Puolustusvaliokunta

PUOLUSTUSVOIMIEN KYBERSUORITUSKYVYN RAKENTUMINEN

Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi, ei ainoastaan puolustusjärjestelmän, vaan koko yhteiskunnan kannalta tarkasteltuna. Kybertoimintaympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä sekä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella. Puolustusvoimien lakisääteisten tehtävien suorittaminen edellyttää jatkossa nykyistä korkeampaa toimintavalmiutta sekä suorituskykyä myös kybertoimintaympäristössä. Puolustusjärjestelmä on riippuvainen kybertoimintaympäristön käytettävyydestä ja sen osajärjestelmien tehokas ja vaikuttava toiminta edellyttää turvallista kybertoimintaympäristöä.

Kyberpuolustus on määritetty Valtioneuvoston puolustusselonteossa yhdeksi puolustusjärjestelmän kehittämisen painopistealueeksi. Kyberpuolustuksella tarkoitetaan kansallisesti kyberturvallisuuden maanpuolustuksellista osa-aluetta, joka muodostuu **tiedustelun, vaikuttamisen ja suojautumisen** suorituskyvyistä. Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuksen suorituskyvyn lakisääteisiä tehtäviään varten osana kansallista kyberturvallisuutta ja yhteiskunnan elintärkeiden toimintojen ja turvaamista.

Puolustusvoimien kyberpuolustussuorituskyvyn kehittämiseksi on määritetty neljä tavoitetta.

TAVOITE 1: Luodaan ja ylläpidetään suojautumisen suorituskyky puolustusvoimien kybertoimintaympäristössä. Puolustusvoimat valvoo ja suojaa ensisijaisesti omat järjestelmänsä siten, että se kykenee suoriutumaan lakisääteisistä tehtävistään normaali- ja poikkeusoloissa huolimatta kybertoimintaympäristön uhkista. Suojaaminen perustuu yhtenäiseen tilannekuvaan ja puolustusvoimien johdon hyväksymään riskitasoon. Onnistuminen tehtävässä edellyttää kykyä puolustusvoimien toiminnan kannalta tärkeiden tietoverkkojen, ase- ja johtamisjärjestelmien sekä tiedon suojaamiseen.

TAVOITE 2: Luodaan ja ylläpidetään kyky hyödyntää kybertoimintaympäristöä tiedustelutiedon tuottamiseksi. Tietoverkkotiedustelulla tuotetaan tietoliikenteestä ja tietojärjestelmistä tiedustelutietoa valtion ja puolustusvoimien johdon päätöksenteon tueksi, toimintaympäris-

tötietoisuuden muodostamiseksi sekä ennakkovaroituksen mahdollistamiseksi. Tietoverkkotiedustelu jakautuu tietojärjestelmä- sekä tietoliikennetiedusteluun.

Puolustusvoimien lakisääteisten tehtävien hoitaminen edellyttää tiedustelua. Merkittäviin uhkiin liittyvä tieto siirtyy yhä enemmän tietoverkkoon. Kybertoimintaympäristöstä hankittua tietoa tarvitaan valtionjohdon ja puolustusvoimien johdon päätöksenteon tueksi ja sillä tuetaan puolustusvoimien operaatioita suojaamalla oman päätöksenteon edellytykset. Tiedustelutoimivaltuuksien saamiseksi on laadittu esitys sotilastiedustelua koskevaksi lainsäädännöksi.

TAVOITE 3: Luodaan ja ylläpidetään kybervaikuttamisen suorituskyky. Kybervaikuttamisen suorituskyvyillä kehitetään omaa suojautumiskykyä sekä tarvittaessa tuetaan puolustusvoimien operaatioita heikentämällä vastustajan tilannetietoisuutta ja toimintavapautta.

TAVOITE 4: Kyetään tukemaan yhteiskunnan kyberturvallisuutta. Kyberuhka kohdistuu niin yhteiskuntaan, viranomaisiin kuin puolustusvoimiinkin. Kansallisen periaatteemme mukaisesti jokainen toimija vastaa omasta suojautumisestaan sekä varautumisesta häiriötilanteisiin.

Puolustusvoimat pystyy tukemaan yhteiskunnan elintärkeiden toimintojen turvaamista muillakin kuin vain kyberpuolustuksen teknisillä keinoilla. Tämä tarkoittaa esimerkiksi tukemalla opetusta ja koulutusta, järjestämällä harjoitustoimintaa, varusmies- ja reserviläiskoulutusta sekä osoittamalla voimavaroja kansalliseen tutkimus- ja kehitystoimintaan. Puolustusvoimat antaa kyberuhkien aiheuttamissa häiriötilanteissa tarvittaessa virka-apua myös muille viranomaisille. Puolustusvoimat saa itse myös tarvittaessa tukea muilta viranomaisilta omien kyberpuolustustehtävien toteuttamisessa.

Puolustusvoimien kybersuorituskyky rakentuu johdonmukaisesti osana puolustusvoimien suorituskykyjen kehittämisohjelmaa vuoteen 2025 mennessä. Materiaalihankkeiden lisäksi merkittävä tekijä on ammattitaitoinen ja osaava henkilöstö. Kyberhenkilöstö koostuu normaalioloissa palkatusta henkilökunnasta sekä koulutuksessa olevista varusmiehistä. Poikkeusoloissa puolustusvoimien henkilökuntaa täydennetään kyberkoulutetuilla ja sijoitetuilla reserviläisillä.

Puolustusvoimien kyberpuolustussuorituskyvyn rakentuminen edellyttää syvällistä kansainvälistä ja kansallista yhteistyötä. Viranomaisyhteistyötä pyritään kehittämään luomalla tarvittavat tekniset ja hallinnolliset tiedonvaihtomenetelmät. Viranomaisyhteistoimintaan kuuluvat myös yhteiset harjoitukset sekä säännöllinen tiedonvaihto.

Yhteistoiminta tutkimus- ja tiedeyhteisön kanssa painottuu tulevaisuuden teknologian tutkimukseen ja osaamisen kehittämiseen, tällöin samalla kehitetään myös kansallista kyberosaamista.

Kansainvälinen kahden- ja monenvälinen yhteistyö kyberpuolustuksessa keskittyy tiedonvaihtoon sekä koulutus- ja harjoitustoimintaan, jolloin kehitetään kansallista kyberpuolustuksen suorituskykyämme.
+ + +