Helsingin yliopisto

Lausunto

03.02.2021 HY/82/00.13.00/2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Helsingin yliopiston lausunto Kyberturvallisuuden kehittämisohjelmasta

Helsingin yliopisto kiittää mahdollisuudesta lausua Kyberturvallisuuden kehittämisohjelmasta.

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta sisältää ajankohtaisia ja tärkeitä suuntaviivoja ja toimenpiteitä kyberturvallisuuden kokonaisvaltaiseen ja pitkäjänteiseen kehittämiseen. Huippuluokan kansallisen osaamisen syntymisen ja ylläpitämisen edistäminen on esityksen kantavia teemoja, ja Helsingin yliopisto pitää sitä erittäin kannatettavana asiana. Osaamisen lisäksi kolme muuta keskeistä kansallisen kyberturvallisuuden ekosysteemin aluetta ovat kiinteä yhteistyö, vahva kotimainen kyberteollisuus sekä tehokkaat kansalliset kyberturvakyvykkyydet. Nämä neljä teemaa muodostavat ekosysteemin, jossa eri alojen ja sektorien vahvuudet tukevat toisiaan. Ehdotuksen toimenpiteet ovat tärkeitä ekosysteemin kehittämiselle, mutta osin ne on määritelty korkealla tasolla. Tarvitaan suunnittelutyötä ja tarkennuksia konkretian lisäämiseksi.

Huippuluokan osaaminen

Osaamisen ja tarpeiden tunnistaminen sekä osaamisen kehittäminen on ehdotuksessa määritelty hyvin korkealla tasolla. Ehdotuksessa ei käsitellä konkreettisia toimenpiteitä osaamisen kehittämiseen ja jatkuvaan oppimiseen.

Helsingin yliopisto pitää mahdollisina toimina yksittäisen substanssialueen osaajien kouluttamista kyberturvaosaajiksi ja avointen verkkokurssien hyödyntämistä sekä osaajien kouluttamisessa että kansallisen osaamispohjan kehittämisessä. Helsingin yliopisto on yhdessä F-Securen kanssa kehittänyt MOOC-verkkokurssin Cyber Security Base, joka tarjoaa 10 opintopisteen koulutuksen tietoturvatehtäviin.

On tarvetta varmistaa kyberturva-alalle riittävä professorien ja tutkijakoulutettavien määrä — nykyisessä tilanteessa aihepiirin tutkimusta tehdään useassa yliopistossa, mutta resursseja on kaiken kaikkiaan vähän. Helsingin yliopiston ja Aalto-yliopiston yhteistyönä on syntynyt Helsinki-Aalto Institute for Cybersecurity, joka toimii tutkimuksen, koulutuksen ja yleisen kybertietoisuuden edistäjänä pääkaupunkiseudulla.

Yhteiskunta- ja käyttäytymistieteellinen tietoperusta tulee myös huomioida kyberturvallisuuden tutkimuksessa, opetuksessa ja osaamisen kehittämisessä. Kyberturvallisuus osana rikoksentorjuntaa tulisi sisältyä kriminologian opetukseen ja tutkimukseen. Kriminologia sisältää myös seuraamusjärjestelmän ja kriminaalipolitiikan roolin kyberturvallisuuden keinovalikoimassa.

Kiinteä yhteistyö

Helsingin yliopisto näkee kansallisen verkostomaisen toiminnan kehittämisen erittäin positiivisena asiana. Nykyisenä etäyhteyksien aikana kansallinen virtuaalinen osaamiskeskus vaikuttaa mahdolliselta tavalta rakentaa akateemista kyberturva-alueen toimintaa synergioiden varaan. Osaamiseen liittyy olennaisesti käytössä oleva opetus- ja tutkimusinfrastruktuuri, jonka osalta on tarve kehittää suorituskykyjä ja joiltain osin myös yhdistää infrastruktuurin osia.

Yhteiset kyberharjoitusympäristöt ovat hyödyllisiä monestakin syystä. Resurssien tehokkaan käytön lisäksi samassa ympäristössä harjoitteleminen kannustaa erityyppisiä toimijoita yhteistyöhön. On siksi hyvä varmistaa, että tällaisiin harjoitusympäristöihin on pääsy myös alan tutkijoilla ja koulutettavilla.

Helsingin yliopisto pitää kehitettäviä yhteyksiä EU:n osaamiskeskittymiin erityisessä arvossa. Yliopiston olemassa olevia yhteyksiä eurooppalaisiin huippuyliopistoihin voidaan hyödyntää tämän tavoitteen saavuttamiseksi.

Vahva kotimainen kyberturvateollisuus

Yliopistoilla on tärkeä rooli uusien innovaatioiden luonnissa ja uusien startup-vaiheen yritysten syntymisessä. On tärkeää luoda mahdollisuuksia tohtorikoulutettavien ja maisterivaiheen opiskelijoiden yhteyksille alan yrityksiin ja muihin toimijoihin. Jatko-opiskelijoille voitaisiin luoda opintojen osaksi harjoitusjakso yrityksessä tai julkishallinnossa. Tällaisen jakson tavoitteena olisi luoda edellytyksiä innovaatioiden luomiseksi sekä tieteellisten tulosten soveltaminen käytännön tilanteissa.

Tehokkaat kansalliset kyberturvakyvykkyydet

Kyberturvallisuusosaamisen ja kyberrikollisuuden torjunnan toimien ja ohjelmien vaikuttavuus kansalaisten turvallisuuteen voidaan todeta vain, mikäli käytettävissä on kansalaisten ja yritysten rikosuhrikokemuksia mittaavia kokonaisturvallisuuden osoittimia. Näillä osoittimilla voidaan seurata mm. kyberturvallisuuden kehitystä, turvallisuustilanteen muutosta ja politiikkaohjelmien vaikuttavuutta.

Yritysuhritutkimusten (YUT) muodostamaa tutkimuslinjaa tulee jatkaa ja vahvista niissä jo olevaa kyberturvallisuuden dimensiota. Kyberturvallisuustutkimus ja -opetus tulee integroida laajempaan kriminologiseen yritysturvallisuuden viitekehykseen.

Kansallisen rikosuhritutkimuksen (KRT) yhteydessä tarkasteltiin 2018 ensimmäistä kertaa yksityiskohtaisemmin suomalaisten kyberrikosten uhrikokemuksia väestötasolla. Tämän tyyppinen seuranta tulee turvata jatkossakin. Kansallisissa ja kansainvälisissä nuorisorikollisuustutkimuksissa (NRK, ISRD) kerätään tietoa perinteisen rikollisuuden lisäksi myös verkossa tapahtuneista uhrikokemuksista; nämä muodostavat keskeisen väestötason tietolähteen uhrikokemuksista myös tekonäkökulmasta.

Kriminologisen rekisteritutkimuksen anti tulee huomioida kyberturvallisuuden tutkimuksessa ja opetuksessa, ja viranomaisrekisterien sekä yksityissektorin rekisteriresurssien tutkimuskäyttöä tulee tehostaa. Jälkimmäinen edellyttää lisääntyvää yhteistyötä elinkeinoelämän toimijoiden ja yliopistojen välillä yhteiskunta- ja käyttäytymistieteitä hyödyntäen.

Kriminologian lisäksi Helsingin yliopistolla on vuosien kokemus kryptologian tutkimuksessa ja salausteknologioiden soveltamisessa. Tätä osaamista voidaan hyödyntää tukemaan AQUA-statuksen saavuttamista.

Lahtinen Ulla
Helsingin yliopisto