10.4.2025

Puolustusvaliokunta

Elisa Oyj:n lausunto puolustusselonteosta

Viite: VNS 9/2024 vp

Eduskunnan Puolustusvaliokunta pyytänyt Elisa Oyj:ltä Valtioneuvoston puolustusselonteosta

Kiitämme mahdollisuudesta tulla kuulluksi asiassa ja lausumme kunnioittaen seuraavaa.

Keskeiset viestit käsillä olevaan esitykseen liittyen

- Koko yhteiskunta – mukaan lukien viranomaiset, elinkeinoelämä ja kansalaisyhteiskunta – osallistuu puolustuskyvyn rakentamiseen ja ylläpitämiseen. Elinkeinoelämän ja viranomaisten toimintaa suunnittelussa, varautumisessa, ja tilanteissa toimimisessa tulee kehittä yhteistoiminnassa. Sääntelyn tulee mahdollistaa ja edistää yhteistoimintaa.
- Varsinkin kriisitilanteessa yhteiskunnan erilaisten intressien ja tarpeiden yhteensovittaminen on olennaista sekä suunnittelussa että operatiivisessa toiminnassa.
- Kyber- ja informaatiopuolustuksessa on erityisen vahvat kytkennät siviiliyhteiskuntaan ja niihin tulee kiinnittää erityistä huomiota. Puolustus toteutetaan osin siviiliyhteiskunnan järjestelmissä ja järjestelmillä. Aktiivinen ja luottamuksellinen yhteistoiminta sekä suunnittelussa että mahdollisissa tilanteissa on keskeistä onnistuneen puolustuksen järjestämisessä.
- Suomea uhkaavaa valtiollista hyökkääjää vastaan puolustettaessa tarvittaneen poikkeavia keinoja verrattuna toimintaan tavanomaisempia kyberuhkia vastaan. Mm. yksityisyyden ja omaisuudensuojaan tai sananvapauteen liittyvät kysymykset vaativat oman tarkastelunsa osana puolustuksen kehittämistä. Vastaavasti viranomaisten toimivaltuudet normaali- ja poikkeusoloissa sekä puolustustilassa edellyttävät tarkastelua ja erilaisten intressien tasapainottamista
- Suomessa merkittävä osa keskeisestä kriittisestä infrastruktuurista on yksityisten yritysten tuottamaa ja hallitsemaa. Keskeisten elinkeinoelämän toimijoiden tuominen vahvemmin mukaan on tarpeen varmistamaan suojaamistoimien vaikuttavuuden ja toteuttamiskelpoisuuden. Varautuminen voi edellyttää merkittäviä, investointeja, joiden toteuttaminen tulee mahdollistaa.
- NATOn resilienssin perusvaatimusten (baseline requirements) huomioiminen edellyttää merkittävää siiliyhteiskunnan ja elinkeinoelämän toimia ja mukanaoloa.

Yleistä

Puolustusselonteko on ajankohtainen ja sen perusteella tehtävä kehittäminen on olennainen osa Suomen turvallisuuden varmistamisessa. Muutokset turvallisuusympäristössä, Venäjä toiminnassa ja sodankäynnissä, sekä Suomen jäsenyys NATO:ssa ovat osaltaan tuonee erilaisia puolustuksen kehittämiseen liittyviä tarpeita sekä kansallisen puolustuksen että liittokunnan puolustuksen kannalta.

Puolustus on laaja kokonaisuus. Tässä lausunnossa keskitytään seuraaviin keskeisiin teemoihin:

- Whole of Society, Siviiliyhteiskunta sekä elinkeinoelämän ja viranomaisten välinen yhteistoiminta
- Kyberpuolustus, informaatiopuolustus ja avaruus-toimintaympäristö
- Kriittisen infrastruktuurin suojaaminen
- NATO-resilienssivaatimukset

Muiden, alle olevien asioiden osana haluamme korostaa puolustuksen ja muu yhteiskunnan toiminnan yhteensovittamisen merkitystä kaikissa turvallisuustilanteissa. Tiivis ja luottamuksellinen yhteistoiminta elinkeinoelämän ja viranomaisten kesken on kriittinen osa tätä ”Whole of society” lähestymistä.

