Tuomo Rusila
Vanhempi osastoesiupseeri
Tietohallintoyksikkö
16.10.2023

Eduskunnan puolustusvaliokunnalle

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksista Euroopan parlamentin ja neuvoston asetuksiksi (kybersolidaarisuussäädös ja kyberturvallisuusasetuksen muuttaminen)

Eduskunnan puolustusvaliokunta on pyytänyt puolustusministeriöltä kirjallista asiantuntijalausuntoa hallituksen esityksestä U 20/2023 vp. Puolustusministeriö kiittää mahdollisuudesta lausua Euroopan parlamentin ja neuvoston ehdotuksesta kybersolidaarisuussäädökseksi ja kyberturvallisuusasetuksen muuttamiseksi. Puolustushallinto on osallistunut kirjelmän laadintaan, näkemykset on kuultu valmistelutyön aikana ja huomioitu kirjelmässä.

Vaikka ehdotetun kybersolidaarisuussäädöksen sisältöön, sen vaikutusten arviointiin tai kustannuksiin liittyykin Valtioneuvoston kirjelmän mukaisia tarkennustarpeita, ja vaikka ehdotuksella on joitakin päällekkäisyyksiä tällä hetkellä oleviin kyberturvallisuuden tilannekuva- ja tiedonvaihtotoimintojen kanssa ja kansallinen soveltaminen edellyttäisi lisäresursseja, puolustusministeriö kannattaa sekä ehdotetun kybersolidaarisuussäädöksen että kyberturvallisuusasetuksen muutoksen tavoitteita.

Kansallisen kyberturvallisuuden – ja puolustuksen tehokas ja tavoitteellinen toteuttaminen edellyttää nykyisten lähestymistapojen päivittämistä niin monikansallisessa kuin kansallisessa viitekehyksessä. Kyberuhkiin vastaaminen edellyttää entistä tiiviimmän, nopeamman ja laajemman tilannekuva- ja tiedonvaihtotoiminnan lisäksi kehittyneempiä kykyjä toteuttaa kriisivastetta sekä erilaisia lisätoimia kriisinkestävyyden vahvistamiseksi. Tavoitteet ovat yhtenäisiä niin kansallisesti, EU:n kuin Naton kyberresilienssin ja -puolustuksen vahvistamisen näkökulmista. Tämä edellyttääkin yhteensovitettuja toimia niin kansallisesti kuin monikansallisesti. Näiden eri toimien synergiat tulee huomioida kokonaisvaltaisesti arvioitaessa kulloinkin esitettyjen keinojen vaikuttavuutta, kustannustehokkuutta tai tarpeita muutoksiin kansallisessa toiminnassa ja lainsäädännössä. Kyberturvallisuuden ja kansallisen turvallisuuden välisen suhteen uudelleenarviointi olisi osa tätä kokonaisuutta. Tällä on erityisesti merkitystä sovellettaessa EU:n säädöksiä kansallisesti, mutta myös kansallisen toiminnan kehittämisessä suhteessa esimerkiksi perusoikeuksiin.

Tämän hetkisiä kansallisia kyberturvallisuuden haasteita on tunnistettu sisä- ja puolustusministeriön johtaman poikkihallinnollisen selvitystyön loppuraportissa (Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa). Selvityksessä kuvataan kyberturvallisuuden ja –puolustuksen kansallista nykytilaa, tavoitteita ja muutostarpeita. Selvitys tunnistaa myös viranomaisten väliseen tiedonvaihtoon liittyviä ongelmia.

Tuomo Rusila
Vanhempi osastoesiupseeri
Tietohallintoyksikkö
16.10.2023

Poikkihallinnollisen selvitystyön tuloksien perusteella Valtioneuvoston kirjelmässä tunnistetut oikeudelliset haasteen kybersolidaarisuussäädöksessä kuvattuun tiedonvaihtoon liittyen tulisivat joka tapauksessa kansallisesti ratkaistavaksi. Vastaavasti Naton Vilnan huippukokouksessa Suomi ilmoitti osallistuvansa Naton niin sanottuun VCISC –toimintaan (Virtual Cyber Incident Support Capability), jolla on yhteneväisyyksiä kybersolidaarisuussäädöksessä esitetyn kyberturvallisuusreservin kanssa. Tämäkin saattaa aiheuttaa tarpeita tarkastella kansallista lainsäädäntöä.

