VNS 9/2024 vp Lausunto

Puolustusvaliokunta

2025-04-11

WITH secure | Consulting

Lausunnon antaja

Päivämäärä	Tekijä	Muutos	Versio
2025-04-11	Antti Laatikainen, Johtava tietoturvakonsultti	Lopullinen versio	1.0

Dokumentin jakelu

Päivämäärä	Vastaanottaja	Organisaatio
2025-04-11	Puolustusvaliokunta	Eduskunta

Toimeksianto

Asia: VNS 9/2024 vp, Puolustusvaliokunnan lausuntopyyntö ulko- ja turvallisuuspoliittiseen selontekoon.

WithSecure perustaa seuraavan lausuntonsa omaan kokemukseensa, teollisuudenalan parhaisiin käytänteisiin, sekä puolustusvaliokunnan esitykseen VNS 9/2024 vp joka toimitettiin WithSecurelle pohjamateriaaliksi.

Lähtökohta lausunnolle

Maailman ja Suomen turvallisuustilanne on viime vuosien aikana muuttunut merkittävästi. Suomeen kohdistuva uhka on todellisempi kuin pitkiin aikoihin lähihistoriassamme. Tämä nostaa varautumisen ja valmistautumisen merkitystä kaikilla yhteiskunnan osa-alueilla, niin yhteiskunnallisesti merkittävissä teollisuuden toimijoissa kuin puolustusvoimissakin.

Kybersietoisuuden rooli digitalisoituvassa yhteiskunnassa on monipuolinen suojaaja, mahdollistaja ja usein kaiken muun toiminnan perusedellytys. Kyberturvallisuus on kokonaispuolustuksen roolina kaiken aikaa vastapuolen, sekä rikollisten että kansallisten toimijoiden, kanssa tekemisissä.

Suomen kriittistä infrastruktuuria ja puolustusvoimien tietoteknisiä kyvykkyyksiä tutkitaan ja koetellaan jatkuvasti. Kansainvälinen rikollisuus, verkkorikollisuus sekä sotilas- ja muu tiedustelu sekoittuvat tietoverkoissa, joten kyberturvallisuus on keskeinen osa kansallista maanpuolustusta.

Kyberturvallisuus pohjaa joka uhkatoimijasta, uhkakuvasta tai hyökkäystavasta huolimatta tietotekniikan perustoimintoihin ja turvalliseen järjestelmäsuunnitteluun. Kyberturvallisuutta voidaan järjestelmätasolla rakentaa vain tiettyjen, hyvin tiedossa olevien perusedellytysten kautta.

Ulko- ja turvallisuuspoliittinen selonteko kuvaa kattavasti ja monipuolisesti muuttunutta maailmankuvaa, sekä uusien teknologioiden huomioimista. WithSecure tunnistaa kyberturvallisuuden olevan huomioituna hyvin ja kattavasti toimintaa tukevana elementtinä muissa puolustuksen ja kokonaisturvallisuuden osa-alueissa, sekä omana puolustuksen toimialanaan.

Kyberulottuvuutta tulisi kuitenkin korostaa tietyissä selonteon osissa, sekä tuoda esiin kyberturvallisuuteen liittyvien perustoiminnallisuuksien merkitystä. Suomessa on vahvaa osaamista ja teollisuutta kyberturvallisuuden suunnitteluun, toteuttamiseen ja ylläpitämiseen.

Lausunto

2.4 Euroopan unioni

WithSecure näkee Euroopan unionin merkittävänä toimijana yhteiskunnallisen infrastruktuurin, teollisuuden ja tutkimuksen kyberturvallisuuden edistämisessä. Voimaan saatettu ja suunnitteilla oleva lainsäädäntö ja regulaatio, joka nostaa kyberturvallisuuden perustasoa, tukee sekä yhteiskunnan vakautta poikkeusoloissa että kansallisten puolustuskykyjen vahvistamista kriittisen infrastruktuurin kybersietoisuuden parantamisessa.

Suomen tulee aktiivisesti tukea ja edistää hyvän ja käyttökelpoisen regulaation kehittämistä sekä EU-tasolla että kansallisesti.

Monet nykyiset murrokselliset teknologiat, kuten tekoäly, tulevat tulevaisuudessa vaikuttamaan laajasti sekä siviilielämään että sotilaallisiin suorituskykyihin, erityisesti tietotekniikan käyttömahdollisuuksiin kyberpuolustuksessa, tilannekuvan muodostamisessa ja nopeassa reagoinnissa.

