Teknologiateollisuus

ASIANTUNTIJALAUSUNTO
5.1.2023

Viite: Sähköpostitse saapunut kirjallisen lausunnon pyyntö 15.12.2022, TaV 11.01.2023

Valtioneuvoston selonteko huoltovarmuudesta (VNS 8/2022 vp)

Teknologiateollisuus ry kiittää mahdollisuudesta lausua otsikkoasiassa. Olemme lausuneet asiasta myös Liikenne- ja viestintävaliokunnalle 11.10.2022.

Tiivistelmä lausuntomme pääviesteistä:

- Teknologiateollisuus pitää erittäin hyvänä, että huoltovarmuudesta tehdään erillinen selonteko ja että prosessi tulee pysyväksi. Huoltovarmuusorganisaatio yrityksineen tulee ottaa jatkossa mukaan selontekojen valmisteluun.

- Teknologiateollisuus yhtyy selonteossa esitettyihin arvioihin huoltovarmuuden nykytilasta ja kehitystarpeista. Teknologiateollisuus kannattaa huoltovarmuuslainsäädännön kokonaistarkastelua tulevalla vaalikaudella sääntelyn ajantasaisuuden varmistamiseksi.

- Kokonaisvaltaisen, myös teollisen valmistuksen sekä materiaaliseen saatavuuteen liittyvän strategisen autonomian riittävä turvaaminen tulisi nostaa myös huoltovarmuustoiminnan yhdeksi tavoitteeksi.

- Suomen tulee viipymättä määritellä kuinka tulevan Nato-jäsenyyden varautumisvelvoitteiden edellyttämät huoltovarmuusjärjestelyt ja -kyvykkyydet käytännössä toteutetaan. Kannatamme pohjoismaisen huoltovarmuusyhteistyön vahvistamista.

- CER-direktiivin toimeenpanon määrittelyyn ja toteutukseen tulee tehdä tiiviissä yhteistyössä huoltovarmuuskeskuksen ja huoltovarmuusorganisaation kanssa.

- Teknologiateollisuus haluaa korostaa selonteossakin mainittuja uusia varautumistarpeita ilmastonmuutoksen aiheuttamiin muutoksiin sopeutumiseen, kyber- ja hybridivaikuttamiseen sekä materiaalien toimitusriskien hallintaan.

- Teknologiateollisuus ehdottaa, että eri sektorit laatisivat omat selvitykset varautumisen ja jatkuvuuden hallinnan osaamistarpeista. Immateriaalinen varautumien eli osaamisen ja tuoteomaisuuden aineettomien oikeuksien hallinta tulisi nähdä osana huoltovarmuustyötä.

- Katsomme selonteon tavoin, että pk-yritysten tietoisuuden sekä osaamisen kehittämiseen on kiinnitettävä nykyistä enemmän huomiota. Teknologiateollisuus pooleineen on käytettävissä tietotarpeita ja osaamisen vahvistamiseen tähtäävien toimenpiteiden valmistelussa ja toteuttamisessa.

Teknologiateollisuus ry

Eteläranta 10, PL 10, 00131 Helsinki
Puhelin 09 192 31
www.teknologiateollisuus.fi
Y-tunnus: 0215289-2

Teknologiateollisuus ry:n lausunto

Tausta ja lausuttavana oleva selonteko

Valtioneuvosto antaa eduskunnalle ensimmäisen kerran huoltovarmuusselonteon, jossa määritellään keskeiset tavoitteet huoltovarmuuden kehittämiselle vuoteen 2030 mennessä. Selonteossa kuvataan myös huoltovarmuuden toimintaympäristöä Suomessa ja kansainvälisessä kontekstissa sekä arvioidaan jatkuvuuden hallinnan kehittämistarpeita muuttuvissa olosuhteissa. Pyrkimyksenä on ennen kaikkea varmistaa huoltovarmuuden riittävä taso ja toimintakyky osana yhteiskunnan kokonaisturvallisuutta. Selonteossa käsitellään ensisijaisesti normaalioloissa tapahtuvaa varautumista ja huoltovarmuustyötä yleisellä tasolla.

