Jyväskylän yliopisto

Lausunto

05.08.2024 VN/36693/2023

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Jyväskylän yliopisto kiittää mahdollisuudesta lausua Suomen kyberturvallisuusstrategiasta.

Toimintaympäristön muutos ja nykytila

Kansallinen kybertoimintaympäristö (kybermaailma, kybertila) koostuu useista eri toimijoista ja toimintokokonaisuuksista. Näitä kyberulottuvuuksia ovat ainakin:

- poliittinen,
- sotilaallinen,
- yhteiskunnallinen,
- teknologinen,
- kansalaisulottuvuus.

Kybertoimintaympäristö poikkeaa perinteisestä kansallisesta toimintaympäristöstä, jossa itsenäisellä valtiolla on selkeästi määritellyt maantieteelliset rajat, jotka määrittävät valtion kansallisen alueen (maa-alueen, vesialueen ja ilmatilan) eli valtion toimivallan alueen. Aluevalvontalaki (18.8.2000/755) kuvaa Suomen valtakunnan aluetta määrittelemällä maa- ja merirajoja ja niiden yläpuolista ilmatilaa. Kybertoimintaympäristön vahvistuminen osaksi kansallista toimintaympäristöä olisi aluevalvontalakia ja siihen liittyviä säädöksiä tarkistettava vastaamaan Suomen kybertoimintaympäristön suojaamisen tarpeita. Selkeä ja tarkkarajainen juridinen määrittely kansallisesta kybertoimintaympäristöstä tarvitaan kansallisen kyberturvallisuuden ja kyberpuolustuksen tehokkaaksi toteuttamiseksi.

Kyberuhat ja -turvallisuus ilmentyvät siten eri tavoin yhteiskunnassa. Kaiken keskiössä on kriittinen infrastruktuuri ja siihen perustuvat yhteiskunnan elintärkeät toiminnot ja julkiset palvelut. Tämän lisäksi kansalaisille Internetistä ja sen palveluista on tullut aivan keskeinen arjen toimintaympäristö. Digitaalinen murros perustuu ihmisten muuttuneisiin odotuksiin, yhteiskunnan palvelurakenteiden ja -tuotannon kasvaneisiin tehokkuusvaatimuksiin ja teknologioiden tarjoamiin mahdollisuuksiin.

1) Poliittinen ulottuvuus

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu yhä enemmän kyberasioiden poliittinen luonne. Kybertoimintaympäristö on voimakkaassa muutoksen tilassa, ja tätä kehitystä pyritään poliittisin keinoin ohjaamaan. Kyberturvallisuuden asiat ovat esillä yhä laajemmin ja vahvemmalla painoarvolla kansainvälisillä foorumeilla ja järjestöissä.

Kyberturvallisuudessa etenkin valtioiden välisen luottamuksen lisääminen on keskeinen kysymys, johon pyritään tiivistämällä valtioiden välistä keskustelua kybertoimintaympäristöön liittyvistä kysymyksistä. Kansainvälisillä yhteistyöfoorumeilla ja valtioiden kahdenvälisissä suhteissa vaikuttaminen on yksi keskeinen keino edistää Suomen kyberturvallisuuden kannalta myönteisiä asioita.

Kybertoimintaympäristö ja kyberturvallisuus on noussut tärkeäksi osaksi Suomen ulko- ja turvallisuuspolitiikkaa. Koska kyberuhat eivät tunne valtioiden rajoja, tarvitaan kyberturvallisuuden vahvistamiseksi ennen kaikkea kansainvälistä yhteistyötä. Suomi yhdessä muiden EU-maiden kanssa katsoo, että kansainvälistä oikeutta koskevat sopimukset ja normit ovat sovellettavissa myös kybertoimintaympäristöön ja niiden tulkintaa tulee tältä osin syventää.

Joulukuussa 2023 EU parlamentti otti kantaa Kiinan pyrkimyksiin muuttaa sääntöpohjaista järjestystä. Päätöslauselmaan mepit esittävät, että EU rajoittaisi tehokkaammin Kiinan otetta eurooppalaisesta kriittisestä infrastruktuurista, ja puolustautuisi paremmin Kiinasta lähtöisin olevia kyberhyökkäyksiä sekä disinformaatiota vastaan.

Strategian kehittämisehdotus:

- Strategiassa esitettäisiin Suomen kyberturvallisuuspolitiikan strategiset tavoitteet ja yhteistoiminta niiden maiden kanssa, jotka jakavat sääntöperustaisen maailmanjärjestyksen.