2.6 Sodan kuva

WithSecure haluaa tuoda esiin, että kappaleessa käsitellään vain rajallisesti siviilipuolen teknologian ja IT-järjestelmien kasvavaa roolia sodan johtamisessa ja siihen vaikuttavissa toiminnoissa. Ukrainassa jopa tulenjohtamista tehdään siviilipuhelimilla, julkisten tietoverkkojen ja siviilikäyttöön tarkoitettujen viestikanavien kautta. Puolustusvoimilla on tämän kehityskaaren tutkimusta varten toteutettu "arjen välineet" -tutkimusprojekti, jossa WithSecure on mukana.

Teknologiaa mukautetaan ja sen käyttötarkoituksia innovoidaan nopeasti, ja kehityssykli on tiivis. Reagointiin tarvittava osaaminen ja innovatiivisuus on valjastettava käyttöön jo rauhan aikana.

WithSecuren näkemyksen mukaan nykyisessä tietoympäristössä siviilipuolen tekniikat, työkalut ja toimintatavat sekoittuvat yritysmaailman ja puolustusvoimien tietoteknisten ratkaisujen kanssa. Riskienhallinnan ja kyberturvallisuuden kannalta tämä on merkittävä muutos, sillä kontrollikeinot siirtyvät pois perinteisen keskitetyn valvonnan ja johdon käsistä. Usein kriittisten tietojärjestelmien, kuten tulenjohtoon käytettävien mobiililaitteiden, kyberturvallisuudesta vastaa käyttäjä oman osaamisensa puitteissa.

Siviiliteknologioiden käyttö tuo mukanaan uusia huomioon otettavia aspekteja sotilastiedusteluun, vakoiluun ja vastatoimien toteutukseen. Ukrainassa on raportoitu tapauksia, joissa kineettisiä iskuja on kohdistettu siviilipuhelinten sijainnin perusteella.

Teknologiaa mukautetaan ja sen käyttötarkoituksia innovoidaan nopeasti, ja kehityssykli on tiivis. Vihollisen uusiin kyvykkyyksiin kehitetään ketterästi vastatoimia, joten tarvittava osaaminen ja innovatiivisuus on valjastettava käyttöön rauhan aikana.

WithSecure suosittelee, että kappaleeseen lisätään kuvaus nykyaikaisen tietotekniikan moninaisuuden ja hallitsemattomuuden merkityksestä, joka tulee ottaa huomioon Puolustusvoimien toimintaa suunniteltaessa. On realistista olettaa, että kriisinaikainen tiedonsiirto, toiminnan ohjaaminen ja johtaminen tapahtuisi vain osittain Puolustusvoimien omilla tietojärjestelmillä.

3. Puolustuksen nykytila

Kaikki määritellyt tavoitetilat palautuvat ruohonjuuritason tietotekniseen tekemiseen, jota täytyy tehdä kaikissa toiminnallisuuteen tai toimintoon vaikuttavissa tietojärjestelmissä.

Kappaleessa kuvattu kyvykkyys valvonnan ja tilannekuvan avulla tapahtuvasta havainnoinnista perustuu konkreettisesti tietoturvalokien keräämiseen, analysointiin ja toiminnan mukauttamiseen havaittujen uhkien perusteella. Mainittu pääsyn estäminen kriittisiin järjestelmiin toteutetaan käytännössä järjestelmätason operoinnilla, asetusten muuttamisella, pääsyjen estämisellä ja käyttäjätilien poistamisella. Mainittu johtamisjärjestelmien toimivuuden varmistaminen tietoturvan ja kybersuojauksen parantamisen kautta tarkoittaa käytännössä tietoturvapäivityksiä, parempaa tunnistautumista, pääsyn rajoittamista järjestelmiä eriyttämällä ja hyökkäyspinnan pienentämistä.

Kaikki määritellyt tavoitetilat palautuvat ruohonjuuritason tietotekniseen tekemiseen, jota täytyy tehdä kaikissa toiminnallisuuteen tai toimintoon vaikuttavissa tietojärjestelmissä.

