Pääesikunta

Lausunto

08.08.2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Pääesikunta kiittää mahdollisuudesta lausua kyberturvallisuusstrategiaan. Periaatepäätös kattaa ne osa-alueet, joita on tarpeen käsitellä strategian näkökulmasta. Strategia on laadukkaasti valmisteltu ja siinä esitetään tavoitteita viranomaisten kannalta merkittäviin kehitettäviin kokonaisuuksiin kuten johtaminen, toimivalta sekä viranomaisyhteistyö.

Kyberpuolustuksen rooli on muutoksessa. Tämä näkyy esimerkiksi keskusteluna kyberpuolustuksen suhteesta kansallisen kriittisen infrastruktuurin ja toimintojen suojaamisessa sekä osallistumisessa liittokunnan puolustukseen ja pelotteeseen. Strategia luo pohjaa sotilaallisen kybertoiminnan kehittämiseksi ja yhteensovittamiseksi muiden yhteiskunnan toimijoiden kanssa. Tehtäessä vertailua kansainvälisesti voidaan havaita, että valtiot ovat päätyneet erilaisiin ratkaisuihin kansallisissa järjestelyissään ja toisaalta järjestelyjä on säädetty ajassa.

Päivitetty käsitteenmäärittely kyberturvallisuuden ja kyberpuolustuksen osalta on perusteltu. Strategia ei käsittele yksityiskohtaisesti sotilaallisen kyberpuolustuksen suhdetta kansalliseen kyberpuolustukseen. Termit sotilaallinen kyberpuolustus ja kansallinen kyberpuolustus on kuvattu, mutta niiden keskinäistä suhdetta ja vastuujakoa ei ole kattavasti käsitelty. Puolustusvoimat tunnistaa, että käsittely tarkentuu kyberpuolustusdoktriinissa, mutta haluaa korostaa selkeyttämisen merkittävyyttä.

Kyberturvallisuusstrategia nostaa yhdeksi pilariksi reagoinnin ja vastatoimet. Sotilaallisesta näkökulmasta tarkasteltuna tämä on perusteltua ja sopii Suomen rooliin osana liittokuntaa. Suomen on kyettävä vastaamaan uhkaan monipuolisella keinovalikoimalla (diplomatia, informaatio, sotilaallinen, taloudellinen). Reagoinnin ja vastatoimien toteuttaminen kybertoimintaympäristössä tai sen kautta jää strategiassa vähemmälle huomiolle, varsinkin normaaliolojen kehyksessä.

Vastuunjako eri viranomaistoimijoiden kesken ei välttämättä ole strategia-asiakirjan sisältöön kuuluva asia, mutta toimeenpano-ohjelmassa ja viimeistään kyberpuolustusdoktriinissa sitä on tarkennettava. Reagoinnin ja vastatoimien käynnistäminen eri tilanteissa tulee olla määritelty viiveettömän toiminnan mahdollistamiseksi ja toimivallan tulee sitä tukea. Vastuunjaon perustuminen erilaisiin kybertoimintaympäristön ilmiöihin voi olla haastavaa, sillä attribuution ongelmallisuuden vuoksi esimerkiksi kyberrikollisuuden erottaminen valtiollisesta kyberoperaatiosta ilmiön ollessa käynnissä voi olla vaikeaa.

Puolustusvoimien näkökulmasta kansallisen kybersuvereniteetin määrittely ja rajaaminen on merkityksellistä. Strategiassa sivutaan tätä kokonaisuutta, mutta sitä ei kuitenkaan tarkemmin käsitellä. Määritelmiin ei ole tuotu kybersuvereniteettia tai valtiollisen kybertoimintaympäristön käsitettä. Puolustusvoimien toiminnalle edellä kuvattu määrittely olisi merkityksellinen erityisesti arvioitaessa toimivaltaa vastatoimien toteuttamisessa sekä vihamielisen toiminnan vakavuutta. Puolustusvoimien näkökulmasta termille tarvitaan strategisen tason määrittely valtionhallinon tasolta.

Tiedonvaihdon tarve kasvaa lähitulevaisuudessa sekä kansallisesti että kansainvälisesti. Tämä kasvattaa dataan ja tietoon liittyvää tiedonhallintaa sekä luo vaatimuksia mahdollistavalle lainsäädännölle. Tiedonvaihdon tulee olla harkittua ja tarpeeseen perustuvaa. Strategiassa tulisi määritellä mihin lainsäädäntöön tai sen osiin tulisi muutostyö ja lainsäädäntövalmistelu käynnistää ja siten vahvistaa sekä huomioida jo laadittujen toimeenpano-ohjelmien ja selvitysten tulosten käytäntöön vientiä.

