

LEADER

Suupohja



KOHTI PUOLUSTUKSEN verkostoja

Raportti

Sisällysluettelo

1.	Hankkeen tarve ja tausta	3
2.	Etelä-Pohjanmaan tilanne puolustusteollisuuden näkökulmasta	3
3.	Puolustusvoimat	3
3.1.1	Puolustusvoimien keskitetty hankintayksikkö (PVLOGL).....	4
3.1.2	Puolustusvoimien kelpoisuusvaatimukset puolustus- ja turvallisuushankinnoissa	4
3.1.3	Mikä on HILMA?	4
3.1.4	Mikä on TED- kanta	4
3.1.5	Puolustusvoimien hankintamenettelyt	5
3.1.6	Tarjoajan soveltuvuus	5
3.1.7	Turvallisuusvaatimukset	5
3.1.8	Kuinka yritys voi päästä Puolustusvoimien toimittajaksi	5
4.	North Atlantic Treaty Organization - NATO	6
4.1.1	Mitä NATO tekee?	6
4.1.2	Yrityksen menestyminen NATO-markkinoilla.....	6
4.1.3	NATO:n hankinnat	7
4.1.4	NSPA ja NCIA	7
4.1.5	NCAGE-koodi	7
4.1.6	NCS – NATO Codification System	8
4.1.7	DoE kelpoisuustodistus (Declaration of Eligibility).....	8
4.1.8	Standardit, standartointi ja yhteentoimivuus	9
4.1.9	AQAP 2110-sertifikaatti	9
4.1.10	ISO 27001	10
4.1.11	Yrityksen turvallisuus selvitys, tietoturvalähteet sekä kyberturvallisuus	10
4.1.12	DIANA (Defence Innovation Accelerator for the North Atlantic)	10
5.	Leader Suupohjan yrityskyselyn tulokset	10
6.	Puolustusteollisuuteen suuntavan konsortion perustaminen	11
7.	Kartoitetut konsortiot, ekosysteemit ja verkostot	12
8.	Yhteenveto.....	15
9.	Lähteet	16

1. Hankkeen tarve ja tausta

Suomen NATO-jäsenyys ja lisääntynyt varautumisen ja puolustuksen tarve globaalissa epävarmuuden ajassa avaa uusia liiketoimintamahdollisuuksia yrityksille. Yksittäisillä yrityksillä ei kuitenkaan usein ole riittäviä resursseja tai osaamista vastata kansainvälisten tarjouskilpailujen vaatimuksiin. Konsortion rakentaminen tai liittyminen olemassa olevaan konsortioon mahdollistaa osaamisen yhdistämisen, riskien jakamisen ja kilpailukyvyyn parantamisen. Hanke vastaa tarpeeseen luoda rakenteita, jotka tukevat yritysten yhteistyötä ja kansainvälistä kasvua turvallisuusalan sektorilla. Nykytilanteessa alueen yrityksillä ei ole selkeää tietoa puolustussektorin markkinoiden edellytyksistä eikä verkostoja, joiden kautta lähteä mukaan. Hankkeen toimien avulla yritykset saavat selkeämmän kuvan puolustusalan mahdollisuuksista, konkreettiset seuraavat askeleet sekä uusia verkostoja, mikä madaltaa kynnystä osallistua tarjouskilpailuihin ja vahvistaa osaamista. Hankkeen tulokset jäävät yritysten ja alueen elinkeinoelämän käyttöön toimintamallina ja tiekarttana, joita voidaan hyödyntää jatkokehittämisessä, uusien yhteistyömuotojen rakentamisessa ja strategisessa päätöksenteossa. Suupohjassa ei ole aiemmin toteutettu vastaavaa esiselvitystä. Tämä esiselvitys tarjoaa paikallisille yrityksille ensimmäisen väylän puolustussektorille ja pohjustaa mahdollista jatkohanketta.

2. Etelä-Pohjanmaan tilanne puolustusteollisuuden näkökulmasta

Etelä-Pohjanmaalla puolustusteollisuuteen liittyvän toiminnan todellinen volyymi on merkittävästi julkikuvaa laajempi, ja alue hyötyy vahvasta huoltovarmuusajattelusta, sisämaan sijainnista sekä korkeatasoisesta teollisesta osaamisesta. Maakunnan yritykset ovat ketteriä ja reagoivat nopeasti markkinoiden muutoksiin.

Alue kohtaa kuitenkin rakenteellisia haasteita. Etelä-Pohjanmaan elinkeinorakenne on perinteisesti alihankintapainotteinen, mikä vaikeuttaa jalansijan löytämistä puolustusteollisuuden toimitusketjuissa. Lisäksi puolustusalan toimijoihin, erityisesti Puolustusvoimiin, koetaan olevan vaikea luoda suoraa yhteyttä, ja markkinoille pääsyyn liittyy paljon byrokratiaa. Yritykset tarvitsevat selkeää erikoistumista ja oman roolinsa määrittelyä puolustussektorilla.

Näiden haasteiden ratkaisemiseksi maakunnassa rakennetaan parhaillaan uutta puolustus- ja huoltovarmuusklusteria. Keskeisiä toimenpiteitä ovat DuoDef EP -hanke, joka kokoaa yhteen alueen yrityksiä ja tutkimusorganisaatioita, sekä Härmänmaan sopimusvalmistuksen kasvuohjelma, joka vahvistaa Kauhavan ja Lapuan alueen yritysten valmiuksia toimia puolustusteollisuuden verkostoissa. Lisäksi maakunnassa on käynnissä useita pienempiä hankkeita, jotka tukevat yritysten kehittymistä.

Etelä-Pohjanmaan yrityksille avautuu merkittäviä mahdollisuuksia erityisesti kaksikäyttöteknologioissa, kuten sensoriratkaisuissa, drone- ja tekoälyteknologioissa, kyberturvallisuudessa ja uusissa materiaaleissa. Pk-yritysten ketteryys ja innovaatiokyky sopivat hyvin alan nopeaan kehitysdynamiikkaan. NATO-jäsenyys avaa uusia verkostoitumis- ja vientimahdollisuuksia, ja rahoituksen tarjonta laajenee muun muassa Business Finlandin, Euroopan puolustusrahaston, Nato DIANA -ohjelman ja ReARM-rahoituksen kautta.

Tämän osio perustuu Riikka Ylikankaan (Team Finland -koordinaattori, Etelä-Pohjanmaa) esittämiin tietoihin, jotka on koottu Kurikan Kohti puolustuksen verkostoja 17.2. tilaisuuden materiaaleista.

3. Puolustusvoimat

Puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtio johdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan kohdistuessa Suomeen.

Puolustusvoimien tehtävät:

- Suomen sotilaallinen puolustaminen.
- Osallistuminen Naton yhteiseen puolustukseen.
- Puolustusvoimat tukevat muita viranomaisia.
- Osallistuminen aluevalvontayhteistyöhön sekä muuhun kansainväliseen avunantoon ja kansainväliseen toimintaan.

- Osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan sekä sotilastehtäviin muussa kansainvälisessä kriisinhallinnassa.

3.1.1 Puolustusvoimien keskitetty hankintayksikkö (PVLOGL)

Puolustusvoimien keskitetty hankintayksikkö vastaa Puolustusvoimien materiaalien, palveluiden ja järjestelmien hankintojen suunnittelusta, kilpailuttamisesta ja toteuttamisesta siten, että hankinnat ovat kustannustehokkaita, yhteensopivia ja tukevat Puolustusvoimien operatiivista suorituskykyä sekä huoltovarmuutta.

Jos yritys haluaa toimia yhteistyössä Suomen Puolustusvoimien kanssa, sen tulee täyttää julkisten hankintojen kelpoisuusvaatimukset. Yrityksen on oltava taloudellisesti ja teknisesti luotettava, noudatettava turvallisuus- ja salassapitovaatimuksia sekä kyettävä toimittamaan tuotteet tai palvelut Puolustusvoimien asettamien ehtojen mukaisesti.

3.1.2 Puolustusvoimien kelpoisuusvaatimukset puolustus- ja turvallisuushankinnoissa

Julkisia hankintoja ohjaavat Suomessa kaksi keskeistä lakia: laki julkisista hankinnoista ja käyttöoikeussopimuksista myöhemmin hankintalaki (1397/2016) ja laki julkisista puolustus- ja turvallisuushankinnoista myöhemmin Putu-laki (1531/2011).