WithSecure näkee suurimpina haasteina selonteossa määritellyn tavoitetilan toteuttamiselle teknisen korjausvelan ja konkreettisen työn määrän suhteessa käytettävissä oleviin henkilöresursseihin. Kansalliseen puolustukseen suoraan tai epäsuorasti vaikuttavien tietojärjestelmien määrä on eri puolustushaaroissa sekä kriittisen infrastruktuurin puolella valtava, ja suuri osa näistä vaatii järjestelmäkohtaista huomiota, konfigurointia ja vianselvitystä.

Tietoturvaa ei voida toteuttaa teknisesti monin eri tavoin, vaan käyttämällä hyvin tunnettuja tietotekniikan parhaita käytänteitä ja toimintoja. Riskienhallinnan näkökulmasta näille tulee määritellä minimitasoja, jotta voidaan luottaa kyberturvallisuuden tasoon.

WithSecure näkee resurssien tehokkaan käytön, sekä lopputuloksena saavutettavan kyberturvallisuuden tavoitteenmukaisen tilan kannalta olennaisen tärkeänä että suunnitteilla olevaan kyberturvallisuusdoktriiniin sisällytetään tietoturvan perustekemisen tavoitetilaa kuvaavat perusmääreet, kuten kyberturvapäivitysten levittämisen aikatavoitteet. Perusmääreiden tulee olla riski- ja uhkamallinnuksen kautta määriteltyjä tavoitetiloja, joihin kaikkien järjestelmien, sekä uusien että vanhojen, tulisi pyrkiä.

WithSecure suosittelee kappaleeseen lisättävän konkreettisia toimia eri toimialojen ja asehaarojen kyberturvallisuuden määrämitallistamiseksi sekä tarvittavien resurssien ohjaamista näiden toimien toteuttamiseksi. Tämä mahdollistaisi suunniteltujen perusparannusten ja toiminnallisten kehityspolkujen toteutumisen.

Selonteossa ei ole korostettu asepalveluksessa olevien suurta keskeyttämismäärää. Kyber- ja avaruusalan osaamista on saatavilla rajoitetusti, ja kyvykkyyksien kehittäminen edellyttää osaavien henkilöiden tunnistamista sekä johdonmukaista mahdollisuutta kehittää heidän osaamistaan asepalveluksen aikana. Tämä edellyttää vaihtoehtoisia keinoja suorittaa varusmies- tai vapaaehtoinen asepalvelus.

4.3 Puolustusjärjestelmän ylläpito ja kehittäminen

Huoltovarmuuden kannalta on olennaista huomioida suomalaisen teollisuuden kyky tuottaa ja kehittää tuotteita ja palveluita. Ukrainan sota on osoittanut, että omavaraisuus osaamisessa mahdollistaa uusien, luovien ratkaisujen tuottamisen, mikä parantaa suorituskykyä merkittävästi, myös osa-alueilla joita ei ole mahdollista hankkia muilla keinoin kriisitilanteessa. Vastaavaa nähtiin Suomessa pandemian aikana, kun osaamista hyödynnettiin kriittisten tarvikkeiden tuotannossa. Suomen innovaatiopääomaa ja uusien yritysten mahdollisuutta osallistua hankintoihin ja innovointiin on vahvistettava.

Nopeasti muuttuva tekninen toimikenttä, uusien teknologioiden mahdollisuuksien käyttöönotto ja nopea reagointikyky on todettu olevan tarpeen nykyaikaisessa kriisinhallinnassa ja jopa avoimen konfliktin aikaan. Siksi WithSecure pitää positiivisena lähtökohtana joustavuuden rakentamista Puolustusvoimien tietotekniikan käyttöönoton ja tietoteknisten toimintatapojen ottamista mukaan tähän selontekoon.

Suomessa suurinta innovaatiopääomaa kyberturvallisuuden, tietotekniikan ja erilaisten tietotekniikkaa hyödyntävien toimintakykyjen kehittämisessä pitää yllä yksityisen sektorin yritykset ja alan oppilaitokset.

WithSecure kuitenkin muistuttaa että Suomessa suurinta innovaatiopääomaa kyberturvallisuuden, tietotekniikan ja erilaisten tietotekniikkaa hyödyntävien toimintakykyjen kehittämisessä pitää yllä yksityisen sektorin yritykset ja alan oppilaitokset.

WithSecure näkeekin tämän tavoitteen täyttymisen ensisijaisena edellytyksenä nykyistä tehokkaamman tiedonvaihdon, yhteistyön ja käyttöönoton operatiivisen tukemisen Puolustusvoimien ja kyvykkyyksiä kehittävän suomalaisen teollisuuden kanssa.