Sotilaallisesta näkökulmasta tiedonvaihdon lisäksi tulee korostumaan kansallisen, liittokunnan ja kumppanien tiedon suojaaminen. Yhteistoiminta ja tiedon jakaminen viranomaisten kesken on tärkeä kehityskohde kyberpuolustuksen näkökulmasta. Strategia nostaa painopisteeksi tiedonvaihdon valtiollisten sekä yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvien vakavien uhkien osalta. Tässä Puolustusvoimien kykyjä tulee kyetä käyttämään yhteiskunnan tukena kaikissa turvallisuustilanteissa normaalioloista alkaen.

Strategiassa on ansiokkaasti nostettu esille osaaminen, teknologia sekä tutkimus, kehitys ja innovaatiotoiminta. Murrosteknologioiden hyödyntäminen ja tavoite niiden käyttöön ottamisesta ensimmäisten joukossa kyberturvallisuuden varmistamisessa on kunnianhimoinen. Salausteknologioiden ja -kyvykkyyden merkitys ja omavaraisuuden tarve on tunnistettu strategiassa. Suomessa voidaan luoda korkean tason osaamista, mutta kaiken kaikkiaan teknologiahaasteeseen vastaaminen edellyttää määrätietoista ja koordinoitua panostusta yhteiskunnan eri sektoreilla osaamisen kehittämisen, tutkimuksen sekä pitkäjänteisten investointien korostuessa.

Strategian tulisi asettaa myös tavoitteita, joilla kehitetään ja nopeutetaan tietojärjestelmien ja salausratkaisuiden tarkastustoimintaa sekä kansallisten että kansainvälisten tarpeiden näkökulmasta. Ilman nopeaa neuvonta-, tarkastus- ja hyväksyntätoimintaa ei järjestelmien ja

ratkaisuiden kehittäminen ole tosiasiallisesti mahdollista. Tässä vaiheessa strategiassa olisi tärkeää määrittää haluttu taso ja toimijat sekä aikataulu. Kansallinen kyky ja osaaminen tietoturva-arviointien ja hyväksyntöjen tekemiseen tulee varmistaa pitkäjänteisesti.

YKSITYISKOHTAISET MUUTOSESITYKSET JA HUOMIOT

Alkuperäinen (s. 12): Nato-jäsenyyden pelotevaikutus saattaa johtaa vihamielisen toiminnan painopisteen siirtymiseen entistä enemmän kybertoimintaympäristöön, jossa tekijän on helpompi kiistää osallisuutensa.

Muutosesitys: Esitetään, että virke jätetään pois. Virke jättää epäselväksi kybertoimintaympäristön suhteen pelotteeseen eikä tuo merkittävästi lisäarvoa.

Alkuperäinen (s. 22): Suomi ottaa etulinjassa käyttöön murrosteknologioiden hyödyt ja edellyttää laitteisiin ja palveluihin sisäänrakennettua turvallisuutta.

Muutosestys: Esitetään, että etulinjassa-sana otetaan pois.

Strategiassa mainitaan sivulla 37 seuraavaa: ”Valtiollisiin kyberoperaatioihin reagoidaan ja vastataan eri tavoin kuin tavanomaisiin kyberuhkiin. Valtiolliseen vihamieliseen kybertoimintaan vastaaminen rikosvastuuseen saattamisen menetelmin ei välttämättä ole tehokkain tapa.” Kirjaus saattaa jättää kuvan, että kansallinen ja kansainvälinen lainsäädäntö ei koskisi samalla tavalla valtiollisia toimijoita. Valtiollisen tiedustelutoiminnan ja vihamielisen vaikuttamisen erottelu toisistaan on tärkeää. Valtiolliseen tiedustelutoimintaan vastaaminen voi edellyttää erilaisia keinoja kuin esimerkiksi sellaiseen kyberhyökkäykseen vastaaminen, jonka nimenomaisena tarkoituksena on yhteiskunnan kriittisten toimintojen lamauttaminen. Käytännön toimien näkökulmasta on keskeistä, että attribuutio ei hidasta toimintaa ja vastetta kyetään valtion tasolla käyttämään joustavasti.