- Strategiassa otettaisiin kantaa, kuinka määritellä kansallinen kybertila maa-, meri- ja ilmatilan tavoin. Tämä antaisi perusteita erityisesti kyberpuolustusdoktriinille.

2) Sotilaallinen ulottuvuus

Lausunnolla oleva Yhteiskunnan turvallisuusstrategia 2024 tunnistaa kokonaisturvallisuuden eri ympäristöjä. Strategialuonnoksen mukaan kyberturvallisuus on kokonaisturvallisuuden toteuttamista kybertoimintaympäristössä ja informaatioturvallisuus on kokonaisturvallisuuden toteuttamista informaatioympäristössä. Lisäksi kokonaismaanpuolustus painottaa yhteiskunnan elintärkeiden toimintojen puolustuskykyä ja sen vahvistamista koko yhteiskunnan voimavaroilla.

Kyberturvallisuusstrategian luonnos tunnistaa strategisena kehitysehdotuksena kyberpuolustuksen kehittämisen. Kansallisen kyberpuolustuksen toteuttamisen tueksi laaditaan kyberpuolustus-doktriini, jossa tarkennetaan kyberpuolustuksen tavoitteita, jota tavoitetta on pidettävä tervetulleena.

Strategian kehittämisehdotus:

- Strategiassa voisi selkeämmin erotella kyberturvallisuuden siviilisektorin ja sotilassektorin toimet ja vastuut.

3) Yhteiskunnallinen ulottuvuus

Yhteiskuntaan kohdistuvan kyberuhan kohteista keskeisiä ovat kansallisen turvallisuuden kohteet sekä yhteiskunnan elintärkeät toiminnot, joilla turvataan kansalaisten elinmahdollisuudet. Crowdstrike-case kesällä 2024 osoitti, kuinka riippuvainen digitaalinen yhteiskunta on toimivasta informaatio- ja kyberturvallisuusteknologiasta. Yhteiskunnan kyberturvallisuuden parantamiseen tarvitaan verkostomaista yhteistekemistä yritysten ja julkisen hallinnon välillä. Kaikki yritykset ja organisaatiot vastaavat omasta kyberturvallisuudestaan, mutta valtiolla on keskeinen rooli lainsäätäjänä.

Strategian kehittämisehdotus:

- Strategiassa voisi nostaa vielä vahvemmin esiin kriittisen infrastruktuuri ja sen nykytila digitaalisen Suomen perustana ja sen resilienssin kehittämisen strategiset tavoitteet askeleineen. (vrt. HVK: Kyberturvallisuuden nykytila eri toimialoilla)

4) Teknologinen ulottuvuus

Teknistaloudellinen kehitys on johtanut tuotannon, palvelujen ja koko yhteiskunnan verkostoitumiseen ja keskinäisten riippuvuuksien kasvuun. Tietoliikenteen, tietojärjestelmien ja viestinnän toimintavarmuus onkin nykyaikaisen yhteiskunnan häiriöttömän toiminnan, turvallisuuden ja kansalaisten toimeentulon välttämätön edellytys. Kuten alussa todettu Yhdysvallat ja Kiina ovat informaatio- ja kyberturvallisuusteknologioiden johtavia valtioita. Suomessa on ollut esillä tarve rajoittaa kiinalaisen teknologian käyttöä, mitä moni EU-maa ja Yhdysvallat ovat jo tehneet.

Strategian kehittämisehdotus:

- Strategia voisi ottaa kantaa, kuinka vahvistaa kansallista informaatio- ja kyberturvallisuusteknologioiden käyttöä ja yhteistoimintaa suomalaiset arvot jakavien kanssa.

Kvanttiteknologia on merkittävä murrosteknologia, mutta se saa strategiassa turhan korostuneen roolin. Todennäköisesti geneerinen tekoäly (GAI) ja laajat kielimallit vaikuttavat enemmän vuoteen 2035 mennessä.

5) Kansalaisulottuvuus

Digitalisaatiosta on tullut yhä tärkeämpi osa yritysten ja ihmisten toimintaa. Digitaalisuus on nykyisin yhä syvemmällä ihmisten arjessa. Digitaaliset palvelut helpottavat yritysten ja ihmisten arkea ja elämää. Kyberturvallisuudessa kyse on kansalaisten luottamuksen ylläpitämisestä yhteiskunnan toimintaan. Siksi kyberturvallisuuden kansalaistaidot ovat yhä tärkeämmässä roolissa digitalisoituvissa yhteiskunnissa.

Strategian kehittämisehdotus:

- Strategiassa voisi kuvata, kuinka lisätä kansalaisten luottamusta digitaalisiin palveluihin.