Whole of Society, Siviiliyhteiskunta sekä elinkeinoelämän ja viranomaisten välinen yhteistoiminta

Selonteossa vahvistetaan kokonaismaanpuolustuksen roolia, jossa koko yhteiskunta – mukaan lukien viranomaiset, elinkeinoelämä ja kansalaisyhteiskunta – osallistuu puolustuskyvyn rakentamiseen ja ylläpitämiseen. Kokonaismaanpuolustusmalli ja kokonaisturvallisuusajattelu luovat perustan, jossa resilienssi rakennetaan sekä "Whole of Government" että "Whole of Society" -lähestymistavoilla (kohta 4.5). Erityisesti huoltovarmuuden turvaaminen, kriittisten materiaalien ja resurssien saatavuus sekä siviilituotannon muuntaminen poikkeusolojen tarpeisiin ovat keskeisiä kansallisen varautumisen osa-alueita. Puolustusteollisuudella on erityinen asema sekä kansallisen turvallisuuden että strategisen riippumattomuuden kannalta.

Selonteossa esitetään, että viranomaisten ja elinkeinoelämän yhteistoimintaa kehitetään strategisten kumppanuuksien avulla. Puolustusteollisuuden tukeminen suuntautuu erityisesti TKI-toimintaan, vientivalmiuksien parantamiseen ja osaavan työvoiman saatavuuteen (kohdat 4.8.6 ja 4.8.7). Huoltovarmuusorganisaation ja viranomaisten roolia kehitetään siten, että siviilituotanto tukee sotilaallista toimintaa entistä tehokkaammin. Yhteisiä valmiussuunnitelmia, harjoituksia ja tiedonvaihtoa laajennetaan.

Lainsäädännön kehittämisen tarpeet liittyvät yritysten rooliin puolustusvalmiuden tukemisessa poikkeusoloissa sekä tilanteissa, joissa kriittisiä resursseja tai järjestelmiä tarvitaan puolustusvoimien tai liittolaisten käyttöön (kohta 4.8.3). Sääntelyllä tulee mahdollistaa resurssien käyttö kansallisen turvallisuuden näkökulmasta, vahvistaa teollista kapasiteettia ja tukea materiaalisen valmiuden ylläpitämistä. Lisäksi tarvitaan selkeä oikeudellinen pohja julkisen ja yksityisen sektorin yhteistoiminnalle osana kokonaisturvallisuutta.

<u>Kokonaisuuteen liittyen haluamme kiinnittää huomiota seuraaviin asioihin</u>

Kokonaismaanpuolustuksen roolin kehittäminen on olennainen lähtökohta. Yhteiskunnan, palveluiden ja teknologian kehittymisen myötä maanpuolustus ei ole erillinen saareke. Sota Ukrainassa, yhteiskunnan sopeutuminen ja teollisuuden kehitys tuovat olennaisia oppeja myös Suomen varautumisen ja valmiuden kehittämiseen maanpuolustuksen lisäksi muilla aluilla.

"Whole of Society" -näkökulma tunnistetaan strategisesti tärkeäksi ja se on selonteon arvolähtökohta. Kuitenkin sen käytännön toteutus jää vähemmän jäsennellyksi kuin hallintokeskeinen "Whole of Government" -mallin, eikä se näy yhtä selkeästi suunnittelun, ohjauksen tai vastuunjaon tasolla.

Riittävästi toimiva yhteiskunta luo edellytykset maanpuolustustahdolle ja onnistuneelle puolustukselle ylipäätään. Turvallisuuteen liittyvän toiminnan kehittäminen on synnyttänyt lukuisia strategia-asiakirjoja, selontekoja tms. dokumentteja. Poikkeusoloihin liittyvä konkreettisen toiminnan tarkastelu on jäänyt osin puolustusselonteontekoa ohuemmalle. Asian merkityksen takia koko yhteiskunnan toiminnan varmistaminen puolustusta tukevana toimintana olisi tässä yhteydessä merkityksellistä, huolimatta siitä, että kysymys on selonteon varsinaista aluetta selvästi laajemmasta kokonaisuudesta.

Selonteko painottaa elinkeinoelämän roolia vahvasti toiminnallisesta ja strategisesta näkökulmasta, mutta samalla korostaa tarvetta kehittää osallistumisen rakenteita ja oikeudellista pohjaa. Elinkeinoelämä nähdään ei vain tukijana vaan osana puolustusjärjestelmää, jolla on oma vastuunsa kriisinsietokyvyn ja resilienssin rakentamisessa. Osallistumisen vahvistaminen edellyttää jatkossa riittävää ja myös mahdollistavaa normiohjausta ja käytännön yhteistyömalleja, jotka takaavat yritysten roolin selkeyden ja toimintakyvyn puolustusjärjestelmän osana. Elinkeinoelämälle tehtävän tiedonjaon mahdollistamien ja siihen liittyvät käytännöt ovat esimerkkejä yhteistä suunnittelua edistävistä asioista.

