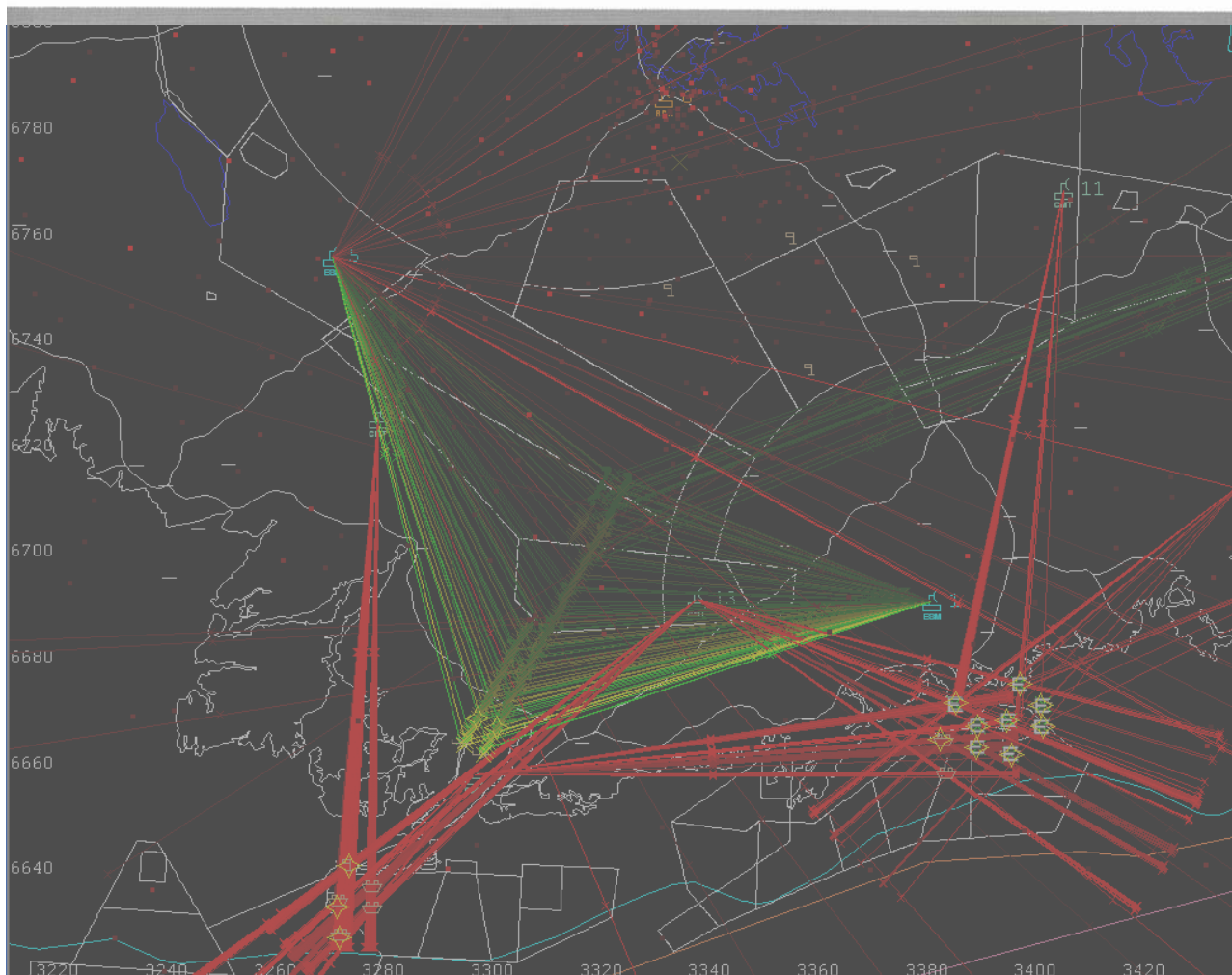




PUOLUSTUSVOIMIEN TEKNOLOGIASTRATEGIA

2012



PÄÄESIKUNTA
Materiaaliosasto



1. Johdanto

Puolustusvoimien teknologiastrategialla tuetaan puolustusvoimien kehittämistä luomalla edellytykset puolustusteknologiaan liittyvien tarkoituksenmukaisten päätösten tekemiselle siten, että puolustusvoimien tavoitetilä kyetään saavuttamaan, sotilaallinen huoltovarmuus turvaamaan ja puolustusjärjestelmän suorituskykyvaatimukset täyttämään.

Strategia on suunnittelua ja päätöksentekoa ohjaava yleislinjaus teknologisen osaamisen luomiseksi ja hallinnoimiseksi. Se tarkentaa ja konkretisoi puolustushallinnon strategiaa puolustusvoimien näkökulmasta. Strategialla osaltaan vastataan puolustusvoimien voimavarojen merkittävään supistumiseen fokusoidulla resursseilla tärkeimpiin alueisiin sekä liittämällä teknologiatoiminta strategiseen päätöksentekoon.

Teknologiastrategiaa ylläpidetään puolustusvoimien strategisen suunnittelun syklissä, joten

se päivitetään lähtökohtaisesti neljän vuoden välein.

