Sisäministeriö
Inrikesministeriet

Lausunto SM1829776

01.10.2018

Eduskunta
Hallintovaliokunta

O 106/2016 vp, EV 245/2014 vp, HaVM 35/2014 vp, HE 54/2013 vp

Sisäministeriön lausunto julkisen hallinnon turvallisuusverkkotoiminnan toimeenpanosta

Hallintovaliokunta on pyytänyt sisäministeriöltä kirjallista asiantuntijalausuntoa julkisen hallinnon turvallisuusverkkotoiminnan toimeenpanosta. Sisäministeriön hallinto- ja kehittämis-, poliisi-, pelastus- ja rajavartio-osastoja on kuultu lausunnon valmistelussa.

Turvallisuusverkon toimivuus

Sisäministeriön näkökulmasta turvallisuusverkko on toiminut lain tarkoituksen mukaisesti normaalioloissa ja niiden häiriötilanteissa (poikkeusolojen toimintaa ei ole ollut) varmistaen turvallisuusviranomaisten yhteistoiminnan edellyttämän viestinnän häiriöttömyyden ja jatkuvuuden.

Turvallisuusuhat TUVE-hankkeen alkuajoista ovat kasvaneet, monimutkaistuneet, hybridivaikuttaminen on jatkuvasti lisääntyvää esimerkiksi kyberhyökkäysten ja tiedon varastamisyritysten kautta. Turvallisuusverkkotoiminnan kannalta tämä aiheuttaa entistä enemmän haastetta turvallisuuteen ja varautumiseen liittyvien toimien jatkuvalle kehittämiselle. Turvallisuusverkon ei pitäisi olla koskaan valmis, vaan sen tulisi jatkuvasti kehittyä ja nykytoiminnan vaatimustenmukaisuutta analysoida sekä ympäröivän maailman haasteita että käyttäjien digitalisaation myötä kehittyviä toiminnallisia ja lakisääteisiä tarpeita vastaavaksi.

Vuorovaikutusta ja yhteistyötä tehdään sekä sisäisten että ulkopuolisten toimijoiden kanssa hyödyntäen näiden palveluita. Integroituminen ja yhteistyö ulkoisten sidosryhmien kanssa, turvallisuusverkon keskeisiä toimintaperusteita vaarantamatta, on edelleen ratkaisematta.

Hallintovaliokunnan mietinnössä (HaVM 35/2014 vp) mainitaan, että lain yksityiskohtaisissa perusteluissa korkean varautumisen tason tieto- ja viestintäteknisten palveluiden tietoturvan tulisi täyttää suojaustasojen IV - II tietoturvavaatimukset ja erityissuojattavalle tietoaineistolle säädetyt vaatimukset. Sisäministeriö korostaa erityisesti näiden palveluiden vaatimustenmukaisuuden tarkastelua ja toteuttamista edelletyille suojaustasoille.

Kirkkokatu 12, Helsinki
PL 26, 00023 Valtioneuvosto
Vaihde 0295 480 171 | kirjaamo@intermin.fi | www.intermin.fi

Taloudelliset vaikutukset ja käyttövelvoite

Turvallisuusverkon käyttäjämäärä ei ole edelleenkään lisääntynyt arvioidussa määrin; kustannukset kasaantuvat nykyisille käyttäjille, yhteistoiminta ei ole vaatimukset täyttävällä tavalla järjestettyä eikä palveluita saada kehitettyä nykyisten käyttäjien pienenevien kehysten johdosta. Suomen kyberturvallisuusstrategian toimeenpanon kannalta on myös tärkeää, että turvallisuusverkko ja sen palvelut otetaan käyttöön käyttövelvoitteen piirissä olevien toimintojen osalta.

TUVE-ohjauksessa on valtiovarainministeriön selvityksen (O 106/2016 vp) mukaan erityisesti kiinnitetty huomioita siihen, kuinka käytettävissä olevalla rahoituksella kyetään kehittämään ja ylläpitämään korkeaa varautumisen ja turvallisuuden tasoa tarvittaessa palvelujen hintoja tarkistamalla ja kehittämiskohteiden siirtämisellä tulevaisuuteen. Käyttäjien kannalta tämä näkyy suoraan turvallisuusverkon palvelujen kehittämiseen suunnattujen sekä käyttäjien omien tietojärjestelmien kehittämiseen ja tuotantoon siirtämiseen liittyvien resurssien vähyytenä, kun palvelutuotannon resurssit ovat sitoutuneena turvallisuusverkon keskeiseen perusajatukseen ja yhteiskuntammekin kannalta erittäin tärkeään korkean varautumisen ja turvallisuuden tason kehittämiseen ja ylläpitoon. Turvallisuusverkon tietoturvan parantamiseen liittyvät toimet aiheuttavat merkittäviä resurssivaikutuksia myös käyttäjille. VM toteaa selvityksensä lopuksi, että digitalisaatio, käyttäjien monipuolistuvat käyttötarpeet ja taloudellisten resurssien rajallisuus edellyttävät turvallisuusverkkotoiminnalta jatkuvaa kehittymistä sekä kykyä hyödyntää laajasti myös turvallisuusverkon ulkopulista ICT-palvelutarjontaa. Tätä kehittymistä ei saada edes alkuun, jos kehittämiskohteita siirretään jatkuvasti tulevaisuuteen.

