Suomen itsenäisyyden juhlarahasto Sitra

Lausunto

08.08.2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Yleistä:

Suomen itsenäisyyden juhlarahasto Sitra kiittää mahdollisuudesta lausua Suomen kyberturvallisuusstrategian lausunnon luonnoksesta. Käsiteltävänä olevan kansallisen kyberturvallisuusstrategian hahmottamista ja sen toteuttamismahdollisuuksien arviointia mukaanluettuna resursointi, edesauttaisi, jos strategiaan olisi suoraan kirjoitettu ehdotettujen toimenpiteiden kohdalle vastuutaho ja resurssien tarvearvio.

Suomen kyberturvallisuusstrategia on uudistettu Petteri Orpon hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. Kyberturvallisuusstrategian uudistamisessa on otettava huomioon kyberturvallisuusdirektiivin (NIS2) vaatimukset kansalliselle kyberturvallisuusstrategialle sekä muu aiheeseen liittyvä keskeinen strategia- ja selontekotyö kuten Kansallinen kvanttiteknologiastrategia, Teollisuuspoliittinen strategia, Teknologianeuvottelukunnan työ, kokonaisturvallisuuden strategia, huoltovarmuuden periaatepäätös sekä kv- ja EU-kontekstissa eurooppalainen kyberturvallisuusstrategia ja muut EU- ja NATO-strategiat ja ohjelmat. Hallitusohjelmaan kirjattu informaatiopuolustus on tarkoitus huomioida osana strategisen viestinnän toimintamallia ja puolustuspoliittista selontekoa. Suomen kyberturvallisuusstrategian tavoitetila ulottuu vuoteen 2035 ja strategia sisältää neljän pilarin alle muodostetut strategiset tavoitteet ja näille yhteiset kehittämistoimet.

Petteri Orpon hallitusohjelmassa Euroopan unioni ja puolustusliitto Nato muodostavat Suomen ulkopolitiikan yhteistyövaraisen ytimen. Suomi on NATO-jäsenyytensä myötä sotilaallisesti liittoutunut maa. Orpon hallitusohjelman mukaan Suomen tavoitteena on EU:n ja Euroopan oman puolustuksen vahvistaminen Naton puitteissa. Uuden aikakauden ulko- ja turvallisuuspolitiikka -

luvussa viitataan globaalin vastakkainasettelun ja suurvaltojen välillä lisääntyneisiin jännitteisiin, joilla on merkittäviä vaikutuksia turvallisuuteen, talouteen, teknologiaan, huoltovarmuuteen, teollisuuteen ja kauppaan. Yhtenä tavoitteena hallitusohjelmassa mainitaan kokonais- ja kyberturvallisuuden johtamisrakenteen uudistaminen hallituskauden aikana pääministerin johdolla.

Kyberturvallisuustrategian tarkoitusta on tarpeen selkeyttää sen osalta, onko strategian olemassaolo itseisarvo vai tavoitellaanko sen avulla konkreettisia toimia. Mikäli strategian on tarkoitus toimia välineenä, olisi tarpeen selventää toimijoiden rooleja ja vastuuttaa nämä toimijat tehtävien toteuttamiseen. Yleisesti strategiassa tulisi selkeämmin osoittaa ja nimetä toimijat ja heidän vastuunsa strategian toteuttamisessa.

Sitra arvioi strategialuonnosta siinä asetettujen tavoitteiden pohjalta arvioimalla, vastaavatko osa-alueiden pilarit ja toimeenpanosuositukset tavoitetilassa asetettuja kansallisia päämääriä kyberturvallisuuden tavoitetilasta. Kansallisen kyberturvallisuuden tavoitetilan edistämiseksi hahmotellut osa-alueet tai pilarit ovat sinällään kannatettavia, mutta Sitra esittää valittuihin painopistealueisiin liittyen jäljemmin huomioita.