Alkuperäinen (s. 39): [Kyberpuolustusdoktriinissa] kuvataan, miten kyberpuolustus toteutetaan hyödyntäen kansalliset ja Naton tuomat kyvykkyydet, muut kyvykkyydet ja toimintamahdollisuudet.

Muutosesitys: Esitetään korvattavaksi ”kansalliset, liittokunnan ja kumppanien kyvykkyydet”.

Alkuperäinen (s.51): Puolustusvoimien tehtävien voidaan katsoa kattavan myös kybertoimintaympäristö (kyberpuolustus ja tiedustelu kybertoimintaympäristössä).

Muutosesitys: Puolustusvoimien lakisääteisten tehtävien toteuttaminen edellyttää toimintaa kybertoimintaympäristössä.

Määritelmissä esitetty (s. 54) ”Kansallinen kyberpuolustus” rajoittaa termin koskemaan ”valtioiden aiheuttamia kyberuhkia”. Termin määrittelyssä tulisi ottaa huomioon myös muut kuin valtiollisten

toimijoiden muodostamat uhat (esimerkiksi terrorismi ja rikollisuus). Kansallinen kyberpuolustus ja siihen liittyvä sotilaallinen kyky on oltava käytettävissä kaikissa valtioon kohdistuvissa uhkissa. Esimerkiksi haasteet attribuutiossa eivät saa olla esteenä vastatoimien toteuttamiselle.

LOPUKSI

Puolustusvoimien näkökulmasta strategia tarjoaa lähtökohdan sotilaallisen kyberpuolustuksen kehittämiseksi. Kyberturvallisuusstrategia on korkean tason asiakirja, joka luo tavoitteita eri toimijoille. Strategia on laaja ja mahdollisuuksien mukaan strategiassa tulisi pyrkiä valtiollisen kybertoiminnan kehittämisen vahvempaan painopisteen ilmaisuun.

Sotilaallisen kyberpuolustuksen kannalta keskeisenä kokonaisuutena kyberturvallisuusstrategian sekä -doktriinin osalta nähdään yhteistoiminnan perusteiden terävöittäminen yhä tehokkaamman toiminnan mahdollistamiseksi niin kansallisten kuin kansainvälisten toimijoiden kesken.

Tunnistetut merkittävät kehitettävät kokonaisuudet sotilaallisessa kyberpuolustuksessa ovat lainsäädäntö ja toimivalta sekä tiedonvaihto. Tällä hetkellä Puolustusvoimilla ei ole yksiselitteistä määritettyä kyberpuolustuksen tehtävää lain tasolla. Kyberpuolustuksen käsite ja käytännön sisältö ovat jääneet aikaisemmissa strategioissa ja määritelmissä tulkinnanvaraisiksi.

Viranomaisten yhteistoiminnan tiivistymisen lisäksi yhteistyö yrityskentän kanssa nousee jatkossa entistä merkittävämpään rooliin. Hyötyjen realisoituminen edellyttää yhteistoiminnan esteiden poistamista ja ketteryyden lisäämistä viranomaisyhteistyöhön sekä julkishallinnon ja elinkeinoelämän välille.

Kyberpuolustusstrategian kirjaukset luovat päivitystarpeita myös muihin valtiohallinnon julkaisuihin. Ajankohtaisimpana nousee esiin kokonaisturvallisuuden mallin päivittäminen kyberpuolustuksen osalta yhteiskunnan turvallisuusstrategiassa.

Puolustusvoimien tehtävän kannalta on tärkeää turvata sekä Puolustusvoimien omat että muut puolustuskykyyn suoraan vaikuttavat järjestelmät ja toimijat kyberuhkilta. Puolustusvoimien rooli kriittisen infrastruktuurin ja yhteiskunnan elintärkeiden toimintojen tukena tulee täsmentää. Tarkastelu tulee tehdä kokonaisuutena ja myös toimivallan ja resurssien näkökulmista.

Strategian toimeenpanon vastuuttamiseen, resurssointiin ja seurantaan sekä vaikuttavuuden arviointiin tulee kiinnittää huomiota. Aikaisempien strategioiden tavoitteiden ja reaalisen toteuman välillä on osin epäsuhtaa, mikä pitää tunnistaa määritettäessä toteuttamiskelpoisia jatkotavoitteita.

Pispa Kimmo
Pääesikunta

Timonen Jussi
Pääesikunta