Hankintalakia sovelletaan tavanomaisiin julkisiin hankintoihin – kuten tavaroihin, palveluihin ja rakennusurakoihin – silloin kun hankinnan arvo ylittää 60 000 euroa (EU-kynnysarvo 140 000 €).

Putu-lakia sovelletaan puolustus- ja turvallisuushankintoihin, kuten puolustustarvikkeisiin sekä turvallisuustarkoituksiin käytettäviin tavaroihin ja palveluihin. Lain soveltaminen tulee kyseeseen, kun hankinta ylittää 100 000 euroa (EU-kynnysarvo 432 000 €). Putu-laki on tarkoitettu tilanteisiin, joissa hankinnan kohde on sotilaalliseen käyttöön suunniteltu ja löytyy EU:n yhteisestä puolustustarvikeluettelosta.

Keskeisimmät erot lakien välillä liittyvät kynnysarvoihin, soveltamisalaan sekä hankintamenettelyihin. Puolustus- ja turvallisuushankintalaissa ei käytetä avointa menettelyä samassa muodossa kuin yleisessä hankintalaissa.

Kaksikäyttötuotteiden osalta ratkaisevaa on, löytyykö tuotteelle soveltuva kohta EU:n puolustustarvikeluettelosta. Jos löytyy, Putu-lain soveltaminen on perusteltua; muissa tapauksissa voidaan käyttää hankintalakia.

Lisäksi hankintalainsäädännön tulkintaan vaikuttaa SEUT 346 -artikla, joka mahdollistaa poikkeamisen hankintadirektiivistä silloin, kun rajoitukset ovat tarpeen keskeisten turvallisuusetujen suojelemiseksi.

Puolustusvoimien oma hankintamääräys täydentää lainsäädäntöä ja sitä sovelletaan kaikissa hankinnoissa. Se sisältää muun muassa hintatiedusteluelvoitteen, kun hankinnan arvo ylittää 30 000 euroa. Kansallisen kynnysarvon alittavat pienhankinnat eivät kuulu hankintalainsäädännön soveltamisalaan, eikä niistä ole lakisäateistä ilmoittamisvelvollisuutta. Niiden toteutusta ohjaa kuitenkin Puolustusvoimien oma hankintamääräys.

Kansalliset kynnysarvot ylittävät hankinnat ilmoitetaan Hilma-palvelussa. EU-kynnysarvot ylittävät hankinnat julkaistaan lisäksi EU:n virallisessa lehdessä ja TED-tietokannassa (Tenders Electronic Daily).

3.1.3 Mikä on HILMA?

Hilma on julkisten hankintojen palvelu, jossa julkisen sektorin ostajat voivat kilpailuttaa hankintojaan sekä ilmoittaa tulevista hankinnoistaan, käynnissä olevista kilpailutuksistaan ja päättyneiden kilpailutustensa tuloksista.

Julkisten hankintojen neuvontayksikkö auttaa yrittäjiä antamalla ohjeita hankintamenettelyistä, kilpailutusvaatimuksista ja turvallisuusvaatimuksista sekä selventämällä, miten yritys voi osallistua Puolustusvoimien tarjouskilpailuihin. Katso lisää: <https://www.hankintailmoitukset.fi/fi/>

3.1.4 Mikä on TED- kanta

TED kanta tarkoittaa TED (Tenders Electronic Daily) järjestelmää, joka on Euroopan unionin virallinen julkisten hankintojen tietokanta. Se on EU:n virallisen lehden liitteen (Supplement to the Official Journal, S-

sarja) sähköinen versio, jossa kaikki EU:n kynnysarvot ylittävät julkiset hankinnat julkaistaan. TED on yrityksille tärkeä, koska se on EU:n virallinen julkisten hankintojen tietokanta, johon kaikki EU-kynnysarvot ylittävät hankinnat on pakko julkaista. Sen kautta yritys voi etsiä tarjouskilpailuja koko Euroopan alueelta, mikä avaa pääsyn laajoihin markkinoihin ja kansainvälisiin liiketoimintamahdollisuuksiin. Lisäksi hankintailmoitukset ovat saatavilla kaikilla 24 EU-kielillä, mikä helpottaa osallistumista eri maiden kilpailutuksiin ja lisää tiedon saavutettavuutta. Katso lisää: <https://ted.europa.eu/fi/>

3.1.5 Puolustusvoimien hankintamenettelyt

Hankinnassa määritellään aina ehdottomat ja mahdolliset toivottavat vaatimukset. Kaikkien ehdottomien vaatimusten on täyttyvä, muuten tarjous hylätään. Toivottavista vaatimuksista voidaan antaa lisäpisteitä, jos näin on ilmoitettu tarjouspyynnössä.

Täytetyt vaatimukset sitovat sopimuksessa, ja tuotteen on täytettävä ne ennen vastaanottoa ja maksua.

Valinta tehdään joko halvimman hinnan perusteella tai kokonaistaloudellisen edullisuuden mukaan, jolloin tarjoukset pisteytetään ennalta ilmoitetuilla kriteereillä ja painoarvoilla. Vertailu on tehtävä täsmälleen tarjouspyynnön mukaisesti. Hankintamenettelyjä on pääsääntöisesti kolme:

Avoin menettely:

Kaikki halukkaat voivat jättää tarjouksen suoraan hankintailmoituksen ja tarjouspyynnön perusteella. Tarjoukset vertaillaan ennalta ilmoitettujen perusteiden mukaisesti.

Rajoitettu menettely:

Hankintailmoituksessa esitetään soveltuvuusvaatimukset, joiden perusteella valitaan ehdokkaat tekemään varsinainen tarjous. Vertailu tehdään tarjouspyynnössä ilmoitetuin perustein.

Neuvottelumenettely:

Soveltuvuusvaatimusten perusteella valitut ehdokkaat jättävät alustavan tarjouksen. Tämän pohjalta käydään neuvottelut, minkä jälkeen annetaan tarkennettu tarjouspyyntö ja pyydetään lopulliset tarjoukset. Vertailu tehdään ilmoitettujen kriteerien mukaisesti.

3.1.6 Tarjoajan soveltuvuus

Soveltuvuusvaatimuksilla varmistetaan, että toimittajalla on edellytykset toteuttaa hankinta. Ne voivat koskea esimerkiksi toimittajan rekisteröitymistä, taloudellista ja rahoituksellista tilannetta, teknistä ja ammatillista pätevyyttä sekä kokemusta vastaavista toimituksista. Puolustus- ja turvallisuushankinnoissa voidaan lisäksi asettaa tietoturvaan ja huoltovarmuuteen liittyviä vaatimuksia. Tällaisia voivat olla esimerkiksi valmius solmia turvallisuussopimus tai riittävä kotimainen valmistus- tai huoltokapasiteetti.

3.1.7 Turvallisuusvaatimukset

Turvallisuusvaatimukset voivat kohdistua sekä tarjoajaan että hankinnan kohteeseen. Toimintaa ohjaavat muun muassa julkisuuslaki (621/1999), Puolustusvoimien tietoturvallisuusmääräys (HQ97) sekä Puolustusvoimien sidosryhmäturvallisuusohje (HS511).

Sidosryhmällä tarkoitetaan kaikkia Puolustusvoimien ulkopuolisia tahoja, joiden kanssa puolustusvoimat tekevät yhteistyötä. Sidosryhmäturvallisuudella tarkoitetaan niitä menettelyjä ja toimenpiteitä, joilla turvataan salassa pidettävä tai turvallisuusluokiteltu tieto yhteistyön aikana.

Salassa pidettävää tietoa voidaan luovuttaa sidosryhmälle tai sen henkilöstölle vasta, kun sidosryhmän turvallisuusjärjestelyt on varmistettu ja turvallisuusmenettelyistä on sovittu.

3.1.8 Kuinka yritys voi päästä Puolustusvoimien toimittajaksi

Yritys voi päästä Puolustusvoimien toimittajaksi ensisijaisesti osallistumalla julkisiin tarjouskilpailuihin. Keskeistä on kehittää aidosti kilpailukykyinen tuote tai palvelu, joka tukee Puolustusvoimien suorituskykyä ja vastaa sen operatiivisiin tarpeisiin. Erityisen vahvassa asemassa ovat yritykset, jotka toimivat toimialoilla, joilla teknologinen osaaminen muodostaa merkittävän kansallisen turvallisuusedun.

