

Asia: VN/13450/2020

Luonnos logistiikan digitalisaatiostrategiaksi

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

1 Johdanto

Liikenne- ja viestintäministeriö on pyytänyt 17.6.2020 päivätyllä asiakirjallaan puolustusministeriöltä lausuntoa logistiikan digitalisaatiostrategian luonnoksesta. Puolustusministeriön lausunto perustuu Pääesikunnalta saatuun lausuntoon.

2 Yleiset havainnot

Puolustusministeriön näkemyksen mukaan strategia kuvaa kattavasti kuljetuslogistiikan digitalisoinnin strategian ja keinot tavoitteisiin pääsemiseksi normaaliolojen näkökulmasta. Logistiikan digitalisaatiostrategiasta puuttuu kuitenkin laaja-alainen kokonaislogistiikan tarkastelu siinä laajuudessa kuin logistiikan laaja merkitys strategian alussa määritellään. Strategiassa ei ole myöskään huomioitu normaaliolojen häiriötilanteita, poikkeusoloja ja mahdollista aseellista hyökkäystä Suomeen sekä niihin varautumista. Jotta logistiikan digitalisaatiostrategia olisi kokonaisvaltainen, tulisi edellä mainitut asiat huomioida tai rajata strategia vain kuljetuslogistiikan digitalisaatiostrategiaksi ja nimetä se esimerkiksi Kuljetuslogistiikan

digitalisaatiostrategiaksi.

Perusajatus eri toimijoiden tietojen keräämisestä ja hyödyntämisestä toiminnan optimointiin kokonaisuutena on erittäin kannatettava. Kuljetustietojen tilastointi ja niistä tehtävät analyysit nähdään tärkeänä kansallisena keinona arvioida kansallista tilaa, esimerkiksi huoltovarmuuden näkökulmaa, häiriötilanteissa. Tietojen kerääminen ja hyödyntäminen korostuvat myös poikkeusoloissa, jolloin Puolustusvoimien näkökulmasta yhteiskunnan resurssien käyttöä on kyettävä optimoimaan yli yksittäisten toimijoiden tai alueiden. Tietojen keräämisestä ja hyödyntämisestä syntyvien palveluiden tietoa, taltiointia ja jakoa on kyettävä rajoittamaan sensitiivisten kuljetusten ja asiakastietojen osalta. Tavoite standardoitujen rajapintojen rakentamisesta edellyttää myös tietomallien yhdentämistä, joka vaatii säädöspohjaa tuekseen.

Viittaukset digitalisoinnin tuomiin ympäristöpäästöjen pienentämiseen ovat kannatettavia. Merkittävä osa Puolustusvoimien sodan ajan käyttöön tarvittavista ajoneuvoista on siviilistä käyttöön otettavia ottoajoneuvoja. Laajamittainen ajoneuvojen sähköistäminen tai korvaavien energiaratkaisuiden käyttöönotto pienentävät Puolustusvoimien mahdollisuutta ottoajoneuvojen käyttöön. Tämä voi pitkällä aikavälillä lisätä Puolustusvoimien rahoitustarvetta sotilaskäyttöön tarkoitettujen ajoneuvojen hankkimiseen.

Strategiassa kuvattu ympäristövaikutusten arviointi tulee tehdä laajempaan kokonaisuutena kattaen koko logistiikkatoimialan sekä tuotantotoiminnan. Vaikka toisaalta kuljettaminen aiheuttaa merkittävän ympäristökuormituksen, kokonaislogistiikan tarkastelulla voidaan ohjata markkinoita. Esimerkkinä tuotteisiin merkittävä ”hiilijalanjälkitieto” voi tulevaisuudessa ohjata tuotantotoiminnan siirtymistä lähemmäs markkina-alueita. Lisäksi asiakastilaukseen (ml. ennusteeseen) perustuvan tuotannon ja ilman välivarastointia tapahtuvan toimituksen

ympäristökuormitus on monessa tapauksessa alhaisin.

Kuljetuslogistiikan digitalisoinnin kehittäminen tulee liittää kiinteäksi osaksi väylästöjen kehittämistä ja rakentaminen on tehtävä rinnakkain olevin tavoittein.

Rajamuodollisuuksien sujuvoittaminen on kannatettavaa ja todettakoon, että Puolustusvoimat toimii aktiivisesti EU:n MILMOB- tavoitteiden edistämiseksi.

3 Havainnot kyber- ja tietoturvallisuudesta

Yhteiskunnan turvallisuusstrategian mukaisesti yhtenä elintärkeänä toimintona määritellään talous, infrastruktuuri ja huoltovarmuus. Tämä liittyy olennaisesti kansalliseen ja kansainväliseen logistiikkaan. Logistiikka ja kuljetukset ovat elinehto kaikissa tilanteissa, joten teknisestä kehityksestä riippumatta tulee kyetä toimimaan ja varmistamaan, että vihamielinen taho ei pysty lamauttamaan yhteiskunnan toimintaa vaikuttamalla logistiikka- ja kuljetusjärjestelmiin tietoverkoissa.

Ajoneuvotietojen ja liikenteen siirtyminen internet-pohjaiseksi edellyttää järjestelmän tietoturvallisuuden varmistamista. Logistiikan digitalisaatiostrategialuonnos ei käsittele riittävästi logistiikan digitalisoitumiseen liittyvää kyber- ja tietoturva-uhkaa. Samasta syystä strategiasta puuttuvat johdetut tavoitteet ja toimenpiteet, joilla noihin uhkiin vastattaisiin ja siten tuettaisiin digitalisoidun logistiikan toimintavarmuutta niin normaalioloissa, niiden häiriötiloissa kuin poikkeusoloissakin. Puolustusministeriö esittää edellä mainittuja seikkoja tarkennettavaksi.

On nähtävissä, että logistiikan digitalisaatio johtaa vastaavaan kehitykseen kuin globalisaatio logistiikan toimitusketjun osalta. Tällöin myös uhkat digitalisaatiolla mahdollistettavalle logistiikalle muodostuvat sekä globaaleiksi että ympärivuorokautisiksi. Onnistunut logistiikan suojaaminen kybertoimintaympäristön

tavanomaisia sekä valtiollisten toimijoiden muodostamia uhkia vastaan edellyttää uhkien kokonaisvaltaista huomioimista. Samoin kyberuhkilta suojautuminen jo normaalioloissa tulisi kuvata orgaaniseksi logistiikkajärjestelmän osaksi, digitalisoituneen logistiikan peruspilariksi.

Vaikuttaminen logistiikkajärjestelmään valmistellaan todennäköisesti jo normaalioloissa osana muuhun kriittiseen infrastruktuuriin vaikuttamisen valmistelua. Viimeistään digitalisaation myötä myös logistiikka verkottuu ja tulee entistä riippuvaisemmaksi muista toimijoista ja tiedon tuottajista, keskinäisriippuvuuden jatkuessa vielä poikkeusoloissakin. Siksi on erittäin vaikeaa jakaa logistiikan järjestelmiä koreihin, joissa yhdessä olisivat kansallisen turvallisuuden ja maanpuolustuksen kannalta tärkeät järjestelmät ja toisessa muut järjestelmät. Tästä syystä kyber- ja tietoturvallisuuden korkean ambitiotason vaatimukset tuleekin ulottaa tavoitteenomaisesti kaikkiin digitalisoituviin logistiikan järjestelmiin. Lisäksi logistiikan kyber- ja tietoturvallisuudessa tulee myös huomioida käytettävien järjestelmien koko elinkaaren aikainen sietoisuus kyberuhkille sekä kyky palautua poikkeamista (resilienssi). Puolustusministeriö esittää, että nämä kokonaisuudet kuvataan osaksi strategian tavoitetilaa.

Strategiassa kuljetuslogistiikka määritellään sen laajan merkityksen mukaan. Tämä korostaa entisestään kyberympäristön huomioimisen tarpeellisuutta. Käsittelyn puuttuminen johtaa siihen, että strategia luo liian optimistisen kuvan kuljetuslogistiikan digitalisaation vaikutuksista. Uhkanäkökulman puuttuminen vaikuttaa myös strategian jalkauttamisen onnistumisen edellyttämään luottamuksen rakentumiseen. Luottamus määritellään yhdeksi keskeiseksi tekijäksi koko verkottuneen ja hajautetun digitalisoidun logistiikan onnistumisessa.

Kyberturvallisuutta käsitellään omassa valtioneuvoston hyväksymässä strategiassa. Logistiikan digitalisaation tieto- ja kyberturvallisuuden varmistamista ei tule kuitenkaan

jättää yksin muissa strategioissa ja niiden toimeenpano-ohjelmissa määrittelyn varaan, sillä niissä ei pääsääntöisesti päästä logistiikan näkökulmasta riittävään tarkkuuteen. Logistiikan tulisi itse huolehtia digitalisoituvan toimintansa turvaamisesta ja jatkuvuuden varmistamisesta. Tästä näkökulmasta kyber- ja tietoturvallisuuden sivuuttaminen tai jättäminen muiden huolehdittavaksi antaa väärän signaalin logistiikan toimijoille, joilla kuitenkin on lopulta kannettavanaan kokonaisvastuu ja liiketoimintariski. Logistiikan toimivuus on keskeinen osa myös kansallista turvallisuutta, kyberturvallisuuden ollessa keskeinen osa logistiikan toimivuutta.

4 Yhteenveto

Puolustusministeriön näkökulmasta päähavainnot logistiikan digitalisaatiostrategialuonnoksesta ovat:

1 sisältö keskittyy kuljetuslogistiikan digitalisaatiostrategiaan, ei kokonaislogistiikkaan

2 poikkeusoloja ja mahdollista aseellista hyökkäystä sekä niiden vaikutusta tulisi käsitellä

3 kyber- ja tietoturvallisuuden käsittelyä tulisi laajentaa ja syventää

Pakanen Aulikki
Puolustusministeriö