2. Keskeiset käsitteet

Teknologia on teknistä tietoa tai apua, jota tarvitaan laitteiden, järjestelmien, ohjelmistojen tai palveluiden kehittämistä, tuotantoa tai käyttöä varten. Tekninen tieto voi olla muodoltaan piirustuksia, suunnitelmia, kaavioita, malleja, kaavoja, taulukoita, suunnittelukonstruktioita tai määritelmiä, kirjallisia tai muulle medialle tai laitteille, kuten levyille, nauhalle tai lukumuistiin, talletettuja käsikirjoja ja ohjeita. Tekninen apu voi olla muodoltaan ohjeita, taitoja, opetusta, työnsuoritus-tietoutta tai konsultointipalveluja ja saattaa sisältää ”teknisen tiedon” siirtoa.

Puolustusteknologia on Euroopan unionin yhteisen puolustustarvikeluettelon tarkoittamien tuotteiden kehittämistä, tuottamista tai käyttöä varten tarvittavaa teknologiaa.

Teknologiatoiminta on puolustusteknologian hankinta-, toimitus- ja ylläpitovalmiuksien kehittämistä ja tähän liittyvien edellytysten luomista sekä järjestelmien sodan ajan toimivuuden ja oikean käyttöperiaatteen varmistamista. Teknologiatoiminnalla myös tuotetaan tietoa puolustusvoimien suorituskykyvaatimusten asettamiseen sekä puolustusjärjestelmän kehittämisvaihtoehtojen arviointiin.

3. Tavoitetilä

Teknologiatoiminnan tavoitetilässa:

- 1) puolustusvoimien toimintaan liittyvät teknologiset riskit ja mahdollisuudet tunnetaan ja kyetään huomioimaan puolustusjärjestelmän kehittämisessä ja suorituskyvyn käytössä sodan ajan yllättävissä tilanteissa
- 2) puolustusvoimat kykenee hankkimaan teknologiaa kokonaistaloudellisesti ja riskit halliten
- 3) Suomella on kyky integroida uutta teknologiaa puolustusjärjestelmään ja ylläpitää sitä kokonaistaloudellisesti kaikissa olosuhteissa



4. Keinot tavoitetaan pääsemiseksi

Teknologiatoiminnan tavoitetilaa saavutetaan:

- 1) seuraamalla teknologian ja sodankäynnin kehittymistä, tutkimalla sodan ja taistelun kuvaan olennaisesti vaikuttavia teknologioita sekä huomioimalla nämä puolustusvoimien strategisessa suunnittelussa ja puolustusjärjestelmän kehittämissuunnitelmissa
- 2) luomalla kehittämisohjelmien ja hankkeiden onnistuneen toteuttamisen edellyttämä kansallinen teknologinen osaaminen jo ennen hankkeiden suunnittelun aloittamista
- 3) tukemalla hankevalmistelua ja hankintojen läpivientiä tutkimuksen tuottamalla tiedolla sekä evaluoimalla järjestelmien toimintaa sodan ajan olosuhteissa
- 4) kehittämällä kansallista teknologista osaamista ja valmiuksia riittävän etupainoisesti sekä verkottumalla kansainvälisesti erityisesti niillä tärkeillä alueilla, joilla kan-

sallista kykyä ei ole tarkoituksenmukaista tai mahdollista luoda

- 5) varmistamalla kotimaassa toimivan teollisuuden kyky ottaa haltuun uutta puolustusteknologiaa ja integroida sitä puolustusjärjestelmään
- 6) varmistamalla kotimaassa toimivan teollisuuden kyky ylläpitää puolustusteknologiaa ja korjata vaurioita
- 7) varmistamalla hanke- ja hankintatoiminnassa valtion keskeisten turvallisuusetujen huomioiminen sekä toteuttamalla niitä puolustusteknologian viennin ja loppukäytön valvonnassa
- 8) luomalla edellytyksiä materiaalsen avun antamiselle ja vastaanottamiselle kriisitilanteissa

5. Kriittiset menestystekijät

Tavoitteiden saavuttamisen kannalta on välttämätöntä taata resurssien minimitaso sekä keskittää resurssit koko puolustusjärjestelmän suorituskyvyn kannalta kriittisille alueille. Käytännössä tämä vaatii sitä, että:

- 1) teknologiatoiminta resursoidaan riittävälle tasolle ja resurssien käyttö suunnitellaan pitkäjänteisesti ja tavoitetilalähtöisesti, koska teknologisen osaamisen luominen kestää 10-15 vuotta
- 2) teknologiatoiminnan prosessi integroidaan puolustusvoimien strategisen suunnittelun prosessiin ja puolustusvoimien strategisen suunnittelun prosessi integroidaan kehittämisohjelmien ja hankkeiden hallinnan prosesseihin
- 3) teknologiatoimintaan osoitetut varat kohdennetaan niille painopistealueille, joilla tehokkaimmin kyetään tukemaan puolustusvoimien suorituskykyjen kehittämistä
- 4) teknologia hankitaan lähtökohtaisesti valmiina ja toimivaksi todennettuna, mutta samalla hanketoiminnassa huomioidaan se, että myös valmiin teknologian integrointi puolustusjärjestelmään edellyttää tutkimus- ja kehitystyötä

