huolehtia viestintäverkkojen toimivuudesta ja käytettävyydestä. Itsestään selvää on, että Suomen elintärkeiden toimintojen jatkuvuus tulee pyrkiä turvaamaan kaikissa tilanteissa kybertoimintaympäristön uhkia vastaan. Valiokunta korostaa, että tämän tulee olla strategian toimeenpanossa ensisijainen tavoite, jonka varmistamiseksi on löydyttävä myös riittävästi resursseja.

Hallitusohjelman tavoitteena on, että Suomi on yksi johtavista maista kyberturvallisuuden kehittämisessä. Strategian keskeisenä visiona taas on, että Suomi on vuonna 2016 maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa. Valiokunta pitää asetettua tavoitetta kunnianhimoisena, mutta aikataulultaan hyvin haasteellisena. Strategian mukaan vuoden

2013 aikana laaditaan vasta strategian käytännön toimenpiteiksi konkretisoivat toimeenpano-ohjelmat, joten konkreettisten toimenpiteiden toteuttamiseen tavoitteen saavuttamiseksi jää kovin vähän aikaa. Valiokunta katsoo, että strategian tavoitteita tulisi pystyä edistämään ilman tarpeetonta viivästystä jo ennen eri toimeenpano-ohjelmien valmistumista ja niiden mahdollista yhteensovittamisvaihetta.

Strategiassa on tunnistettu Suomen etuina kyberturvallisuuden toteuttamisen näkökulmasta mm. osaaminen, pienestä koosta johtuva kyky nopeisiin liikkeisiin ja osin ehkä myös pienestä koosta johtuva yksityisen ja julkisen sektorin toimiva ja pitkään jatkunut luottamuksellisen yhteistyön ja verkostoitumisen perinne. Strategian mukaan Suomella on erinomaiset edellytykset nousta näillä eväillä kyberturvallisuuden kärkimaaksi. Valiokunta pitää erittäin tärkeänä, että näitä edellä mainittuja etuja pyritään edelleen kehittämään ja hyödyntämään täysimääräisesti strategiassa määritellyn vision tavoittelemisessa.

Kansallinen koordinaatio ja johtaminen

Valiokunta näkee strategian tavoitteiden saavuttamisen kannalta keskeisenä eri alojen strategian toimeenpano-ohjelmien koordinoimisen, varautumistoimenpiteiden koordinoimisen ja johtosuhteet varsinaisissa häiriötilanteissa. Myös rahoituksella ja sen riittävyydellä on käytännössä avainasema lopputuloksen kannalta.

Strategian mukaan kyberturvallisuuteen liittyvät asiat kuuluvat pääsääntöisesti valtioneuvoston toimivaltaan ja kyberturvallisuuden johtamisen ylimmän tason muodostaa valtioneuvosto. Valiokunta toteaa, että kyberturvallisuuden varmistaminen edellyttää poliittista ohjausta ja myös rajallisten resurssien tarkoituksenmukaista kohdentamista.

Strategia ei lähtökohtaisesti vaikuta viranomaisten nykyisiin toimivaltarajoihin. Strategian mukaan kukin ministeriö vastaa omalla toimialallaan valtioneuvostolle kuuluvien kyberturvallisuuteen liittyvien asioiden valmistelusta ja toteuttamisesta. Strategiassa kuitenkin kiinnitetään huomiota erityisesti poliisia ja puolustusvoimia koskevien toimivaltuuksien muutostarpeiden arviointiin. Valiokunta kiinnittää huomiota siihen, että turvallisuusviranomaisilla voi olla sen kaltaista osaamista, jota voitaisiin hyödyntää nykyistä paremmin myös muilla sektoreilla kyberturvallisuuden edistämiseksi. Eri hallinnonalojen osaamisen ja hyvien käytäntöjen siirtäminen on välttämätöntä rajallisten resurssien vuoksi.

Strategiassa puhutaan monin paikoin koordinoinnista ja sen tarpeesta, mutta tätä tehtäväkokonaisuutta ei selkeästi osoiteta millekään yksittäiselle elimelle. Valiokunta toteaa, että lähtökohta, jossa kukin ministeriö varautuu oman hallinnonalansa osalta periaatteessa erikseen, on haastava. Valiokunnan saaman selvityksen mukaan kyberympäristö haastaa perinteisiä hallinnonalojen rajoja ja rakenteita ja saattaa tehdä ne myös joltain osin vanhanaikaisiksi. Valiokunta korostaa, että kybertoimintaympäristö ei tunnista valtioiden, saatikka ministeriöiden, välisiä raja-aitoja ja kybertoimintaympäristökokonaisuuden turvallisuuden hallinta vaatii siten välttämättä tehokasta johtamista ja hyvin tiivistä yhteistyötä. Strategian linjauksen (strateginen linjaus 1) mukaan Suomessa luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli. Strategian mukaan tavoitteena on yhteinen ja jaettu tilannetietoisuus ja yhteistoimintaa harjoitellaan säännöllisesti. Lisäksi tiedonvaihtoa viranomaisten ja elinkeinoelämän kesken edistetään kehittämällä sääntelyä ja yhteistyötä. Koska strategiassa on pääosin päädytty säilyttämään nykyiset viranomaisten tehtäväkokonaisuudet ja -rajat, valiokunta pitää strategian tavoitteiden saavuttamisen ja strategian toimeenpanon kannalta tehokkaiden yhteistoimintamallien kehittämistä yhtenä keskeisimmistä tavoitteista.