Suorat yhteydenotot ja tuote-esittelyt johtavat harvoin hankintoihin, sillä ostot perustuvat pääosin kilpailutuksiin ja tarkkoihin kelpoisuusvaatimuksiin, kuten taloudelliseen vakavaraisuuteen, laatu- ja

tietoturvastandardeihin sekä tarvittaessa turvallisuusselvityksiin. Käytännössä monelle yritykselle realistisin reitti on hakeutua alihankkijaksi Puolustusvoimien strategisille kumppaneille, kuten Patrialle tai Milloglle, ja rakentaa sitä kautta asemaa puolustussektorin toimitusketjussa.

Kilpailutuksiin osallistumisen ohella verkostoituminen on keskeistä. Esimerkiksi puolustus- ja turvallisuusalan messut, toimialajärjestöt sekä Business Finlandin puolustussektorin ohjelmat tarjoavat mahdollisuuksia rakentaa kontakteja, ymmärtää tulevia tarpeita ja asemoida oma osaaminen osaksi laajempaa puolustusteollista ekosysteemiä.

Tämän osion tiedot perustuvat Puolustusvoimien logistiikkalaitoksen esikunnan kehittämisjohtaja Kai Laineen (PVLOGL) esittämiin tietoihin. Aineisto on koottu Kurikan Kohti puolustuksen verkostoja -tilaisuuden (17.2.) materiaaleista sekä Puolustusvoimien verkkosivujen julkaisemista tiedoista.

4. North Atlantic Treaty Organization - NATO

NATO on lyhenne englanninkielisistä sanoista North Atlantic Treaty Organization, joka suomeksi tarkoittaa Pohjois-Atlantin puolustusliittoa. NATO on sotilasliitto, joka perustettiin vuonna 1949 turvaamaan jäsenmaidensa yhteinen puolustus ja turvallisuus. Vuonna 2025 NATOssa on 32 jäsenmaata, mukaan lukien kaikki Pohjois-Amerikan ja useimmat Euroopan maat. Suomi liittyi 4. huhtikuuta 2023.

4.1.1 Mitä NATO tekee?

NATO on jäsenmaidensa välinen sotilasliitto, jonka ensisijainen tehtävä on kollektiivinen puolustus. Hyökkäys yhtä jäsenmaata vastaan katsotaan hyökkäykseksi kaikkia vastaan, ja jäsenet sitoutuvat auttamaan toisiaan puolustuksessa tarvittaessa. Tämä on liittokunnan ydintehtävä.

Nato toimii myös kriisinhallinnassa ja pyrkii ehkäisemään kriisejä sekä hallitsemaan niitä ennen, niiden aikana ja jälkeen konfliktien. Liitto käyttää sekä poliittisia että sotilaallisia keinoja tilanteiden hallintaan ja osallistuu tarvittaessa rauhanturva- ja vakauden tukemisen operaatioihin.

Yhteistyö on olennainen osa Naton toimintaa. Jäsenmaat harjoittelevat yhdessä ja kehittävät yhteisiä sotilaallisia ja poliittisia standardeja, jotta joukot voivat toimia tehokkaasti yhdessä. Tähän kuuluu myös teknologinen ja sotilaallinen yhteensopivuus, eli kyky käyttää ja jakaa järjestelmiä, tiedonvaihtoa ja toimintatapoja niin, että erilaiset joukot ja teknologiat toimivat saumattomasti yhteen.

NATO järjestää säännöllisesti yhteisiä harjoituksia ja operaatioita, joiden avulla jäsenmaat ylläpitävät valmiutta, kehittävät kykyjään ja varmistavat tehokkaan yhteistyön kaikissa mahdollisissa turvallisuustilanteissa.

4.1.2 Yrityksen menestyminen NATO-markkinoilla

1. Tunnistakaa yrityksenne vahvuudet ja rooli NATO-markkinoilla

Kartoittakaa yrityksenne ydinosaaminen, teknologiset vahvuudet ja kilpailuedut. Pk-yritysten etuna on ketteryys, nopea reagointikyky ja erikoistunut osaaminen. Suuret toimijat arvostavat joustavuutta ja syvää teknistä kompetenssia, ja suomalaisilla yrityksillä on usein vahva kyky toimia vaativissa olosuhteissa (esim. arktinen ympäristö tai erikoisteknologia). Arvioikaa, millaista osaamista yrityksellänne on, jota NATO tai jäsenmaat voivat tarvita.

2. Perehtykää NATO:n hankintakäytäntöihin ja toimijoihin ja rekisteröitykää NATO hankintayksiköiden verkkoportaaleihin.

NATO-hankkeissa on omat prosessinsa, organisaationsa ja ilmoituskanavansa. Keskeisiä toimijoita ovat mm.

NSPA (NATO Support and Procurement Agency)

NCIA (NATO Communications and Information Agency)

Yrityksen kannattaa selvittää, miten rekisteröityminen, hankintaportaalit, tarjouskilpailut ja sopimusmenettelyt toimivat. Näiden tuntemus nopeuttaa markkinoille pääsyä ja kasvattaa kilpailukykyä.

3. Hankkikaa rekisteröitymiseen liittyen NATO kelpoisuusvaatimustodistus DOE

DoE-kelpoisuustodistus (Declaration of Eligibility) on keskeinen edellytys NATO-hankintoihin osallistumiselle. Se on Puolustusvoimien myöntämä virallinen hyväksyntä, joka varmistaa

yrittäjien luotettavuuden ja soveltuvuuden NSPA:n ja NCIA:n kilpailutuksiin. Ilman tätä todistusta yritys ei voi osallistua kyseisiin tarjousprosesseihin.

- 4. Rakentakaa kumppanuuksia – yhteistyö on tehokkain reitti NATO-markkinoille**
NATO-markkinoille ei mennä yksin. Pk-yrityksille ensimmäinen askel on usein yhteistyö suuremman toimijan kanssa, osana tämän alihankintaketjua. Kumppanuudet avaavat ovia, jakavat riskejä ja lisäävät uskottavuutta.
- 5. Varmistakaa lainsäädännön, laatujärjestelmien ja turvallisuusvaatimusten täyttyminen**
Huolehdi siitä, että tuotteenne ja prosessinne täyttävät turvallisuus- ja laatuluokitukset. Investoi kyberturvallisuuteen, laadunhallintaan ja toimitusvarmuuteen. Luotettavuus on arvokas kilpailuvälittö. Selvittäkää, mitä vaatimuksia AQAP-laatujärjestelmät ja STANAG-standardit asettavat. (AQAP – Allied Quality Assurance Publications, STANAG – Standardization Agreement)
- 6. Kehittäkää näkyvyyttä ja verkostoja puolustussektorilla**
Osallistukaa puolustus- ja turvallisuusalan tapahtumiin, foorumeihin ja messuihin. Verkostoituminen lisää tunnettuutta ja luottamusta, jotka ovat edellytyksiä yhteistyölle kansainvälisten toimijoiden kanssa. Yrityksen kannattaa hyödyntää myös kotimaisia ja alueellisia verkostoja, jotka toimivat sillanrakentajina puolustusalan markkinoille.

4.1.3 NATO:n hankinnat

Kaupallinen toiminta Naton eri organisaatioiden kanssa noudattaa yhteisiä periaatteita, mutta käytänteet vaihtelevat jossain määrin. Yleisesti yritykseltä edellytetään rekisteröitymistä ja puolustusvoimien logistiikkalaitoksen antamaa kelpuutustodistusta (DoE= Declaration of Eligibility). Lisäksi turvaluokitelluissa tapauksissa tarvitaan kansallisen turvallisuusviranomaisen todistus. Yhteistä NATO:n hankintaorganisaatioille on pyrkiä suosimaan hankinnoissa jäsenmaiden yrityksiä ja toteuttaa hankinnat ensisijaisesti kansainvälisinä kilpailutuksina. Hankinnat julkaistaan NATO:n portaaleissa tietoturvan mahdollistamissa puitteissa ja ovat saatavilla rekisteröityneille käyttäjille.

Yrittäjien kannalta merkittäviä hankinta- ja yhteistyöorganisaatioita ovat Naton logistiikka- ja hankintavirasto (NSPA) sekä Naton tietojärjestelmävirasto (NCIA).

