TRAFICOM LAUSUNTO
Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

Hallintovaliokunta
HaV@eduskunta.fi

Päiväys/Datum
17.02.2021
Dnro/Dnr
TRAFICOM/60558/03.03.01/2021
Viite/Referens
Hallintovaliokunta perjantai 19.02.2021 klo 11.15 / VNS 4/2020 vp / Asiantuntijapyyntö

Liikenne- ja viestintäviraston lausunto valtioneuvoston ulko- ja turvallisuuspoliittisesta selonteosta

Liikenne- ja viestintävirasto kiittää mahdollisuudesta lausua asiassa ja lausuu seuraavaa selonteosta erityisesti kyberturvallisuuden näkökulmasta.

Selonteossa esitetty toimintaympäristön kuvaus kyberturvallisuuden tilasta ja sen kehittymisestä vastaa suurilta osin sitä kuvaa, mikä Liikenne- ja viestintävirastolla on asiassa. Nopea teknologian kehittyminen ja digitalisaatio lisäävät yhteiskunnan tehokkuutta, mutta samalla myös haavoittuvuutta, toimintojen riippuvuutta toisistaan ja sitä kautta mahdollisten kyberhyökkäyksien mahdollisia kohteita ja vaikuttavuutta. Suojautumistoimenpiteitä on tehtävä jatkuvasti uusia muotoja saavan kybervaikuttamisen ja kyberuhkien hallitsemiseksi. Myös riippuvuus Suomen rajojen ulkopuolisista toimijoista ja toiminteista lisääntyy. Kansallisten ja kansainvälisten riippuvuuksien lisääntyminen voi johtaa tilanteisiin, joissa Suomi ja suomalaiset joutuvat kyberoperaation sivullisiksi uhreiksi ja sijaiskärsijöiksi.

Hybridivaikuttaminen on lisääntynyt merkittävästi maailmalla ja vaikuttamistoimenpiteitä on myös kohdistettu Suomeen ja suomalaisiin. Hybridivaikuttamisessa on käytetty ja voidaan käyttää hyväksi suuria globaaleja ilmiöitä, kuten pandemiat ja suuronnettomuudet, jotka itsessään aiheuttavat epätietoisuutta ja vaikuttaa oleellisesti yleiseen turvallisuudentunteeseen. Kyberrikollisuus on myös ilmiö, joka on edelleen yleistynyt ja monimuotoistunut niin maailmalla kuin Suomessa. Kyberrikollisuus on yleensä globaalia ja se ei tunnusta maiden rajoja. Kyberrikolliset toimivat siellä, missä niillä on parhaat edellytykset toiminnalleen ja missä esimerkiksi lainsäädäntö ja sitä valvovat viranomaiset ovat heikkoja rikollisuuteen puuttumiseksi. Kyberrikollisuus on hyvä esimerkki osa-alueesta, jolla muun muassa EU-tason yhteistyö on ehdoton edellytys tilanteen hallitsemiselle.

Teknologinen omavaraisuus ja erityisosaaminen ovat korostuneet viimeisten vuosien aikana esimerkiksi koronaviruksen ja Yhdysvaltain talouspakotepolitiikan seurauksena. Teknologinen omavaraisuus ja erityisosaaminen ei ole enää vain kilpailukeino erottautua muista maista vaan sillä ajetaan myös muita tavoitteita. Osaltaan tämä on johtanut lyhyen aikavälin tavoitteiden tavoitteluun pitkän aikavälin tavoitteiden kustannuksella sekä oman maan intressien ajamiseen. 5G-verkkojen yhteydessä nähty keskustelu ja kehitys eivät varmasti jää tässä aihepiirissä viimeiseksi. Varautumisessa on myös huomioitava se, että esimerkiksi kyberturvallisuustuotteista merkittävä valtaosa kehitetään ja valmistetaan nykyisin EU:n ulkopuolella. EU:n sisäisen kyberturvallisuusteollisuuden toimintaedellytyksien

turvaaminen on keskeinen osa tulevaisuuden varautumista.

Liikenne- ja viestintävirasto jakaa monelta osin selonteossa esitetyt näkemykset Suomen ulko- ja turvallisuuspolitiikan tavoitteista ja painopisteistä kyberturvallisuuden takaamisen osalta. Suomessa turvallisuutta on rakennettu vuosikymmenien ajan tiiviin yhteistyön varaan, ja on tärkeää, että tätä työtä jatketaan ja tiivistetään edelleen. Yhteistyöllä meillä on mahdollista saada käyttöön paras osaaminen rakentaa entistä turvallisempaa yhteiskuntaa ja reagoida nopeasti muuttuvaan maailmaan ympärillämme. Yhteistyötä tulee tehdä kansainvälisesti ja luonnolliset yhteistyökumppanit löytyvät muista Pohjoismaista ja EU-jäsenmaista. Kansallisesti hallinnonalojen yhtenäisyys ja yhteiskuntaa läpileikkaava yhteistyö äärettömän tärkeätä, jotta rajalliset resurssit saadaan hyödynnettyä optimaalisesti. Kyberturvallisuuden kannalta on erityisesti tärkeää tehdä tiivistä yhteistyötä sellaisten maiden kanssa, joiden kautta Suomen kannalta tärkeimmät kansainväliset verkkoyhteydet ja tietoliikenne ohjautuvat muualle maailmassa sekä joissa on Suomen kannalta kriittisten toimialojen yrityksien toimipisteitä. Kyberturvallisuuteen liittyvät ilmiöt ja uhat ovat lähes poikkeuksetta globaaleja ja niihin vastaaminen edellyttää yhä tiiviimpää kansainvälistä yhteistyötä. Siten myös yhteisen tilannekuvan jakamisesta ja muodostamisesta tulee entistä tärkeämpää globaaleihin uhkiin varautumisessa.