Strategian mukaan strategian toimeenpano-ohjelma koostuu eri toimijoiden ja hallinnonalojen laatimista suunnitelmista ja niiden pohjalta laadittavista poikkihallinnollisista toimenpiteistä. Valiokunta toteaa, että tavoitteiden saavuttamiseksi asetetuissa aikatauluissa on hajautetus-

ta toimeenpanosta ja yhteistyömallista huolimatta pystyttävä luomaan kokonaisnäkemys tarvittavista toimenpiteistä. Valiokunta katsoo, että tämä vaatii joko selkeästi toimenpiteiden koordinaatiosta vastaavan tahon määrittelyä jatkossa tai poikkeuksellisen tiivistä ja aidosti kokonaishyötynäkökulmasta lähtevää yhteistyötä eri ministeriöiden välillä. Tämä koskee toimeenpano-ohjelmien laatimisen lisäksi myös operatiivista toimintaa häiriötilanteissa, joissa eri hallinnonalojen on välttämätöntä tukea tietyssä käytännön tilanteessa päävastuussa olevan hallinnonalan toimintaa. Koordinaatiolla tulee pystyä myös varmistamaan, etteivät käynnistettävät toimenpiteet tarpeettomasti kilpaile samoista resursseista.

Valiokunnan saaman selvityksen mukaan Alankomaissa ollaan kyberstrategian suhteen jo selkeästi strategian toimeenpanovaiheessa. Alankomaissa on perustettu Kyberturvallisuusneuvosto, joka suunnittelee ja toimeenpanee strategian implementoinnin. Lisäksi on perustettu (kuten Suomessakin tullaan perustamaan) Kyberturvallisuuskeskus, jolla on kuitenkin Alankomaissa selkeästi myös operatiivisen toiminnan ohjaamiseen liittyviä tehtäviä. Lisäksi ollaan perustamassa kyberturvallisuuden koulutus- ja harjoituskeskusta. Alankomaissa on siten lähdetty toimeenpanon osalta huomattavasti Suomea keskitetympään toiminta- ja johtamismalliin. Kun Suomessa kukin ministeriö vastaa itsenäisesti omasta hallinnonalastaan myös kyberturvallisuuden osalta, Alankomaissa Kyberturvallisuusneuvostolla ja osin myös Kyberturvallisuuskeskuksella on valiokunnan saaman selvityksen mukaan selkeä rooli myös operatiivisessa johtamisessa.

Valiokunta pitää strategian selkeänä heikkoutena komentoketjukokonaisuuden määrittelyn puuttumista, mikä todennäköisesti vähentää strategian toteuttamisen tehokkuutta. Vakavassa häiriötilanteessa tulisi kaikille toimijoille olla täysin selvää, miten kokonaisuuden hallinta toimii ja kuka vastaa kokonaisuuden yhteensovittamisesta. Valiokunta pitää tärkeänä, että jatkovalmistelussa pohditaan johtamisrakenteisiin ja vastuunjakoon liittyviä kysymyksiä ja pyritään kehittämään toimivia prosesseja toiminnan tehokkuuden varmistamiseksi.

Strategiassa ei esitetä kyberturvallisuustyössä käytettävissä oleviin resursseihin muutoksia tai tuoda esille kustannusarvioita. Strategian mukaan ministeriöt, virastot ja laitokset sisällyttävät kyberturvallisuusstrategian toimeenpanon edellyttämät voimavarat omiin toiminta- ja taloussuunnitelmiinsa. Nykyisessä taloudellisessa tilanteessa ei resursseja ole kovin helposti osoitettavissa uusiin käyttötarkoituksiin, mikä vaatinee priorisointia myös strategian toteutuksen painopisteiden osalta. Valiokunta katsoo, että kokonaisuuden kannalta energia- ja tietoliikennesektorit ovat eräitä keskeisiä painopistealueita, joihin panostamalla voidaan saavuttaa laajaa vaikuttavuutta koko yhteiskunnan kannalta. Valiokunta toteaa, että kyberturvallisuudesta huolehtiminen on kallista, mutta siihen panostamalla saatetaan välttyä vielä suuremmilta kustannuksilta.

Valiokunta katsoo, että strategiassa on jossain määrin painotettu enemmän uhkiin varautumista tilannekohtaisen reagoinnin ja palautumiskyvyn sijasta. Valiokunta toteaa saamansa selvityksen perusteella, että kaikkien relevanttien toimijoiden varautuminen on välttämätöntä asetettujen tavoitteiden saavuttamiseksi. Ennakollisella varautumisella on keskeinen merkitys siihen, miten tehokkaasti käytännön häiriötilanteissa pystytään toimimaan. Normaaliaikojen varautumisella luodaan käytännössä myös pohja poikkeusoloissa toimimiselle. Lähtökohtaisesti esimerkiksi tieto- ja viestintäjärjestelmien osalta tulee jo normaalioloissa huolehtia siitä, että ne ovat riittävän suojattuja ja varmennettuja kestääkseen lähtökohtaisesti kaikissa turvallisuustilanteissa niihin kohdistuvia uhkia. Varautuminen on kuitenkin usein hyvin kallista, ja kyberympäristön vaikean ennakoitavuuden vuoksi varautumisella ei koskaan pystytä vastaamaan kaikkiin mahdollisiin tapahtumiin. Lisäksi valiokunnan saaman selvityksen mukaan mm. tietojärjestelmien tietojen käytettävyyden vaatimus saattaa asettaa rajoituksia hyvin pitkälle viedyn etukäteisen varautumisen toteuttamiselle. Tästä syystä on valiokunnan käsityksen mu-

kaan tärkeää, että häiriötilanteiden operatiiviseen toimintakykyyn ja häiriöistä toipumiskykyyn panostetaan voimakkaasti.