Selonteon laadinta ja päivitysprosessi

Teknologiateollisuus pitää erittäin hyvänä, että huoltovarmuudesta tehdään erillinen selonteko ja että prosessi tulee pysyväksi. Koska kyseessä on ensimmäinen huoltovarmuusselonteko, on sen pääpaino pikemminkin kokonaisuuden kuvauksessa kuin varsinaisia toimenpiteitä esittämisessä. Teknologiateollisuus pitkälti yhtyy selonteossa esitettyihin arvioihin huoltovarmuuden nykytilasta ja kehitystarpeista. Haluamme muistuttaa, että selonteon valmistelu yhdessä varsinaisen pooliorganisaation kanssa olisi tasapainottanut kokonaisuutta ja korostanut yritysten omaa toimintaa varautumisessa ja jatkuvuuden hallinnassa. **Tulevaisuudessa selontekojen valmistelu yhdessä pooliorganisaation kanssa on mielestämme välttämätöntä.**

Katsomme valtioneuvoston tavoin, että perinteikäs suomalainen huoltovarmuus perustuu kriittisillä sektoreilla toimivien yritysten kykyyn reagoida poikkeusoloihin, sietää kriisi- ja häiriötilanteita sekä palautua niistä nopeasti. Huoltovarmuustoiminnoissa yhteistyö yksityisen, julkisen ja kolmannen sektorin välillä on meillä hyvää ja toimivaa. Kansainvälisen toimintaympäristön painoarvon kasvusta ja muutoksista huolimatta tulee huoltovarmuusjärjestelmässä huolehtia kansallisesta varautumisesta ja toimista. Haluamme kuitenkin muistuttaa siitä, että selonteon näkökulma on varsin hallintolähtöinen eikä se juurikaan käsittele asiaa yritysten tarpeita tai mahdollisuuksia huoltovarmuuden turvaamiseksi. Toivomme, että tulevissa selonteon tarkistuksissa tullaan tarkastelemaan jatkuvuuden hallintaa myös elinkeinoelämän tarpeiden valossa.

Luku 2. Kansainvälinen yhteistyö

Selonteossa on korostetusti todettu, että Suomen huoltovarmuusmalli perustuu markkinaehtoisuuteen, mikä edellyttää monipuolisia poliittisia ja kaupallistaloudellisia kansainvälisiä suhteita sekä avoimen sääntöpohjaisen kansainvälisen kauppajärjestelmän vakaata toimintaa. Teknologiateollisuus näkee asian samoin.

Euroopan unionissa on lisääntynyt keskustelu häiriönsietokyvystä sekä kriittisten toimien ja tuotantojen varmistamisesta COVID-pandemian, Venäjän Ukrainaan kohdistaman

hyökkäyssodan sekä viime aikoina myös kriittisten materiaalien ja komponenttien Kiina-riippuvuuksien seurauksena. Strategisten teknologioiden saatavuuteen, teollisen valmistuksen jatkuvuuteen ja materiaalien saatavuuteen liittyvän autonomian riittävä turvaaminen tulisi nostaa myös huoltovarmuustoiminnan yhdeksi tavoitteeksi.

Selonteon mukaan Suomen kansallinen huoltovarmuusmalli vastaa nykyisellään hyvin Naton seitsemän perusvaatimuksen tarpeisiin ollen jopa sitä kattavampi. Eduskunnan puolustusvaliokunta on valtioneuvoston ajankohtaisselonteosta antamassaan lausunnossa todennut, että Suomen Nato-jäsenyys parantaisi Suomen huoltovarmuutta, mikä on hyvä seikka. Naton perussopimuksen kautta jäsenmaille syntyy velvoite pitää yllä omatoimisesti jatkuvaa kansallista vastustuskykyä aseellisille hyökkäyksille. **Suomen tuleekin viipymättä määrittää kuinka varautumisessa tarvittavat huoltovarmuusjärjestelyt ja -kyvykkyydet käytännössä toteutetaan kansainvälisissä verkostoissa.**

Tulevasta pohjoisatlanttisen puolustusliiton jäsenyydestä huolimatta katsomme selonteon tavoin, että nykyisessä toimintaympäristössä on tärkeää vahvistaa niin **Suomen ja Ruotsin** kahdenvälistä huoltovarmuusyhteistyötä kuin laajemminkin pohjoismaista yhteistyötä huoltovarmuustoimissa ja –toiminnassa kaikenlaisten poikkeusolojen ja kriisitilanteiden osalta. Selonteossa on tunnistettu mielestämme aivan oikein, että tässä **yhteistyössä keskeisiä toimialoja ovat muun muassa tietoliikenneinfrastruktuuri ja -palvelut, logistiikka sekä energian- ja ruoantuotanto**.