- Suomessa tarvittaisiin kokonaisvaltainen kansalaisten kyber- ja informaatioturvallisuusohjelma, jolla vahvistettaisiin kansalaisten luottamusta digitaalisiin palveluihin ja vahvistettaisiin pohjaa kansalaisten digi- ja informaatioturvallisuudelle.

I Osaaminen, teknologia ja tutkimus-, kehitys- ja innovaatiotoiminta (TKI)

Kyberturvallisuuden osaamisen ja koulutuksen osalta strategia nostaa hyvin esiin alan koulutuksen ja harjoitustoiminnan merkityksen. Yhdeksi strategiseksi tavoitteeksi tulisi asettaa kansallinen kyberturvallisuuden TKI-ohjelman organisointi. Ohjelma voisi toimia EU- ja NATO-hankkeissa tarvittavana vastinrahoitusinstrumenttina sekä selkeänä kansallisena rahoituksena (vrt. kansallinen Cyber Trust-hanke 2014–2018). Kansallisen rahoituksen käyttö on perusteltua, koska kansallinen TKI-toiminta ei voi perustua vain kansainväliseen kilpailtuun rahoitukseen.

Osaamisen vahvistaminen edellyttää lisäresursseja korkeakouluissa kyberturvallisuuden tutkintokoulutukseen, jatkuvaan oppimiseen sekä muunto- ja täydennyskoulutuksiin. Kansallisen kyberturvallisuusosaamisen vahvistamiseksi tulisi laatia osana strategian toimeenpanoa laaja-alainen kyberturvallisuusosaamis- ja koulutusohjelma, jossa osaamistarpeet on katettu monipuolisesti.

Kyberharjoitustoiminnan tulisi kattaa laajasti kriittisen infrastruktuurin toimijoiden lisäksi julkishallinto ja yrityssektori. Tarvitaan myös laajaa kansainvälistä harjoitustoimintaa. Tätä toimintaa tulisi tukea julkisin varoin, sillä kyberturvallisuusosaaminen vahvistaa kansallista resilienssiä ja siten vähentää mahdollisia kyberhyökkäysten vaikutuksia ja taloudellisia menetyksiä.

Strategian kehittämisehdotus:

- Strategia voisi edellyttää seuraavien ohjelmien laatimista, joissa määriteltäisiin selkeät tavoitteet ja resurssit niiden saavuttamiseksi:
- Kansallinen kyberturvallisuuden TKI-ohjelma.
- Kansallisen kyberturvallisuusosaamis- ja koulutusohjelma.
- Kansalaisten kyber- ja informaatioturvallisuusohjelma.
- Kansallinen kyberharjoitussuunnitelma.

II Varautuminen

Suomen turvallisuus, hyvinvointi ja huoltovarmuus ovat aiempaa riippuvaisempia yhteiskunnan keskeisten, useasti rajat ylittävien ja kansallisen toimivallan ulottumattomissa olevien toimintojen jatkuvuudesta. Huoltovarmuusajattelussa onkin ryhdytty painottamaan organisaatioiden toimintaprosessien jatkuvuuden varmistamista ja kriittisen infrastruktuurin turvaamista jo normaalioloissa.

Toimintaverkoston huoltovarmuutta on mahdotonta ylläpitää tai hallita kansallisin toimin. Toiminta edellyttää rajat ylittävää verkostokyvykkyyttä ja kansainvälistä yhteistyötä. Kyberturvallisuuden varmistamista ja kyberhuoltovarmuuden turvaamista haastavat lisäksi toimintaympäristön hajanaisuus, muutosten nopeus ja vaikeasti ennustettava kehitys.

Strategian kehittämisehdotus:

- Strategiaan voisi liittää tarpeen laatia/ottaa käyttöön kyberturvallisuuden riskienhallintakehikko yritysten ja organisaatioiden tarpeisiin.
- Strategia voisi ottaa kantaa varautumisen sekä normaali- ja poikkeusolojen häiriötilanteiden strategiseen johtamiseen.

III Yhteistoiminta

Strategialuonnoksessa ehdotetaan, että ”Julkinen ja yksityinen sektori kehittävät tiiviimpää ja luottamusta vahvistavaa yhteistoimintamallia.” Strategiassa voisi ottaa kantaa siihen, millaisilla rakenteilla tavoitetta kohdin edetään.

Strategian kehittämisehdotus:

- Strategiassa tulisi kuvata tarkemmin yhteistoimintamallin rakenteet ja erityisesti, miten yksityinen sektori otetaan osaksi toimintaa.