Pilarit ja niiden strategiset tavoitteet:

Esitämme valittuihin painopistealueisiin lisättäväksi: Keskinäisriippuvuudet, teknologian maanpuolustuskurssi-pilotti, taloudellinen turvallisuus ja kognitiivinen vaikuttaminen

Osaaminen, teknologia ja TKI-pilarin painopisteen tavoitteet ovat kannatettavia, mutta Sitra esittää painopistealueeseen lisättäväksi seuraavia tarkennuksia: Kyberturvallisuuden ekosysteemin osalta on huomioitava, että kansallisesti valmisteilla olevat teollisuuspoliittinen strategia, kvanttiteknologiastrategia ja sen ympärille muodostettava kvanttiekosysteemi ovat olennaisia myös kyberturvallisuuden ekosysteemin kannalta. Lisäksi Teknologiateollisuuden koordinoima puolijohdestrategia on kyberturvallisuuden infrastruktuurin kannalta merkittävä meneillään oleva työ. Tuottavuutta ja tehokkuutta kansallisesti lisäävän kyberekosysteemin kannalta on tärkeää, että yhteistoiminta osittain päällekkäisten meneillään olevien strategiatöiden osalta on toimivaa. Teollisuuspoliittisen strategian valmistelua ohjaa tavoite vahvistaa suomalaisen teollisuuden kilpailuasetelmaa globaaleilla markkinoilla ja tuottaa arvonlisää ja hyvinvointia Suomeen. Lisäksi teollisuuspoliittisen strategian tavoitteena on hyödyntää mahdollisuudet käyttää dataa ja murroksellisia teknologioita, kuten kvanttilaskentaa, robotiikkaa ja tekoälyä uusien ratkaisujen luomiseen. Nämä tavoitteet ovat yhdensuuntaiset kyberturvallisuusstrategian kyberekosysteemin ja yritysten kilpailukyvyn vahvistamiseen liittyvien tavoitteiden kanssa. Sitra kannustaa strategiatyössä vahvaan yhteistyöhön temaattisesti päällekkäisten mutta eri sektoriministeriöistä käsin edistettävien asioiden eteenpäin viemiseksi siiloutumisen sijaan.

Osaamisen vahvistaminen laajasti yhteiskunnan eri tasoilla on kannatettava tavoite, joka edellyttää eri teknologioiden keskinäisriippuvuuksien tunnistamista. Suomalaisen kyberturvallisuusosaamisen varmistaminen tulisi taata kasvatuksen, koulutuksen ja opetuksen sekä yhteiskunnan ja työelämän kaikkien tasojen lisäksi erityisesti vaikuttajien ja päättäjien keskuudessa. Päättäjien tukemiseksi on vahvistettava kokonaisvaltaista kansainvälisen yhteistyön ja EU:n tieto- ja teknologiapolitiikan ymmärrystä, jonka yhtenä osana kyberturvallisuus on. Innovatiivinen kyberturvallisuuden ekosysteemi ja yritysten kilpailukyvyn edistäminen murroksellisia teknologioita hyödyntämällä edellyttää päättäjätason näkemystä ja johtajuutta kriittisistä teknologioista ja EU:n tieto- ja teknologiapolitiikasta. Suomen haasteena on korkeasta osaamisesta huolimatta matala kaupallistamisen taso kriittisissä teknologioissa. Suomi tarvitsee strategisuutta kyberekosysteemin tukemiseksi ja kyberturvallisuusalan mahdollisuuksien lunastamiseksi. Tämän tavoitteen edistämiseksi tulisi toteuttaa tieto- ja teknologiapolitiikkaan keskittynyt teknologian maanpuolustuskurssi, jossa yhteiskunnan päättäjät voisivat perehtyä kriittisten teknologioiden ja EU:n tieto- ja teknologiapolitiikan kannalta keskeisiin strategisiin kysymyksiin sekä tunnistaa keinot, joiden avulla Suomi voi varmistaa oman asemansa kiristyneessä kilpailussa tieto- ja teknologiapolitiikan kentällä.

Strategialuonnoksessa todetaan, että kyberuhkiin varautuminen, suojautumisen kehittäminen ja suomalaisten kyberturvallisuusalan yritysten kasvu on mahdollista vain, mikäli osaavaa työvoimaa on saatavilla. Osaamisen varmistaminen edellyttää siten myös pärjäämistä kilpailussa osaajista. Kansainvälisesti Suomi tunnetaan korkean luottamuksen yhteiskuntana ja mielletään usein edelläkävijäksi eurooppalaiseen arvopohjaan perustuvan teknologiapolitiikan edistäjänä. Arvopohjainen lähestymistapa on Suomelle kilpailutekijä. Kilpailu on kuitenkin kovaa ja sitä käydään etenkin osaajista. Osaamisen varmistamisen kannalta strategiassa on tärkeää huomioida myös se, että Suomi kilpailee kansainvälisistä osaajista ja on koko yhteiskunnan asia edistää toimia, joiden avulla voidaan lisätä Suomen mielenkiintoa huippuosaajien suuntaan globaalisti.

