7.8.2024 N:tta

PLM/PO/NVM Juhani Karjomaa

SUOMEN KYBERTURVALLISUUSSTRATEGIA 2024-2035

Puolustusministeriö kiittää mahdollisuudesta lausua valmistelussa olevaan valtioneuvoston periaatepäätökseen Suomen kyberturvallisuusstrategiasta 2024-2035. Puolustusministeriö on osallistunut strategian laadintaan puheenjohtajistossa, sihteeristössä kuin työryhmässä ja osallistuu tiiviisti sen päivittämiseen sekä kehittämissuunnitelman tekemiseen. Lausunto perustuu valmistelutyön ulkopuolisiin havaintoihin, jotka halutaan saattaa työryhmän arvioitaviksi.

Yleisesti voidaan todeta, että kyberturvallisuusstrategia on kokonaisuudessaan kehittynyt edellisestä strategiasta toimintaympäristön muutoksen ja uhkaympäristön huomioivaan suuntaan. Kyberpuolustuksen roolin ja kehittämistarpeiden huomiointi kaikissa valmiustiloissa osana sotilaallista maanpuolustusta ja kokonaismaanpuolustusta sekä suvereniteetin turvaamista antaa perusteita kehittämiselle ja yhteistoiminnalle sekä muun muassa kyberpuolustusdoktriinin laatimiselle.

Toimeenpanon (ml. rahoitus ja resurssit) kannalta johdon (yritysten, kuntien, virastojen, valtion) sitouttaminen on erittäin oleellista. Strategiassa voisi harkita linjattavaksi keinoja, joilla kyberturvallisuuden toteuttaminen liitetään nykyistä tiiviimmin osaksi organisaatioiden johtamista, toimintakulttuuria ja laatujärjestelmiä.

Toimintaympäristön muutoksen kuvauksessa olisi hyvä tunnistaa muutostekijänä myös tekoälyn nopea kehittyminen. Asiaa on hiukan sivuttu murroksellisten teknologioiden yhteydessä, mutta strategiassa olisi syytä tarkastella hiukan laajemmin, miten tekoäly muuttaa kyberhyökkäysten ja niiltä suojautumisen luonnetta ja millaisia uhkia tai mahdollisuuksia tekoäly muodostaa kyberturvallisuudelle lähivuosien aikana, vastaavasti kuin kvanttiteknologiaa on käsitelty erillisessä alaluvussa.

Muutostekijäksi (sekä nykytilan kuvaukseen) tulisi tunnistaa myös työnteon murros, johon liittyy vahvasti digitalisaatio (mitä työtä tehdään jatkossa manuaalisesti ja miten pitkälle esim. tekoälyn tuottamaan luotetaan huomioiden siihen liittyvät riskit) sekä monipaikkainen, hybridi- ja etätyö, joissa Suomi on kärkimaita Euroopassa. Suomessa ja myös muualla maailmassa etätyöntekijöiden määrä on nelinkertaistunut COVID-pandemiaa edeltäneestä ajasta ja työpisteen ulkopuolella tehtävän työn määrä on pysyvästi vakiintunut korkealle tasolle. Useilla eri toimialoilla voidaan siis puhua jopa historiallisesta ja pysyvästä muutoksesta.

Strategiassa tulisi tunnistaa ja kuvata kyberturvallisuuden, tekoälymurroksen ja yhteiskunnan elintärkeiden toimintojen riippuvuussuhteet sekä määritellä näille suojaamisen tarve - miten pitkälle mennään ja miten kaikki keskinäisriippuvuudet suojataan, mitkä elintärkeät toiminnot tulisi yhä jatkossa varmistaa manuaalisilla prosesseilla jne. Tässä on myös vahva linkitys tekeillä olevaan yhteiskunnan turvallisuusstrategiaan (joka tulisi myös näkyä viittauksena).

Suomalainen kyberturvallisuusosaamisen tarve yksilö- ja organisaatiotasoilla on hyvin tunnistettu (pilari I). Asiaa kannattaisi tarkastella myös huoltovarmuuden, varautumisen ja jatkuvuudenhallinnan näkökulmasta; onko osaamista ja taitoa riittävästi ja kuinka sen jatkuvuus Suomessa turvataan? Mikä on huoltovarmuusorganisaatioiden

rooli, mistä löytyy riittävä kyvykkyys esim. laajemman vaikuttamisen/hyökkäyksen yhteydessä.

Strategialinjauksissa ei määritellä vastuutahoja yhdellekään toimenpiteille, vaan todetaan, että ehdotusten perusteella laaditaan erillinen tarkempi, aikataulutettu ja vastuutettu toimeenpanosuunnitelma. Vastuutahot olisi tärkeää tunnistaa myös strategiassa, jotta mahd. aukkokohdat ja puutteet tulevat näkyviksi. Ehkä myös organisaatioita olisi tarve perustaa, kehittää tai uudistaa sekä asettaa tähän liittyvät tavoitteet.
Toimeenpano ja seuranta olisi luontevaa käsitellä asiakirjan lopussa eikä ennen kehittämisehdotuksia. Vaikka varsinainen työkuorma siirretäänkin toteutettavaksi toimeenpanon suunnittelussa, keskeiset tavoitteet, aikataulu ja mitattavissa olevat kriteerit kannattaisi ohjata tarkemmin jo strategiatasolla, jotta jatkosuunnittelulle luodaan tavoitetila ja kehittäminen ja seuranta jatkossa on tuloksellista.

Kansainvälisen yhteistyön näkökulma on huomioitu hyvin strategian luvussa. Kansainvälinen yhteistyö vahvistaa Suomen kyberturvallisuutta. Luku kuvaa kansainvälisen toiminnan näkökulmasta vaatimuksia ja mahdollisuuksia kohtuullisen kattavasti.