Strategiassa puhutaan kyberuhkien sietokyvystä ja sen mitoittamisesta siitä näkökulmasta, että sietokyvyllä tulee kyetä luomaan kokonaisturvallisuuden vaatimusten mukainen varautumis- ja ennakointikyky, toimintakyky häiriötilanteissa ja häiriöiden jälkeinen toipumis- ja palautumiskyky. Valiokunta toteaa, että toimeenpano-ohjelmien laatimisen yhteydessä olisi hyvä arvioida yleisesti periaatteellisena kysymyksenä myös sitä, miten kauan häiriöihin tulee suhtautua siten, että keskitytään vain haittojen vähentämiseen ja ehkäisemiseen.

Valiokunta kiinnittää huomiota siihen, että kyberympäristö on omiaan hämärtämään myös perinteistä normaaliolojen, häiriötilanteiden ja poikkeusolojen sekä erityistilanteiden määrittelyä. Reaalimaailmassa totutut mallit eivät välttämättä sellaisinaan sovellu ongelmatilanteiden luokitteluun ja niiden pohjalta tehtäviin johtopäätöksiin. Keskeinen haaste jatkossa on tunnistaa, missä vaiheessa ja millä kriteereillä jokin häiriö muuttuu tavanomaisesta normaaliajan häiriötilanteesta joksikin muun luonteiseksi tilanteeksi, mikä voi vaikuttaa tietyssä häiriötilanteessa myös toimivaltaisen viranomaisen määräytymiseen.

Valiokunta kiinnittää huomiota siihen, että strategian mukaan kokonaisturvallisuuden alalla toimivaksi varautumisen yhteistoimintaelimeksi perustetaan Turvallisuuskomitea, jonka tehtävistä säädetään erikseen. Strategian (strateginen linjaus 10) mukaan komitea seuraa ja yhteensovittaa strategian toimeenpanoa. Yhteensovittamisen tavoitteina tuodaan esille päällekkäisen toiminnan välttäminen, mahdollisten puutteiden tunnistaminen ja varmistuminen vastuutahoista. Strategian taustamuistiossa taas tuodaan esille, että komitea koordinoi varautumista, seuraa strategian toimeenpanoa ja tekee esityksiä sen jatkokehittämiseksi. Varsinaiset päätökset toimeenpanossa tekisi kuitenkin vastuuministeriö. Kyse lienee ennen kaikkea neuvoa-antavasta asiantuntijaelimestä, jolla parhaimmillaan kuitenkin saattaisi valiokunnan käsityksen mukaan olla toteutustavasta riippuen keskeinen asema yksittäisten toimenpiteiden järkevän koordinoinnin kannalta. Kaiken kaikkiaan komitealle annettava rooli, sen kokoonpano ja toimintapaikka jäävät kuitenkin strategiassa hyvin avoimiksi.

Tilannekuvan merkitys ja Viestintäviraston rooli

Johtamisen ja häiriötilanteiden hallinnan näkökulmasta on ensiarvoisen tärkeää, että tehtävien päätösten perustaksi on saatavilla luotettavaan tietoon ja sen analysointiin perustuva ajantasainen ja kattava tilannekuva. Jos tilannetta koskevien tietojen todenperäisyyteen, ajantasaisuuteen ja eheyteen ei voida luottaa, päätösten tekeminen vaikeutuu huomattavasti.

Strategian mukaan (strateginen linjaus 2) elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten tahojen tilannetietoisuutta parannetaan tarjoamalla koottua, ajantasaista ja analysoitua tietoa haavoittuvuuksista, häiriöistä ja niiden vaikutuksista. Strategiassa esitetään, että Viestintäviraston yhteyteen perustetaan tätä tarkoitusta varten Kyberturvallisuuskeskus. Keskuksen tehtävänä on palvella ja toimia yhteistyössä viranomaisten, elinkeinoelämän ja muiden toimijoiden kanssa. Toiminnassa korostuu myös kansainvälinen ulottuvuus ja kansainvälisen yhteistyön tarve uhkien analysoinnissa ja niiden vaikutusten arvioinnissa. Käytäntö on osoittanut, että suurimittaisissa kyberympäristön häiriötilanteissa ei ole mahdollista toimia optimaalisesti ilman tehokkaita kansainvälisiä yhteistyöverkostoja.

Kyberturvallisuuskeskuksen päätehtävät ovat strategian mukaan tilannekuvan muodostaminen ja jakaminen, riskianalyysin kokoaminen ja ylläpito, viranomaisten ja yksityisen sektorin tukeminen laajojen kyberhyökkäysten hallinnassa ja yhteistyön tehostaminen sekä osaamisen kehittämisen tukeminen. Strategian mukaan kyberturvallisuuden toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta- ja analysointijärjestelmään, yhteiseen tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteis-

toimintaan varautumisessa. Valiokunta katsoo, että Kyberturvallisuuskeskuksella on oma roolinsa kaikissa tämän toimintamallin osa-alueissa ja myös operatiivisen yhteistyön mahdollisuuksien luomisessa.