Kyberpuolustus, informaatiopuolustus ja avaruus-toimintaympäristö

Puolustusselonteossa todetaan, että kybertoimintaympäristön merkitys puolustuksessa on kasvanut strategiselle tasolle. Valtiollisten ja valtiollisesti tuettujen toimijoiden kyberuhat kohdistuvat jatkuvasti Suomen kansallisiin järjestelmiin, päätöksenteon tukirakenteisiin ja kriittisiin palveluihin (kohta 4.3.4). Vaikuttaminen voi ilmetä sekä tiedusteluna että operatiivisena häirintänä, ja sen kohteena voivat olla myös siviili-infrastruktuuri ja tiedonvälityksen keinot. Kyberuhat voivat vaikuttaa olennaisesti yhteiskunnan toimintakykyyn ilman, että kyse on perinteisestä aseellisesta konfliktista.

Selonteossa informaatiopuolustus muodostaa kiinteän osan kyberpuolustusta ja kattaa toimet, joilla torjutaan vaikuttamisoperaatioita ja suojataan kansallista päätöksentekokykyä sekä puolustusjärjestelmän toimintaedellytyksiä (kohta 4.3.5 ja 4.8.10). Informaatiopuolustuksen tavoitteena on tukea tilanteen hallintaa ja viestinnällistä vaikuttamista kaikissa turvallisuustilanteissa sekä suojata yhteiskunnan kriittisiä toimintoja väärän ja harhaanjohtavan tiedon vaikutuksilta.

Selonteossa avaruuden käyttö tunnistetaan osaksi modernia puolustuskykyä, erityisesti tilannekuvan, viestinnän, paikannuksen ja tiedustelun välineenä (kohta 4.3.6). Avaruuteen liittyvät järjestelmät ovat kriittisiä myös ohjuspuolustuksessa ja yhteensopivuudessa Naton kanssa. Avaruustoimintaan kohdistuvat riskit – kuten häirintä ja estäminen – edellyttävät varautumista ja suojautumiskykyä.

Selonteossa esitetään, että Puolustusvoimien kykyä torjua valtiollisia ja laaja-alaisia kyberuhkia on vahvistettava. Kyberpuolustusta kehitetään teknisesti, organisatorisesti

ja operatiivisesti, ja se kytketään tiiviimmin osaksi kansallista turvallisuussuunnittelua sekä Naton kyberpuolustusrakenteita. Informaatiopuolustus integroidaan osaksi kyberpuolustusta, ja sen tehtävänä on tukea vaikuttamisen torjuntaa, operatiivista johtamista ja tiedonhallintaa (kohta 4.8.10). Kehittämistyössä korostetaan jatkuvaa valmiutta ja kykyä toimia kaikissa turvallisuustilanteissa – normaalioloista poikkeusoloihin.

Lainsäädännön osalta selonteossa esitetään tarve päivittää sääntelyä siten, että Puolustusvoimilla on toimivaltuudet toimia kyberympäristössä myös tilanteissa, joissa kyse ei ole aseellisesta hyökkäyksestä (kohta 4.8.3). Lisäksi tarvitaan sääntelyä, joka mahdollistaa tietojen tehokkaan ja turvallisen vaihdon kansainvälisten liittolaisten kanssa sekä kansallisten tietoturvastandardien yhteensovittamisen Naton vaatimuksiin. Kyberpuolustuksen järjestäminen osana kansainvälisiä operaatioita vaatii myös Puolustusvoimien tehtävien ja vastuiden tarkentamista laissa. Avaruuden osalta Selonteossa esitetään lainsäädäntöön selkeytystä puolustuksellisesta avaruustoiminnasta, mukaan lukien oikeus käyttää ja suojata kriittisiä avaruusperusteisia järjestelmiä kansainvälisten velvoitteiden mukaisesti.

<u>Kokonaisuuteen liittyen haluamme kiinnittää huomiota seuraaviin asioihin</u>

Kyber- ja informaatiopuolustuksen korostuminen ja niiden vahvempi yhteensovittaminen on välttämätöntä uhkien hallitsemiseksi ja niihin vastaamiseksi.

Kyber- ja informaatiopuolustuksessa on erityisen vahvat kytkennät siviiliyhteiskuntaan ja niihin tulee kiinnittää erityistä huomiota. Puolustus toteutetaan osin siviiliyhteiskunnan järjestelmissä ja järjestelmillä. Aktiivinen ja luottamuksellinen yhteistoiminta sekä suunnittelussa, että mahdollisissa tilanteissa on keskeistä onnistuneen puolustuksen järjestämisessä.