Yritysten kilpailukyvyn tukeminen edellyttää konkreettisten toimien lisäksi riittävää viestintää, jotta EU:n ja Naton tarjoamia kansainvälisiä yhteistyö- ja rahoitusmahdollisuuksia pystytään hyödyntämään. Kansainvälisten rahoitusmahdollisuuksien hyödyntämisen osalta on kannatettavaa, että strategiassa huomioidaan rahoitusohjelmien osallistumisen hyötynä olevan myös Suomen ja suomalaisten toimijoiden tunnettavuuden lisääminen. Esimerkiksi Naton innovaatiorahasto (NIF) on Naton DIANA kiihdyttämöstä ja Natosta erillinen toimija. Naton DIANA-kiihdyttämön ohjelma ja siihen osallistuminen tarjoaa kuitenkin näkyvyyttä myös NIFin suuntaan. Naton innovaatiorahasto taas identifioi itsensä puolustusteollisuusrahaston sijaan syväteknologiarahastoksi, joka investoi korkean tason tieteeseen ja teknologiakasvuyrityksiin, joilla on mahdollisuus vahvistaa puolustusta, turvallisuutta ja resilienssiä. Naton innovaatiorahaston toimialaa voidaan pitää laajana ja Suomen kokonaisturvallisuusajattelun kanssa yhdenmukaisena. Naton innovaatiorahaston sijoitusten tarkoituksena on kollektiivisen turvallisuuden ja hyvinvoinnin edistäminen ja ne voivat kohdistua energiaan, materiaalitieteeseen, tekoälyyn ja dataan, laskentatehoon, autonomiaan, kvanttilaskentaan, bioteknologiaan tai avaruuteen.

Kyberhygienian edistämisen ja kansalaisten kyberturvallisuusosaamisen tulisi kattaa lisäksi digitaalisen informaatiolukutaidon ja tekoälylukutaidon vahvistaminen. Tämä tarkoittaa puuttumista myös sellaisiin uhkiin, joita tekoälyn avulla tuotettu disinformaatio aiheuttaa esimerkiksi sosiaalisen median alustoilla. Kyberhygienian osaksi tulisi lisäksi sisällyttää kansalaisten taitojen vahvistaminen kognitiivisen vaikuttamisen tunnistamiseksi.

Sitra huomioi, että kyberturvallisuusstrategian luonnoksessa ei mainita yhteiskunnallisen resilienssin rinnalla taloudellisen turvallisuuden, eli yhteiskunnallisen toimintavarmuuden ja kilpailukyvyn, vahvistamista. Taloudellinen turvallisuus tulisi lisätä strategiaan yhdeksi tavoitteeksi, jota pyritään edistämään panostamalla strategisesti kyberturvallisuudenkin kannalta keskeisiin murrosteknologioihin kuten tekoäly, kvantti- ja suurteholaskenta, uudet matkaviestinverkkosukupolvet (5G ja 6G), puolijohteet ja bioteknologia. Kyberturvallisuuden varmistamisen ja murroksellisten teknologioiden hyödyntämisen kannalta on erittäin tärkeää, että strategiassa huomioidaan kattavammin kriittiset teknologiat. Strategialuonnoksessa listataan ainoastaan tekoäly, kvanttiteknologia ja uudet matkaviestinverkkosukupolvet ja tämä lista on riittämätön.

Varautumisen osalta strategiset tavoitteet ovat kannatettavia, mutta Sitra huomioi, että osaamisen varmistaminen on myös varautumista. Osaamisen varmistamista tulisi edistää osana kokonaisvaltaisen tilanneymmärryksen muodostamista sillä se on kriittinen osa yhteiskunnan kyberresilienssiä ja toimintavarmuutta edistävää varautumista. Osana suomalaista kokonaisturvallisuuden mallia, viranomaisten tulee tehdä kyberturvallisuuden varautumistyötä ja osaamisen kehittämistä tiiviissä yhteistyössä keskeisten sidosryhmien, kuten yritysten, järjestöjen ja kansalaisten kanssa. Lisäksi kriittisen infrastruktuurin toimivuus ja murrosteknologioiden mahdollisuuksien hyödyntäminen kulkevat käsi kädessä. Osana kriittisen infrastruktuurin toimivuuden takaamista tulisi pystyä myös ennakoimaan aiempaa paremmin esimerkiksi tekoälyjärjestelmien kehittämisen kannalta kasvavat energiatarpeet.