Selonteon kansainvälisiä sopimuksia kuvaavasta luvusta 2 puuttuu kuitenkin maininta pohjoismaisesta (Nordefco) puolustusmateriaalialan sopimusjärjestelystä ja ns. liitesopimus sotilaallisesti huoltovarmuudesta. Se on toki mainittu luvussa 6, mutta ansaitsee oman paikkansa muiden sopimusten joukossa. Esitämmekin, että selonteon johdantoon ja lukuun 2.2. sisällytetään mainita em. Nordefco-sopimuksesta.

Keskeiset huoltovarmuuteen vaikuttavat EU-hankkeet

Selonteon mukaisesti kriittisten toimijoiden häiriönsietokykyä koskeva CER-direktiivi (Resilience of Critical Entities) ja sen kansallinen toimeenpano tukevat Suomen huoltovarmuustoimintaa. Epäselväksi jää, mikä on niiden sektoreiden painoarvo, jotka jäävät direktiivissä mainittujen kriittisten sektoreiden ulkopuolelle. Näin on mm. puolustusteollisuuden kohdalla. Luokittelu kriittiseksi sektoriksi on puolustusteollisuudelle tärkeää. Koronapandemian liikkumisrajoitukset osoittivat luokittelun tärkeyden.

Toisaalta haluamme tuoda esiin sen, että pidämme erinomaisena, että myös kriittistä infrastruktuuria tuottavia yrityksiä tukeva teollisuus luokitellaan kriittiseksi. Puolustus- ja turvallisuusteknologiaa tuottavien yritysten ratkaisut ovat usein keskeisessä osassa kriittisen infrastruktuurin turvaamisessa.

Teknologiateollisuus esittää, että selontekoon kirjataan myös CER-direktiivin soveltamisalan ulkopuolelle jäävien toimialojen asemasta ja todetaan niiden kriittisyys tämän selonteon hengen mukaisesti. Lisäksi on tärkeää huomioida, että CER-direktiivin soveltamisala on osin sama kuin NIS-direktiivin, joiden on yhdessä tarkoitus kattaa

kyberfyysiset rajapinnat ja huomioida sektori- ja valtiorajat ylittävät keskinäisriippuvuudet. Näin ollen CER-direktiivin toimeenpanon määrittely ja toteutus tulee tehdä tiiviissä yhteistyössä huoltovarmuuskeskuksen ja huoltovarmuusorganisaation sekä NIS2-direktiivin toimeenpanoa valmistelevien toimijoiden kanssa. Lisäksi muistuttaisimme siitä, että huoltovarmuusorganisaatio jo nykyisellääänkin toteuttaa monia CER-direktiivissä määriteltyjä tehtäviä, joten huoltovarmuusorganisaatio yrityksineen on olennainen toimija direktiivin toimeenpanossa.

Luku 3. Huoltovarmuuden toimintaympäristön kehitys ja sen vaikutukset

Teknologiateollisuus yhtyy valtioneuvoston selonteossa esittämään arvioon siitä, että Venäjän sota Ukrainassa on muuttanut perustavanlaatuisella tavalla turvallisuus- ja toimintaympäristöä. Vaikutukset ovat laaja-alaisia ja pitkäkestoisia, ja ne vaativat tarkastelua myös huoltovarmuuden näkökulmasta. Tarkastelussa on tarpeen ottaa huomioon konfliktin välilliset vaikutukset geopolitiikkaan ja -ekonomiaan sekä kansainvälisiin kauppasuhteisiin. Samalla on erityisen tärkeää ylläpitää tietoon pohjautuvaa tilannekuvaa ja -arviota muihin kehityskulkuihin, jotka sisältävät merkittäviä geopoliittisia ja -ekonomisia uhkia. Kansallisen huoltovarmuuden tulee perustua asiantuntijatyön tuottamaan parhaaseen ymmärrykseen mahdollisista kehityskuluista ja niiden todennäköisyyksistä.