Suomea uhkaavaa valtiollista hyökkääjää vastaan puolustettaessa tarvittaneen poikkeavia keinoja verrattuna toimintaan tavanomaisempia kyberuhkia vastaan. Mm. yksityisyyden ja omaisuudensuojaan tai sananvapauteen liittyvät kysymykset vaativat oman tarkastelunsa osana puolustuksen kehittämistä. Vastaavasti viranomaisten toimivaltuudet normaali- ja poikkeusoloissa sekä puolustustilassa edellyttävät tarkastelua ja erilaisten intressien tasapainottamista.

Toimivaltuuksien kehittäminen etenkin normaaliolojen, mutta myös poikkeusolojen osalta edellyttää perusteellista tarkastelua ja vuoropuhelua mm. elinkeinoelämän kanssa.

Keskeisten asiantuntijoiden sijoittaminen PV:n joukkoihin voi synnyttää haastavia tilanteita varsinkin alueilla, joissa on lähtökohtaisesti rajallisesti osaamista. Puolustusvoimiin perustettavien joukkojen koulutusta tulee kehittää siten, että joukot eivät perustu yrityksissä tai hallinnossa työskenteleviin keskeisiin, ja kriisitilanteissa tarvittaviin, osaajiin.

Suomessa on vahva ja kehittyvä kyberturvallisuuteen liittyvä yrityskenttä. Puolustukseen liittyvä kaupallinen ja kehittämiseen liittyvä yhteistoiminta luo edellytyksiä puolustuksen tukemiselle, alan elinvoimalle, kehitykselle ja myös viennille mm. liittokunnan jäsenmaihin.

Avaruustoiminnan tuominen esiin selonteossa on tervetullutta ja varautumista tulee edistää koko yhteiskunnan laajuudelta. Laadukkaiden ja edullisten PNT (Position, Navigation, Time) palveluiden hyödyntäminen on laajaa yhteiskunnassa ja niihin liittyvää poikkeustilanteisiin varautumista tulee tehdä sekä puolustukseen, että siviiliyhteiskunnan resilienssin kehittämiseen liittyen.

Kriittisen infrastruktuurin suojaaminen

Selonteossa todetaan, että kriittinen infrastruktuuri – kuten liikenneverkot, tietoliikenneyhteydet, energiahuolto ja logistiikkaratkaisut – muodostaa haavoittuvan ja helposti häirittävän osan yhteiskunnan ja puolustusjärjestelmän toimintakykyä (kohta 4.8.8). Vaikuttaminen infrastruktuuriin voi olla osa hybridivaikuttamista, jolla pyritään heikentämään yhteiskunnan toimintaa, painostamaan poliittisesti tai estämään liittolaisten toimintaa Suomen alueella. Tilanne on korostunut erityisesti Venäjän hyökkäyssodan myötä, ja infrastruktuurien suojaamistarpeet ovat nousseet keskeiseksi turvallisuuspoliittiseksi kysymykseksi.

Selonteossa esitetään, että infrastruktuurin suojaamistarpeet on kartoitettava laajasti ja koordinoidusti puolustusministeriön johdolla. Suojauksen kehittämisen painopisteitä ovat erityisesti Pohjois-Suomi, rajat ylittävät yhteydet sekä sotilaallisen liikkuvuuden mahdollistavat järjestelmät. Samalla infrastruktuuria kehitetään tukemaan liittolaisten tukeutumista Suomen alueella osana Naton alueellista puolustusta ja mahdollisia DCA-sopimukseen perustuvia järjestelyjä (kohta 4.8.6). Lisäksi huomioidaan logistiset reitit, huoltovarmuuden kannalta kriittiset järjestelmät sekä energiasiirtymän vaikutukset puolustusvalmiuteen.

Lainsäädäntöön esitetään muutoksia, jotka mahdollistavat infrastruktuurin suojaamistoimenpiteet myös silloin, kun uhkat jäävät aseellisen hyökkäyksen kynnyksen alapuolelle (kohta 4.8.3). Tarvitaan sääntelyä infrastruktuurin käytöstä ja käyttöoikeuksista tilanteissa, joissa liittolaisten läsnäolo tai Naton suunnitelmien toimeenpano sitä edellyttää. Lisäksi on tärkeää säätää viranomaisten yhteistoiminnasta ja vastuista infrastruktuurin turvaamiseen liittyvissä kriisitilanteissa.

<u>Kokonaisuuteen liittyen haluamme kiinnittää huomiota seuraaviin asioihin</u>

Selonteossa esiin nostetut kasvaneet kriittisen infrastruktuurin suojaamisen tarpeet ovat ilmeisiä.
Selonteossa käsitellään luonnollisesti sotilaallista huoltovarmuutta. Koska keskeiset kriittisen infrastruktuurin toiminnot tuottavat palveluita koko yhteiskunnalle, tulee Whole of Society-näkökulma tuoda korostetusti esiin.