Valtioneuvoston yhteisten strategisen tason kyberturvallisuuden johtamisen resurssien keskittäminen valtion kyberturvallisuusjohtajan toimistoon ovat sinänsä kannatettavia, mutta Sitra huomioi, että liikenne- ja viestintäministeriön yhteydessä toimivan kyberturvallisuusjohtajan toimiston tulisi pyrkiä takaamaan riittävä yhteistyö yritysten kanssa. Osana yritysten ja yksityisen sektorin kanssa tehtävää yhteistyötä tulisi arvioida, miten yritykset ja yksityinen sektori olisi mahdollista osallistaa kansalliseen kyberturvallisuusstrategiatyöhön. Strategiassa tulisi määritellä, millä tavoin kansalaisten kyberturvallisuusosaamista aiotaan kehittää ja kenen vastuulla kehittämistyö on, jotta tavoite kyberturvallisuusvastuunsa tuntevista kansalaisista toteutuisi.

Yhteistoiminnan osalta Sitra pitää kannatettavana kansallisen ja kansainvälisen yhteistoimintamallin tukemiseksi asetettuja strategisia tavoitteita. Sitra kiinnittää kuitenkin huomiota siihen, että kansainvälisen yhteistoiminnan, kybertoimintaympäristöä koskevan normatiivisen kansainvälisen yhteistyön ja kyberdiplomatian edistämiseksi kirjatut toimet eivät ole riittävän konkreettisia. Tavoitellaanko kansainvälisessä yhteistoiminnassa erityisesti yhteisymmärryspöytäkirjojen (Memorandum of understanding) allekirjoittamista samanmielisten maiden välillä vai muodollisempia tiede- ja teknologia-alan sopimuksia. Miten taataan se, että kansainvälisen yhteistoiminnan strategisuus ja kokonaiskuva säilyy. Lisäksi on epäselvää, miten Suomen vaikuttaminen kyberturvallisuutta, kyberrikollisuutta ja kyberpuolustusta koskevaan päätöksentekoon tullaan toteuttamaan YK:n, EU:n, Naton ja muiden kansainvälisesti keskeisten

verkostojen ja järjestöjen osalta (kuten OECD) tullaan resursoimaan aktiivisen vaikuttamisen ja Suomen intressien edistämisen takaamiseksi. Yhteistoiminnan ja päätöksentekoon vaikuttamisen tulisi olla ennakoivaa reaktiivisen sijaan, jonka vuoksi on myös pohdittava, tulisiko vaikuttamistoimet sisällyttää osaksi kokonaisturvallisuusajattelun varautumista. Pitkän aikavälin suunnittelussa tulisi myös olla riittävän selkeästi huomioituna toimivaltakysymykset ja niiden merkitys Nato:n ja EU:n kontekstissa. Tämä tarkoittaa esimerkiksi sitä, että Suomen pitää pystyä ennakoida ja varautua tilanteisiin, jossa EU:n rooli puolustusteollisuuden kilpailukykyä edistävänä toimijana kasvaa.

Yhteistoiminnan edistäminen EU:ssa, Natossa ja muissa kansainvälisissä verkostoissa sekä kahdenvälisesti yhdessä samanmielisten maiden kanssa on kriittistä Suomen kyberturvallisuuden tavoitetilaan pääsemisen kannalta. Strateginen yhteistoiminta auttaa Suomea hyödyntämään teknologiset mahdollisuudet paremmin ja muodostamaan tilannekuvaa murrosteknologioiden kehittämiseen liittyvistä geopoliittisista jännitteistä ja kybertoimintaympäristöön liittyvistä uhkista. Strategialuonnoksen johdannossa on nostettu esille geopoliittisen tilanteen muutos, jonka vaikutuksen kuvataan lisänneen kansallisen ja kansainvälisen yhteistyön merkitystä kyberturvallisuuden varmistamisessa. Lisäksi osassa IV: Reagointi ja vastatoimet geopoliittinen tilanne nostetaan haasteeksi, johon Suomen tulee vastata aktiivisilla kyberdiplomatian, -puolustuksen ja -turvallisuuden toimilla itsenäisesti ja osana monenvälistä toimintaa. Geopoliittiseen tilanteeseen vastaamisen ei tulisi rajoittua vain reaktiiviseksi vastatoimeksi vaan Suomen pitäisi kyberturvallisuusstrategiassa pyrkiä ennakoivaan ja pitkäjänteiseen teknologiayhteistyöhön sekä tavoitella lisäämään ymmärrystä siitä, miten tieteen ja teknologian kehitys vaikuttavat Suomen kybertoimintaympäristöön.