Valiokunta pitää Kyberturvallisuuskeskuksen perustamista Viestintäviraston yhteyteen hyvin perusteltuna. Viestintävirastolla on jo nykyisin mm. kyberturvallisuuden selkärankana toimivien viestintäverkkojen toimintaan ja turvallisuuteen liittyviä tehtäviä, sillä on tarvittavaa osaamista ja mm. CERT-FI-yksikön toiminnassa luotuja kansainvälisiä kontakteja. Valiokunnan käsityksen mukaan Viestintävirasto on kaikkien toimijoiden, myös elinkeinoelämän, kannalta neutraalina toiminnon sijoituspaikkana omiaan edistämään toimivan, tiiviin ja luottamuksellisen yhteistyön syntymistä eri toimijoiden välille. Molemminpuoliseen luottamukseen perustuvan yhteistyön kehittäminen keskuksen ja muiden toimijoiden välille on välttämätöntä tiedon tehokkaan ja molempiin suuntiin tapahtuvan vaihdon mahdollistamiseksi.

Koska yksityinen sektori hallinnoi valtaosaa siitä infrastruktuurista ja niistä toiminnoista, jotka ovat yhteiskunnan toiminnan kannalta kriittisiä, myös keskuksen toiminnan yksi keskeinen painopiste tulee olla yritysten tukeminen kyberuhkilta suojautumisessa ja niiden torjunnassa. Erityisen tärkeää on pyrkiä siihen, että laadittavalla tilannekuvalla on mahdollisimman suuri hyöty huoltovarmuuden kannalta kriittisten yritysten toteuttamien turvallisuustoimenpiteiden kannalta. Alkuvaiheessa lienee keskeistä tunnistaa eri toimijoiden tiedontarpeet, jotta keskuksen toimintaa ja toimintatapoja voidaan suunnitella tämän mukaisesti. Valiokunta pitää myös tärkeänä, että keskuksen työn tueksi kootaan tehtävään sitoutunut verkosto kaikista niistä toimijoista, joiden tulee varautua kyberturvallisuutta koskeviin häiriöihin ja loukkauksiin.

Strategian mukaan (strateginen linjaus 4) huolehditaan myös siitä, että poliisilla on tehokkaat edellytykset ennaltaehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia. Lisäksi strategisena linjauksena (strateginen linjaus 5) on tuotu esille, että puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään. Valiokunta pitää tärkeänä, että poliisin, puolustusvoimien ja perustettavan Kyberturvallisuuskeskuksen välille luodaan toimivat yhteistoimintamallit.

Valiokunta pitää kokonaisuuden ja päällekkäisen toiminnan ehkäisemisen kannalta erityisen tärkeänä, että perustettavan Kyberturvallisuuskeskuksen toiminta ja yhteistoiminnan toteuttaminen ulotetaan tehokkaasti teleyritysten ja huoltovarmuuden kannalta kriittisten yksityisen sektorin toimijoiden lisäksi myös valtionhallinnon toimijoihin. Valiokunta pitää hyvin tärkeänä, että kyberturvallisuutta tavoitellaan ilman tarpeettomia päällekkäisiä ja resursseja syöviä toimintoja tai tiedon jakamisen rajoitteita. Valtioneuvoston ohjesäännön mukaan valtionhallinnon tietoturvallisuus kuuluu valtiovarainministeriön toimialaan, mikä koskee myös valtiokonsernin tietoturvaloukkauksia ja uhkia käsittelevän niin sanotun GovCERT-toiminnon järjestämisvastuuta.

Valiokunta korostaa, että perustettava Kyberturvallisuuskeskus on kriittisen tiedon lähteenä erityisen kiinnostava kohde kyberhyökkäyksille. Keskuksen suojaamiseen tulee siten kiinnittää erityistä huomiota keskuksen toimintakyvyn turvaamiseksi ja tietojen luottamuksellisuuden säilymiseksi.

Valiokunta pitää Kyberturvallisuuskeskuksen perustamista strategian yhtenä keskeisimmistä ja vaikuttavuudeltaan merkittävimmistä linjauksista, jolla on kaikkia sektoreita hyödyntäviä vaikutuksia. Keskuksen tehtävien toteuttamiseksi tulee siten ehdottomasti huolehtia siitä, että toimintaan varataan tehokkaaseen ja uskottavaan ympärivuorokautiseen toimintaan riittävät ja toimintoon kohdistettaviin odotuksiin nähden linjassa olevat henkilöstö- yms. resurssit. Resurssien tarvetta tulee seurata jatkossa siten, että myös mahdollinen toimintaympäristön muutoksista johtuva tehtävien lisääntyminen otetaan huomioon resurssien määräytymisessä.