Toimintaympäristön pitkäjänteinen seuranta ja ajankohtaiset uhat

Selonteossa on aivan oikein todettu, että tulevaisuudessa perinteiset uhat yhdistyvät uusiin uhkiin, kuten kyber- ja hybridivaikuttamiseen. **Teknologiateollisuus haluaa korostaa selonteossa mainittujen geopolitiikan ja geoekonomian sekä yhteiskunnan huoltovarmuussektoreiden muiden merkittävien muutosajureiden, kuten vihreän siirtymän ja digitalisaation yhteisvaikutuksia, jotka väistämättä aiheuttavat muutostarpeita materiaalisen varautumiseen sekä globaalien arvo- ja toimitusketjujen jatkuvuuden varmistamiseen ja monipuolistamiseen.** Selontekoon kirjattu tahtotila siitä, että Suomella on oltava riittävä varautumisen taso ja mahdollisuuksien rajoissa myös tarvittava omavaraisuus kaikkein välttämättömimpien hyödykkeiden osalta, on ehdottoman kannatettava. Tämä koskee myös soveltuvin osin myös digitaalisia hyödykkeitä, kuten ohjelmistoja.

Ilmastonmuutos

Tuemme myös selonteon kirjausta siitä, että huoltovarmuustyössä on tärkeää tarkastella ilmastonmuutoksen vaikutuksia erityisesti kriittisen infrastruktuurin, tuotannon ja palvelujen jatkuvuuden näkökulmista.

Teknologiateollisuus tukee selonteon näkemyksiä uudistuvan energian käyttöönotosta sekä energiamurroksen vaikutuksesta huoltovarmuuteen, joskin aihetta on selonteossa käsitelty varsin lyhyesti ja kapeasti sen merkittävyyteen nähden. Selonteosta puuttuu esimerkiksi pohdinta murroksen vaikutuksista puolustusvoimien suorituskykyyn. Yhteiskunnan laaja siirtyminen käyttövoimaltaan sähköisiin

ja hybridiajoneuvoihin sekä yleisemminkin kestäviin liikkumismuotoihin vaikuttaa myös puolustusvoimien - sekä sitä tukevan teollisuuden - mahdollisuuksiin ns. ottoajoneuvojen hyödyntämiseen. Perinteisten energialähteiden saatavuus on varmistettava, jotta kaikki sektorit kykenevät toimimaan poikkeustilanteessa mahdollisimman normaalisti.

Digitalisaatio ja kyberturvallisuus

Erityisesti digitaalisessa turvallisuudessa huoltovarmuus on suoraan riippuvainen kotimaisten yritysten liiketoiminnan ja toimitusvarmuuden jatkumisesta kaikissa tilanteissa. Liiketoiminnan jatkuvuus erilaisissa tilanteissa tulee olla huoltovarmuuden keskiössä, mitä seikkaa selonteossakin tulisi korostaa. Vuoden 2022 digibarometrin tulosten mukaan 80 % suomalaisista on joutunut kyberrikoksen tai sen yrityksen kohteeksi kuluneen vuoden aikana. Kyselyssä ei ole eroteltu sitä, onko verkkorikosta yritetty työ- tai yksityiselämän piirissä. Vain murto-osa yrityksistä tekee rikosilmoituksen, kun se itse on ko. rikoksen kohteena. Voidaan siis sanoa, että digitaalinen turvallisuus on välttämätöntä yksittäisten sekä lukuisuuteen perustuvien vakavien rikosten, kuten sabotaasi-, häirintä- ja vakoilutapausten torjumiseksi. Korkea uhkatila ole suinkaan riippuvainen esimerkiksi Venäjän hyökkäyssodasta. Tietoverkkorikollisuuden maailmanlaajuiset vuotuiset kustannukset ovat ennen sotaakin olleet arviolta 5,5 biljoonaa euroa.