Strategialuonnoksesta puuttuvat Suomen pitkän aikavälin tavoitteet kyberturvallisuuden edistämiselle ja näiden tavoitteiden peilaaminen arvioihin Euroopan komission juuri alkaneen viisivuotiskauden agendaan koskien kyberturvallisuutta ja kilpailukykyä. On myös oleellista, että strategiassa huomioidaan yhteydet EU:n digitaalisen vuosikymmenen tilaa koskevan raporttiin, jossa on raportoitu esimerkiksi Suomen kohdalla alhaisesta luottamuksesta koskien kansallisia toimia turvallisen digitaalisen ympäristön takaamiseksi lapsille ja nuorille. Strategiassa tulisi lisäksi yksilöidä tarkemmin, miten kyberturvallisuuden kannalta merkittäviä teknologioita tullaan edistämään, mitä nämä murrosteknologiat ovat ja kenen kanssa sekä millä foorumilla yhteistyötä tullaan tekemään. Yhteistoiminnan osalta on myös merkittävä huomioida eri toimijoiden toimivalta edistää kyberturvallisuuden kannalta merkittäviä asioita ja pyrkiä strategisuuteen siinä, miten yhteistoimintaa edistetään Suomen etua parhaiten tukevalla tavalla.

Resursointi, toimeenpano ja seuranta:

Reagoinnin ja vastatoimien osalta strategiset tavoitteet oikea-aikaisen uhkiin reagoimisen ja turvatun suvereniteetin edistämiseksi ovat sinänsä kannatettavia, mutta vaativat tarkennusta kyberpuolustuksen tehtävien ja roolien osalta. Kansallisen kyberpuolustuksen toteuttamisen tueksi laadittavaksi suunniteltu kyberpuolustusdoktriini on näin ollen kannatettava tapa tarkentaa kyberpuolustuksen tavoitteita. Kansallisten ja Naton tuomien, sekä muiden kyvykkyyksien ja toimintamahdollisuuksien lisäksi siinä tulisi kuvata lisäksi teknologiapolitiikan kannalta keskeisiä

geopoliittisia riippuvuuksia ja huomioida lisäksi muut kriittisten teknologioiden kehittämiseen liittyvät keskinäisriippuvuudet. On lisäksi huomioitava, että teollisuuspoliittisen strategian ja kvanttiteknologiastrategian valmistelussa esiin nousevat asiat ovat vähintään osittain päällekkäisiä kyberturvallisuustrategian kanssa. Lisäksi Teknologiateollisuuden koordinoiman puolijohdealan kasvustrategia on myös kyberturvallisuusstrategian ja kansallisen kriittisen infrastruktuurin kannalta olennainen. Teollisuuspoliittisen strategian kannalta tulisi huomioida globaalin kilpailutilanteen ja geopolitiikan muutosten aiheuttamat jännitteet ja teollisuuspoliittisen strategian tavoite pyrkiä vahvistamaan suomalaisen teollisuuden kilpailuasetelmaa globaaleilla markkinoilla. Kansallisen kvanttiteknologiastrategian tavoitteiden ja kyberturvallisuusstrategian välillä on synergiaetuja, ja päällekkäisyyksien sijaan strategioiden valmistelutyön välillä tulisi tehdä läheistä yhteistyötä ja hyödyntää sidosryhmien osallistuminen strategiatyön valmisteluun. Lisäksi teollisuuden tarvitsemien osaajien saatavuuden takaaminen on sekä kvanttiteknologiastrategian, teollisuuspoliittisen strategian, kyberturvallisuusstrategian ja puolijohdealan kasvustrategian kannalta kriittistä.