Yksityisten toimijoiden rooli

Valtaosa yhteiskunnan elintärkeästä infrastruktuurista on yksityisessä omistuksessa, ja sen käyttö ja ylläpito perustuu liiketoiminnallisiin lähtökohtiin. Tämä koskee myös tietojärjestelmiä, viestintäverkkoja ja niiden tietoturvan toteuttamista. Käytännössä strategian tavoitteiden saavuttaminen edellyttäisi siten erityisesti yritysmaailman aktiivisia toimenpiteitä. Valiokunta pitää tästä syystä erittäin tärkeänä, että elinkeinoelämä pidetään strategian toimeenpano-ohjelmien laatimisessa tiiviisti mukana ja toimeenpanossa pyritään tehostamaan entisestään yksityisen ja julkisen sektorin välistä, molempia osapuolia hyödyntävää yhteistyötä. Erityisen tärkeää on varmistaa tiedon kulku molempiin suuntiin.

Viranomaisten välisen tai julkisen ja yksityisen sektorin välisen yhteistyön lisäksi on erittäin tärkeää kehittää ja tiivistää yhteistyötä myös yksityisen sektorin toimijoiden välillä. Erityisen tärkeää olisi varmistaa selkeästi toisistaan riippuvaisten ja tämän lisäksi huomattavasti muihin yhteiskunnan kriittisiin toimintoihin vaikuttavien teleyritysten ja energiayritysten välisen yhteistyön saumattomuus esimerkiksi myrsky- tai muiden häiriötilanteiden hallitsemiseksi ja tämänkaltaisista häiriöistä toipumisen nopeuden varmistamiseksi. Esimerkiksi energiayhtiöiden korjaustöitä koskevilla valmiuksilla ja korjaustöiden tilannetta koskevalla tiedolla on keskeinen merkitys teleyritysten viestintäverkkojen ja palvelujen toiminnan kannalta.

Strategian mukaan (strateginen linjaus 9) Suomessa määritellään viranomaisille ja elinkeinoelämälle tehtävät kyberturvallisuuden toteuttamisessa siten, että kukin hallinnonala tekee analyysin, jolla tunnistetaan keskeiset haavoittuvuudet ja niiden hallinnan nykytila. Tältä pohjalta laaditaan hallinnonalan toimeenpano-ohjelmat ja tuetaan elinkeinoelämän vastaavien ohjelmien tekemistä. Strategian mukaan (strateginen linjaus 3) yhteiskunnan elintärkeiden toimintojen kannalta keskeisten yritysten ja muiden organisaatioiden kykyä havaita ja torjua kyberuhkia sekä toipua häiriöistä kehitetään. Käytännössä tämä tarkoittaa strategian mukaan mm. sitä, että kyseiset toimijat ottavat turvallisuus- ja valmiussuunnittelussaan huomioon kyberuhat ja niiden haitallisten vaikutusten minimoimisen. Toimijat kehittävät sietokykyään siten, että niiden toiminta ei keskeydy esim. kyberhyökkäysten alaisena. Valiokunta pitää näitä linjauksia kannatettavina. Yksityisten toimijoiden kannalta toimeenpano-ohjelmien laatimisessa olisi olennaista pohtia myös sitä, millä logiikalla ja intressillä yritykset lähtevät tehokkaasti toteuttamaan kansallisen strategian edellyttämiä toimia. Omat haasteensa tähän kysymyksenasetteluun tuovat yritystoiminnan kansainvälistyminen, aiemmin kotimaisten yritysten ulkomainen omistus ja toimintojen ulkoistaminen.

Kansainväliset yritykset pitävät yritystoiminnan sijoittumispaikkoja ja investointeja koskevissa arvioinneissa yhtenä tekijänä myös toimintaympäristön turvallisuutta. Kyberturvallisuudella voidaan siten nähdä olevan myös huomattava taloudellinen arvo mm. investointien näkökulmasta. Valiokunta näkee tämän selkeänä mahdollisuutena Suomelle. Tavoittelemalla asetettua visiota pystytään paitsi kehittämään kansallista turvallisuutta myös edistämään Suomeen kohdistuvia investointeja. Valiokunta toteaa lisäksi, että Suomessa on jo nykyisellään kyberturvallisuuden toteuttamiseen liittyvää tietoturva- yms. huippuosaamista, mille pohjalle on mahdollista rakentaa toimintaedellytyksiä kehittämällä myös uutta kotimaista ja mahdollisesti myös vientikelpoista tuotekehitystä ja muuta liiketoimintaa. Kyberturvallisuuden alueella tapahtuu kansainvälisesti lähivuosina paljon, ja Suomen on hyvä pyrkiä saamaan osansa näistä kehittyvistä markkinoista.

Valiokunta katsoo, että kyberturvallisuuden näkökulmasta olisi tarpeen pohtia turvallisten hankintamenettelyjen vaatimuksia erityisesti kriittisen tieto- ja viestintäinfrastruktuurin tai ohjelmistojen toimittajien arvioinnissa. Valiokunta haluaa kiinnittää huomiota myös Suomen kansainvälisten viestintäyhteyksien järjestämiseen. Valiokunnan saaman selvityksen mukaan turvallisuuden ja yhteyksien häiriötilanteiden sietokyvyn kannalta voisi hyvinkin olla perusteltua, että vaihtoehtoisten kansainvälisten yhteyk-

sien määrää pyrittäisiin lisäämään nykyisestä. Vastaavasti saattaisi olla hyödyllistä pohtia joidenkin hyvin kriittisten viestintää koskevien järjestelmien maantieteellisen sijoittumisen merkitystä ja sen mahdollisia vaikutuksia kyberympäristön kokonaisturvallisuuteen.