4.1.4 NSPA ja NCIA

NSPA (NATO Support and Procurement Agency) on Naton logistiikka- ja hankintavirasto, joka vastaa jäsenmaiden yhteisten materiaalien, palvelujen ja järjestelmien hankinnoista sekä niiden elinkaaren aikaisesta tuesta. Yrityksen näkökulmasta NSPA on tärkeä, koska suuri osa puolustusmateriaalihankinnoista kulkee tämän viraston kautta, ja rekisteröityminen NSPA:n järjestelmiin sekä DOE-kelpoisuuden saaminen ovat keskeisiä edellytyksiä osallistumiselle Naton tarjouskilpailuihin ja toimitusketjuihin.

NCIA (NATO Communications and Information Agency) hankkii sekä nopeasti käyttöön otettavia kaupallisia IT- ja viestintäratkaisuja että suuria, kansainvälisesti kilpailutettuja järjestelmäkokonaisuuksia. Yhteistyö NCIA:n kanssa avaa yrittäjille pääsyn kansainvälisille markkinoille, pitkäjänteisiin hankintoihin ja korkean turvallisuustason projekteihin erityisesti kyberturvallisuuden, komentamis- ja johtamisjärjestelmien, data-analytiikan ja viestintäteknologioiden alueilla.

Edellä mainittujen virastojen lisäksi myös Naton muut organisaatiot (esim. ACT - Allied Command Transformation ja STO - Science- and Technology Organization) hankkivat tarvitsemiaan palveluita ja tuotteita. Virastojen ja organisaatioiden kilpailutuksiin voivat osallistua lähtökohtaisesti kaikki kelvolliset jäsenmaiden yritykset.

4.1.5 NCAGE-koodi

NCAGE-koodi (NATO Commercial and Government Entity): on ensimmäinen konkreettinen askel puolustus- ja NATO-markkinoille. Yrityksille, jotka harkitsevat kansainvälisiä puolustussektorin markkinoita, NCAGE-koodi kannattaa hakea varhaisessa vaiheessa osana markkinoille menon valmistelua.

NCAGE-koodi on Naton myöntämä viisinumeroinen tunniste, jolla yksilöidään yritykset ja organisaatiot puolustus- ja turvallisuushankinnoissa. NCAGE koodi vastaa suomalaista Y-tunnusta.

Sitä käytetään erityisesti Nato- ja EU-projekteissa sekä kansainvälisissä tarjouskilpailuissa toimittajien tunnistamiseen. Suomessa NCAGE-koodi tarvitaan, jos yritys haluaa osallistua Naton tai muiden maiden puolustushankintoihin. NCAGE-koodi avaa oven tarjouskilpailuihin.

Miten NCAGE-koodi haetaan?

1. Yritys tekee hakemuksen NSPA:n sähköisessä palvelussa
– Koodi haetaan NSPA:n Cage Code Request Tool -portaalin kautta:
eportal.nspa.nato.int/Codification/CageTool/home
2. Hakemus siirtyy automaattisesti Suomen Puolustusvoimien Nimikkeistökeskukseen
– Suomessa NCAGE-koodit myöntää Puolustusvoimien Nimikkeistökeskus.
3. Nimikkeistökeskus käsittelee hakemuksen ja myöntää koodin
– Koodin myöntämisen jälkeen yritys voidaan liittää NATO-nimikkeistöjärjestelmään.

NCAGE-koodin saamisen jälkeen yrityksen kannattaa hakea tuotteilleen NSN-koodit, jotta ne voidaan liittää NATO-nimikkeistöjärjestelmään ja hyväksyä käytettäviksi NCS-järjestelmän mukaisissa hankinnoissa.

4.1.6 NCS – NATO Codification System

NATO Codification System (NCS) on järjestelmä, jonka avulla puolustussektorin tuotteet tunnistetaan ja luokitellaan yhtenäisellä tavalla NATO-maiden välillä. Sen kautta yrityksen tuotteille voidaan antaa NSN-tuotenumero (NATO Stock Number) mikä mahdollistaa tuotteiden kansainvälisen tunnistettavuuden ja yhteensopivuuden. NSN- koodin voi saada tuotteelle, jos se on jo käytössä jossain NATO maassa. Koodin voi hakea kyseisen maan asevoimat. Pyyntö koodin hakemisesta tulee tehdä yhdessä asevoimien edustajien kanssa. Koodin saamisen jälkeen se näkyy NATO:n yhteisessä kalustokatalogissa ja helpottaa esim varaosahankintoja. Suomessa nimikoinnista vastaa Puolustusvoimien Nimikkeistökeskus. NCS-nimikointi on keskeinen edellytys osallistumiselle NATO-hankintoihin ja puolustusmateriaalien toimitusketjuihin.

Mikä on NCS?

- Järjestelmä, joka antaa jokaiselle tuotteelle yksilöllisen NATO-tuotenumero NSN:n (NATO Stock Number).
- Mahdollistaa, että eri maiden puolustusvoimat voivat tunnistaa ja käyttää toistensa tuotteita ilman tulkintaongelmia.
- Tärkeä osa NATO-yhteensopivuutta ja materiaalin yhteiskäyttöä.

Suomessa Puolustusvoimien Nimikkeistökeskus vastaa NSN-nimiköinnistä.

4.1.7 DoE kelpoisuustodistus (Declaration of Eligibility)

Oleellinen askel on DoE-kelpoisuustodistuksen hankkiminen. DoE-kelpoisuustodistus on NATO-hankinnoissa käytettävä virallinen hyväksyntä, jolla Puolustusvoimat vahvistaa yrityksen olevan taustoiltaan ja toimintakyvyiltään soveltuva NSPA:n ja NCIA:n kilpailutuksiin. Ilman DoE kelpoisuustodistusta yritys ei voi osallistua näiden organisaatioiden tarjousprosesseihin. Puolustusvoimat (PVLOGLE KAUPOS) tarkistaa yrityksen taustat ja antaa DoE-todistuksen NSPA:lle/NCIA:lle Suomen NATO-edustuston kautta.

Miten DoE kelpoisuustodistusta haetaan?

1. Yritys hakee rekisteröitymistä esimerkiksi NSPA:n tai NCIA:n portaaleihin.
2. NSPA/NCIA pyytää Suomelta DoE-kelpoisuustodistusta yritystä varten.
3. Puolustusvoimat tarkistaa yrityksen taustat ja antaa DoE-kelpoisuustodistuksen NSPA:lle/NCIA:lle Suomen NATO-edustuston kautta.
4. Yritys hyväksytään rekisteriin ja voi osallistua kilpailutuksiin.

Jos NSPA/NCIA ohjeistaa, yritys voi myös itse pyytää DoE kelpoisuustodistusta Puolustusvoimista — tällöin pyyntö ohjataan osoitteeseen kirjaamo.pvlogle@mil.fi.

4.1.8 Standardit, standartointi ja yhteentoimivuus

NATO jäsenmaiden kehittämien suorituskykyjen yhteentoimivuus (Interoperability) varmistetaan yhteisillä standardeilla ja standardien käytöllä, testeillä ja harjoituksilla.

STANAG (Standardization Agreement) on NATO:n jäsenmaiden välinen sopimus yhteisistä standardeista, joiden tarkoituksena on varmistaa yhteentoimivuus – eli se, että eri maiden joukot ja varusteet toimivat saumattomasti yhdessä. STANAGit kattavat esimerkiksi viestinnän, ammusten mitat, kaluston yhteensopivuuden ja toimintamenetelmät. Jos yritys tähtää NATO-markkinoille, sen pitää varmistaa, että sen tuotteet tai palvelut täyttävät tarvittavat STANAG-standardit, jotta ne ovat yhteensopivia NATO-maiden järjestelmien kanssa.

Lue lisää: <https://www.nato.int/en/what-we-do/deterrence-and-defence/standardization>

Naton standardien hallinnoinnista vastaa Nato Standardization Office (NSO). Standardeista osa on julkisia, mutta osa on ei-julkisia tai turvaluokiteltuja. Lue lisää: <https://nso.nato.int>

4.1.9 AQAP 2110-sertifikaatti

AQAP-sertifiointi vahvistaa yrityksen valmiuksia toimia puolustusalan vaativissa toimitusketjuissa. Sertifiointi mahdollistaa osallistumisen Naton tarjouskilpailuihin sekä osoittaa yrityksen sitoutumisen kansainvälisesti tunnustettuihin laatustandardeihin. AQAP-vaatimusten käyttöönotto parantaa organisaation riskienhallintaa, jäljitettävyyttä ja prosessien hallintaa, mikä lisää kilpailukykyä puolustusteollisuuden hankinnoissa. Sertifikaatti tarjoaa myös asiakkaille ja yhteistyökumppaneille varmuuden tuotteiden ja palvelujen laadusta sekä tukee toimintojen jatkuvaa kehittämistä ja puolustusalan muuttuvien vaatimusten noudattamista.