Resursoinnin, toimeenpanon ja seurannan osalta Sitra viittaa aiempaan huomioon siitä, että kyberosaamiseen panostaminen tulisi koulutuksen ja tutkimuksen lisäksi näkyä erityisesti vaikuttajien ja päättäjien osaamisen vahvistamisen tukemisena. Päättäjien tukemiseksi on vahvistettava kokonaisvaltaista kansainvälisen yhteistyön ja EU:n tieto- ja teknologiapolitiikan ymmärrystä, jonka yhtenä osana kyberturvallisuus on. Innovatiivinen kyberturvallisuuden ekosysteemi ja yritysten kilpailukyvyn edistäminen murroksellisia teknologioita hyödyntämällä edellyttää päättäjätason näkemystä ja johtajuutta kriittisistä teknologioista ja EU:n tieto- ja teknologiapolitiikasta. Osaamiseen panostamisessa tulisi huomioida myös Digikompassin tavoite siitä, että “vuonna 2030 Suomi on digitaalisesti sivistynyt maa”. Teknologisen ja yhteistoiminnallisen varautumisen ohella kyberuhkien torjunnassa on oleellista inhimillisen pääoman - digitaalisen sivistyksen - pitkäjänteinen kehittäminen laajasti suomalaisessa yhteiskunnassa.

Sitra yhtyy toteamukseen siitä, että kaikkien strategisten tavoitteiden ja kehittämistoimien toteuttamiseen on suunnattava lisää resursseja. Resurssien suuntaamisen ei kuitenkaan pitäisi olla itseisarvo, vaan resursseja tulisi pystyä suuntaamaan strategisesti siten, että Suomen kyberprofiilin nostaminen olisi todellisuudessa mahdollista. Murrosteknologioihin kohdistuvan korkeatasoiseen tutkimus- ja kehitystoimintaan ja kyberturvallisuuteen tehtävät investoinnit ovat tarpeen, mutta niiden lisäksi on tärkeää tukea yhteistoimintaa viranomaisten ja yksityisen sektorin välillä sekä päättäjiä kyberturvallisuuteen ja teknologiapolitiikkaan liittyvässä päätöksenteossa ja strategisissa valinnoissa. Suomella on mahdollisuus vaikuttaa kyberturvallisuusstrategian kannalta merkittävään EU:n tieto- ja teknologiapolitiikkaan panostamalla startup-ekosysteemiin ja houkuttelemalla enemmän EU:n tutkimusrahoitusta sekä osallistumalla konsortioihin. Suomella on paljon annettavaa kyberturvallisuusstrategian kannalta keskeisten kriittisten teknologioiden kehittämisessä osana EU:ta ja Natoa, mutta murrosteknologioiden osalta on pyrittävä takaamaan realistinen tilannekuva siitä, miten ja missä teknologioissa Suomen on mahdollista yksin pyrkiä teknologiseen omavaraisuuteen. Tilannekuvan muodostaminen on tärkeää myös Suomen etua edistävien strategisten päätösten tekemisen edistämiseksi.

Sitra tukee tavoitetta Naton innovaatiorahoituksen ja EU:n kehittämisrahoituksen hyödyntämisestä osana Suomen kyberekosysteemin kehittämistä. Yhteisen ymmärryksen varmistamiseksi Sitra pyytää strategian tekstiin selvennystä siitä, viitataanko tällä Naton DIANA innovaatioaloitteeseen lisäksi myös Natosta irrallaan toimivaan Naton innovaatiorahastoon. Naton innovaatiorahasto investoi

puolustusta, turvallisuutta ja resilienssiä vahvistaviin syväteknologiayrityksiin ja kattaa laajan toimialan voiden kohdistua energiaan, materiaalitieteeseen, tekoälyyn ja dataan, laskentatehoon, autonomiaan, kvanttilaskentaan, bioteknologiaan tai avaruuteen. Lisäksi Sitra huomioi, että strategialuonnoksessa ei yksilöidä EU:n Horisontti Eurooppa ja Digitaalinen Eurooppa (DEP) -puiteohjelmien rahoituksen lisäksi muita EU:n rahoitusinstrumentteja tai puolustusteollisuuden yhteistyöalustoja kuten Euroopan puolustusrahasto (EDF). Euroopan puolustusrahaston edunsaajina ovat lähtökohtaisesti teollisuus- ja tutkimuskonsortiot ja rahaston toiminnan tavoitteena on vahvistaa yhtenäisiä ja avoimia EU:n sisämarkkinoita tukemalla vähintään kolmen eri EU-jäsenvaltiossa tai assosioituneessa maassa (Norja) sijaitsevan toimijan välillä yhteistyössä tehtäviä toimia.