Sisäministeriö korostaa varautumisen ja turvallisuuden lisäksi palvelujen kehittämisen tärkeyttä käyttäjien toiminnallisten tarpeiden turvaamiseksi sekä turvallisuusverkon käytön laajentamista käyttövelvoitteen mukaisesti. Turvallisuusverkko toimii, mutta sen toiminnan keskeisten perusteiden, korkean käytettävyyden, turvallisuuden sekä häiriötilanteisiin ja poikkeusoloihin varautumisen lisäksi tulisi verkon pystyä vastaamaan käyttäjien jokapäiväisen toiminnan kehittyviin tarpeisiin.

Turvallisuusverkon perusinfrastruktuuri palvelutuotantoineen sekä tähän liittyvä varautumisen ja turvallisuuden tason kehittäminen ja ylläpito tulisi saattaa vaatimuksien mukaiselle tasolle ensitilassa ja tähän suunnattava rahoitus tulisi olla keskitettyä budjettirahoitusta eikä asiakkailta perittäviä palvelumaksuja tulisi käyttää jatkuvasti tähän. Palvelumaksut tulisi kohdentaa turvallisuusverkon palveluiden kehittämiseen asiakkaiden toiminnallisia ja lakisääteisiä tarpeita vastaaviksi.

Vuosittaista taloudellista ohjausta tulisi sisäministeriön näkemyksen mukaan aikaistaa nykyisestä, koska sen hallinnonalan virastojen toiminnan kannalta seuraavan vuoden palvelumaksuista päätetään liian myöhään syksyllä. Virastot eivät ehdi ennakoida seuraavan vuoden kustannusvaikutuksia omissa budjeteissaan eivätkä niiden vaikutuksista toimintaansa kohdistuvia muutoksia, jos suunniteltuja turvallisuusverkon kehittämiskohteita päätetään siirtää tulevaisuuteen varautumisen ja turvallisuuden tason ylläpitämiseksi.

Sisäministeriön näkemyksen mukaan turvallisuusverkon käyttäjämäärä ei ole lisääntynyt arvioidussa aikataulussa, jolloin yksikkökustannukset eivät ole laskeneet eikä nykyisten käyttäjien pienenevien kehyksien vaikutuksia ole pystytty kattamaan tai tasapainottamaan. Sisäministeriön kehyksestä turvallisuusverkon palvelumaksuihin hallinnonalalle osoitettu lisärahoitus on pienentynyt 3,2 miljoonaa edellisestä vuodesta, mikä näkyy erityisesti poliisin maksettavana olevien kustannusten huomattavana nousuna.

Palvelutuotannon järjestäminen

Valtoriin yhdistetty TUVE ja TORI -toiminta tai näiden ohjaus ei ole asiakkaiden näkökulmasta näyttäytynyt yhtenäiseltä julkisen hallinnon ICT-kokonaisuudelta.

Sisäministeriö on aiemmissa lausunnoissaan valtiovarainministeriölle sekä TUVE-lain eduskuntakäsittelyn aikana tuonut esille, että sisäministeriö on pitänyt ensisijaisena ja edelleen pohdittavana ja analysoitavana vaihtoehtona TUVE -toiminnan tai sen nykyistä laajemman osan keskittämistä yhdelle toimijalle, Suomen Erillisverkot konsernille. ERVEn yhtiömuoto mahdollistaisi asiakaskunnan laajentamisen ja yhtenäisyyden myös kehitteillä olevan viranomaisten tulevan langattoman laajakaistaviestintäratkaisun (ns. viranomaisradioverkko VIRVE 2) kanssa, jonka asiakkaina tulevat olemaan valtiollisten toimijoiden lisäksi kuntatoimijat ja huoltovarmuuskriittiset toimijat.