Yhteiskunnan kyberturvallisuus julkishallinnon kyberturvallisuus mukaan lukien on vahvasti riippuvainen palveluita tarjoavien ja itsessään huoltovarmuuskriittisten yritysten digitaalisesta turvallisuudesta. Merkittäviä keskinäisriippuvuuksia on kotimaisten yritysten, mutta myös suurten kansainvälisten yritysten kanssa. Lisäksi selonteossa olisi ollut tarpeen kirkastaa, että vain pieni osuus digitaalisesta turvallisuudesta on sellaista, joka soveltuu tavanomaisiin varautumistoimiin. Digitaalinen turvallisuus koostuu ensisijaisesti ja valtaosin digitaalisten riskien hallinnasta ja se on luonteeltaan ennakoivaa, eikä niinkään jälkikäteiseen palautumiseen tähtäävää. Digitaalisen huoltovarmuuden ytimen muodostavat pelisäännöt, joilla määritellään näiden eri toimijoiden ja tasojen välinen yhteistoiminta.

Ukrainassa käytävä sota on osoittanut, että mm. pilvipalveluiden käyttö on yritysten liiketoiminnan ja koko yhteiskunnan jatkuvuuden kannalta kriittistä. Yritysten kustannusrakenteen ja toiminnallisen ketteryyden kannalta näin on ollut jo paljon ennen tämänhetkistä kriisiä. Kansallisen kyberturvallisuuden kokonaistilan parantamisessa on eri toimijoilla eri rooleja; huoltovarmuuskeskuksen ja huoltovarmuusorganisaation (poolit) tehtävinä on tunnistaa ketjun kriittisiä yritystoimijoita ja varmistaa, että ne myös kehittävät kyberturvallisuuttaan. Samalla, kun yritykset huolehtivat omasta turvallisuudestaan, on niiden tarpeen vaikuttaa digitaalisten palveluiden turvallisuuden kehittymiseen omissa alihankintaketjuissaan. Tukea ja kehitystä tarvitaan niin organisaatioiden strategisella kuin operatiivisella tasolla. Selonteon sektorikohtaisen varautumisen lähtökohtia koskevassa kohdassa 5.1.5 on lisäksi hyvä korostaa, että digitaalinen turvallisuus on kaikille selonteossa esitetyille aloille oleellista. Tähän tavoitteeseen liittyen selonteossa ei ole kuitenkaan hyödynnetty esimerkiksi Digitaalinen turvallisuus 2030 -ohjelman konkreettisia myönteisiä vaikutuksia. Ohjelmasta tulisikin rahoittaa toimia, jotka tosiasiallisesti muuttavat ko. yritysten digitaalisten riskien hallintakykyä, kuten vuonna 2022 tietoturvasetelin avulla huoltovarmuuskriittisiin yrityksiin kohdistuvia kehittämistoimia.

Luku 6. Sotilaallinen huoltovarmuus

Teknologiateollisuuden piirissä toimiva MIL-pooli on selonteon luonnosvaiheessa annetuissa kommenteissa korostanut tyytyväisyyttä siihen, että sotilaallinen huoltovarmuus on käsitelty selonteossa omana lukunaan. **Teknologiateollisuus muistuttaa, että teknologiset ratkaisut muodostavat saumattoman kokonaisuuden, jonka sisällä ei ole mielekästä tai tarpeen tehdä jakoa ns. puolustusteollisuuden ja ns. siviiliteollisuuden välillä.**

Selonteko suhtautuu varauksetta eurooppalaisiin puolustusteollisuuden kehitysaloitteisiin. Teknologiateollisuus pitää aloitteita tervetulleina, mutta haluamme samalla muistuttaa kokonaisuuden tarkastelun tärkeydestä myös Suomen pitkäaikaisen kansallisen edun kannalta. Eurooppalaista keskustelua käydään ennen kaikkea suurten jäsenmaiden teollisuuden näkökulmasta ja on riski, että komission aloitteet hyödyttävät ensisijaisesti suurten jäsenmaiden suuria yrityksiä. Suomen tulisikin hyödyntää eurooppalaiset kehitysaloitteet proaktiivisemmin myös huoltovarmuusnäkökulmasta.

Huoltovarmuusselonteko toistaa hyvin mm. puolustusselonteon linjauksia ja Teknologiateollisuus tukee niitä. Huomauttaisimme kuitenkin siitä, että tästäkin selonteosta puuttuu linjausten toimeenpano, vaikka siinä on todettu sotilaallisen maanpuolustuksen kannalta kriittisen materiaalin, tuotannon, teknologian ja osaamisen on oltava saatavissa ja käytettävissä kaikissa turvallisuustilanteissa. Selonteossa on vieläpä todettu, että ”erityisen tärkeää on varmistaa kriittisten teknisten järjestelmien yllä- ja kunnossapito ja maanpuolustuksessa käytettävän kriittisen kulutusmateriaalin tuotanto.”