Kansallisesti tunnistettuihin kehitystarpeisiin sekä Naton ja EU:n piiristä esitettyihin kyberturvallisuuden – ja puolustuksen kehittämistavoitteisiin voitaisiin jatkossa vastata paremmin yhteensovittamalla kansallisia osallistumis- ja kehittämiskeinoja sekä tehostamalla kansallisesti ja monikansallisesti siviili-sotilasyhteistyötä. Tämä mahdollistaisi myös kansallisen rahoituksen ja eri EU:n rahoitusmekanismeista saatavan rahoituksen nykyistä tehokkaamman hyödyntämisen. Tällöin kohtuullisilla kansallisilla rahoitusosuuksilla saataisiin mahdollisesti kokonaissäästöjä, mutta myös kumuloituvia vaikutuksia, jos kehitystoimi olisi joka tapauksessa kansallisestikin tehtävä. Kybersolidaarisuussäädöksen osalta tilannekuva- ja tiedonvaihtoyhteistyön kehittäminen ja kyberturvallisuusreservi ovat esimerkkejä tällaisista toimista.

Vaikka kybersolidaarisuussäännöksen esittämien uusien tilannekuva- ja tiedonvaihtotoimintojen perustamisessa tulisikin välttää päällekkäisyyksiä jo olemassa olevien toimintojen kanssa, on huomioitava, että osa nykyisistä toiminnoista ei kykene eri syistä niin syvälliseen ja laaja-alaiseen yhteistyöhön kuin uhkien näkökulmista olisi tarkoituksenmukaista. Lisäksi uusilla tilannekuva- ja tiedonvaihtotoiminnoilla on toisiaan täydentävä vaikutus, jolloin myös liian tarkkarajainen päällekkäisyyksien poisto voisi kääntyä itseään vastaan. Uudet toiminnot mahdollistavat samalla myös joidenkin vanhojen haasteiden pienentämistä. Kyberturvallisuusviranomaisilla ja kyberpuolustusviranomaisilla on pääsääntöisesti omat monikansalliset tilannekuva- ja tiedonvaihtotoiminnot, mikä aiheuttaa haasteita molempien toimintaedellytyksille ja yleensäkin siviili-sotilasyhteistyölle. Soveltamalla kansallisesti kybersolidaarisuussäädöksen ehdotuksia molempien toimijoiden näkökulmasta mahdollistavasti kyettäisiin näitä haasteita ainakin osin pienentämään.

Vaikka kybersolidaarisuussäädöksen ehdottamien kansallisten SOC-toimijoiden ja rajat ylittävien SOC-yhteenliittymien välisestä tietojenvaihdosta sekä komissiolle annettavasta toimivallan siirrosta tarvitaankin lisätietoja, on ehdotuksessa merkittävästi myös sellaista mitä tulisi kansallisesti joka tapauksessa kehittää. Suomi on tällä hetkellä mukana Tanskan johtamassa SOC-yhteenliittymän valmistelutyössä. Valmistelu tehdään Pohjoismaiden ja Baltian NB8-kokoonpanossa, mikä on alueellisen kyberyhteistyön ja keskinäisen luottamuksen kehittämisen näkökulmasta mielekäs viitekehys. Työssä on

tunnistettu vastaavia kybersolidaarisuusehdotukseen liittyviä haasteita kuin Valtioneuvoston kirjelmässä.

Käynnissä olevasta SOC-yhteenliittymätyöstä on saatavissa potentiaalisten operatiivisten hyötyjen lisäksi myös mahdollisia kustannussäästöjä. Työ toimii parhaimmillaan myös laajemmankin monikansallisen ja kansallisen kehityksen moottorina. Puolustushallinnon tahtotilana on olla mukana niin kansallisten SOC-toimijoiden kuin SOC-yhteenliittymän kehitystyössä sekä osallistua tiiviisti niiden operatiiviseen toimintaan. Kehitystyö tukee kyberpuolustuksen suorituskyvyn kehittämistä sekä tiedonvaihto- ja tilannekuvatarpeiden täyttämistä, mutta myös kansallisesti keskeisen siviili-sotilasyhteistyön edelleen kehittämistä. Kehitystöillä on potentiaalia tukea myös julkisen ja yksityisen sektorin yhteistyön kehittämistä kyberuhkiin varautumiseksi ja niiden torjumiseksi.

Puolustusministeriön näkemyksen mukaan Valtioneuvoston kirjelmä on hyvin valmisteltu ja muotoiltu ja esitetty valtioneuvoston kanta on edellä todettu huomioiden tarkoituksenmukainen.