Suomen Erillisverkot -konsernin toimintaa on määrätietoisesti kehitetty laajemmaksi turvallisuusalueen toimijaksi ja tätä kehitystä on mahdollista entisestään parantaa. Eri liiketoiminta-alueiden synergioita voidaan jo nyt hyödyntää merkittävästi. ERVEn toiminta kattaa lukuisia turvallisen tietoliikenteen ratkaisuja sekä infrastruktuuriratkaisuja konesali-, tietoliikenne- ja palvelinhotellipalveluille. Tällä organisaatiomallilla olisi kaikkein eniten synergiaetuja, mm. laaja turvallisuus- ja asiakkuusosaamisen varmistaminen, mukaan lukien kuntaintegraatio sekä nykyiset ja tulevat VIRVE -palvelut. Yhden toimijan malli selkiyttäisi myös TUVE -toiminnan hallintaa, valvontaa ja ohjausta sekä olisi synergiaedut huomioiden varautumisen, turvallisuuden ja mahdollisesti myös kustannushyötyjen, käytettävyyden ja käyttäjien näkökulmasta tarkoituksenmukaista.

TUVE-lain eduskuntakäsittelyn aikana ohjausrakenteen monimutkaisuuteen liittynyt huoli kohdistui erityisesti verkko - ja infrastruktuuripalvelujen tuottajaan, Suomen Erillisverkot Oy:öön, ja sen tytäryhtiöön Suomen Turvallisuusverkko Oy:öön. Käytännössä tämä on ollut asiakkaiden näkökulmasta ongelmattomin osuus turvallisuusverkkotoiminnan ohjausta, kun taas Valtoriin keskitetty tieto- ja viestintäteknisten ja integraatiopalvelujen ohjaus on osoittautunut haasteelliseksi osittain jo aikaisemminkin arvioituna TUVE-toiminnan ohjaukseen ja päätöksentekoon sekä Valtorin TUVE-toimintaan alimitoitettujen resurssien vuoksi.

Käyttäjien näkökulmasta turvallisuusverkon reilut 35 000 loppukäyttäjää eivät näy tämän laajan käyttäjäjoukon edellyttämällä painoarvolla Valtorin TUVE-palveluiden kehittämisessä ja resursoinnissa.

Turvallisuusverkon palveluiden käyttö ja tarkoituksenmukaisuus osana julkista hallintoa

Turvallisuusverkon palveluilla mahdollistetaan jokapäiväinen työskentely sekä operatiivisessa toiminnassa että hallinnollisissa tehtävissä. Hallinnollisten tehtävien jokapäiväistä hoitamista on enenevässä määrin alkanut haitata valtion muiden yhteisten palveluiden osalta niiden suunnittelemattomuus, kyvyttömyys ja joissain tapauksissa valittujen ratkaisujen myötä estetty toimimattomuus turvallisuusverkon palvelujen kanssa. Esimerkkinä valtioneuvoston kanslian toimeenpanema valtioneuvoston asianhallinnan digitalisointi (VAHVA-hanke), jossa tavoitteena on yhtenäistää valtioneuvoston toimintatapoja laajalti ja siirtyä uuden asianhallintaratkaisun myötä kohti digitaalista toimintakulttuuria. Hankittu asianhallintajärjestelmä, joka otetaan käyttöön kaikissa ministeriöissä vuosien 2018–2020 aikana, perustuu ratkaisuun, jolla estetään tämän järjestelmän käyttö turvallisuusverkosta turvallisuusverkon päätelaitteilla. Valtioneuvoston ohella monet virastot, jotka ovat TUVE-lain käyttövelvoitteen piirissä, käyttävät samoja valtion yhteisiä tietojärjestelmiä jokapäiväisessä hallinnollisessa työssä, mutta näiden yhteisten järjestelmien käytettävyys valtionhallinnon laajimmin käytetyn yhtenäisen tieto- ja viestintäteknisen palvelukokonaisuuden kautta on osoittautunut erittäin haastavaksi ja uusien valtioneuvosta yhtenäistävien kehityshankkeiden myötä tulevaisuudessa jopa mahdottomaksi.

TUVE-hankkeen yhtenä peruslähtökohtana oli yhtenäistäminen ja poistaa turvallisuuden ja varautumisen vaatimukset täyttävien erillisratkaisujen rakentaminen ja ylläpitäminen yksittäisiltä viranomaisilta. Valtion yhtenäisten tietoturvaltaan perustasoisienkin ratkaisujen suunnittelussa tulisi huomioida turvallisuusverkon käyttövelvoitteeseen kuuluvat käyttäjäryhmät sekä TUVE-toimintaympäristö, jotta erillisratkaisuja jokapäiväiseen hallinnolliseen työhön ei tarvitse erikseen rakentaa tai heikentää näiltä käyttäjiltä työn tekemisen mahdollisuuksia.