- 5) mikäli teknologian hankkiminen valmiina ei ole mahdollista tai tarkoituksenmukaista, kehittämisresurssit pyritään kohdentamaan kotimaahan
- 6) puolustusvoimien omat henkilöresurssit keskitetään sellaisiin osaamisalueisiin ja valmiuksiin, jotka puolustusvoimien on välttämätön hallita itse
- 7) luodaan strategisia kumppanuuksia niille alueille, jotka on tehtävä kansallisesti
- 8) verkotutaan kansallisesti ja kansainvälisesti synergiaetujen ja yhteensopivuuden lisäämiseksi sekä avun vastaanottokyvyn varmistamiseksi
- 9) puolustusvoimien sopeuttamistoimenpiteet kohdistetaan niille alueille, joiden merkitys sodankäynnin kannalta on vähäisin ja joissa voidaan tukeutua muihin toimijoihin
- 10) kriittisten teknologioiden alueella varmistetaan kotimainen osaaminen

6. Painopistealueet

Strategiset osaamisalueet ovat teknistoiminnallisia osaamisalueita, joiden hallinta on välttämätöntä puolustusjärjestelmän kehittämisen ja käytön varmistamiseksi. Strategiset osaamisalueet perustuvat toisaalta arvioon sotateknologisesta kehityksestä ja toisaalta puolustusjärjestelmän tavoitelasuunnitelmaan ja siinä kuvattuihin puolustusvoimien kyvykkyysvaatimuksiin sekä sotilaallisen suorituskyvyn käyttöperiaatteisiin.

Kyvykkyysalueittain korostuvat seuraavat strategiset osaamisalueet:

- **Toimintaympäristötietoisuuden** luomisessa korostuu kyky seurata omien joukkojen tilaa ja sijaintia sekä kyky nopeaan maalitukseen.
- **Johtamisessa** korostuu kyky johtaa hajautettuja liikkuvia joukkoja ja päätöksenteon nopeuttaminen vaihtoehto- ja seurannaisvaikutusanalyysin



- **Verkostotoiminnassa** korostuvat järjestelmien yhteensopivuuden varmistamisessa välttämättömien informaatorajapintojen ja sähkömagneettisen spektrin hallinta sekä tietoverkkosodankäyntikyky
- **Voimankäytössä** korostuu täsmävaikutuskyky sekä sitä tukeva nopean tulenavauksen mahdollistavat maalitus, omien seuranta ja omatunnistuskkyky
- **Suojautumisessa** korostuu kyky havaita erilaiset uhat ajoissa ja vaikutuksen kohdentumisen välttäminen toimintaympäristötietoisuuden, herätteen hallinnan, hajauttamisen, liikkeen ja harhauttamisen keinoin. Suojan toissijainen kerros muodostuu kohdentuneen uhkan vaikutusten minimoimisesta ja toipumisesta, jossa mukana on kyky havaita CBRN-uhka ja kyky toimia lyhytaikaisesti sen alla sekä tarkoituksenmukainen ballistinen suoja.
- **Logistiikassa** keskeistä on logistiikan johtaminen, materiaalivirtojen hallinta, kunnossapito ja taisteluvaurioiden korjauskyky.
- **Joukkotuotannossa** puolustusteknologian kannalta on keskeistä joukkojen harjoittaminen toimintaan sodan ajan olosuhteita vastaavissa oloissa, mikä edellyttää kykyä mallintaa ja simuloida joukon ja järjestelmien toimintaa ja taisteluita sekä kykyä simuloida sodan ajan olosuhteet ja vihollisvaikutus todellisiin harjoitustilanteisiin.
- **Toiminnanohjauksessa** keskeistä on sekä koko puolustusjärjestelmän (systems of systems) hallintaan liittyvien menetelmien hallitseminen että hankkeiden läpiviennin edellyttämä osaaminen.

Kriittiset teknologiat ovat teknologioita, joiden on oltava puolustusvoimien käytössä strategisten osaamisalueiden hallitsemiseksi ja joihin liittyy selkeä sotilaallisen suorituskyvyn kehittämistarve. Puolustusvoimien teknologia-toimintaan kohdistamien resurssien niukkuuden vuoksi kriittisiä teknologioita voi olla vain muutamia. Nämä ovat tärkeysjärjestyksessä:

1. **informaatioteknologia**, jonka avulla luodaan toimintaympäristötietoisuus ja johtamiskyky sekä verkostopuolustusjärjestelmä.
2. **materiaalitekhnologia**, jossa keskeistä on häiveteknisen ja ballistisen suojan mahdollistaminen ilman tarvetta lisätä logistista taakkaa tai tinkiä liikkuvuudesta.
3. **suorituskyvyn hallinnan menetelmät** (Systems Engineering ja Systems-of-Systems Engineering), joka muodostuu joukosta metodeja ja niitä tukevia työkaluja, joilla varmistetaan, että suorituskykytavoitteet kyetään määrittämään ja saavuttamaan.
4. **Bio- ja kemian teknologiat**, joista tärkeimpiä ovat kemiallisten ja biologisten aseiden suojelutiedustelukyvyn varmistavat teknologiat.



