20.4.2022

Eduskunta
Liikenne- ja viestintävaliokunta

Asia: VNS 1/2022 vp Ajankohtaisselonteko turvallisuusympäristön muutoksesta / Asiantuntijapyyntö

Lausunto: Ajankohtaisselonteko turvallisuusympäristön muutoksesta

Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Kyberala kiittää mahdollisuudesta lausua otsikkoasiassa kiinnittäen huomionsa *digitaaliseen toimintaympäristöön (ml. tietoliikenne)*.

Kyberala uusintaa ja tarkentaa Teknologiateollisuuden pääviestejä seuraavasti:

- Ehdotamme, että Suomessa kiinnitetään aiempaa enemmän huomiota digitaaliseen taloudelliseen yhteistyöhön autoritaaristen valtioiden kanssa.
- Ehdotamme, että valtioneuvosto laatii kattavan selvityksen muuttuneen turvallisuustilanteen vaikutuksista Suomen maakuvaan ja vetovoimaan sekä yritysten toiminta- ja investointiympäristöön ja seuraa pitkäjänteisesti tilanteen kehitystä.
- Painotamme hallituksen tarvetta tehostaa toimenpiteitä julkisen talouden tasapainottamiseksi ja yritysten toimintaedellytysten parantamiseksi.
- Kannatamme kansallisen kyberturvallisuus ja -puolustuskykymme kehittämistä nopeutetulla aikataululla.
- Ehdotamme yhteisen kyberturvallisuuden ekosysteemin kehittämistä ja yritysten kyberresilienssin vahvistamista.
- Sitoudumme elinkeinoelämän yhteiseen näkemykseen Suomen Nato-jäsenyyden tarpeellisuudesta ja hyödyistä.

Valtioneuvosto on selonteossaan arvioinut, että Venäjän hyökkäyksellä Ukrainaan on pitkäkestoisia vaikutuksia turvallisuusympäristöön Euroopassa ja Suomen lähialueilla. Digitaalisen toimintaympäristön osalta Venäjä on osoittanut jo kauan ennen Ukrainan sotatoimia, **ettei se kunnioita valtioiden suvereniteettia eikä noudata kansainvälisen oikeuden velvoitetta estää ja torjua oikeudenkäyttöpiirissään olevan digitaalisen infrastruktuurin käyttämistä toisia valtioita vastaan ja puuttumiselta niiden sisäisiin asioihin.**

Globaali digitaalinen toimintaympäristö, internet ja kaikki sen päällä jo olevat ja myöhemmin rakentuvat palvelut perustuvat luottamukseen. Maailman jakautuminen geopoliittisesti erilaisiin blokkeihin sisältää myös käsitykset siitä, miten digitaalista toimintaympäristöä tullaan hyödyntämään. Valtiokeskisessä hallintomallissa digitaalisen toimintaympäristön avoimuus ja luottamus voivat toimia vain, mikäli keskinäisen **digitaalisen taloudellisen yhteistyön ehtoina on ihmisoikeuksien kunnioitus ja kansanvallan toteutuminen vapaissa vaaleissa.** Tämä tarkoittaa sitä, että pakkovaltaisten maiden kanssa tehtävän yhteistyön hyötyjen voidaan arvioida jäävän haittoja vähäisemmiksi.

Selonteko ei tunnista riittävän kattavasti teollisuuden roolia kokonaisturvallisuuden ja hyvinvoinnin tuottajina. **Suomen korkean teknologian yritykset ovat myös teollisuusvakoilun kohteita digitaalisessa ympäristössä ja tämän riskin voidaan arvioida**

Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi

kasvavan entisestään Suomen ja Venäjän välisen suhteen heiketessä. Erityisesti tämä koskee puolustus- ja turvallisuusteknologiaa tuottavia yrityksiä ja näiden alihankintaketjuja.