AQAP-sertifiointiprosessi etenee vaiheittain ja alkaa palvelun validoinnista, jossa varmistetaan sertifiointiin liittyvät akkreditointivaatimukset sekä mahdolliset maakohtaiset edellytykset. Tämän jälkeen tehdään alustava arviointi, jossa tarkastellaan yrityksen nykyistä laadunhallintajärjestelmää ja tunnustetaan AQAP 2110 -standardin edellyttämät puutteet ja kehityskohteet. Arvioinnin pohjalta siirrytään valmisteluvaiheeseen, jossa yritystä tuetaan tarvittavien lisäprosessien rakentamisessa, kuten riskienhallinnan, jäljitettävyyden ja konfiguraationhallinnan kehittämisessä.

Kun tarvittavat valmiudet on luotu, sertifiointielin suorittaa varsinaisen tarkastuksen eli auditoinnin, jossa arvioidaan AQAP 2110 -vaatimusten ja ISO 9001 -standardin noudattaminen. Mahdolliset havaitut puutteet korjataan korjaavien toimenpiteiden vaiheessa ennen sertifiointipäätöstä. Kun kaikki vaatimukset täytyvät, yritykselle myönnetään AQAP 2110 -sertifikaatti. Sertifioinnin jälkeen yritys osallistuu säännöllisiin valvontatarkastuksiin, joiden tarkoituksena on varmistaa jatkuva vaatimustenmukaisuus ja laadunhallintajärjestelmän ylläpito.

Yritys voi valmistautua AQAP-sertifiointiin mm seuraavilla toimilla:

1. Varmistamalla vahva ISO 9001 -pohja
2. Analysoimalla yrityksen nykytila
3. Kehittämällä AQAP-vaatimusten edellyttämät keskeiset laadunvarmistusprosessit
4. Kouluttamalla henkilöstöä ja sitouttamalla yrityksen johtoa prosessiin
5. Päivittämällä yrityksen dokumentaatio vastaamaan AQAP-vaatimuksia
6. Suorittamalla yrityksessä sisäisen auditoinnin
7. Valitsemalla sertifioinnin suorittajan hyvissä ajoin.

Ennen kuin yritys voi saada AQAP-sertifikaatin, sen täytyy laittaa oma laadunhallinta kuntoon. AQAP perustuu ISO 9001 -standardin vaatimuksiin, joten yrityksellä täytyy olla toimiva ISO 9001-tasoinen järjestelmä. Varsinaista ISO-sertifikaattia ei ole pakko olla, mutta yrityksen on pystyttävä näyttämään, että sen toimintatavat täyttävät ISO 9001:n perusvaatimukset. Tämän jälkeen yrityksen kannattaa selvittää, missä kohdin sen nykyiset toimintatavat eivät vielä vastaa AQAP-vaatimuksia. Sen tarkoitus on yksinkertaisesti löytää ne kohdat, joita pitää parantaa ennen auditointia. AQAP edellyttää myös joitakin lisäkäytäntöjä, joita ISO 9001 ei sisällä yhtä tarkasti. Näitä ovat esimerkiksi riskienhallinta, selkeä jäljitettävyyden, muutosten hallinta sekä projektikohtainen laadunvarmistus. Nämä prosessit kannattaa rakentaa valmiiksi jo ennen auditointia, jolloin sertifiointi etenee sujuvammin.

Henkilöstön koulutus ja johdon sitoutuminen ovat tärkeitä, koska AQAP vaikuttaa koko yrityksen toimintaan. Kaikkien tulee tietää, mitä vaatimuksia se tuo heidän omalle työlleen. Ennen virallista auditointia yrityksen

kannattaa tehdä oma sisäinen tarkastus. Se auttaa löytämään puutteet ajoissa ja korjaamaan ne, jolloin varsinainen auditointi onnistuu paremmin. Lopuksi on hyvä valita sertifiointiorganisaatio jo varhaisessa vaiheessa, koska heiltä saa neuvoja, aikataulun ja selkeät ohjeet etenemisestä.

4.1.10 ISO 27001

ISO 27001 on kansainvälinen standardi tietoturvallisuuden hallintajärjestelmälle (ISMS). Se auttaa organisaatioita rakentamaan järjestelmällisen ja jatkuvasti kehittyvän tavan suojata tietojaan.

NATO- hankkeissa yrityksen tulee osoittaa kykynsä käsitellä tietoa turvallisesti. ISO 27001 antaa rakenteen, joka tukee turvallisuusluokitellun tiedon hallintaa ja helpottaa viranomaisten hyväksyntäprosessien läpisyä. Standardi auttaa yritystä ymmärtämään tietoturvariskinsä ja rakentamaan niihin sopivat hallintatoimet. Monet puolustussektorin ja kansainväliset kumppanit vaativat tai suosivat ISO 27001-sertifioituja toimijoita.

4.1.11 Yrityksen turvallisuus selvitys, tietoturvalähteet sekä kyberturvallisuus

Suojelupoliisi voi tehdä yritysturvallisuus selvityksen suomalaisesta yrityksestä, joka toimii viranomaisen sopimuskumppanina ja tarvitsee oikeuden käsitellä turvallisuusluokiteltuja kansallisia tai kansainvälisiä viranomaistietoja. Jos yrityksen on tarkoitus hoitaa puolustusvoimien antamaa tehtävää tai yritys liittyy puolustusvoimien hankintoihin, yritysturvallisuus selvityksen laatii pääesikunta.

Kun suomalaiset yritykset osallistuvat kansainvälisiin hankkeisiin tai tarjouskilpailuihin, ne saattavat käsitellä kansainvälistä turvallisuusluokiteltua viranomaistietoa. Silloin Suojelupoliisi (Designated Security Authority, DSA) laatii suomalaisten yritysten yritysturvallisuus selvitykset (FSC) kansallisen turvallisuusviranomaisen NSA:n pyynnöstä. Turvallisuus selvitys on usein edellytys puolustus- ja turvallisuushankinnoille, joten ilman yritysturvallisuus selvitystä yritys voi jäädä kilpailutuksen ulkopuolelle. Hyvän käsityksen turvallisuuteen liittyvistä vaatimuksista saa Katakri 2020-dokumentista. Katakri (Kansallinen turvallisuus auditointikriteeristö) on suomalainen viranomaisten työkalu organisaatioiden tietoturvallisuuden arviointiin.

Lakia kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sovelletaan erityissuojattaviin tietoaineistoihin. Laki 588/2004 koskee yrityksiä silloin, kun ne osallistuvat turvallisuusluokiteltua tietoa sisältäviin NATO- tai puolustushankintoihin. Yrityksen on tällöin täytettävä kansainväliset tietoturva vaatimukset ja suoritettava tarvittavat yritysturvallisuus selvitykset (FSC) ja mahdolliset henkilöturvallisuus selvitykset, jotta se voi käsitellä salassa pidettävää materiaalia hankinnan eri vaiheissa. Tämä on edellytys sille, että yritys voi osallistua kilpailutuksiin, joissa käsitellään luokiteltua tietoa.

Kyberturvallisuuskeskus tarjoaa lakisääteisiä arviointi- ja hyväksyntä palveluja organisaatioille, jotka käsittelevät kansallisesti tai kansainvälisesti turvallisuusluokiteltua tietoa. Palvelua annetaan erityisesti valtionhallinnolle, huoltovarmuuskriittisille toimijoille sekä yrityksille, jotka hakeutuvat yritysturvallisuus selvitykseen (FSC) tai osallistuvat EU- tai NATO-tiedon käsittelyä edellyttäviin hankkeisiin.