IV Reagointi ja vastatoimet

Strategialuonnoksessa todetaan, että kyberdiplomatian, -puolustuksen ja -turvallisuuden

toimilla vastataan kyberuhkiin. Strategiassa jää hieman epäselväksi mikä on kansallisen kyberturvallisuuden ja kansallisen kyberpuolustuksen ero. Sekä siviili- että sotilassektori käyttävät kriittistä infrastruktuuria, josta noin 80 % on yksityisessä omistuksessa. Tämän vuoksi tulisi määritellä mahdollisimman tarkkarajaisesti vastuut sotilaallisista, lainvalvonnan, diplomatian ja muista hallinnollisista toimista.

Kehittämisehdotukset:

- Kyberturvallisuuden, -puolustuksen ja -diplomatian vastuita ja tavoitteita tulisi selventää.

Resursointi, toimeenpano ja seuranta

Strategian resursointi, toimeenpano ja seuranta ovat strategian onnistumisen kannalta keskeisiä. Strategian toimeenpanon resurssit määrittävät sen, kuinka strategiassa esitettyihin tavoitteisiin päästään. Strategiassa, tai sen toimeenpano-osassa voisi esittää strategiset toimenpiteet priorisoituna ja niihin suunnitellut toimijat ja resurssit.

Strategian kehittämisehdotus:

- Strategian toimeenpanotoimet ja niille osoitetut resurssit tulisi priorisoida tärkeys- tai painopistejärjestykseen.

Loppupäätelmiä

Kyberturvallisuusstrategian rakenne neljän pilarin alle voidaan pitää perusteltuna. Strategia ottaa hyvin huomioon eri toimijoiden välisen yhteistyön ja kansallisten sekä kansainvälisten kyberturvallisuusekosysteemien tärkeyden. Strategia antaa hyvän pohjan kansallisen kyberturvallisuuden kehittämiselle. Kyberturvallisuudessa tulee ottaa huomioon eri kybertoimintaympäristön ulottuvuudet, joissa tarvitaan erilaisia toimia ja yhteistyömuotoja.

Kyberturvallisuuden osaamisen ja koulutuksen osalta strategia hyvin nostaa esiin alan koulutuksen ja harjoitustoiminnan merkityksen. Pilarissa I strateginen tavoite on hyödyntää EU:n ja NATO:n yhteistyö- ja rahoitusmahdollisuuksia, mikä on välttämätöntä. Tämän lisäksi tarvittaisiin myös kansallinen merkittävä rahoitusohjelma, joten yhdeksi pilari I:n strategiseksi tavoitteeksi tulisi kirjata laaja-alainen kyberturvallisuuden TKI-ohjelma. Strategiassa mainitaan myös, että tavoitetilan saavuttamiseksi varmistetaan riittävät resurssit, ja niitä käytetään tehokkaasti, mikä onkin aivan välttämätöntä asetettujen tavoitteiden saavuttamisessa.

Yritysten kilpailukyvyn edistäminen on välttämätöntä sekä alan liiketoiminnan vahvistamiseksi että kansallisen kyberomavaraisuuden kehittämiseksi. Kilpailukyvyn edistämisessä yritysten lisäksi toimintaan osallistuvat korkeakoulut ja tutkimuslaitokset, siksi vahva kotimainen kyberturvallisuusalan TKI-toiminta on keskeistä toimivan kyberturvallisuuden ekosysteemin kehittämiseksi ja ylläpitämiseksi. Siksi kansallisen kyberturvallisuusosaamisen vahvistamiseksi tulisi laatia osana tämän strategian toimeenpanoa laaja-alainen kyberturvallisuusosaamis- ja koulutusohjelma, jossa katetaan osaamistarpeet ”vauvasta vaariin”.

Kyberharjoitustoiminnan lisääminen on erittäin tärkeää. Harjoitustoiminnan tulisi kattaa laajasti kriittisen infrastruktuurin toimijoiden lisäksi julkishallinto ja yrityssektori. Tarvitaan myös vahvaa kansainvälistä harjoitustoimintaa. Lisäksi kansalaisille tarvitaan mahdollisuuksia harjoitteluun, jota voivat erityisesti tarjota alan yritykset. Tätä toimintaa pitäisi tukea julkisin varoin.

Strategian resursointi, toimeenpano ja seuranta ovat onnistumisen kannalta aivan keskeisiä. Erillisillä ohjelmilla voitaisiin syventää kansallisia tavoitteita kyberturvallisuuden kehittämiseksi. Strategian toimeenpanon resurssit määrittävät sen, kuinka strategiassa esitettyihin tavoitteisiin päästään.

Lehto Martti
Jyväskylän yliopisto - Informaatioteknologian tiedekunta