Informaatioteknologialla on keskeinen merkitys myös voimankäytön, suojan ja logistiikan suorituskyvyissä. Informaatioteknologian merkittävä tai jopa keskeisin rooli kaikissa puolustusvoimien suorituskyvyissä tekee siitä ensisijaisen kriittisen teknologian. Informaatioteknologian avulla joukkojen suorituskykyä kyetään kehittämään kustannustehokkaasti. Toisaalta siinä yleinen teknologinen kehitys sekä ase-vasta-ase-kilpailu ovat erityisen nopeita. Materiaalitekhnologian kehitys mahdollistaa joukkojen tehokkaamman suojaamisen, mutta sen kehitys on informaatioteknologiaa hitaampaa. Järjestelmien kompleksoituessa ja verkottuessa sekä keskenään kansallisesti että kansainvälisesti yhteisten suorituskykyjen ja yhteisoperaatioiden myötä puolustusjärjestelmäkokonaisuuden tekninen hallinta vaatii vaatimusten, arkkitehtuurin, konfiguraation ja elinjaksokustannusten hallintaa. Koska yritykset hinnoittelevat epämääräis-

ten vaatimusten ja yleistasoisten suunnitelmien sisältämät riskit tarjouksiinsa, Systems Engineering -menetelmillä (mukaan lukien design-to-cost) kyetään myös hillitsemään suorituskyvyn rakentamisen kustannuksia.

Kriittiset teknologiat on määritelty yksityiskohdaisesti liitteessä 1.

7. Toimenpiteet

7.1 Puolustusvoimien resurssien kehittäminen

Puolustusvoimien resursseja kehitetään strategisten osaamisalueiden ja kriittisten teknologioiden alueilla. Puolustusvoimien teknologiaan liittyvät tutkimus- ja kehittämisresurssit keskitetään niille alueille, joissa:

- 1) osaamisen on oltava puolustusvoimien hallussa ja toiminnan puolustusvoimien johtamassa
- 2) teknologiaa tai palveluita ei salattavuussyistä voida hankkia muualta
- 3) halutaan säilyttää muista riippumaton kyky tuottaa puolueetonta tietoa, materiaalia tai palveluita

Puolustusvoimien omien resurssien käytön kustannustehokkuutta parannetaan tuotteistamalla teknologiatoiminnan palvelut ja keskittämällä toiminta tärkeimpiin tuoteryhmiin. Tärkeimmät tuoteryhmät ovat sotavarustuksen testaus ja evaluointi, teknologiaennakointi, mallinnus ja simulointi sekä hanke- ja hankintatoiminnan konsultointi teknisissä kysymyksissä.

Puolustusvoimien tutkimuslaitokset tarkentavat omissa strategioissaan tuoteryhmittäin ne tuotteet, joihin tutkimustoiminnan painopisteillä mainittujen periaatteiden ohjaamana luodaan sekä miten muiden teknologioiden ja palveluiden saatavuus varmistetaan.

7.2 Kumppanuuksien hyödyntäminen



Kumppanuuksia kehitetään etenkin alueilla, joilla on varmistettava kansallinen osaaminen, mutta sen ei ole tarkoituksenmukaista olla puolustusvoimien omassa hallussa. Strategisia kumppanuuksia luodaan alueille, joilla on keskeinen merkitys puolustusvoimien sodan ajan toiminnalle sekä puolustusjärjestelmän pitkäjänteiselle kehittämiselle. Kumppanuuksilla varmistetaan myös sotilaallinen huoltovarmuus.

7.2 Osaamisverkostot

Teknologiaohjelmia tukemaan ja niissä syntyvää osaamista ylläpitämään luodaan tarvittavat osaamisverkostot. Niiden avulla puolustusvoimien, turvallisuusviranomaisten sekä kotimaisen tiedeyhteisön ja teollisuuden teknologia-alan yhteistoiminta järjestetään siten, että kriittisten teknologioiden osaaminen saatetaan vastaamaan vaadittuja tasoja ja resursseja kyetään käyttämään tehokkaasti. Osaamisverkostot toimivat yhteistyöeliminä, tiedonvaihtofoorumeina ja yhteisten ohjelmien kehittäjinä. Osaamisverkostoon kuuluvien jäsenten kanssa luodaan tutkimus- ja kehittämispalveluiden hankinnan puitejärjestelyt puolustus- ja turvallisuushankintalain määräysten mukaisesti.

7.4 Teknologiaohjelmat

Teknologiaohjelmilla luodaan kotimaahan puolustusjärjestelmän kokonaisuuden kannalta kriittistä osaamista, jolla tuetaan puolustus-



voimien kriisiajan suorituskyvyn hallintaa, puolustusvoimien kykyä toimia osaavana ja kustannustietoisena ostajana sekä luodaan huoltovarmuuden perustana olevaa teknologista osaamista.

