Sisäministeriö
Inrikesministeriet

Lausunto

26.4.2022

Eduskunta
Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

Sisäministeriön lausunto liikenne- ja viestintävaliokunnalle valtioneuvoston selvitys (E 45/2022 vp): Komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi unionin turvallisten yhteyksien ohjelman perustamiseksi vuosiksi 2023-2027

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt sisäministeriöltä lausuntoa valtioneuvoston selvityksestä (E 45/2022 vp) Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi unionin turvallisten yhteyksien ohjelman perustamiseksi vuosiksi 2023-2027. Sisäministeriö on osallistunut selvityksen laatimiseen ja katsoo selvityksen tuovan esiin komission ehdotuksen keskeiset asiasisällöt.

Viranomaisten käytössä oleva luotettava, häiriönsietokykyinen ja tietoturvallinen satelliittiviestintäjärjestelmä tukee myös sisäisen turvallisuuden viranomaisten kuten rajavartiolaitoksen, pelastustoimen ja poliisin toimintaa. Turvalliset ja häiriöiltä suojatut satelliittiviestintäyhteydet varmistavat osaltaan, että viranomaisille on käytössään tarvittavat johtamisyhteydet niin poikkeusoloissa kuin luonnonkatastrofitilanteissa. Ilmastonmuutoksen myötä lisääntyvät vahinkoja aiheuttavat sään ääri-ilmiöt, jotka uhkaavat maanpäällisten viestiverkkojen häiriötöntä toimintaa ja häiritsevät näitä viestiverkkoja hyödyntävien viranomaisten viestintää. Satelliittiviestintäjärjestelmät sekä varmentavat viranomaisten käytössä olevia johtamis- ja viestiyhteyksiä että mahdollistavat viestiyhteyksien saamisen harvaanasutuille alueille, joissa maanpäällinen viestintäinfrastruktuuri puuttuu tai on vaurioitunut. Lisäksi turvallisten yhteyksien ohjelman puitteissa rakennettavat satelliittiviestintäjärjestelmät ja viranomaispalvelut mahdollistavat aiempaa paremman kattavuuden ja viestintäyhteydet myös laajemmin arktisilla alueilla.

Suomen ulko- ja turvallisuuspoliittisen toimintaympäristön vakaus on Ukrainan konfliktin myötä heikentynyt. Konflikti on myös konkretisoinut moderniin sodankäyntiin liittyvän hybridivaikuttamisen eri ilmiöt. Ukrainan viestintäverkot ovat olleet useaan otteeseen kyberiskujen kohteena, joilla on pyritty lamauttamaan viestiyhteyksiä. Hybridivaikuttaminen voi käynnistyä ennen sotilaallista hyökkäystä, jolloin poliisi-, raja- ja pelastusviranomaiset ovat keskeisessä roolissa vastaamaan vaikuttamisyrityksiin. Tässä tilanteessa tehokkaan ja oikea-aikaisen viranomaistoiminnan edellytyksenä ovat osaltaan toimivat, häiriösietokykyiset ja

varmennetut viestintäjärjestelmät, jotka sietävät myös kyberhyökkäyksiä ja ovat yhteiskäyttöisiä Euroopan laajuisesti viranomaisten, hallintojen ja kriittisten infrastruktuurioperoijien kesken. Turvalliset satelliittiviestintäjärjestelmät sekä suojaavat viranomaisviestinnän luottamuksellisuutta että luovat tarvittavaa, maanpäällisiä viestintäverkkoyhteyksiä täydentävää redundanssia myös hybridivaikuttamista vastaan.

Yhteinen, eurooppalainen viranomaisten käytössä oleva satelliittiviestintäjärjestelmä ja sen mahdollistamat viranomaispalvelut luovat tarvittavia edellytyksiä kriisitilanteissa vastaan otettavan tuen ja avun tehokkaalle koordinoinnille ja hyödyntämiselle. Yhteisen järjestelmän käytöllä voidaan myös saavuttaa kustannusten hallinnan kannalta riittävän laaja käyttäjäkunta, jotta palveluiden ja päätelaitteiden kustannukset eivät muodosta estettä käytölle esimerkiksi Suomen viranomaisten näkökulmasta. Toimivien viranomaisviestiyhteyksien merkitys aikakriittisissä hätätilanteissa on keskeinen niin vastattaessa luonnon katastrofeihin kuin Suomeen kohdistuvaan kansallista turvallisuutta vaarantavaan vihamieliseen vaikuttamiseen. Satelliittiviestijärjestelmien viestiliikenteen sekä saatavuuden että luottamuksellisuuden turvaamiseen tulee kiinnittää huomiota. Valmisteilla olevan komission ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi kriittisten toimijoiden häiriönsietokyvystä (nk. CER-direktiivi) tullessa voimaan, asetetaan todennäköisesti tämän kaltaisille monikansallisille satelliittiviestintäjärjestelmille erityisiä riskienhallintavaatimuksia, jotka osaltaan vahvistavat järjestelmien tietoturvallisuutta ja resilienssiä vaikuttamisyrityksiä vastaan.

Erityisasiantuntija Hannu Kotipelto