4.1.12 DIANA (Defence Innovation Accelerator for the North Atlantic)

DIANA on NATO:n perustama innovaatio-ohjelma, joka tukee yrityksiä kehittämään kaksikäyttöisiä (dual-use) teknologioita, joilla voidaan ratkaista liittokunnan keskeisiä puolustus- ja turvallisuus haasteita. DIANA tarjoaa yrityksille mahdollisuuden kehittää ja testata kaksikäyttö teknologioita NATO-tasoisessa innovaatio ympäristössä. Yritykset voivat saada rahoitusta, asiantuntijamentorointia, sekä pääsyn laajaan verkostoon, joka sisältää yli 200 kiihdyttämöä ja yli 180 testikeskusta eri NATO-maissa. Tämä helpottaa teknologioiden nopeaa kehitystä, validointia ja markkinoille pääsyä niin siviili- kuin puolustus sektorille. Lisätietoa: <https://www.diana.nato.int>

5. Leader Suupohjan yrityskyselyn tulokset

Kysely toteutettiin Leader Suupohjan alueella 11/25–1/26 välisenä aikana. Kuntien elinkeinon kanssa kartoitettiin alueelta potentiaaliset yritykset, koostettiin yrityskysely ja lähetettiin se kartoitetuille yrityksille. Lisäksi kyselyä jaettiin alueen yrittäjä yhdistyksiin, yrityskyselystä kerrottiin sosiaalisen median kanavissa, uutiskirjeissä sekä suorissa yhteydenotoissa yritys siin.

Kyselyyn vastanneista 33 yrityksestä valtaosa näki merkittävää kasvupotentiaalia puolustus-, turvallisuus- ja NATO-markkinoilla sekä kaksikäyttö tuotteiden parissa. Vastanneista yrityksistä 17 oli alle 10 henkilöä

työllistäviä mikroyrityksiä, 12 oli 10–49 henkilöä työllistäviä pienyrityksiä, 2 oli 50–249 henkilöä työllistäviä yrityksiä. Kaksi vastaajista ilmoitti toimivansa yksinyrittäjänä. Vastaukset vahvistivat jo olemassa oleva tietoa, että suuri osa alueemme yrityksistä toimivat valmistavan teollisuuden parissa: kone- ja laitevalmistus sekä metalliteollisuus muodostivat yhdessä lähes 40 % kaikista vastauksista. Lisäksi nousivat esille elintarviketeollisuus, erilaiset palvelualat, rakentaminen puu- ja huonekaluteollisuus sekä asiantuntijapalvelut. Yritysten aiempi kokemus julkisista hankinnoista ja korkean turvallisuuden toimintaympäristöistä vaihteli merkittävästi. Osalla yrityksistä on kohtuullista tai hyvää kokemusta, mutta monilla kokemus on vähäistä tai olematonta. Laatu-, tietoturva- ja sertifiointikäytännöissä on havaittavissa selkeitä kehitystarpeita. ISO 9001 -sertifikaatti tai vastaava laatujärjestelmä on käytössä vain osalla yrityksistä, mikä kertoo laadunhallinnan vaihtelevasta kypsyydestä. Puolustussektorin erityisvaatimuksiin liittyvät järjestelmät, kuten AQAP, puuttuvat useimmilta toimijoilta, mikä voi rajoittaa mahdollisuuksia toimia vaativissa puolustusalan hankkeissa.

Tietoturvallisuuden osalta ISO 27001 -standardin mukaiset hallintajärjestelmät ovat vielä harvinaisia, vaikka niiden merkitys ja tarve tiedostetaan aiempaa paremmin. Useat yritykset pystyvät ainakin osittain dokumentoimaan tuotantoketjunsä ja varmistamaan jäljitettävyyden. Valmius henkilöstön turvallisuusselvityksiin on pääosin hyvä. Yritykset tunnistivat tämän keskeiseksi edellytykseksi puolustus- ja turvallisuussektorilla toimimiselle. Useilla yrityksillä on jonkin verran vientikokemusta tai halukkuutta kansainvälisille markkinoille, mutta osa vastaajista koki osaamisen vielä rajalliseksi. Lähes kaikki vastaajat kertoivat olevansa halukkaita osallistumaan konsortioihin ja yhteistyöhön muiden yritysten kanssa.

Yritysten mielenkiinto yritysryhmähankkeeseen

Hankeaikana kartoitettiin myös hanketilaisuuksiin osallistuneiden yritysten kiinnostusta yritysryhmähankkeen käynnistämiseen. Yritysryhmähanke on vähintään kolmen yrityksen yhteinen kehittämishanke, jossa yritykset voivat edetä yhdessä kohti puolustus- ja turvallisuusmarkkinoita. Yritysryhmähanke voisi tarjota yrityksille kustannustehokkaan ja hallitun tavan kehittää osaamistaan, verkostojaan ja markkinavalmiuksiaan.

Puolustusteollisuuteen suuntautuville yrityksille keskeisiä kehittämisteemoja voivat olla esimerkiksi:

- laatu- ja tietoturvavaatimukset
- puolustusalan hankintaprosessit
- verkostoituminen ja konsortioiden muodostaminen
- markkinoiden ja sääntely-ympäristön ymmärtäminen

Yritysryhmähanke voisi tarjota ratkaisun, jonka avulla yritykset voivat vahvistaa valmiuksiaan ja rakentaa yhteisiä toimintamalleja puolustus- ja turvallisuussektorille suunnattuihin hankkeisiin. Mielenkiintoa yritysryhmähankkeeseen vaikuttaisi alueemme yrityksillä olevan.

6. Puolustusteollisuuteen suuntavan konsortion perustaminen

Hankesuunnitelmassa todettiin, että hankkeen aikana selvitetään ja tuotetaan malli konsortion perustamiselle. Selvityksen edetessä ymmärrys kuitenkin vahvistui siitä, että uuden konsortion perustaminen on yksi mahdollinen polku kohti puolustuksen verkostoja, mutta monelle yritykselle tarkoituksenmukaisempi ja vaikuttavampi vaihtoehto voisi olla liittyä jo olemassa olevaan konsortioon, klusteriin tai ekosysteemiin. Näissä toimijoissa on usein valmiiksi rakennettuja yhteyksiä puolustusteollisuuden verkostoihin, mikä nopeuttaa yrityksen pääsyä mukaan alan hankkeisiin ja yhteistyömahdollisuuksiin.

Alla esitetty polku konsortion perustamiselle on esimerkinomainen ja laadittu Copilot-tekoälytyökalun tuottaman aineiston pohjalta. Kuvatut vaiheet ovat yleisluonteisia eivätkä välttämättä vastaa täsmällisesti todellisessa tilanteessa perustettavan konsortion tarpeita tai edellytyksiä.

Konsortion perustaminen tarjoaa yrityksille mahdollisuuden:

- vahvistaa asemaansa kasvavassa markkinassa
- vastata suurempien hankkeiden vaatimuksiin

- päästä mukaan kotimaisiin, NATO-hankkeisiin ja EU-rahoitteisiin projekteihin
- hyödyntää kasvavaa kysyntää myös kaksikäyttöteknologioissa

Kun alueelta löytyy yrityksiä, joilla on vahva osaaminen ja halu perustaa oma konsortio, ensimmäinen vaihe on kartoittaa mukana olevien yritysten osaaminen, palvelut ja tuotteet sekä pohtia, mihin Puolustusvoimien tai kansainvälisiin tarpeisiin nämä voivat soveltua. Tämän jälkeen luodaan konsortion perusrakenne, jossa sovitaan vastuut, kustannus- ja resurssijako, immateriaalioikeudet sekä muut käytännöt.

Jos konsortio suuntaa puolustusteollisuuteen, tulee huomioida alan erityisvaatimukset. Turvallisuus ja salassapito ovat keskeisiä, sillä puolustushankkeissa käsitellään usein salassa pidettäviä tai turvallisuusluokiteltuja tietoja. Tämä vaikuttaa yrityksen tietoturva-vaatimuksiin, toimitusketjun auditointeihin sekä mahdollisiin taustaselvityksiin ja yritysturvallisuusselvityksiin. Toimintaa ohjaa PUTU-laki (1531/2011), joka perustuu EU:n puolustus- ja turvallisuushankintadirektiiviin 2009/81/EY. Konsortion on huomioitava rajoitetut kilpailutusmenettelyt, turvallisuusasiakirjojen käsittelyvaatimukset sekä toimittajien soveltuvuusvaatimukset.

Verkostoituminen oikeiden toimijoiden kanssa on keskeistä. Suomessa tärkeitä kontakteja ovat PiA ry, joka tarjoaa alan verkostoja ja kansainvälisiä yhteyksiä, sekä Puolustusvoimien logistiikkalaitos (PVLOGL), joka vastaa Puolustusvoimien hankinnoista, julkaisee tarjouskilpailut Hilmassa ja TEDissä ja ohjaa yrityksiä NATO-hankintoihin. Lisäksi teknologiaklusterit ja alueelliset ja kansainväliset tapahtumat tarjoavat käytännön kontakteja alan asiantuntijoihin.