Strategiset kehittämisehdotukset:

Sitra lähtökohtaisesti kannattaa strategialuonnoksessa esitettyjä kehittämisehdotuksia, mutta esittää niihin seuraavia tarkennuksia:

- Kirkastetaan Suomen asemoitumista kyberturvallisuudessa ja kyberpuolustuksessa, kehitetään osallistumista kansainväliseen kyberturvallisuuden yhteistoimintaan, luodaan tätä varten tarvittava kansallinen koordinaatio ja varmistetaan yhteistoiminta valtionhallinnon ja yksityisen sektorin sekä muiden valmisteilla olevien strategiatöiden välillä.

- Varaudutaan uusien murrosteknologioiden, erityisesti kvanttilaskennan, tekoälyn, puolijohteiden, suurteholaskennan, 6G:n ja avaruusteknologian, kehittymisen tuomiin uhkiin ja mahdollisuuksiin.

- Edistetään teknologisen suvereniteetin ja kyberturvallisuuden ekosysteemin kehittämistä ja varmistetaan Suomen teknologinen edelläkävijyys ja uudet innovaatiot.

- Kehitetään viranomaisten yhteistoimintaa ja yhteistä tilanneymmärrystä luomalla tarvittavat yhteistyörakenteet ja koordinointimallit, selkeyttämällä roolit ja vastuut sekä varmistamalla tiedonvaihdon ja tiedonsaannin edellytykset. Panostetaan ennakoivaan yhteistyöhön.

- Muutetaan säädöspohjaa, normeja ja ohjeita strategian kehittämistoimien edellyttämällä tavalla.

- Vahvistetaan viranomaisten, alue- ja paikallishallinnon, yksityissektorin ja kansalaisyhteiskunnan yhteistoimintaa ja yhteistä varautumista ja yhtenäistetään kansainvälinen yhteistoiminta minimoimalla strategista ohjaamista rajoittavat rakenteelliset tekijät. Tämä tapahtuu keskittämällä erityisesti kansainvälisen yhteistyön kannalta merkittävä strateginen koordinaatio kyberturvallisuusjohtajan toimistolle.

- Ylläpidetään ja parannetaan luottamusta turvallisilla ja toimintavarmoilla julkisilla palveluilla

- Suunnitellaan ja seurataan kyberturvallisuusresursseja pitkäjänteisesti. Tämän lisäksi panostetaan viestintään tarjolla olevista EU- ja kv-rahoitusmahdollisuuksista. Määritetään toimija, joka vastaa viestinnästä.

- Kehitetään osaamista sekä kansalaisten ja kansalaisyhteiskunnan kybervalmiuksia ja varautumista. Määritetään toimija, joka ottaa roolin kybervalmiuksien ja digi- ja tekoälylukutaidon vahvistamiseksi.

- Kehitetään harjoitustoimintaa ja harjoitusympäristöjä varautumisen ja osaamisen lisäämiseksi.

- Kehitetään toimintaympäristötuntemusta muun muassa turvaamalla kansallinen havainnointikyky sekä turvallisuus- ja tiedusteluviranomaisten mahdollisuudet tietojen hankkimiseksi kybertoimintaympäristöstä yksityisyydensuoja huomioiden.

- Edistetään kokonaisvaltaista kyberrikollisuuden torjuntaa.

- Kehitetään kyberpuolustusta osana kokonaismaanpuolustusta, Suomen suvereniteetin turvaamista ja integroitumista liittokunnan puolustukseen. Vahvistetaan kyberpuolustusosaamista kokonaisvaltaisesti huomioiden teknologioiden väliset keskinäisriippuvuudet.

- Arvioidaan kyberturvallisuusnäkökulmia kaikissa lainsäädäntöhankkeissa.

Kristine Alanko

Asiantuntija, Suomen itsenäisyyden juhlarahasto Sitra

kristine.alanko@sitra.fi

Reijo Aarnio,

Vanhempi neuvonantaja, Suomen itsenäisyyden juhlarahasto Sitra

reijo.aarnio@sitra.fi

Alanko Kristine
Suomen itsenäisyyden juhlarahasto Sitra