Turvallisuusverkko ja sen palvelut laitteineen on tarkoitettu ja käyttöön on TUVE-lain 3 §:n mukaan velvoitettukin turvallisuusviranomaisten lisäksi valtioneuvostosta annetussa laissa (175/2013) tarkoitetut ministeriöt niiden hoitaessa korkean varautumisen tai turvallisuuden vaatimukset täyttävää yhteistoimintaa ja viestintää. Sisäministeriön näkemyksen mukaan TUVE-lain peruslähtökohdat ja tarkoitus ovat edelleen ajankohtaisia ja yhteiskuntamme kannalta niin merkityksellisiä, että niitä ei pidä ilman selkeitä syitä sivuuttaa.

Poliisitoimi

Poliisitoimen osalta sisäministeriö korostaa poliisin ICT-ympäristön täyttä sidonnaisuutta turvallisuusverkkoon, turvallisuusverkon palvelujen toimivuuteen ja luotettavuuteen sekä näiden palvelujen soveltuvuuteen poliisin toiminnallisiin tarpeisiin. Poliisi tehostaa työtään uusilla tietojärjestelmäpalveluilla sekä hyödyntää laajasti digitaalisessa muodossa olevaa tietoa turvallisuuden ylläpitämiseksi päivittäisen työn lisäksi erityistehtävissä. Yhteistyötä tehdään laajasti myös turvallisuusverkon ulkopuolisten toimijoiden kanssa, jolloin integraatio näiden toimijoiden verkkoihin sekä yhteisten palveluiden käyttö asettavat erityisiä vaatimuksia sekä turvallisuusverkkotoiminnan turvaamiseksi että näiden ulkoisten palveluiden käytettävyyden varmistamiseksi.

Turvallisuusverkkoon liittyvien kustannusten osalta on poliisin maksuosuus kasvanut sekä toiminnallisista tehostamistarpeista lisääntyneen ICT-ympäristön käytön hyödyntämisen että sisäministeriön kehyksistä turvallisuusverkon palvelumaksuihin osoitetun lisärahoituksen vähentymisen seurauksena. Palvelumaksuja tasapainottavien tekijöiden jäätyä samassa tahdissa puutteellisiksi on poliisille aiheutunut merkittäviä kustannushaasteita.

Rajavartiotoimi

Rajavartiolaitos on yksi turvallisuusverkkolain käyttövelvoitteen piiriin kuuluva palveluiden käyttäjä, ja Rajavartiolaitoksen tehtävien suorittaminen on voimakkaasti riippuvaista turvallisuusverkossa tarjottavista palveluista. Rajavartiolaitoksen tehtävien kannalta tarkasteltuna käyttövelvoitteessa korostuu rajaturvallisuuteen, merellisiin turvallisuustehtäviin, sotilaalliseen maanpuolustukseen, yleiseen järjestykseen ja turvallisuuteen sekä maahanmuuttoon liittyvä viranomaisten sisäinen, välinen ja ulkoinen yhteistoiminta, jossa noudatetaan korkean varautumisen tai turvallisuuden vaatimuksia. Käyttövelvoitteen osalta tulisi huolehtia siitä, että käyttövelvoitteen piiriin kuuluvat loput viranomaistahot, erityisesti turvallisuusviranomaiset (Tulli), saatetaan myös tosiasiallisesti ja täysimääräisesti turvallisuusverkon käytön ja palveluiden piiriin. Käyttövelvoitteiden noudattaminen poistaa monia ajankohtaisia haasteita, niin verkon tietoturvallisuuden, integraatioratkaisujen kuin kustannuspaineidenkin osalta.

Rajavartiotoimen näkökulmasta suurimmat turvallisuusverkon palveluihin liittyvät haasteet liittyvät tieto- ja viestintäteknisiin palveluihin sekä integraatiopalveluihin. Tieto- ja viestintäteknisissä palveluissa tämä näkyy palveluiden hitautena, erityisesti toimialasidonnaisiin järjestelmiin liittyen, ja saatujen tietojen mukaan taustalla on Valtorin TUVE-yksikön jatkuva resurssipula. Valtorin TUVE-yksikön tuottama Integraatiopalvelu on toteutunut korkeintaan välttävästi, ellei jopa huonosti. Tämä aiheuttaa tarpeettomia riskejä turvallisuusverkkotoiminnalle sekä vaikeuttaa hallinnollisten tehtävien jokapäiväistä hoitamista. Valtion muiden yhteisten palveluiden osalta ei huomioida riittävässä määrin, että puolet valtionhallinnon käyttäjistä käyttää näitä yhteisiä palveluita turvallisuusverkosta, turvallisuusverkon työasemilla. Käytettävyyden ja kustannustehokkuuden ohella palveluiden turvalliseen käyttöön ei kiinnitetä tarvittavaa huomiota.