Kansainvälisesti keskeisiä verkostoja ovat NSPA, joka mahdollistaa osallistumisen Naton yhteishankintoihin, sekä NCIA, joka vastaa tietoturva- ja C4ISR-järjestelmien hankinnoista. Suomalaiset yritykset voivat osallistua NATO hankintoihin PVLOGL:n myöntämän NATO Eligibility Certificate -todistuksen avulla.

Puolustusteollisuuden tähtävien yritysten tulee varautua tiukkoihin sertifiointi- ja laatuvaatimuksiin, kuten ISO 9001 -laatuja järjestelmään, ISO 27001 -tietoturvastandardiin ja NATO:n AQAP-laatuvaatimuksiin, sekä kyvykkyyden toimia turvallisuusluokittelussa toimitusketjussa.

Puolustustarvikkeiden vienti on tarkasti säädeltyä. Vienti vaatii Puolustusministeriön luvat, ja tuotteiden tulee kuulua EU:n puolustustarvikeluetteloon. Jos tuotteissa tai komponenteissa on Yhdysvaltain teknologiaa, yrityksen on huomioitava ITAR- ja EAR-sääntelyn vaatimukset. ITAR säätelee sotilastuotteiden ja puolustuspalvelujen vientiä, kun taas EAR koskee erityisesti kaksikäyttötuotteita, joilla on sekä siviili- että mahdollinen sotilaskäyttö.

Suomen Teollisuussijoitus Oy:n 23.9.2024 julkaistun selvityksen mukaan suomalainen puolustusteollisuus on voimakkaassa kasvussa: Suomessa toimii jo silloin noin 370 alan yritystä, joista suurin osa oli nopeasti kasvavia startup- ja kasvuyrityksiä. Erityisen nopeaa kasvua on kaksikäyttöteknologioissa sekä digitaalisissa ratkaisuissa, kuten AR/VR-teknologiassa ja robotiikassa.

Yleisenä huomiona voidaan todeta, että suomalaisen puolustusteollisuuden kasvu ja monipuolistuminen heijastavat laajempaa kansainvälistä trendiä, jossa turvallisuusteknologioiden tarve, toimitusvarmuus ja uudenlainen geopolittinen tilanne lisäävät alan merkitystä. Yrityksille tämä avaa mahdollisuuksia rakentaa uusia yhteistyömalleja, vahvistaa omaa kilpailukykyään sekä osallistua yhä laajemmin sekä kotimaisiin että kansainvälisiin puolustushankkeisiin.

7. Kartoitetut konsortiot, ekosysteemit ja verkostot

Suomessa puolustusteollisuuden verkostot ja ekosysteemit kasvavat voimakkaasti. Kansalliset innovaatiokeskittymät, kuten DEFINE ja Pirkanmaan turvallisuusklusteri, yhdistävät yrityksiä, tutkimuslaitoksia ja julkisia toimijoita kehittämään puolustus- ja kaksikäyttöteknologioita. Samalla syntyy kansainvälisiä yhteistyömahdollisuuksia EU- ja Nato-hankkeissa. Tämä vahvistaa alueellista osaamista, edistää innovaatioita ja tukee yritysten kansainvälistymistä sekä siviili- että puolustussektorilla. Keräsimme yhteen muutamia esimerkkejä verkostoista ja innovaatiokeskittymistä. Koska puolustusteollisuus on voimakkaassa kasvussa, uusia verkostoja ja ekosysteemejä syntyy todennäköisesti jatkuvasti.

Pia Ry

Puolustus- ja Ilmailuteollisuus PIA ry on Suomessa toimivan puolustus-, ilmailu-, avaruus- ja turvallisuusteollisuuden etujärjestö. Se on toiminut yli 30 vuotta ja edistää jäsenyritystensä toimintaedellytyksiä, kilpailukykyä ja verkottumista sekä Suomessa että kansainvälisesti. PIA ry toimii myös linkkinä yritysten ja viranomaisten välillä tukien Suomen ja Euroopan kokonaisturvallisuutta sekä osallistuen alan kehittämiseen ja vaikuttamiseen.

PIA ry:n jäsenyys kannattaa, koska se auttaa yritystä pääsemään mukaan puolustusteollisuuden verkostoihin ja markkinoille, jotka ovat usein vaikeasti saavutettavia ilman oikeita kontakteja. Jäsenyys tuo suoran yhteyden keskeisiin kotimaisiin ja kansainvälisiin toimijoihin sekä tarjoaa tukea kansainvälistymiseen erityisesti EU- ja Nato-ympäristössä. Lisäksi PIA edistää jäsentensä etuja vaikuttamalla alan sääntelyyn ja rahoitusmahdollisuuksiin sekä jakaa ajankohtaista tietoa hankkeista ja kehitysrahoituksesta. Kokonaisuutena jäsenyys vahvistaa yrityksen uskottavuutta, kilpailukykyä ja kasvumahdollisuuksia puolustus- ja turvallisuusosalalla.

Lue lisää: <https://teknologiateollisuus.fi/pia/>

Defence Innovation Network Finland (DEFINE)

DEFINE on Riihimäen kaupungin käynnistämä avoin innovaatioekosysteemi, joka yhdistää Puolustusvoimat, yritykset, oppilaitokset ja tutkimusorganisaatiot kehittämään kansainvälisesti kilpailukykyisiä puolustus- ja turvallisuusalan ratkaisuja. DEFINE vahvistaa Suomen turvallisuutta ja tukee yritysten kasvua ja vientiä.

Lue lisää: <https://www.definefinland.fi>

Savo Defence

Savo Defence on Itä-Suomessa toimiva osaajaverkosto, joka kokoaa yhteen huippuyrityksiä kehittämään luotettavia ja joustavia ratkaisuja puolustus- ja kaksikäyttömarkkinoille. Savo Defence tarjoaa puolustusorganisaatioille testattuja, suorituskykyisiä teknologiaratkaisuja ja alihankkijoille väylän kansainvälisiin, vaativiin puolustushankkeisiin. Yhteistyössä Puolustusvoimien kanssa ja osana NATOA he toimivat luotettavana kumppanina globaalissa puolustusekosysteemissä.

Lue lisää: <https://savodefence.com>

Pirkanmaan turvallisuusklusteri

Pirkanmaan turvallisuusklusteri on Tampereen seudun laaja turvallisuuden innovaatio- ja yhteistyöverkosto, joka kokoaa yhteen yrityksiä, oppilaitoksia, tutkimuslaitoksia, julkisia toimijoita ja järjestöjä ratkaisemaan digitalisoituvan yhteiskunnan turvallisuushaasteita. Se tarjoaa matalan kynnyksen innovaatio-, tutkimus- ja kehitysmahdollisuuksia, verkostoitumista sekä pilotointiympäristöjä turvallisuus- ja puolustusratkaisuille, ja sitä koordinoi Business Tampere.

Lue lisää: <https://businesstampere.com>

Digital Defence Ecosystem

Digital Defence Ecosystem (DDE) on suomalainen puolustus- ja teknologiayritysten sekä tutkimuslaitosten verkosto, joka kehittää yhdessä uusia digitaalisia puolustusratkaisuja vastaamaan tulevaisuuden tarpeisiin. Verkosto kokoaa yhteen johtavia toimijoita digitaalisesta puolustusteknologiasta ja tarjoaa alustan yhteistyölle, jonka tavoitteena on vahvistaa Suomen ja liittolaisten puolustus- ja turvallisuustoimintaa sekä tuoda innovaatioita kansainvälisille markkinoille.

Lue lisää: <https://www.digitaldefence.fi>

Ostrobothnian Dual-Use, Defence and Security Hub

ODDS Hub on Vaasan ammattikorkeakoulun perustama innovaatioekosysteemi, jonka tavoitteena on vauhdittaa puolustusteollisuuden ja kaksoiskäyttöteknologian innovaatioita erityisesti Pohjanmaan alueella. Se tarjoaa pk-yrityksille, startupeille ja tutkimuslaitoksille verkostoitumis- ja yhteistyöympäristön, joka edistää teknologista kehitystä, osaamisen kehittämistä ja uusien liiketoimintamahdollisuuksien syntymistä. Hubi toimii myös linkkinä kansallisiin verkostoihin ja rahoitusmahdollisuuksiin, tukien yritysten kykyä hyödyntää turvallisuusympäristön muutoksista avautuvia mahdollisuuksia.