Strategian mukaan parannetaan (strateginen linjaus 7) kaikkien yhteiskunnan toimijoiden kyberosaamista ja asiaa koskevaa ymmärrystä. Tässä tarkoituksessa mm. panostetaan ohjeistojen kehittämiseen, koulutukseen ja harjoitustoimintaan sekä perustetaan kyberturvallisuuden strateginen huippuosaamisen keskittymä ja panostetaan tutkimukseen. Valiokunta korostaa, että säännöllisillä ja kaikkien keskeisten julkisen ja yksityisen sektorin toimijoiden välisillä kyberturvallisuutta koskevilla harjoituksilla voi olla käytännössä huomattava merkitys operatiivisen yhteistyön toimivuuden kannalta. Valiokunta korostaa, että asiaa koskevan kotimaisen tutkimuksen edistämisen lisäksi tulisi pyrkiä aktiivisesti myös hyödyntämään ulkomaisia tutkimustuloksia.

Kansalaisten näkökulma

Valiokunta kiinnittää huomiota siihen, että strategiassa on varsin vähän käsitelty kansalaisten roolia kyberturvallisuuden kannalta. Kyberympäristön tulee olla kansalaisten kannalta turvallinen siten, ettei heidän oikeuksiaan loukata tässä ympäristössä. Toisaalta kansalaisten omalla toiminnalla on vaikutuksia kyberympäristön turvallisuuteen. Kyberturvallisuudella voidaan myös edistää kansalaisten luottamusta toimintaympäristöön, mikä on esimerkiksi sähköisen kaupankäynnin ja sähköisen asioinnin yleistymisen perusedellytyksiä.

Kyberturvallisuuden yksi ulottuvuus on perusoikeuksien toteutuminen kyberturvallisuusympäristössä häiriötilanteidenkin aikana. Kyberturvallisuuden toteuttamisessa tulee varmistaa, ettei esimerkiksi kansalaisten luottamuksellisen viestin suojaa tai laajemmin yksityisyyden suojaa rajoiteta perusteettomasti. Toisaalta lähtökohtaisesti voidaan nähdä, että kyberturvallisuuden edistämisellä edistetään samalla myös yksityisyyden- ja luottamuksellisen viestin suojan toteutumista. Strategian toimeenpanossa tulee pystyä vastaamaan tähän erilaisten tavoitteiden ja oikeuksien tasapainottelua vaativaan haasteeseen.

Kansalaisten henkilötiedot, salasanat ja luottokorttitiedot voivat olla kyberympäristössä petosten tekemisen välineitä, joita pyritään hankkimaan esimerkiksi tietojen kalastelun (phishing), näppäimistönauhureiden (keylogger) taikka kansalaisten tietoja käyttävien palveluiden tietojärjestelmiin murtautumalla. Kansalaisten sähköisen indentiteetin suojaaminen kyberympäristössä on yksi keskeinen haaste tulevaisuudessa, johon tulisi kiinnittää huomiota myös strategian toimeenpanossa. Tältä kannalta henkilötietoja sisältävien tietokantojen keskittäminen suurempiin kokonaisuuksiin saattaa olla omiaan lisäämään kyberympäristön haavoittuvuutta.

Jokainen kyberympäristön toimija vaikuttaa osaltaan toimintaympäristön turvallisuuteen. Näin ollen myös kansalaisten viestintäverkkoihin liitetyt päätelaitteet tulisi pystyä suojaamaan siten, että niitä ei pystytä esim. kaappaamaan käytettäväksi palvelunestohyökkäysten tai roskapostin lähettämisen välineenä eikä niistä muutoinkaan aiheudu haittaa joko kansalaisille itselleen tai muille kyberympäristön toimijoille. Kansalaisten tulisi myös osata käyttää päätelaitteitaan ja hallinnoimiaan verkkoja siten, että tästä ei aiheudu haittaa esim. viestintäpalveluiden tai viestintäverkkojen toiminnalle. Myös kansalaisten matkapuhelinten ja erilaisten mobiilien päätelaitteiden laitetason turvallisuudella ja niihin sisältyvillä haavoittuvuuksilla tulee jatkossa todennäköisesti olemaan nykyistä suurempi merkitys kyberturvallisuuden kannalta, kun näiden yleiseen viestintäverkkoon kytkettyjen hyvin erilaisten päätelaitteiden määrä lisääntyy maailmanlaajuisesti. Laitteiden tai niiden käyttöjärjestelmien turvallisuusominaisuuksiin on kuitenkin vaikeaa vaikuttaa puhtaasti kotimaisin keinoin.

Ennen kaikkea kansalaisten toimintaan ja käyttäytymiseen kyberympäristön valveutuneina käyttäjinä voidaan kansallisin keinoin vaikuttaa koulutuksen ja ohjeistuksen lisäämisen kaut-

ta, missä viestintäpalvelun tarjoajalla on oma roolinsa. Keskeistä olisi myös huomioida erikseen lapset ja heidän erityistarpeensa kyberympäristön toimijoina esimerkiksi koulujen opetuksen sisällössä. Valiokunta näkee koulutuksen kustannustehokkaana tapana edistää kyberturvallisuuden kehittymistä ja kansalaisten osaamista kybertoimintaympäristön käyttäjinä.