Jotta Suomessa toimiva teollisuus kykenee tukemaan puolustusvoimia ja tuottamaan sotilaallista huoltovarmuutta, tulee sillä olla riittävästi jatkuvaa tilauskantaa koti- ja ulkomailta. Suomessa toimiva teollisuus ei kykene tuottamaan huoltovarmuutta myöskään ilman kansainvälisen liiketoiminnan tuomaa tukea. On pidettävä kirkkaana, että valtaosa yritysten TKI-toiminnasta rahoitetaan yritysten asiakkailta tulevilla varoilla. Tilaukset ovat elintärkeitä myös osaamisen kehittämisen ja ylläpidon näkökulmasta.

Teknologiateollisuus esittääkin selontekoon seuraavia sotilaallista huoltovarmuutta koskevia täydennyksiä:

- lisätään kirjaus EU-aloitteiden aktiivisesta hyödyntämisestä siten, että aloitteet hyödyntävät myös suomalaista alan teollisuutta sekä tukevat huoltovarmuutta.
- lisätään kirjaus Suomessa toimivan puolustusteollisuuden merkityksestä teknologisen avun vastaanotossa ja antamisessa.
- lisätään selkeämpi kirjaus hallinnon tuesta Suomessa toimivan puolustusteollisuuden vientitoiminnalle.

Luku 7. Huoltovarmuuden kehittämislinjaukset

Kansallinen toimeenpanovalta kriisitilanteiden johtamisessa

Teknologiateollisuuden piirissä toimiva teknologiapooli on nimennyt erääksi keskeiseksi kehityskohteeksi yhteiskunnan kriisitilanteiden johtamisen toimeenpanovallan selkeyttämisen. Yritykset mainitsevat esimerkkinä COVID19-pandemian aikaisiin tilanteisiin, joissa toimeenpanovalta oli hajautettu eri viranomaisille ja koordinaatio näyttäytyi ajoittain puutteellisena. Yritykset toivovat, että huoltovarmuusselonteosta kuvattaisiin selkeästi myös kriisitilanteisen johtaminen ja se, kuinka varautuminen ja siirtyminen poikkeusoloihin käytännössä tapahtuu.

Lainsäädännön uudistamistarpeet

Selonteossa on todettu, että vuodelta 1992 olevan huoltovarmuuden turvaamista koskevan lain säännösmuutostarpeiden kokonaisarvio olisi tarpeen. **Teknologiateollisuus kannattaa sääntelyn kokonaisuudistusta,** jotta se saatettaisiin ajan tasalle suhteessa muuttuneeseen toimintaympäristöön ja sen vaatimuksiin nähden. Kokonaisuudistuksessa tulisi huomioida myös nopeasti kasvava ongelma yhteiskunnan kriittisiin toimintojen tai toimijoiden tai kriittisen infrastruktuurin määrittelyyn, sillä näille termeille ei ole vakiintunutta, kaikkialla lainsäädännössä tunnustettua tarkkarajaista sisältöä. Tällaisena ei voida pitää valtioneuvoston huoltovarmuuspäätökseen (1048/2018) sisältyviä määrittelyjä. Yhä useammin sekä EU- että kotimaisessa lainsäädännössä käytetään erilaisia toisistaan poikkeavia määritelmiä siitä, mitä ovat kriittiset toimijat ja kriittinen toiminta. On tärkeää, että selonteossakin todettu kriittisen infrastruktuurin määrittämis- ja tunnistamistyö tehdään mahdollisimman ripeästi, sillä se on edellytyksenä kriittisen intrastruktuurin systemaattiselle suojaamiselle.

Osaamisen varmistaminen ja kokonaisturvallisuuden koulutus

Selonteossa on mielestämme hyvin kuvattu se, kuinka teknologinen kehitys vaikuttaa ratkaisevasti sotilaallisten suorituskykyjen sekä huoltovarmuuden kehittämiseen. Uusien teknologioiden hyödyntämisessä nimenomaisesti kansallisen osaamisen merkitys korostuu. Teknologiateollisus painottaa selonteon tavoin, että **erityisesti kriittisten teknologioiden osalta on ylläpidettävä ja kehitettävä omaa osaamista,** jotta Puolustusvoimien keskeisten järjestelmien itsenäinen käyttö voidaan varmistaa kaikissa olosuhteissa.

