Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Puolustushallinnon turvallisuus

Sisällysluettelo

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Eteläinen Makasiinikatu 8

PL 31, 00131 HELSINKI

www.defmin.fi

Taitto: Tiina Takala/puolustusministeriö

ISBN: 978-951-25-2228-6 pdf

Tiivistelmä

Turvallisuus on olotila, jossa ei ole tosiasiallista uhkaa tai tiedossa olevat uhat eivät aiheuta merkittävää riskiä. Mahdolliset turvallisuutta heikentävät riskit ovat hallinnassa hyväksyttävällä tasolla ja uhkien ehkäisemiseksi sekä torjumiseksi on olemassa riittävät edellytykset. Lisäksi olotila koetaan turvalliseksi ja pysyväksi. Turvallisuus on puolustushallinnon kaikkeen toimintaan kuuluva ominaisuus, josta koko hallinnonalan henkilöstön tulee kantaa vastuuta. Turvallinen toiminta vahvistaa puolustushallinnon uskottavuutta ja myönteistä julkisuuskuvaa ja on osa kansallista turvallisuutta.

Puolustushallinnon turvallisuuden strategia edistää hallinnonalan ydintehtävien onnistumista. Strategian tarkoituksena on ohjata hallinnonalan organisaatioiden turvallisuutta pitkäjänteiseen suunnitteluun, toteutukseen ja kehittämiseen sekä hankintojen ja voimavarojen tarkoituksenmukaiseen kohdentamiseen. Strategiassa kuvattu puolustushallinnon turvallisuuden tavoitetila 2020 antaa tähän perusteet.

Tavoitetilassa puolustushallinnon päätehtävien häiriötön toteuttaminen ja kriittisten toimintojen jatkuvuus turvataan kaikissa tilanteissa siten, etteivät turvallisuusuhat aiheuta ydintehtäville haittaa. Jos haittaa aiheutuu, sen vaikutukset rajataan mahdollisimman pieniksi ja lyhytaikaisiksi. Muita viranomaisia tuetaan osana kansallista turvallisuutta yhteiskunnan elintärkeiden toimintojen turvaamisesta sovittujen[1] käytäntöjen mukaisesti, käytettävissä olevien voimavaroin.

Puolustushallinnolla on oltava jatkuva kyky turvallisuutta vaarantavien tapahtumien hallintaan. Turvaamisen painopiste on ennakoivassa toiminnassa. Näin havaitaan, tunnistetaan ja torjutaan hallinnonalaa uhkaavat tekijät sekä varaudutaan uhkaavien tekijöiden hallintaan. Puolustushallinnolla on myös kyky vastata nopeasti muuttuviin vaaratilanteisiin, häiriötilanteiden hallintaan sekä haittavaikutusten lieventämiseen ja niistä toipumiseen hallitusti, niin kotimaan kuin kansainvälisissä tehtävissä.

Puolustushallinnon turvallisuuden tavoitteet saavutetaan noudattamalla riskienhallinnan periaatteita. Turvallisuusriskienhallinnalla tarkoitetaan järjestelmällistä tapaa taata hallinnonalan toimintojen turvallinen toteutuminen kaikissa olosuhteissa. Näin turvataan organisaatioiden voimavarat siten, että kokonaisriskit ovat mahdollisimman pienet ja organisaation toiminnan tavoitteet voidaan saavuttaa.

Puolustushallinto luo, toteuttaa ja ylläpitää menettelyt, joilla se määräajoin arvioi turvallisuutensa tavoitetilan vaatimusten täyttymistä.

1 Yhteiskunnan turvallisuusstrategia

Johdanto

Puolustushallinnon turvallisuuden strategia edistää hallinnonalan ydintehtävien onnistumista. Se perustuu Puolustushallinnon strategiseen suunnitelmaan 2030 ja on sen osastrategia. Tarkoituksena on ohjata hallinnonalan organisaatioita turvallisuuden pitkäjänteiseen suunnitteluun, toteutukseen ja kehittämiseen sekä hankintojen ja voimavarojen tarkoituksenmukaiseen kohdentamiseen.

Puolustushallinnon turvallisuuden kokonaisuuden kannalta on oleellista, että hallinnonalana luodaan kyky ennakoida ja vastata turvallisuuteen vaikuttaviin ilmiöihin, tapahtumiin ja niiden mahdollisiin ennusmerkkeihin riittävän ajoissa. Oleellista on myös kyetä keskittämään riittävät voimavarat haittaa aiheuttavan tilanteen hallintaan, haitallisten jälkiseurausten minimointiin ja haitallisesta tilanteesta toipumiseen.

Strategiassa otetaan huomioon yhteiskunnan turvallisuusstrategian, sisäisen turvallisuuden ohjelman sekä turvallisuus- ja puolustuspoliittisten selontekojen linjaukset. Strategiassa otetaan huomioon myös Suomea velvoittavat kansainväliset sopimukset ja normit sekä kansallinen lainsäädäntö[2] ja muut hallinnonalaa ohjaavat normit.

Turvallisuuden strategia on laadittu yhteistyössä hallinnonalan organisaatioiden kanssa ja sitä päivitetään osana puolustusministeriön strategista suunnittelua. Strategian päivittämisestä vastaa puolustusministeriö. Päivitystyö tehdään yhteistyössä hallinnonalan organisaatioiden kanssa.