On tärkeää luoda riskilähtöiset päätöksentekoprosessit, joilla uusien järjestelmien, toimintatapojen ja salausratkaisujen käyttöönottoa arvioidaan systemaattisesti ja kaikki uhat huomioiden. WithSecuren kokemuksen mukaan tällainen riskiarviointi toimii parhaiten poikkitoiminnallisissa dynaamisissa arviointityöpajoissa, joissa on laajasti asiantuntijoita käsiteltävästä aiheesta. WithSecure korostaa, että näissä työpajoissa tulisi olla mukana kyberturvallisuuden riskienhallinnan erityisosaajia. Suomessa on laaja, aktiivinen ja maailman huippua edustava kyberturvallisuuden teollisuus, konsultointi ja opetus.

Selonteossa korostetaan, että Puolustusvoimat rakentaa, suojaa, ylläpitää ja operoi sotilaallisen toimintaympäristön edellyttämät operatiiviset tietojärjestelmät itse. Toimialan kumppanuuksia kehitetään kohti verkostomaista toimintamallia. WithSecure näkee tehokkaampana ekosysteemin luomisen, johon myös PK-yritykset ja startupit voivat osallistua yhdessä vakiintuneiden kumppanien kanssa.

Kriittisen infrastruktuurin kyberturvallisuus on olennaisen tärkeää yhteiskunnan kokonaisturvallisuuden kannalta. Kriittinen infrastruktuuri on myös keskeinen osa kansallisen maanpuolustuksen toteutumisessa. WithSecure pitää hyvänä lähtökohtana selonteossa määriteltyä tavoitetilaa, jossa kriittisen infrastruktuurin kybersuojaaminen toteutetaan paikallisjoukoilla, hyödyntäen vahvasti siviilipuolen osaamista. WithSecure näkee tarpeelliseksi korostaa eri toimijoiden, kuten teollisuuden ja puolustusvoimien, välisen tilannekuvan muodostamista, tiedonjaon ja mahdollisen tukeutumisen määrittelyä. Tämä estäisi eri toimijoita toimimasta siiloissa ja varmistaisi kyberturvallisuuden kokonaistason arvioitavuuden.

Toimittajariskit kriittisessä infrastruktuurissa johtuvat usein siitä, että toimittajat ovat monikansallisia suuryrityksiä tai ulkomailla toimivia pienempiä yrityksiä. Kansalliset valmiudet vastata tukitarpeisiin tai kriittisten toimijoiden operatiivisiin vaatimuksiin ovat rajalliset, erityisesti kriisiaikojen kansainvälisten yhteyshäiriöiden aikana.

4.3.4 Kyberpuolustus

Teknologian nopea kehitys ja käytetyn teknologian muodostama velka, luovat kybersietoisuuden ylläpitämiselle merkittäviä haasteita. Verkostoituneet tietojärjestelmät ja reaaliaikaiset kansainväliset tiedonvaihtokanavat tuovat olemassa olevaan toimintakenttään uusia mahdollisuuksia ja uhkia.

Kyberpuolustuksen kentässä elinkaariajattelumalli on nopea ja kyvykkyys pitää luoda viikoissa tai kuukausissa, toisaalta toteutettu ratkaisu voi jäädä tarpeettomaksi vuodessa.

Kansallisella teollisuudella on kyky innovatiivisiin ratkaisuihin, mutta ekosysteemin koordinointi ja ohjaus vaatii panostusta. Kahden tai useamman NATO kumppanimaan kanssa tehtävillä kehityshankkeilla mahdollisestaan ekosysteemiin osallistuvien yrityksien osallistuminen ratkaisujen tuottamiseen.

Kyberpuolustuksen kentässä elinkaariajattelumalli on nopea ja kyvykkyys pitää luoda viikoissa tai kuukausissa, toisaalta toteutettu ratkaisu voi jäädä tarpeettomaksi vuodessa.

Nykyinen tiedonjako ja tilannekuva eivät vastaa selonteossa esitettyä tavoitetilaa rikollisuuden tai hybridivaikuttamisen uhan torjumiseksi tehokkaasti. WithSecure pitää välttämättömänä reaaliaikaisen, operatiivisen tilannekuvan luomista, joka tukee jäsenvaltioihin kohdistuvan tietojärjestelmien vaikuttamisen ja kyberrikollisuuden

valvontaa. Tilannekuvan tarkkuus ja konkretian taso ovat keskeisiä, jotta sen avulla voidaan toteuttaa konkreettisia ennaltaehkäiseviä ja suojaavia toimenpiteitä.