Teknologiateollisuus kiittää siitä, että MIL-poolin teettämä osaamisen selvitystyö on mainittu selonteossa. Selvityksen suositusten toimeenpanoa on esitetty työ- ja elinkeinoministeriön poikkihallinnolliselle työryhmälle. Teknologiateollisuus toivoo, että toimeenpano etenee pikaisesti ja että vastaavia tarkasteluja tehtäisiin muillakin keskeisillä sektoreilla.

Teknologiateollisuus tukee selonteon linjausta siitä, että huoltovarmuusasioita ja kansalaisvarautuminen ml. kyberturvallisuus sisällytettäisiin eri koulutusasteiden opetussuunnitelmiin. Tämä on kuitenkin tehtävä huolellisesti koulutusjärjestelmien ominaispiirteiteitä kunnioittaen ja jo tehtyjen selvitysten perusteella. Huoltovarmuuden kannalta tulee varmistaa kriittisen osaamisen syntyminen ja pysyminen kansallisessa käytössä. Myös **kansalaisvarautumisen työkalupakkiin tulisi jatkossa kuulua perustasoiset kyberturvallisuustaidot**, kun kansalaisten arkinen toiminta on jo pitkälle

digitalisoitunut ja kotien koneet ja laitteet ovat jo tulleet osaksi maailmanlaajuista tietoverkkoa.

Tulevaisuudessa ns. immateriaalinen varautumien eli osaamisen ja tuoteomaisuuden aineettomien oikeuksien hallinta tulisi nähdä osana huoltovarmuustyötä. Huoltovarmuustoimenpiteenä tämä voisi tarkoittaa mm. yritysten kanssa tehtäviä sopimuksia kyvykkyyksien ja osaamisen ylläpidosta, jotta se on häiriötilanteissa yhteiskunnan käytettävissä.

Katsomme selonteon tavoin, että pk-yritysten tietoisuuden sekä osaamisen kehittämiseen on kiinnitettävä nykyistä enemmän huomiota. Teknologiateollisuus on käytettävissä tietotarpeita ja osaamisen vahvistamiseen tähtäävien toimenpiteiden valmistelussa ja toteuttamisessa. Esimerkiksi tietoturvasetelin jatkoa pohdittaessa huomio tulisi kiinnittyä kaikkiin Suomeen sijoittautuneihin pk-yrityksiin.

Julkiset hankinnat

Teknologiateollisuus tukee selonteon kirjauksia ja toimenpide-esityksiä koskien julkisia hankintoja. **Kannatamme selonteossa mainittua perusperiaatetta, jonka mukaan huoltovarmuuden toteutumista julkisissa hankinnoissa on edistettävä systemaattisesti osana Hankinta-Suomi -toimenpideohjelmaa.** Aihe on entisestään korostunut viime aikaisten toimintaympäristömuutosten seurauksena.

Huoltovarmuuskriittisten yritysten lupamenettelyt

Huoltovarmuuskriittisten yritysten lupamenettelyjä (esim. turvallisuusselvitykset ja -auditoinnit) tulisi priorisoida lupaviranomaisten toiminnassa. Tällä hetkellä raskaat ja hitaat hallinnolliset menettelyt viivästävät mm. rekrytointeja ja siten toimituskykyä. Prosesseja tulisi helpottaa näiden hankkeiden osalta, jos on kyse huoltovarmuuden varmistamisesta.

Kansallisen kiertotalousohjelman kehittäminen

Tuomme esille vahvan tukemme kansallisen kiertotalousohjelman kehittämiselle, koska se vahvistaa yritysten kykyä varautua mm. kriittisten materiaalien toimitusriskeihin myös keskipitkällä ja pitkällä aikavälillä. Kiertotalousratkaisujen ja -teknologioiden kautta yrityksille syntyy kasvava globaali vientimahdollisuus.

Lisätiedot:
Johtaja Helena Soimakallio
helena.soimakallio@teknologiateollisuus.fi
040 - 550 7706

Johtaja Matti Mannonen
matti.mannonen@teknologiateollisuus.fi
040 - 544 7047