Lainsäädännön kehittäminen

Strategian mukaan (strateginen linjaus 8) Suomessa kartoitetaan kybertoimintaympäristöön ja turvallisuuteen vaikuttava ja liittyvä lainsäädäntö ja sen kehittämistarpeet ja laaditaan tältä pohjalta lainsäädännön kehittämisehdotukset. Ehdotuksilla pyrittäisiin mm. varmistamaan, että lainsäädäntö mahdollistaa kaikille toimijoille yhteiskunnan elintärkeiden toimintojen turvaamiseksi välttämättömät toimenpiteet. Erityisesti tämä koskenee viranomaisten toimivaltuuksia ja mm. tietojen käsittelyä ja luovuttamista eri toimijoiden välillä koskevia säännöksiä. Valiokunta pitää näitä linjauksia kannatettavina.

Suomessa on jo pitkään pyritty myös lainsäädännöllisin toimenpitein varmistamaan, että viestintäpalvelut ja viestintäverkot ovat toimintavarmoja ja turvallisia. Teleyrityksillä on viestintämarkkinalain (393/2003) 90 §:n perusteella velvollisuus huolehtia siitä, että niiden toiminta jatkuu mahdollisimman häiriöttömästi myös valmiuslaissa tarkoitetuissa poikkeusoloissa sekä normaaliolojen häiriötilanteissa. Varautumisesta teleyrityksille aiheutuvien ylimääräisten huomattavien kustannusten korvaamisesta säädetään viestintämarkkinalain 94 §:ssä. Viestintäviraston määräyksillä on määritetty tarkemmin, mitä nämä velvoitteet teknisesti tarkoittavat. Käytännössä varautuminen vaatii esimerkiksi henkilöstön kouluttamista, laitteiden ja järjestelmien teknistä suojaamista tai esimerkiksi varajärjestelmien rakentamista. Teleyritysten on myös toimitettava Viestintävirastolle tietoja erilaisista vika- ja häiriötilanteista ja tietoturvaloukkauksista, ja Viestintävirasto valvoo näiden vaatimusten täyttämistä. Valiokunnan näkemyksen mukaan teleyrityksiä koskee jo tällä hetkellä varsin kattava varautumista, tietoturvallisuutta ja mm. erilaisista häiriöistä ilmoittamista koskeva sääntely. Teleyritysten rooli kyberympäristön turvallisuuden kannalta on valiokunnan käsityksen mukaan keskeinen, mutta toisaalta valiokunta pitää erittäin todennäköisenä, että teleyritysten toiminnoissa on huomioitu tietoturvallisuus keskimäärin selkeästi paremmin kuin monissa muissa yhteiskunnan elintärkeiden toimintojen kannalta kriittisissä toiminnoissa.

Valiokunta kiinnittää huomiota siihen, että poikkeusoloja koskevan valmiuslain viranomaisten toimivaltuuksia koskevat säännökset ovat käytettävissä vasta siinä vaiheessa, kun tilanne on jo edennyt hyvin vakavaksi. Mikäli tilanteessa on kyse vakavasta viestintäverkkojen kautta toteutettavasta hyökkäyksen kaltaisesta tapahtumasta, kynnys ottaa valmiuslaki käyttöön on todennäköisesti erittäin korkea. Valmiuslain heikko kohta kyberympäristön kannalta on myös se, että toimivaltuuksien käyttöönottoon menee aikaa. Valmiuslain toimivaltuuksia koskevaa mekanismia voidaan pitää varsin hitaana kyberympäristössä, jossa erilaisia toimenpiteitä tulee voida toteuttaa hyvin nopeassa aikataulussa ja jossa erilaisten häiriötilanteiden vaikutukset voivat levitä muutamassa tunnissa tai jopa minuuteissa huomattavan laajalle. Kybertoimintaympäristön luonteesta ja ongelmien erittäin nopean etenemisen vuoksi vakavaa kyberhyökkäystä koskeva tilanne voisi olla esimerkiksi viestintäverkkojen toiminnan osalta jo menetetty siinä vaiheessa, kun valmiuslain toimivaltuuksia pyritään ottamaan käyttöön.

Kybertoimintaympäristön häiriöiden osalta on joitakin äärimmäisiä tilanteita lukuun ottamatta toimittava normaaliaikojen lainsäädännön pohjalta. Tästä syystä normaaliaikojen lainsäädännön muutostarpeiden ja -mahdollisuuksien arviointi on tärkeää kyberturvallisuuden näkökulmasta. Lainsäädäntö ei saa tarpeettomasti estää kybertoimintaympäristön turvallisuudesta huolehtimista, ja yhteiskunnan elintärkeiden toimintojen turvaamiseksi välttämättömän tiedon välittämisen tulee olla mahdollista. Valiokunta kuitenkin toteaa, että se pitää muutostarpeiden arvioinnissa erityisen tärkeänä, että kansalais-

ten perusoikeuksien, kuten luottamuksellisen viestin suojan ja laajemmin yksityisyyden suojan, toteutumisesta huolehditaan myös kyberympäristössä. Valiokunta pitää tätä hyvin tärkeänä myös toimintaympäristöä kohtaan tunnettavan luottamuksen kannalta.