Turvallisuusverkko toimii, mutta sen olemassa olon ja toiminnan keskeisten perusteiden, eli korkean varautumisen ja turvallisuuden taso ei Rajavartiolaitoksen näkemyksen mukaan vastaa TUVE -laissa edellytettyjä vaatimuksia. Turvallisuusverkko ja sen palvelut tulisi saattaa säädösten edellyttämälle tasolle; palvelutuottajien tulisi taata tietojärjestelmien ja palveluiden osalta niille TUVE -lain 7 ja 9 §:ssä säädetty velvoite turvallisuus- ja jatkuvuusvaatimusten toteutumisesta.

Rajavartiolaitos esittää vielä lisähuomiona, että TUVE-lain edellyttämä varautumis- ja valmiussuunnitteluvelvoite koskee vain verkko- ja infrastruktuuripalvelujen tuottajana toimivaa Suomen Turvallisuusverkko Oy:tä. Tämä sama lakipohjainen velvoite tulisi pikimmiten säätää koskemaan

myös tieto- ja viestintäteknisten palvelujen sekä Integraatiopalvelujen tuottajaa.

Rajavartiolaitos tukee sisäministeriön aiempaa esitystä siitä, että ensisijaisena ja edelleen pohdittavana vaihtoehtona tulisi olla TUVE -toiminnan keskittäminen yhdelle toimijalle, Suomen Erillisverkot konsernille.

Pelastustoimi

Pelastustoimi on kunnallisena toimijana turvallisuusverkon käyttövelvoitteen piirissä ja siten velvollinen noudattamaan valtiohallinnolle määrättyä tietoturvallisuusasetusta. Asetuksen ja turvallisuusverkon turvallisuusmääräysten vaatimustenmukaisuuden toteuttaminen ja noudattaminen luo kunnallisille toimijoille lisäkustannuksia. Sisäministeriön pelastusosaston näkemyksen mukaan näiden lisäkustannusten kattaminen tulisi tehdä keskitettynä valtion rahoituksena, jolloin taataan tasapuolinen ja ensisijaisuuteen perustuva kestävä toimintamalli. Tällä edesautetaan turvallisuusverkon turvallista, tehokasta ja laaja-alaista hyödyntämistä.

Lainsäädäntöhankkeet pelastustoimen uudistuksesta samoin kuin maakunta-uudistuksesta ovat valmistelu- ja päätösvaiheessa. Tällä on laaja merkitys turvallisuusverkkotoimintaan pelastustoimessa.

Lopuksi

Sisäministeriö ja sen hallinnonala käyttävät laajasti turvallisuusverkkoa ja sen palveluita jokapäiväisessä toiminnassaan. Turvallisuusverkko ja sen tieto- ja viestintäteknisten palveluiden toiminta poikkeuksellisen korkeine käytettävyysvaatimuksineen vaikuttavat merkittävästi Poliisin, Rajavartiolaitoksen ja Hätäkeskustoiminnan sekä tulevaisuudessa myös pelastustoimen lakisääteisten tehtävien hoitamiseen. Turvallisuusverkon korkean varautumisen palvelut eri turvallisuuden tasoilla ovat näiden viranomaisten ydintoimintojen perustana.

Turvallisuusverkon varautumis-, tietoturva-, integraatio- ja käytettävyysratkaisujen tulee olla vaatimustenmukaisia, mutta ne tulee suunnitella ja toteuttaa käyttäjäorganisaatioiden lakisääteistä toimintaa tukeviksi ja tehostaviksi sekä niiden tulee mahdollistaa viranomaisten sisäisen toiminnan lisäksi yhteistoiminta muiden toimijoiden kanssa.

Sisäministeriö korostaa vielä lopuksi hallinnonalansa toimijoiden toimintaympäristöä maalla, merellä ja ilmassa, yhteistyössä kansallisten, EU:n ja muiden kansainvälisten toimijoiden kanssa; toimintaympäristöä, jossa turvallisuusverkon tietoliikenneratkaisujen ja päätelaitteiden luotettavuus ja käytettävyys on jatkuvan ja tehokkaan toiminnan perusta.

Lisätietoja

Lisätietoja sisäministeriön lausunnosta antaa tietohallintojohtaja Tapio Aaltonen.