Lue lisää: <https://www.vamk.fi>

The Defence Innovation Accelerator for the North Atlantic (DIANA)

DIANA on Naton innovaatioekosysteemi. Se yhdistää startup-yrityksiä, tutkijoita ja teollisuutta liittoutuneista maista kehittämään läpimurtoteknologioita, joilla on kaksikäyttöpotentiaalia. Valtion teknillinen

tutkimuskeskus (VTT) johtaa Suomessa toimivaa NATO DIANA -accelerator-ohjelmaa. Ohjelma tarjoaa yrityksille koulutusta, mentorointia, puolustusteknistä asiantuntemusta, rahoitusta sekä pääsyn investointiverkostoihin. VTT:n ja DIANA-verkoston testikeskukset tarjoavat yrityksille mm mahdollisuuden testata ja arvioida teknologioitaan sekä todentaa niiden soveltuvuus puolustus- ja kaksikäyttökäyttöön. Lue lisää: <https://www.vttresearch.com>

DefTech Cluster

Oulun alueella toimii Oulu DefTech Cluster, joka yhdistää yrityksiä, tutkimuslaitoksia ja julkisia toimijoita kehittämään teknologioita sekä siviili- että puolustuskäyttöön. Klusterin ytimessä on innovaatioiden tukeminen ja kansainvälisen kilpailukyvyn vahvistaminen puolustusteknologian ja kaksikäyttökäyttötekniikoiden saralla Klusterin tavoitteena on vahvistaa Oulun teknologista osaamista, edistää pk-yritysten kansainvälistymistä ja rakentaa kestävää puolustus- ja turvallisuusteknologian ekosysteemiä. Se tarjoaa puitteet yhteistyölle, uusille innovaatioille ja teknologiakehitykselle, joka palvelee sekä siviili- että puolustussektoria.

Lue lisää: <https://oulu.com>

E-P:n puolustus- ja kaksikäyttöteollisuusklusteri – DuoDef E-P

DuoDef E-P on Etelä-Pohjanmaan puolustus- ja kaksikäyttötekniikan kehittämishanke, jota toteuttavat Into Seinäjoki, Seinäjoen ammattikorkeakoulu ja Tampereen yliopisto. Hanke tukee paikallisia yrityksiä kasvamaan turvallisuus- ja puolustustekniikan markkinoilla, kokoaa toimijat yhteistyöverkostoksi ja linkittää ne kansallisiin ja kansainvälisiin verkostoihin.

Lue lisää: <https://intoseinajoki.fi>

8. Yhteenveto

Puolustus- ja turvallisuusmarkkinat tarjoavat yrityksille merkittäviä kasvumahdollisuuksia niin kotimaassa kuin kansainvälisesti. Markkinoille pääsy mahdollistaa pitkäjänteisiä asiakkuuksia, kansainvälistymisen sekä kilpailukyvyyn vahvistumisen muun muassa laatu-, turvallisuus- ja toimituskyvykkyyksien kehittymisen kautta. Lisäksi kaksikäyttöteknologioiden kasvu avaa yrityksille uusia liiketoiminta-alueita.

Toimialalle pääsy edellyttää kuitenkin yrityksiltä määrätietoista kehittämistä. Keskeisiä tekijöitä ovat laatu- ja tietoturvajärjestelmien kehittäminen, hankintaprosessien ymmärtäminen sekä oman roolin tunnistaminen osana laajempia toimitusketjuja. Erityisen tärkeäksi nousee verkostoituminen: puolustus- ja turvallisuussektorilla toimiminen perustuu käytännössä yhteistyöhön, kumppanuuksiin ja konsortiomalleihin. Yksittäisen yrityksen on harvoin mahdollista edetä markkinoille yksin.

Suupohjan alueella toteutettu yrityskysely osoitti, että alueen yrityksillä on selkeä kiinnostus sektoria kohtaan ja vahva halu kehittää omaa osaamistaan. Samalla tunnistettiin kehittämistarpeita erityisesti laatujärjestelmissä, tietoturvassa ja puolustusalan erityisvaatimusten ymmärtämisessä. Yritysten valmius yhteistyöhön ja verkostomaiseen toimintatapaan oli kuitenkin erittäin korkea.

Hankkeen projektiryhmä toteaa, että hanke on saavuttanut sille asetetut tavoitteet. Hanke tavoitti merkittävän määrän yrityksiä ja onnistui lisäämään tietoisuutta toimialasta. Yritysten välinen verkostoituminen vahvistui ja osoittautui hankkeen keskeisimmäksi ja vaikuttavimmaksi tulokseksi. Hankkeessa tuotettu materiaali tukee yritysten omaa perehtymistä aiheeseen sekä jatkotoimenpiteiden, kuten yritysryhmähankkeen, suunnittelua ja valmistelua.

Projektiryhmän arvion mukaan kyseessä on ollut onnistunut kokonaisuus, joka on vastannut alueen yritysten ja elinkeinon tarpeisiin sekä synnyttänyt uusia yhteistyöyhteyksiä.

Puolustus- ja turvallisuussektorin merkitys tulee todennäköisesti kasvamaan edelleen tulevina vuosina osana laajempaa geopoliittista muutosta ja varautumisen lisääntymistä. Samalla sektorin rooli ei rajoitu pelkästään sotilaallisiin tarpeisiin, vaan se kytkeytyy yhä vahvemmin myös yhteiskunnan kokonaisturvallisuuteen, huoltovarmuuteen sekä kriittisen infrastruktuurin suojaamiseen. Tämä kehitys avaa yrityksille mahdollisuuksia osallistua myös laajempiin turvallisuuteen liittyviin ratkaisuihin, joissa yhdistyvät siviili- ja puolustustarpeet. Pitkällä aikavälillä kilpailukyky perustuu kykyyn uudistua, kehittää yhteistyötä ja vastata nopeasti muuttuvan toimintaympäristön vaatimuksiin.

Hankkeen luontevana jatkona valmistellaan yritysryhmähanketta, jonka tavoitteena on parantaa yritysten valmiuksia osallistua puolustus- ja turvallisuussektorin hankintoihin. Yritysryhmähankkeen kautta yritykset voivat kehittää osaamistaan, vahvistaa verkostojaan ja edetä hallitusti kohti uusia markkinoita yhdessä muiden toimijoiden kanssa.

9. Lähteet

Lähdeluettelo:

<https://puolustusvoimat.fi/etusivu>

<https://www.hankintailmoitukset.fi/>

<https://www.hankinnat.fi/>

<https://www.finlex.fi/fi/lainsaadanto/1999/621>

<https://www.finlex.fi/fi/lainsaadanto/2016/1397>

<https://www.finlex.fi/fi/lainsaadanto/2011/1531>

<https://www.nato.int/en>

<https://www.definefinland.fi>

<https://savodefence.com>

<https://businesstampere.com/ekosysteemit-ja-verkostot/tampereen-seudun-turvallisuus-ekosysteemi/pirkanmaan-turvallisuusklusteri/>

<https://www.digitaldefence.fi>

<https://www.vamk.fi/ajankohtaista/odds-hub-vauhdittaa->

<https://oulu.com>

<https://www.vttresearch.com>

<https://www.kiwa.com/en/services/certification/aqap-2110-certification/>

[AQAP NATO Quality Standards Awareness Course | DNV](#)

www.logistiikkalaitos.fi/nimikkeistokeskus

<https://teknologiateollisuus.fi/pia/>

<https://eportal.nspa.nato.int/Codification/CageTool/home>

<https://www.ncia.nato.int/business>

<https://www.nspa.nato.int/business/procurement>

<https://supo.fi/yritysturvallisuusselvitys>

<https://ted.europa.eu>

[Tesi-puolustusteollisuusselvitys-2024-mediasetti.pdf](#)

<https://www.diana.nato.int>

<https://nso.nato.int>

<https://www.kyberturvallisuuskeskus.fi>

[Puolustus-, ilmailu-, avaruus- ja turvallisuusteollisuuden etujärjestö - Pia-ry.fi](#)

Tiedon hakemiseen ja tekstin tiivistämiseen ja oikolukuun on käytetty Copilot tekoälytyökalua. Tämä raportti on laadittu alkuvuodesta 2026, ja sen sisältämät tiedot perustuvat hankkeen tilaisuuksien esitysmateriaaleihin (PVLOGL, Pia Ry, Patria Group, Team Finland), haastatteluihin, sekä verkosta haettuun tietoon. Tiedot kuvaavat raportin laatimishetken tilannetta, eikä niiden paikkansapitävyyttä voida taata myöhemmässä vaiheessa.