Mikäli tämä katsotaan tarpeelliseksi ja tarkoituksenmukaiseksi, tulevaisuudessa on mahdollista vapaaehtoisiin yhteistyömalleihin perustuvan toiminnan lisäksi pohtia, olisiko nykyistä, lähinnä teleyrityksiä kyberympäristön toimijoina koskevan sääntelyn kaltaista tietoturvasääntelyä tai häiriöistä ilmoittamista koskevaa sääntelyä tarpeen joltain osin laajentaa koskemaan joitain muitakin kyberympäristön turvallisuuden tai yhteiskunnan elintärkeiden toimintojen kannalta keskeisimpiä toimijoita. Valiokunta pitää kuitenkin vapaaehtoista tai sopimusperusteista toimintamallia pakottavaa sääntelyä toivottavampana asetettujen tavoitteiden saavuttamisessa.

Kansainvälisenä ilmiönä kyberturvallisuuden häiriöt vaatisivat myös oikeudellisen tehokkuuden lisäämistä kansainvälisesti. Kyberympäristön ja siihen kuuluvien ongelmien kansainvälisen luonteen vuoksi kansainvälinen yhteistyö on käytännössä välttämätöntä kaikilla tasoilla ja kyberturvallisuuden kehittymisellä muissa maissa on positiivisia vaikutuksia myös Suomen kyberturvallisuuden kannalta. Strategian mukaan (strateginen linjaus 6) keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan tulee osallistua aktiivisesti kyberturvallisuuden osalta. Valiokunta toteaa, että erityisen tärkeää on pyrkiä seuraamaan ja omaksumaan hyviä kansainvälisiä käytänteitä ja osallistua aktiivisesti erityisesti EU-tason asioiden valmisteluun ja tehtävien linjausten määrittelemiseen. Valiokunta kiinnittää huomiota mm. valmisteluvaiheessa olevan EU:n verkko- ja tietoturvadirektiivin sekä EU:n kyberstrategian mahdollisiin vaikutuksiin toimeenpano-ohjelmien laatimisessa ja toteaa, että mainitun direktiivin valmisteluun tulee osallistua erittäin aktiivisesti.

Kyberturvallisuuden vaikutukset liikenteen toimintaan

Liikenne- ja viestintävaliokunta toteaa, että liikenne ja kuljetusten toimivuus ovat yhteiskunnan toiminnan kannalta kriittisiä toimintoja. Kuljetusten toimivuudella on keskeinen merkitys koko yhteiskunnan — viranomaisten, yritysten, teollisuuden ja kansalaisten — toimintakyvyn ja toiminnan kannalta. Monien yhteiskunnan elintärkeiden toimintojen jatkuminen vaatii myös sitä, että tietyt ihmiset pääsevät kaikissa tilanteissa työpaikalleen.

Liikenteen toiminta ja sujuvuus perustuu tänä päivänä olennaisesti tieto- ja viestintäjärjestelmien hyödyntämiseen. Riippuvuus näistä järjestelmistä vaihtelee eri liikennemuotojen välillä, mutta vakava, esimerkiksi joihinkin liikenteen ohjausjärjestelmiin tai sähkönjakeluun kohdistuva kyberympäristön häiriö voisi haitata merkittävästi liikennejärjestelmän toimintaa ja turvallisuutta. Liikennesektorilla on myös keskeisiä tietojärjestelmiä, jotka periaatteessa saattavat olla jonkin tahon kannalta kiinnostavia hyökkäyksen kohteita.

Valiokunta pitää älyliikenteen kehittämistä erittäin tärkeänä mm. liikenneturvallisuuden ja liikenteen sujuvuuden edistämiseksi. Älyliikenteen sovellusten kehittymisen ja yleistymisen myötä liikenteen riippuvuus kyberympäristöstä kuitenkin kasvaa ja riippuvuudet ulottuvat autotekniikan kehittymisen myötä myös ajoneuvojen toimintaan.

Valiokunta pitää erittäin tärkeänä, että kyberturvallisuusstrategian toimeenpano-ohjelman laatimisessa otetaan kattavasti huomioon myös kybertoimintaympäristön ja liikennejärjestelmän riippuvuussuhteet ja mahdolliset haavoittuvuudet.

Lopuksi

Valiokunta pitää kyberturvallisuusstrategiaa selkeästi eteenpäin vievänä askeleena, jonka toimeenpanoa ja vaikutuksia tulee seurata tiiviisti ja tarvittaessa olla kykeneviä myös riittävän nopeisiin suunnanmuutoksiin toimintaympäristön ja uhkakuvien muuttuessa.

Lausunto

Lausuntonaan liikenne- ja viestintävaliokunta esittää,

että ulkoasiainvaliokunta ottaa edellä olevan huomioon.

Helsingissä 3 päivänä huhtikuuta 2013

Asian ratkaisevaan käsittelyyn valiokunnassa ovat ottaneet osaa

pj.	Kalle Jokinen /kok	Johanna Ojala-Niemelä /sd
vpj.	Osmo Kokko /ps	Raimo Piirainen /sd
jäs.	Mikko Alatalo /kesk	Janne Sankelo /kok
	Thomas Blomqvist /r	Eila Tiainen /vas
	Markku Eestilä /kok (osittain)	Ari Torniainen /kesk
	Ari Jalonen /ps	Reijo Tossavainen /ps
	Jukka Kopra /kok	Oras Tynkkynen /vihr
	Merja Kuusisto /sd	Mirja Vehkaperä /kesk.

Valiokunnan sihteerinä on toiminut

valiokuntaneuvos Juha Perttula.