Teknologiaohjelmissa tutkitaan ja demonstroidaan teknologian soveltuvuutta puolustusvoimien käyttöön. Niissä ei tehdä tuotekehitystä, mutta niiden tuloksina syntyy

- tutkimusraportteja, uhka-arvioita, sovellettu-analysejä ja toteutettavuusselvityksiä
- kyky laatia toteuttamiskelpoisia ja kustannustehokkaita konsepti- ja järjestelmämäärittelyitä, suorituskyky- ja arkkitehtuuri-vaatimuksia
- teknologian kehitys- ja evaluointivalmiuksia
- uusia teknologisia järjestelmäkomponentteja ja palvelukonsepteja
- keksintöjä ja patentteja
- teknologia-, konsepti- ja järjestelmädemostrattoreita

Teknologiatoiminnan piiriin otetaan lähtökohtaisesti strategiaan osaamisalueisiin liittyvää kriittistä teknologiaa, joka on tasolla TV2 (teknologian sovelluskonsepti on määritelty ja sen tieteellinen perusta on olemassa, vaikka käytännön sovelluksista ei vielä ole näyttöä).

Puolustusvoimien hankintavalmiuden tulisi olla tasolla HV2 (teknologian kehitysaikataulu, toiminnallisuus, vahvuudet ja heikkoudet ymmärretään). Kuvaukset teknologian hankinta- ja toimitusvalmiuksien tasoista on liitteenä 2.

Teknologiaohjelmat suunnitellaan ja koordinoitetaan keskitetysti Pääesikunnan johdolla. Teknologiaohjelmien projektit kootaan suorituskykyaluejaon mukaisiksi aliohjelmiksi. Teknologiaohjelmien valmistelussa selvitetään teknologian monikäyttöpotentiaali ja sotilaallinen tarkoituksenmukaisuus huomioiden pyritään vahvistamaan sitä.

Teknologiaohjelma 2013 avulla tuetaan kehitettäviä suorituskykyjä sekä maavoimien uutta taistelutapaa keskittämällä resurssit toimintaympäristötietoisuuden, johtamisen ja joukon kokonaissuojan parantamiseen.

7.5 Tekninen kehittäminen kehittämisohjelmissa

Kehittämisohjelmat vastaavat itse omien hankkeidensa edellyttämästä teknologisesta tutkimuksesta ja kehittämisestä. Suorituskyvyn elinjaksonhallintaa kehitetään siten, että mikäli hankittava teknologia ei ole sarjahankintaan vaadittavalla tasolla, sarjahankintaa edeltää kehittämisvaihe.

7.6 Teknologian hankinta

Teknologian tuonti ulkomailta tapahtuu suorilla kaupoilla sekä poikkeustapauksissa vasta-kauppanenettelyillä. Kotimaassa toimivan teollisuuden osuus pyritään kohdentamaan kriittisten teknologioiden alueille sekä järjestelmien huoltovarmuuden kannalta kriittisille alueille. Kotimaisen tiedeyhteisön ja teollisuuden osaamista pyritään mahdollisuuksien mukaan hyödyntämään ottamalla se mukaan hankkeiden ideointivaiheessa tehtävään konseptityöhön. Tällä lisätään puolustusvoimien suorituskyky- ja elinjakso kustannustietoisuutta sekä parannetaan järjestelmien integrointi- ja ylläpitövalmiuksia. Kotimaisen teollisuuden vientiponnisteluja pyritään mahdollisuuksien mukaan edistämään.

7.7 Immateriaalioikeudet

Immateriaalioikeuksien hallinnalla pyritään toisaalta varmistamaan kriittisten järjestelmien toimintakyky kriisitilanteessa ja toisaalta luomaan kotimaassa toimivalle teollisuudelle mahdollisimman hyvät toimintaedellytykset. Kriisiajan tarpeet edellyttävät joidenkin teknologioiden salassa pitämistä, viennin ja käytön kontrollointia sekä kykyä muokata teknologisia ratkaisuja sodan ajan yllätysten luomiseksi ja vihollisesta johtuviin yllätyksiin reagoimiseksi.

Teollisuuden toimintaedellytysten kannalta on tärkeää, että teknologisen kehityksen tuloksena syntyy mahdollisimman monenlaisia tuotteita, joilla on mahdollisimman useita kohderyhmiä. Tämä laajentaa liiketoimintavolyymia puolustusvoimien asiakkuutta laajemmalle ja hyödyttää samalla puolustusvoimia.

Teknologisen kehittämisen tuloksena syntyy monikäyttöisiä tuloksia, joista voidaan kehittää tuotteita sekä puolustusvoimien että muiden kohderyhmien tarpeisiin. Tämän vuoksi on tarkoituksenmukaista, että teknologiatoinnassa immateriaalioikeudet ovat teknologiaohjelmien osalta lähtökohtaisesti teollisuudella. Poikkeuksena on kriittinen teknologia, joka on joko salassa pidettävä tai joka on välttämätön