Turvallisuusympäristössä kybertoiminnassa kansallisen ja kansainvälisen toiminnan välille on vaikeaa tehdä selvää rajaa palvelujen, tieto- ja viestintäverkkojen ja niihin kytkeytyvän infrastruktuurin keskinäisriippuvuuksien takia. Kansainväliseen toimintaan (esim. NATO:n kyberpuolustus) osallistuminen on nähtävä osana kansallisen kyberturvallisuutta eikä yhteistyötä tule käsitellä niinkään erillisenä kokonaisuutena. Kansainvälisen toiminnan näkökulma olisi hyvä strategiassa huomioida kaikissa luvuissa.

Kuten lausuntopyynnön saatteessa todetaan geopoliittisen tilanteen muutos korostaa kansallisen ja kansainvälisen toiminnan merkitystä kyberturvallisuuden varmistamisessa. Erityisesti on kasvanut tarve viranomaisten ja elinkeinoelämän väliselle yhteistyölle, yhteiskunnan kriisinkestävyyden tukemiselle sekä vihamieliseen toimintaan vastaamiselle. Tiivistelmässä ja johdannossa on huomioitu hyvin EU NIS2 ja sen toimeenpano, Suomen NATO jäsenyys on kansallisesti ajatellen merkittävän kokoluokan muutosajuri, jäsenyys ja sen vaikutukset olisi hyvä nostaa esiin jo tiivistelmässä ja johdannossa.

Kyberturvallisuusstrategian sisältöön liittyvät huomiot on käsitelty alla luvuittain.

<u>Suomeen kohdistuva vihamielinen kybertoiminta lisääntyy</u>
Kyberturvallisuusstrategiassa todetaan, että vihamielisen kybertoiminnan lisääntyminen ja kohdistuminen yhä laajemmin myös hallituksiin, demokraattisiin instituutioihin, yritys-elämään ja kansalaisiin. Tämän vuoksi oman toimintaympäristön, tietojärjestelmien ja etenkin näiden välisten keskinäisriippuvuuksien tuntemus on entistä tärkeämpää. Kybertoiminnan luonne korostaa kasvaa tarvetta rajat ylittävälle yhteistyölle. Yhteistyön rakenteiden, toimintatapojen ja koordinoinnin on perustuttava kansallisen, eri toimijoiden yhteisen tarpeen määrittämiseen. Kansallisen tarvemäärittelyn perusteella omat toiminnot on mahdollista linkittää NATO:n, EU:n rakenteisiin sekä muodostaa kansalliset tavoitteet kansainvälisten toimintojen kehittämiseen, jossa huomioidaan sekä siviili- ja sotilasviranomaisten ja teollisuuden yhteistyö sekä toiminnan koordinointi.

<u>Toimitusketjujen turvallisuus korostuu</u>
Teknologinen murros ja yhteiskuntien digitalisaatio kasvattavat mahdollisuuksia vahingolliselle kybertoiminnalle ja hyökkäyksille. Olemassa olevien ja kehitettävien tietojär-

jestelmien kyberturvallisuuden teknisen varmistamisen lisäksi kyberturvallisuuden toimeenpanossa on huomioitava kattavasti operatiiviset toiminnot ja järjestelmät. Keskinäisriippuvuudet edellyttävät myös, että kriittisten toimintojen ja infran osalta varmistetaan toimintojen ylläpidossa ja kehittämisessä käytettävien kumppanien luotettavuus. NATO:ssa on hyväksytty politiikka, jossa on määritetty periaatteet ”Trustworth suppliers” käytöstä kumppaneina. Luotettavuuden arviointi sisältää myös ao. kumppanien käyttämien kolmansien osapuolien teknisten järjestelmien ja komponenttien luotettavuuden arvioinnin. Seuraavassa vaiheessa valmistellaan ’minimivaatimukset’ käyttäville kumppaneille. Kansallisen kyberturvallisuuden toimeenpanossa on huomioitava EU NIS2 lisäksi myös NATO määrittämä politiikka ja vaatimukset sekä niiden vaikutukset kansalliselle teollisuudelle.

Yritysten kilpailukykyä edistetään

Resilienssin parantamisessa ja erityisesti sotilaallisesti kriittisten toimintojen turvaamisen näkökulmasta ’avaruuspohjaisten’ ratkaisujen lisäksi olisi hyvä nostaa esille Advanced 5G ja FutureG kaupallisten ratkaisujen adoptointi sotilas-/turvallisuuskäyttöön. Uuden sukupolven ratkaisut kattavat communications as a service (CaaS) kokonaisuuden, jolla myös linkitys avaruuspohjaiseen tietoliikenteeseen. Tämä liittyy myös kansallisten yritystemme kilpailukyvyn/liiketoimintamahdollisuuksien edistämiseen.

Kyberhäiriöiden- ja uhkatilanteiden johtamismallia kehitetään

Strategian luonnoksessa määritetty johtamismalli ja kansallisen yhteistoimintamallin kehittäminen sekä seuranta vaikuttavat toimeenpanokelpoisilta. Kyberpuolustuksen kansallinen määrittely ja kytkentä kyberturvallisuuden kokonaisuuteen on määritetty hyvin ja on sovitettavissa NATO käyttämään CIV-MIL terminologiaan ja rakenteeseen. Yhteistoimintamallin toimeenpanossa on keskeistä varmistaa toimintatasojen (poliittinen, operatiivinen ja tekninen) sekä toimijoiden välinen keskinäiskoordinaatio. NATO ja EU toiminnot edellyttävät riittävän joustavaa mekanismia, jolla varmistetaan kansallisen kannan tilanteenmukainen ja koordinoitu valmistelu.

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi