Eduskunta
Puolustusvaliokunta
puv@eduskunta.fi

Asia: VNS 8/2021 vp; Valtioneuvoston puolustusselonteko

Sisäministeriö kiittää puolustusvaliokuntaa kutsusta kuultavaksi ja esittää lausuntonaan seuraavaa:

Valtioneuvoston puolustusselonteko noudattaa aiempien selontekojen, erityisesti ulko- ja turvallisuuspoliittisen selonteon kirjauksia, tehden täsmentäviä ja maanpuolustuksen kannalta keskeisiä nostoja.

Selonteon toimintaympäristöosuudessa kuvataan, kuinka Suomen ja Euroopan lähialueiden turvallisuustilanne on epävakaa ja vaikeasti ennakoitava. Myös kansalliseen turvallisuuteen liittyvät uhat, jotka monelta osin koskevat sisäministeriön hallinnonalaa, ovat keskeisesti esillä.

Toimintaympäristön muuttuessa ja sisäisen ja ulkoisen turvallisuuden kytkeytyessä toisiinsa, kasvaa myös tarve valtioneuvoston yhteistyölle ja yhteistoiminnalle.

Nostan puheenvuorossani esiin sisäministeriön toimialan kannalta keskeiset kokonaisuudet. Näitä ovat laaja-alaiseen vaikuttamiseen (hybridiuhkiin) varautuminen, yhteiskunnan kriisinkestävyyden ja kyberturvallisuuden parantaminen ja tiedustelutoimialan kehittäminen.

Hybridiuhkiin varautuminen

Suomeen kohdistuva valtiollinen hybridivaikuttaminen on lisääntynyt ja monimuotoistunut ja sen keinovalikoima on laaja. Puolustusselonteossa tätä uhkakokonaisuutta lähestytään laaja-alaisena vaikuttamisena, joka voi muiden keinojen ohella sisältää sotilaallista painostamista, jopa sotilaallisen voiman käyttöä.

Sotilaallisen voimankäytön uhkalla ja siinä tapahtuvilla muutoksilla on vaikutus myös sisäiseen turvallisuuteen. Sotilaallisten uhkien ennakkovaroitusajan lyheneminen edellyttää sisäisen turvallisuuden viranomaisten päätöksentekokykyyn ja valmiuteen vastaavia vaatimuksia kuin sotilaalliselle puolustukselle.

Puolustusselontekoon on kirjattu, että puolustusvoimat varautuu laaja-alaiseen vaikuttamiseen yhdessä muiden toimijoiden kanssa. Laaja-alaisen vaikuttamisen torjumisessa keskeistä on poikkihallinnollinen toimintatapa. Vaikuttamiseen tulee varautua johdonmukaisesti ja riskiperusteisesti, laatimalla yhteisiä valmiussuunnitelmia ja parantamalla turvallisuusviranomaisten toimivaltuuksia. Lainsäädäntötyössä huomiota tulee kiinnittää valtion toimintakyvyn turvaamiseen ns. harmaan alueen tilanteissa ja pohtia keinoja, joilla esimerkiksi valmiuslain keinovalikoima olisi mahdollista ottaa käyttöön sekä poikkeusoloiksi katsottavissa uhkatilanteissa että sellaisissa yhteiskunnan toimintakykyyn

vaikuttavissa tilanteissa, joissa poikkeusolot eivät vielä ole käsillä, mutta joissa normaalilainsäädännön viranomaisille antamat toimivaltuudet eivät tilanteen asianmukaiseksi hoitamiseksi ole riittäviä. Myös kriisitilanteiden strategisen johtamisen kokonaisuuteen ja valtionhallinnon joustavaan resurssien käyttöön on tärkeää kiinnittää huomiota.

Hybridivaikuttaminen voi tapahtua samanaikaisesti usealla eri politiikkalohkolla. On tärkeää, että jatkamme kansallista varautumistyötä hybridiuhkien torjumiseksi sekä tuemme aktiivisesti EU:n yhteisten toimien kehittämistä.

Selonteossa nostetaan esiin, kuinka EU:n turvallisuus- ja puolustuspoliittisen yhteistyön suuntaa ja tavoitteita määritetään parhaillaan strategisen arvioinnin ja ohjauksen prosessilla, niin kutsutulla strategisella kompassilla. Sisäministeriö osallistuu tähän työhön erityisesti hybridiuhkien torjumisen ja kriisinkestävyyden kehittämisen näkökulmista. Aivan viime aikaiset tapahtumat EU:n ulkorajoilla korostavat tarvetta tiivistää edelleen turvallisuus- ja puolustuspolitiikan sekä oikeus- ja sisäasioiden yhteistyötä ja siviili-sotilasyhteistyötä.

Kriisinkestävyyden parantaminen

Kriisinkestävyyden parantaminen on puolustusselonteossa kytketty osaksi kansallisen puolustuskyvyn ylläpitämistä. Puolustusvoimien toiminnan todetaan olevan riippuvainen yhteiskunnan infrastruktuurista.

Kriisinkestävyyden parantaminen on tärkeä instrumentti nopeasti muuttuvassa toimintaympäristössä, jossa pyritään vahvistamaan toimintakykyä häiriötilanteissa varautumalla monitahoisiin yhteiskunnan toimintakykyyn ja turvallisuuteen vaikuttaviin uhkiin.

Kaikelta ei voi suojautua, mutta yhteiskunnan toimintakyvyn lamauttamisen voi tehdä merkittävästi vaikeammaksi kohtuullisilla panostuksilla ja sektorikohtaisella suunnittelulla. Parantamalla kriisinkestävyyttä, voidaan yhteiskunnan toimintakykyä suojata myös teknologisen kehityksen mukanaan tuomilta uhilta, olivatpa ne luonteeltaan fyysisiä tai kybermaailmasta tulevia.

Kansallisesti kriittiset järjestelmät ja palvelut eivät enää tänä päivänä rajaudu valtioiden rajojen sisäpuolelle. Keskinäisriippuvuudet sektoreiden välillä, jopa rajojen yli, muodostavat potentiaalisia haavoittuvuuksia, joiden tunnistaminen on sekä Euroopan unionissa että Natossa erityisen kiinnostuksen kohteena. Sisäministeriö on osallistunut tähän työhön aktiivisesti.

Tässä yhteydessä on myös hyvä todeta sisäisen turvallisuuden selonteon kirjaus, jossa todetaan tarve määrittää lähitulevaisuudessa kansallinen kriittinen infrastruktuuri ja selvittää sen suojaamiseen liittyvät lainsäädäntötarpeet. Suomelle on tärkeää lähestyä infrastruktuurisääntelyä yhdenmukaisin menettelyin EU-maiden kanssa, rajaten kuitenkin sen ulkopuolelle kansallisen turvallisuuden ja maanpuolustuksen kannalta keskeiset kokonaisuudet.

Kansallisen kyberturvallisuuden parantaminen

Suomen toimintaympäristö ja siihen kytkeytyvät uhat kehittyvät ja muuttuvat kiihtyvällä vauhdilla digitalisoituvan yhteiskuntamme luodessa samalla uusia haavoittuvuuksia. Selonteossa todetaan, että puolustuksen toimintakyky ja järjestelmät ovat yhä enemmän riippuvaisia digitalisaatiosta, informaatiosta ja avaruuteen sijoitetun infrastruktuurin hyödyntämisestä.

Valtiolliset ja ei-valtiolliset toimijat kehittävät kybersuorituskykyjä, joiden avulla ne voivat häiritä, vahingoittaa tai hyödyntää niin tietojärjestelmien kuin kriittisen infrastruktuurinkin haavoittuvuuksia tavoitteidensa saavuttamiseen. Kyberhyökkäykset ovat lisääntyneet yhteiskunnan eri sektoreilla ja hyökkäyksiä on suunnattu valtion ohella myös kuntatason toimijoita kohtaan.

Niin ikään verkkorikollisuus on kasvava uhka, ei vain yrityksille ja yksittäisille kansalaisille, vaan myös valtionhallinnolle ja julkisille palveluille. Tässä toimintaympäristön muutoksessa kyberuhkien merkitys kasvaa ja ne muodostavat jatkossa aiempaa suuremman uhan kansalliselle turvallisuudelle.

Puolustusselonteko nostaa esiin kybersuorituskyvykkyyksien kehittämistarpeen. Kirjaukset kyberuhkien estämisestä ja torjumisesta on laadittu tiiviissä yhteistyössä. Selonteko korostaa tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä.

On tarpeen arvioida viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa, ottaen huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuva kehittyminen.

Tiedustelutoimialan kehittäminen

Turvallisuusympäristön muutos ennakoimattomampaan suuntaan korostaa tiedustelulla hankitun analysoidun tiedon merkitystä päätöksenteossa. Puolustusselonteko toteaa, että tiedonhankinnan turvaamiseksi tiedustelu- ja valvontajärjestelmää kehitetään ja analyysi- ja tiedonhallintakykyjä vahvistetaan. Sotilastiedustelu toimii yhteistyössä sisäministeriön ohjaaman siviilitiedustelun kanssa valtiollisten uhkien tiedustelussa. Yhteistyötä sekä ohjauksessa että tiedusteluviranomaisten kesken tulee tiivistää entisestään. Tähän liittyen valtioneuvosto antaa eduskunnalle selonteon tiedustelulakeihin liittyen tämän vuoden loppuun mennessä.