Turvallisuuden kehittämisen ohella viranomaisten toimivaltuuksien lisäämisen tai käytön ei tule kuitenkaan heikentää yritysten kilpailukykyä tai toimintamahdollisuuksia, vaan niiden tulee olla vahvassa sopusoinnussa elinkeinopoliittisten kysymysten kanssa. Digitalisaatio voimistaa yrityssalaisuuksien sekä muun liiketoimintaa koskevan tiedon luottamuksellisuutta yritysten elinehtona. Oikeushenkilöitä koskevan luottamuksellisen viestinnän suojaa koskevan oikeuden merkitys on kasvanut entisestään**.** Tähän vaikuttaa erityisesti tietoliikenteen ja datan jakaminen yli valtionrajojen (mm. pilviteknologian yleistyminen). Perusoikeudet ja lainsäädännön takeet toimintaympäristön luottamuksellisuudesta sekä viranomaisten toiminnasta lisäävät luottamusta digitaalisessa ympäristössä. Digitaalisessa ympäristössä rikollisten toimijoiden (ml. vakoilu) aiheuttaman pelon lisäksi on vältettävä maakuvaa, että Suomessa viranomaiset ”urkkisivat” yritysten luottamuksellisia tietoja – edes puolustustarkoituksiin.

Selonteon painopiste on luonnollisesti turvallisuuteen liittyvissä kysymyksissä. Kyberala kannattaa kuitenkin kattavampaa selvitystä ja seurantaa muuttuneen turvallisuustilanteen vaikutuksista Suomen maakuvaan ja vetovoimaan sekä yritysten toiminta- ja investointiympäristöön. Toimenpiteitä yritysten kasvun tukemiseksi on lisättävä erityisesti korkeaa arvonlisää tuottavilla toimialoilla kuten kyberala. **Hallituksen on tehostettava toimenpiteitä julkisen talouden tasapainottamiseksi ja yritysten kasvuedellytysten parantamiseksi myös kyberturvallisuuden näkökulmasta.**

Kybertoimintaympäristön turvaamisen kannalta oikea, laaja-alainen ja jaettu tilannekuva ja kehittämissuunnitelma on olennainen. On hyvä, että tämä on todettu selonteossa ja että tilannekuvan tuottamiseksi ja jakamiseksi nykyistä tehokkaammin tehdään myös konkreettisia toimia nopealla aikataululla. **Suomeen kehitettävän vahvan kyberturvallisuuden ekosysteemin luomista ja kehittämistä tulee kiirehtiä.** Myös kansainvälinen tutkimus- ja kehitysyhteistyö on tässä suhteessa tärkeää ja välttämätöntä. Kuitenkaan edes selonteon tavoitteiden kannalta ei ole tarpeen keskittää kyberturvallisuuden johtamista ja koordinaatiota turvallisuusviranomaisille tai -ministeriöille, vaan kehittämisessä on pidettävä kybertoimintaympäristön elinkeino- ja kansalaisyhteiskuntaan liittyvät poliittiset kysymykset erottamattomasti osana keskinäistä kehittämistä. Erityisesti lainsäädännön perusoikeuksien, kansantaloudellisten ja yritysvaikutusten seurantaan on siis kiinnitettävä edelleen huomiota.

Samalla voidaan todeta, että tällä hetkellä kyberturvallisuuden (digitaalisen) turvallisuuden vastuut ovat valtionhallinnossa liian hajallaan. Kyberturvallisuus on kaiken toiminnan poikkileikkaava teema, jonka kehittäminen ei saa kompastua hallinnollisiin rakenteisiin, jakautuneeseen rahoitukseen tai resursseihin. Selonteossa todetaan, että kyberturvallisuuden osalta on ymmärrettävä koko arvoketjun riskit ja tunnistettava myös erilaiset saumakohdat, joiden vastuut jäävät helposti epäselviksi. Muutos on korostanut entisestään julkisen ja yksityisen sektorin yhteistoiminnan merkitystä kyberympäristössä ja yritysten roolia kokonaisturvallisuudessa. Yritysten rooli kyberturvallisuuden ratkaisujen kehittäjänä ja tuottajana, yhteistyössä julkisen sektorin kanssa, on aivan olennainen. **Kyberala pitää tärkeänä, että puolustuskykyä kehitettäessä kohdistetaan kriittisen alojen hankintoja kotimaahan. Yhtä lailla on tärkeää resursoida turvallisuus- ja puolustushallinnon TKI-toimintaa ja kehittää kansallista yhteistyötä kyvykkyyksien kehittämiseksi**.

Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi

20.4.2022

Kyberturvallisuuden kannalta huoltovarmuuskriittiset yritykset ovat usein keskiössä. Huomioiden Suomen elinkeinorakenteen mikro- ja pk-yritysten suuren osuuden, pidämme tärkeänä, että tätä yritysjoukkoa ei unohdeta, vaan pyritään luomaan aidosti toimivia ratkaisuja niiden oman kyberturvallisuuden kehittämiseksi. Suomessa on ainakin 150 000 yritystä, jotka eivät tiedä miten toimia tietoturvaloukkauksen kohdatessa. Tämä joukko yrityksiä tarvitsee laajasti sekä hallinnollista, että kyberteollisuuden tukea, palveluita ja ratkaisuja turvallisuutensa parantamiseksi. **Julkishallinnon kehittäminen ja resursointi ei yksinään riitä, vaan lisäksi tulee vahvistaa yritysten kyberturvallisuutta tukien perustason toimenpiteiden toteutusta esimerkiksi kannustimin ja kampanjoin.**

Yhteiskunnan laajuisen kyberturvallisuuden kehittäminen on pitkäjänteistä toimintaa. On varmistettava, että kesäkuussa 2021 vahvistettu kyberturvallisuuden kehittämisohjelma sekä ns. Titukri -periaatepäätös pannaan täysimääräisesti täytäntöön. **Samoin on varmistettava, että kyberturvallisuuden kehitykseen varmistetaan ylihallituskautinen, riittävä rahoitus. Kehysriihessä huhtikuussa 2022 tehdyt päätökset ovat tässä hyvä alku.**

Selonteossa ehdotetaan, että kansallista puolustuskykyä kehitetään nopeutetulla aikataululla muuttuneen toimintaympäristön kasvaneiden vaatimusten mukaisesti puolustukseen osoitettavilla lisäresursseilla. Erityisesti selonteossa nostetaan esiin uskottavan puolustuskyvyn ylläpito. Tämän puolustuskyvyn tulisi sisältää myös sen määrittäminen, miten Suomen suvereniteettia puolustetaan myös kyberavaruudessa. Tällä hetkellä Suomi keskittyy lähinnä suojautumiseen niin, että kukin toimija vastaa suojautumisestaan itse. **Uhkatoimijoiden tunnistaminen ja jäljittäminen, sekä mahdolliset vastatoimet tulisi määritellä ja kuvata toimintapoliittisella tasolla koko kaikkien politiikkalohkojen ja ulkosuhteiden keinovalikoiman laajuisesti.** Määritelty toimintapolitiikka on tarpeen vihamielisen valtion toimintavapauden ja -halukkuuden rajoittamiseksi. Asia ei ole yksinomaan sotilaallisen puolustuksen kysymys, vaan toimintapolitiikka tulisi nojautua ensisijaisesti rikosoikeudellisiin keinoihin ja siitä johdettuihin muihin painostuskeinoihin, päättyen (kyber)aseelliseen itsepuolustukseen. Kansallinen kyberpuolustus ei sinänsä poistaisi edellä mainittujen tahojen velvollisuuksia suojata omaa toimintaansa, mutta se toisi uuden suojauskerroksen nostamalla vihamielisesti toimivan valtion toimintakynnystä jäljittämisen ja vastatoimien pelossa.

Kyberoperaatioita, eli vakavia kyberrikoksia toteutetaan jo rauhan aikana, pitkään ennen poikkeusoloja tai mahdollista sotatilaa. Niiden kohteena voivat olla Suomen kriittinen infrastruktuuri, jonka varaan yhteiskuntamme toiminta nojautuu tai esimerkiksi laajamittaisesti kaikkialle leviävä vakavia vahinkoja aiheuttava haittaohjelma. Nykyistä lainsäädäntöä tulisi päivittää esitettyä toimintapolitiikkaa vastavaksi niin, että viranomaisilla on tarvittavat toimivaltuudet hybridioperaatioiden torjuntaan myös rauhan aikana. Tässä kontekstissa **tulisi ottaa huomioon kansallinen ”kyberomavaraisuus”, mukaan lukien mahdollisissa jäljittämiseen ja vastatoimiin liittyvien kyvykkyyksien kehittämisessä.**

Kyberala ry on Teknologiateollisuus ry:n ja (siten myös Elinkeinoelämän Keskusliiton jäsen) ja olemme sitoutuneet elinkeinoelämän yhteiseen näkemykseen Suomen Nato-jäsenyyden tarpeellisuudesta ja hyödyistä.

Lisätiedot:

Toimitusjohtaja, Peter Sund
sähköposti: peter.sund@teknlogiateollisuus.fi
puhelin: 050 565 0621

Eteläranta 10, PL 10, 00131 Helsinki
www.fisc.fi