uuden teknologian integroimisessa osaksi puolustusjärjestelmää. Harkinta on aina tehtävä tapauskohtaisesti koko elinjakson tarpeet huomioon ottaen ja huomioiden teollisuuden oman kehittämisrahoituksen osuus. Luovutettaessa teknologian immateriaalioikeudet puolustusvoimien ulkopuolelle, puolustusvoimien edut tulee turvata sopimalla puolustusvoimille yksityiskohtainen käyttöoikeus käyttää ja kouluttaa teknologiaa Suomessa ja ulkomailla, tuottaa teknologiaa, mikäli toimittaja lopettaa teknologian toimittamisen tai ei toimita sitä kohtuullisin ehdoin sekä kriisitilanteessa edelleen kehittää ja modifioida teknologiaa, mikäli puolustusjärjestelmän toimivuuden varmistaminen sitä edellyttää. Lisäksi on sovittava miten toimitaan tilanteessa, jossa yritys on siirtymässä ulkomaiseen omistukseen. Puolustusvoimien teknologiainvestointien tavoitteena olevasta palauttamisesta rojalTIMAKSUIN on sovittava koskien myyntiä valtionhallinnon ulkopuolelle. RojalTIT on sovittava siten, että toisaalta tuetaan orastavan liiketoiminnan kehittymistä, mutta toisaalta valtiolliset investoinnit saadaan takaisin, kun liiketoiminta on tuottavaa.

Esimerkkejä teknologioista, joiden kehittämishankkeissa immateriaalioikeuksien tulee tyypillisesti olla puolustusvoimilla, ovat salausalgoritmit (COMSEC ja TRANSEC) ja niiden implementointiratkaisut, elleivät ne ole avoimia, salausavainten generointialgoritmit ja välineet, tiedustelu-, valvonta-, johtamis-, navigointi-, paikantamis- ja asejärjestelmien häirinnänväistömenetelmät, tiedonsiirto- ja häirintäaaltomuodot, tiedonvaihdon mallit ja protokollat, elleivät ne ole avoimia sekä järjestelmien herätteet. Näiltä osin työssä syntyvien teknologioiden käyttöoikeudesta (esim. vientiversiot) sovitaan toimittajien kanssa tapauskohtaisesti.

On varmistettava, että teknologian omistus- tai käyttöoikeudet koskevat koko puolustusvoimia ja että käyttöoikeuksissa huomioidaan myös puolustusvoimien kaikki kolme tehtävää.



7.8 Teknologisen tiedon suojaaminen

Puolustusjärjestelmän kannalta kriittinen tieto suojataan. Salassapito voi liittyä tietoon teknologian ominaisuudesta, ylipäänsä teknologian olemassaoloon järjestelmässä, tai jopa ominaisuuden puuttumiseen tai teknologian soveltamatta jättämiseen. Salassa pidettävää voi olla siten sekä se mitä puolustusjärjestelmässä on että se, mitä ei ole. Suorituskykyvasteuulliset Pääesikunnan osastot määrittelevät mitkä teknologiset ratkaisut ovat salassa pidettäviä sekä mikä näiden asioiden suojaustaso on. Tämän mukaisesti Pääesikunnan materiaali-osasto ohjeistaa teknologiaohjelmissa käytettävät suojaustasot ja huolehtii viennin seurannasta. Kehittämishjelmien omistajat ohjeistavat kehittämisohjelmiensa tutkimus- ja kehittämisohjelmissa noudatettavat suojaustasot. Nämä luokitukset tulee huomioida tutkimus-, kehittämis-, hankinta-, koulutus-, operointi- ja logistiikkatoiminnassa. Liitteessä 3 on soveltamisohjeita. Loppukäytön valvontaan liittyen suojataan kolmansien osapuolten teknologia. Teknologiatiedon määrittäminen salassa pidettäväksi perusteena puolustusjärjes-

telmän toimivuuden takaaminen muodostaa perusteen teknologian, järjestelmäkomponentin tai järjestelmän hankinnan rajaamiseksi puolustus- ja turvallisuushankintalain ulkopuolelle.

7.9 Kansallinen yhteistyö

Viranomaisten välistä yhteistyötä, koordinaatiota ja päätöksentekoa lisätään osana yhteiskunnan turvallisuusstrategian toimeenpanoa ja yhteiskunnan laajan turvallisuuskäsitteen mukaista yhteistä teknistä tutkimusta ja kehittämistä. Tällä pyritään osaltaan varmistamaan voimavarojen riittävyys kansallisen turvallisuuden edellyttämälle tekniselle tutkimus- ja kehittämistoiminnalle. Puolustusvoimien ja Maanpuolustuksen Tieteellisen Neuvottelukunnan (MATINE) välisellä yhteistyöllä pyritään tukemaan puolustusvoimien suorituskykyjen kehittämiseen liittyvien innovaatioiden ja osaamisen syntymistä. Puolustusvoimien ja Teknologian ja innovaatioiden kehittämisskeskuksen (TEKES) välisellä yhteistyöllä pyritään auttamaan yrityksiä muuttamaan kehittämiskelpoisia ideoita liiketoiminnaksi. Puolustusvoimien ja TEKESin välisen yhteis-

työn tavoitteena on tunnistaa teknologian kahtais- ja monikäyttöpotentiaalia ja tukea sen kehittymistä.