Samalla suojataan Puolustuskyvylle kriittinen infrastruktuuri kyberuhkilta. Puolustusvoimien on kyettävä käynnistämään puolustuksen edellyttämät kyberoperaatiot ja muut vastatoimet ennakoivasti.

Tilannekuvan tulisi olla jäsenmaiden viranomaisten käytettävissä erilaisiin tarkoituksiin, kuten kansainväliseen verkkorikostutkintaan ja hybridivaikuttamisen torjuntaan. Nykyinen, viranomaisilmoituksiin perustuva ilmoituskanava reagoi parhaimmillaankin päivissä, ja sen kautta saatu tietoisuus on usein vain valmiuden kohottamiseen käytettävää informaatiota.

WithSecure ei pidä nykyisiä EU-aloitteita, kuten Joint Cybercrime Action Taskforce (J-CAT) [1]ja ENISAn alaisuudessa toimivaa European Cyber Crisis Liaison Organisation Network CyCLONe[2], riittävinä tarjoamaan kriittisen infrastruktuurin tietoturvahenkilöstölle ajantasaista ja kohdennettua näkyvyyttä muiden jäsenvaltioiden häiriöihin ja hyökkäyksiin. WithSecure uskoo, että Suomen tulisi ottaa aktiivinen rooli tehokkaamman ja operatiivisesti käyttökelpoisen tilannekuvan luomisessa. Suomessa on vahvaa osaamista tällaisten toimintojen suunnittelussa ja toteuttamisessa.

4.8.3 Lainsäädäntö

WithSecuren kanta on että puolustusvoimilla tulee olla lain sallimat toimintaoikeudet toimia kybertoimintakentässä kansallisen turvallisuuden vaatimilla, perusteltavissa olevilla tavoilla.

4.8.6 Sotilaallinen huoltovarmuus ja kumppanuudet

Huoltovarmuuden vahvistamiseksi on tärkeää, että Suomessa on riittävästi kyberturvallisuuden osaamista ja TKI-kyvykkyyksiä sekä julkisella että yksityisellä sektorilla. Yksityisen sektorin TKI-toiminnan ja kotimaisen osaamisen vahvistamisen edellytyksiä ovat rahoituksen saatavuus sekä riittävän suuri kohdemarkkina liiketoiminnalle. Suomi itsessään on pieni markkina ja siksi yksityisen sektorin on pystyttävä toimimaan laajasti Euroopassa sekä NATO:ssa. Tässä olennaista on sekä EU-laajuisen regulaation ja yhteistyön kehittäminen että Puolustusvoimien tuki kotimaiselle teollisuudelle niin referenssiasiakkaana kuin verkostoitumisen ja yhteistyön edistäjänä kansainvälisesti.

Tämän mahdollistaa vain aktiivinen toiminta poliittisella, sekä virkamiestasolla. Kumppanuus ja yhteistyö kybersektorin toimijoiden kanssa on edellytys kyvykkyyden säilyttämisessä kansallisesti.

5 Johtopäätökset

WithSecure painottaa johtopäätöksistä seuraavia ja ehdottaa niiden täydentämistä seuraavasti:

15. Puolustushallinnon omaa kykyä ja kapasiteettia teknologian seurantaan ja hallintaan sekä kotimaisten ja kansainvälisten TKI-instrumenttien hyödyntämiseen vahvistetaan. Puolustusteollisuuden toimintaedellytyksiä parannetaan ja toimia tuotantokyvyn nostamiseksi tuetaan sotilaallisen huoltovarmuuden turvaamiseksi.

<uusi>. Kyberturvallisuusdoktriiniin tai sen yhteyteen luotava riskienhallinnan raami ja tavoitetilat, joita peilaamalla voidaan yhteensovittaa kansallisen turvallisuuden toimijoiden ja kriittistä infrastruktuuria operoivan suomalaisen teollisuuden kyberturvallisuuden operatiivisen kyberturvallisuuden kyvyt, resurssit ja teholliset odotukset.

---

[1] https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce
[2] https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone

Lausunnon antaja:

Helsingissä, 11.4.2025

Antti Laatikainen
Johtava tietoturvakonsultti
WithSecure Consulting

antti.laatikainen@withsecure.com
+358406372163