Liikenne- ja viestintävirasto pitää tärkeänä, että kyberturvallisuuteen kiinnitetään huomioita kaikilla toiminnan tasoilla ja tarvittavat kyberturvallisuutta parantavat toimenpiteet suunnitellaan ja toteutetaan huolella. Tähän tarvitaan oikein kohdistettua rahoitusta ja kansallista yhteistyötä. Esimerkiksi yleisiä viestintäverkkoja ja -palveluja käyttävien toimijoiden tulee huolehtia myös omasta kyberturvallisuudestaan eikä ne voi tuudittautua vain siihen, että teleyritykset ovat huolehtineet viestintäverkkojen ja -palveluiden kyberturvallisuudesta. Toimijoiden tulee myös ymmärtää omaan toimintaansa suoraan kohdistuvat kuin myös niihin riippuvuussuhteessa olevien toimijoiden kautta epäsuorasti kohdistuvat kyberturvallisuusuhat ja varauduttava näihin kaikkiin uhkiin. Kaikkiin palveluiden ja tuotteiden tarjoajiin tulee suhtautua kriittisesti ja terveen epäluuloisesti kyberturvallisuusriskejä arvioitaessa.

Liikenne- ja viestintävirasto pitää myös tärkeänä, että Suomessa jatketaan vuosikymmeniä tehtyä määrätietoista työtä entistä turvallisempien ja toimintavarmempien viestintäverkkojen ja -palvelujen kehittämiseksi huomioiden uudet verkkoteknologiat ja yhteiskunnan entistä suurempia riippuvuus toimivista ja luotettavista viestintäverkoista ja -palveluista. Kehittämistyössä tulee jatkossakin huomioida varautuminen niin normaaliolojen häiriötilanteisiin kuin poikkeusoloihin. Kehittämistyön tulee olla kokonaisvaltaista eikä se saa keskittyä liikaa vain yksittäisiin toimenpiteisiin kyberturvallisuuden parantamiseksi. On myös tärkeää, että osana varautumista, Suomessa ja EU:ssa entistä enemmän kiinnitettään huomioita merkittävien kansainvälisten tietoliikenneyhteyksien, mukaan lukien merikaapeleiden, omistajuuteen. Viime vuosina on tehty merkittäviä kansainvälisiä yhteyksiä koskevia omistusjärjestelyitä ja tällä hetkellä esimerkiksi merkittävä osa Euroopan kansainvälisten yhteyksien omistuksesta on EU:n ulkopuolella. Myös osaaminen ja rakentamisessa tarvittavan kaluston, esimerkiksi merikaapeleiden rakentamiseksi ja huoltamiseksi, omistus on monelta osilta siirtynyt EU:n ja Suomen ulkopuolelle. Kansainvälisten yhteyksien kannalta tulee vähintäänkin varmistaa, että Suomesta on yhteyksiä muuhun maailmaan useiden eri maiden kautta, jolloin Suomen riippuvuutta yksittäisten naapurimaiden kautta kulkevista kansainvälisistä yhteyksistä voidaan alentaa. Tässä arktisen alueen hyödyntäminen uusien

merikaapelireittien rakentamiseksi Suomesta ulkomaille ja uusien palvelinkeskusten houkuttelemisen Suomeen tulee olemaan merkittävässä asemassa.

Poliittisesti vakaa yhteiskunta ja EU, jossa noudatetaan ihmisoikeuksia ja oikeusvaltioperiaatteita sekä edistetään demokratiaa, rauhaa, vapautta, yhdenvertaisuutta ja tasa-arvoa, ovat perusta, jolle voidaan rakentaa myös vakaa kyberturvallisuusympäristö. Ilman näitä perusrakenteita myös kyberturvallisuuden rakentaminen on haastavaa. Liikenne- ja viestintävirasto pitää tärkeänä, että korkeasta yksityisyydensuojan tasosta ja sen mahdollistamasta tietoliikenteen salauksesta pidetään huolta, kun suunnitellaan toimia esimerkiksi terrorismin torjumiseksi. Tietoliikenteen salauksen heikentäminen ei ainoastaan heikennä yksittäisten henkilöiden yksityisyydensuojaan, vaan se heikentää myös yhteiskunnan kyberuhkilta suojautumista.

Sauli Pahlman

vt. Ylijohtaja

Liikenne- ja viestintävirasto

Tämä asiakirja on allekirjoitettu sähköisesti. Liikenne- ja viestintävirasto (Traficom) 17.2.2021. Allekirjoituksen oikeellisuuden voi todentaa sähköisiä allekirjoituksia tukevalla lukijaohjelmalla tai Traficomin kirjaamosta.

Pahlman Sauli
Johtaja