7.10 Kansainvälinen yhteistyö

Kansainvälistä teknologiayhteistyötä kehitetään siten, että se perustuu nykyistä tiukemmin puolustusvoimien strategiseen tutkimukseen, osaamisverkostojen kehittämiseen, teknologiaohjelmaan ja puolustusvoimien kehittämisohjelmiin. Euroopan puolustusvirasto (EDA) on tärkein puolustusteknologisen tutkimuksen ja kehittämisen yhteistyöfoorumi. EDA-yhteistyön tavoitteena on tukea suorituskykyjen kehittämistä liittämällä kansallinen teknologian tutkimus osaksi yhteiseurooppalaista tutkimusta, jolloin voidaan saavuttaa synergiaetuja ja kustannussäästöjä sekä luoda edellytyksiä yhteishankkeille, yhteensopivuudelle ja avun vastaanottokyvyille. Teknologian monikäyttöpotentiaalia pyritään kehittämään osallistumalla EDA:n EFC-ohjelmaan. Pohjoismaisen puolustusyhteistyön (NORDEFCO) puitteissa pyritään kehittämään tutkimus- ja evaluointi-

resurssien yhteiskäyttöä sekä tekemään yhteistyötä teknologiaennakoinnin alalla. NATO-yhteistyö liittyy erityisesti toiminnallisen ja teknisen yhteensopivuuden kehittämiseen, tekniikan hankinnassa ja toimittamisessa noudatettaviin menettelyihin sekä koulutukseen.



Monenkeskiseen yhteistyöhön osallistutaan tarvittaessa yhteentoimivuuden kehittämiseksi ja tulevien materiaalihankkeiden kustannusten pienentämiseksi. Kahdenväliseen yhteistyöhön pyritään erityisesti sellaisilla alueilla, joilla teknologian vapautuskysymykset tai kansallisen turvallisuuden kannalta olennaiset salassapitosyyt tätä edellyttävät.

Strategia löytyy internetistä osoitteesta
www.puolustusvoimat.fi/paaesikunta/materiaaliosasto/julkaisut
 ja Torni-portaalista pääesikunta/materiaaliosasto/julkaisut.

Pääesikunta, Materiaaliosasto
 PL 919, 00131 Helsinki

Kuvat: SA-kuva, Scantarp, Desigence, Sensinode

LIITE 1: Kriittiset teknologiat

Informaatioteknologia

Radiotaajuinen tiedonsiirto (HF-SHF-alueet) sisältäen elektronisen suojautumisen (LPI, AJ) ja ohjelmistoradioteknologian (aaltomuodot, kognitiivinen radio, joustava spektrin käyttö)

Tietotekniset arkkitehtuurit, tietoturvallisuus (arkkitehtuuri, ohjelmistot, salaus, autentikointi, pääsyn hallinta), tietoturvallisuuden (IA) ja tietoverkkoturvallisuuden valmiudet (Kyber-strategia), järjestelmien integrointi ja verkottaminen ja yhteensopivuuden varmistaminen sekä elinjakson hallinta (arkkitehtuuri, ohjelmistot, tiedonvaihto, rajapinnat ja protokollat)

Radiotaajuinen elektroninen vaikuttaminen tiedonsiirto-, sensori- ja asejärjestelmiin (häirintä, heitteet), radiotaajuiset sensorit ja signaalinkäsittely (elektroninen tiedustelu ja valvonta, hakupäät)

Optiset sensorit ja hahmontunnistus (tiedustelu ja valvonta, hakupäät), optinen vaikuttaminen ase- ja sensorijärjestelmiin (laser, heitteet)

Aseiden ohjautusmekanismit

Päätöksenteontuki, tiedon hallinta, louhinta ja informaatiofuusio, käsite- ja tiedonvaihtomallit

Vedenalaiset sensorit ja tiedonsiirto

Materiaali- ja rakenneteknologia

Tutkaherätteen hallinta (mmW, SAR; herätausta, kohteen heräte, herätteen pienentäminen, olosuhteiden vaikutus, valemaalien valmistus ja toimivuuden arviointi)

Lämpöherätteen hallinta (herätausta, kohteen heräte, herätteen pienentäminen, olosuhteiden vaikutus, valemaalien valmistus ja toimivuuden arviointi)

Ultravioletialueen herätteen hallinta (lavetit ja asejärjestelmät; herätausta, kohteen heräte, herätteen pienentäminen, olosuhteiden vaikutus)

Ballistinen suoja ja vaikuttaminen (kineettinen, termobarinen)

Vedenalaisten herätteiden hallinta ja vedenalainen vaikuttaminen ja suoja

Sähkömagneettinen suoja (HPM, EMP)

Komposiittimateriaalien korjaus

Systems engineering ja systems-of-systems engineering

Vaatimustenhallinta, puolustusjärjestelmän arkkitehtuurin hallinta sisältäen konfiguraation hallinnan