Varsinkin kriisitilanteessa yhteiskunnan erilaisten intressien yhteensovittaminen on olennaista. sekä suunnittelussa että operatiivisessa toiminnassa. Priorisointi ei voi olla kaavamaista vaan tilanteisiin sidottua.

Suomessa merkittävä osa keskeisestä kriittisestä infrastruktuurista on yksityisten yritysten tuottamaa ja hallitsemaa. Selonteossa esitetään vahvasti hallintolähtöistä

kriittisen infrastruktuurin suojaamisen tarkastelua. Keskeisten elinkeinoelämän toimijoiden tuominen vahvemmin mukaan on tarpeen varmistamaan suojaamistoimien vaikuttavuuden ja toteuttamiskelpoisuuden. Tehokkaan toiminnan varmistamiseksi keskeisten elinkeinoelämän toimijoiden tulee saada riittävät perusteet ja osallistua soveltuvin osin myös puolustukseen liittyvien tarpeiden suunnitteluun ja toteuttamiseen.

Infrastruktuurin kehittäminen edellyttää usein ennakointia ja merkittäviäkin invertointeja, joiden rahoitusta ja käytössä olevia rahoitusinstrumentteja tulee tarkastella suojaamistarpeiden ja vaatimusten yhteydessä.

NATO-resilienssivaatimukset

Selonteossa todetaan, että Nato-jäsenyys on muuttanut Suomen puolustusratkaisun perusteellisesti. Suomi osallistuu täysimääräisesti Naton yhteiseen puolustukseen ilman kansallisia rajoitteita (kohta 4.2). Suomen puolustus kytketään osaksi Naton pelotetta, puolustussuunnittelua ja komentorakenteita. Suomen alueen puolustaminen on osa Naton alueellista puolustussuunnitelmaa, ja tämä edellyttää rakenteellista yhteensopivuutta, johtamisjärjestelmien uudistamista sekä joukkojen sijoittamisen ja harjoitusten mahdollistamista.

Selonteossa esitetään, että Suomen tulee toteuttaa Naton alueelliset puolustussuunnitelmat, mukaan lukien komentorakenteiden kehittäminen ja infrastruktuurin vahvistaminen liittolaisten läsnäoloa varten (kohdat 4.2.4 ja 4.7.4). Puolustusvoimat osallistuu Naton puolustussuunnitteluprosessiin (NDPP), ja kansallinen järjestelmä sovitetaan sen ohjaamiin suorituskykytavoitteisiin. Lisäksi painotetaan sotilaallisen liikkuvuuden, logistisen tuen ja isäntämaatukijärjestelyjen kehittämistä osana Naton kollektiivista puolustusta.

Lainsäädännön kehittäminen on välttämätöntä, jotta Puolustusvoimien henkilöstön ja asevelvollisten osallistuminen Naton tehtäviin voidaan toteuttaa oikeudellisesti selkeästi (kohta 4.8.3). Lisäksi tarvitaan sääntelyä, joka määrittää Naton joukkojen aseman, toimivaltuudet ja vastuut Suomessa. Tietoturva- ja tiedonhallintastandardien yhteensovittaminen Naton vaatimusten kanssa edellyttää myös kansallisten tietojärjestelmien sääntelyä ja viranomaisvastuiden tarkentamista (kohta 4.8.10)

<u>Kokonaisuuteen liittyen haluamme kiinnittää huomiota seuraaviin asioihin</u>

NATO-jäsenyyden myötä Suomen puolustusjärjestelmään tulee uusia elementtejä, joita on käsitelty selonteossa keskeisiltä osin. Suomessa varautumista on kehitetty pitkäjänteisesti kansallisista lähtökohdista. Jäsenyyden myötä NATOn vaatimukset myös siviilivarautumiselle vaativat huomioimista ja toimenpiteitä.

Siviilivarautuminen synnyttää sietokykyä, joka osaltaan mahdollistaa NATOn pelotteen ja puolustuksen.

NATOn resilienssin perusvaatimusten (baseline requirements) huomioiminen edellyttää merkittävää siiliyhteiskunnan ja elinkeinoelämän toimia ja mukanaoloa. Tämä

näkökulma tulee huomioida vahvemmin selonteossa sekä kehitettäessä puolustusvalmiutta ja -järjestelmää.

Allekirjoitus

Jaakko Wallenius
turvallisuusjohtaja
Elisa Oyj