Ketterä sovelluskehitys

Operaatioanalyysi ja sitä tukeva mallinnus ja simulointi

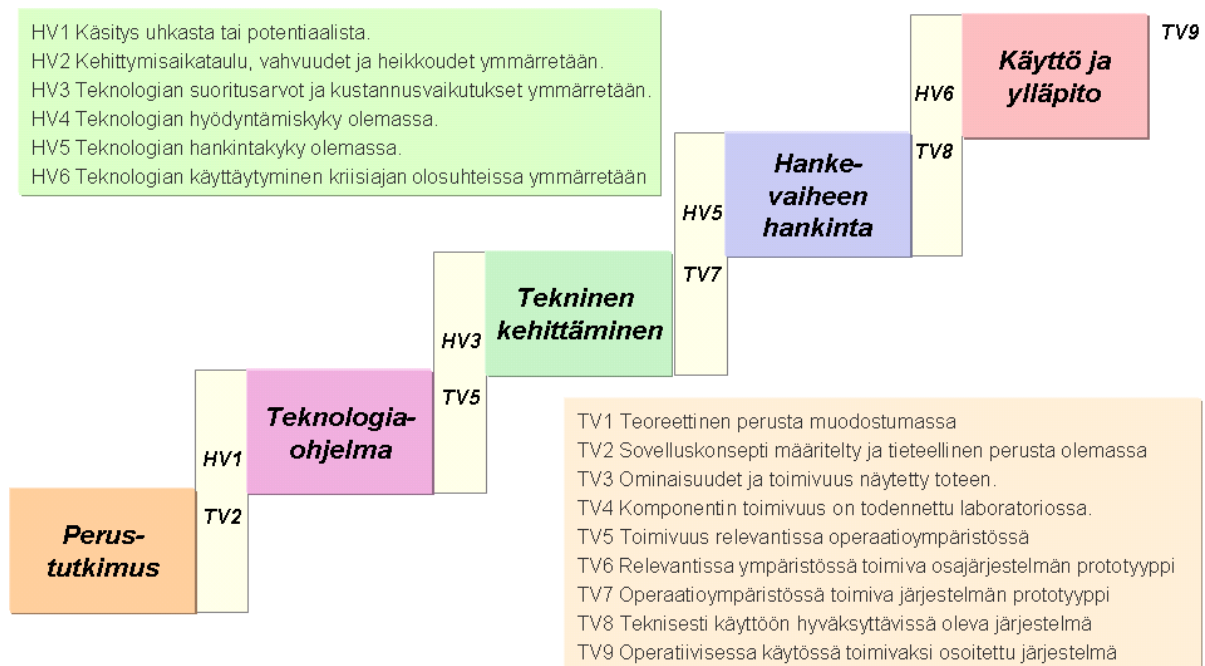
Bio- ja kemianteknologia

Kemiallisten aseiden suojelutiedustelukyky

Biologisten aseiden suojelutiedustelukyky

Räjähdeturvallisuuden varmistavat teknologiat

LIITE 2 Teknologian hankinta- ja toimitusvalmiustasojen kuvaus



Toimitusvalmiustasot perustuvat USAn käyttämiin TRL-tasoihin (Technology Readiness Levels), jotka käytännössä kuvaavat osajärjestelmätoimittajan valmiutta toimittaa laitteisto järjestelmään. Ne eivät kuvaa millään tavoin hankkivan organisaation kykyä toimia kyseisen teknologian osaavana ostajana. Koska puolustusvoimat on ensisijaisesti teknologian ostaja, ei kehittäjä, pelkkä toimitusvalmius ei ole riittävä teknologisen valmiuden kuvaaja.



LIITE 3 Teknologisen tiedon luokittelu



Ellei muuta ole ohjeistettu, noudatetaan seuraavia yleisperiaatteita:

Salaisia ovat

- Salausavainten generointialgoritmit ja väli-
neet sekä generoidut avaimet
- Salausalgoritmien ST II -tasoiseen suojauk-
seen tarkoitettujen algoritmien implemen-
toinnit,
- Tiedustelu-, valvonta-, johtamis-, navigoin-
ti-, paikantamis- ja asejärjestelmien häirin-
näväistömenetelmien parametrit, kuten
todellinen taajuusalue, hyppytnopeus,
levityskaista SA-moodissa.
- Häirintäaaltomuodot ja niiden implemen-
toinnit
- Puolustusjärjestelmän hydroakustiset ja säh-
kömagneettiset herätteet sekä muut sellaiset
herätteet, jotka mahdollistavat ilmaisun,
tunnistamisen ja yksilöinnin
- Asejärjestelmien hakupäiden ja maalin-
seurainten seuranta-algoritmien parametrit,
jotka mahdollistavat häirintämenetelmien
optimoinnin
- Salatun tiedonsiirron takaavien aaltomuoto-
jen implementoinnit, ellei ole erityistä
perustetta pitää niitä luottamuksellisina

Luottamuksellisia ovat

- Salausalgoritmit (COMSEC ja
TRANSEC), elleivät ne ole avoimia
- Tiedustelu-, valvonta-, johtamis-, navi-
gointi-, paikantamis- ja asejärjestelmien
häirinnäväistömenetelmien yksityiskoh-
tainen toteutus sekä menetelmät, jotka
eivät ole yleisesti tiedossa
- Tiedonsiirtoaaltomuodot
- Tiedonvaihdon mallit ja protokollat, ellei-
vät ne ole avoimia
- Toimintaympäristön herätetausta
- Järjestelmäkokonaisuuden EMP/HPM-
suojaustasot
- Asejärjestelmien hakupäiden ja maalin-
seurainten seuranta-algoritmien parametrit
- Suorituskykyyn kohdistuvien analyysien
algoritmit ja toteutukset

Salassa pidettävää on myös lainsäädäntöön tai
sopimusvelvoitteeseen perustuva salassa pidet-
tävä tieto.