Strategian liitteessä 1 on esitetty osatavoitteet tavoitetilan saavuttamiseksi. Puolustushallinnon organisaatiot vastaavat turvallisuuden tavoitetilan saavuttamiseksi tarvittavien toimenpiteiden toteuttamisesta strategian linjausten mukaan. Turvallisuuden strategiasta johdettavat konkreettiset ja mitattavissa olevat tavoitteet asetetaan tähän osastrategiaan perustuvilla organisaation omilla suunnitelmilla ja normeilla. Strategian linjaukset toteutetaan hallinnonalan toiminta- ja taloussuunnitelmissa sekä asettamalla tulossopimuksiin ja tulostavoitteisiin tämän osastrategian kehittämislinjauksia tukevia mitattavissa olevia tavoitteita.

Liitteessä 2 määritellään tässä osastrategiassa esille tulevia käsitteitä. Liitteessä on mukana myös muita organisaation turvallisuutta koskevia määritelmiä, minkä tarkoituksena on yhdenmukaistaa puolustushallinnon organisaatioturvallisuuden käsitteistöä.

2 esim. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa

Laajeneva uhkaympäristö

Uhkaympäristö muuttuu yllätyksellisemmäksi ja vakavammaksi. Ulkoinen ja sisäinen turvallisuus kytkeytyvät yhä tiiviimmin yhteen. Useat laaja-alaisista turvallisuusuhkista ovat kytköksissä toisiinsa. Ne ovat vaikeasti ennustettavia, monimuotoisia ja varoitusajaltaan lyhyitä. Laaja turvallisuuskäsitys kattaa sellaiset turvallisuuskysymykset, jotka kehittyessään saattavat muodostua uhkiksi ja aiheuttaa merkittävää vaaraa tai haittaa Suomelle, väestölle tai suomalaisen yhteiskunnan elintärkeille toiminnoille. Tällaiset laaja-alaiset turvallisuusuhkat ovat joko ihmisten toimintaa tai luonnon ääri-ilmiöitä ja niiden seurauksia.

Julkisen hallinnon ja elinkeinoelämän tarjoamat yhteiskunnan palvelut ovat yhä useammin sidoksissa tietoliikenteen kautta tietojärjestelmiin. Yhteiskunta on kiihtyvällä nopeudella muuttumassa ympäristöksi, jossa yhä useammat palvelut ovat tietoteknisesti ohjattuja tai muutettu kokonaan sähköisiksi palveluiksi. Sähköisiin järjestelmiin liittyvät riskit lisäävät merkittävästi yhteiskunnan haavoittuvuutta. Järjestelmien verkottuessa toisiinsa lisääntyy mahdollisuus, että yhden järjestelmän pettäminen vaikuttaa myös muiden teknisten järjestelmien toimintakykyyn. Järjestelmien häiriöt saattavat vaikuttaa hyvin laajasti yhteiskunnan toimintoihin. Ylläpitoon ja huoltoon tarvittavien asiantuntijaresurssien ulkoistaminen lisää häiriöiden vaikuttavuutta.

Langattoman tiedonsiirron yleistyessä järjestelmien käytettävyys laajenee mutta toimintavarmuus saattaa heiketä. Useimmat yksityisistä ja julkisista palveluista perustuvat jatkossakin sähköisten järjestelmien nopeisiin ja luotettaviin toimintoihin.

Uusi teknologia ja taktiikka muuttavat sodankäyntiä. Nopeus, tempo, liikkuvuus, tilannetietoisuus, vaikuttamisen ulottuvuus sekä avaruuden hyödyntäminen korostuvat. Informaatio- ja tietoverkkosodankäynti sekä eri toimijoiden välinen yhteistyö lisääntyvät. Verkostojen käyttötarve ja -mahdollisuudet lisääntyvät samalla, kun informaation määrä sekä vaikuttavuus kasvavat. Laittomaan hyödyn tavoitteluun liittyvän tietoteknisen osaamisen käyttö toisen valtion informaatio- ja tietoverkkosodankäynnin voimavarana lisääntyy, ja uutta osaamista voidaan käyttää painostuksen välineenä. Tarkastelukauden aikana symmetrinen ja asymmetrinen informaatio- ja tietoverkkosodankäynti yleistyy ja saa uusia muotoja, kohteita ja vaikutuskanavia. Käytössä olevat ja uudet vaikutuskeinot ovat saatavilla niin valtiollisille kuin ei-valtiollisille rikollisesti tai poliittisesti motivoituneille ryhmittymille ja kynnys tämän keinovalikoiman käyttöön laskee ilmiön arkipäiväistyessä.

Korkean teknologian maana Suomi on jatkuvasti tiedustelun kohteena. Huolimatta huipputeknologian mahdollisuuksista ei salassa pidettävän tiedon hankkiminen perinteisen vakoilun avulla ole menettänyt merkitystään. Avoimen tiedonhankinnan lisäksi tiedustelupalvelut pyrkivät värväämään avustajikseen sellaisia henkilöitä, joiden avulla ne pääsevät käsiksi haluamaansa tietoon. Suomalaisiin ja Suomen intresseihin kohdistuu tiedustelua myös maamme ulkopuolella. Sotilastiedustelun kohteina Suomessa ovat muun muassa Suomen puolustuspolitiikka, sotilaallinen valmius ja suorituskyky, kalustohankinnat ja kansainvälinen sotilasyhteistyö sekä tutkimus- ja kehitystoiminta. Tietoteknologian ja viestiliikenteen kehittyminen on avannut signaalitiedustelulle uusia mahdollisuuksia. Osa valtioiden tietojärjestelmiä vastaan tehdyistä verkkohyökkäyksistä palvelee myös tiedustelua.

Järjestäytyneen rikollisuuden määrä on kasvussa. Suomessa vaikuttava järjestäytynyt rikollisuus tiivistää verkostoitumistaan ja keskinäistä yhteistyötään. Rikollisryhmien keskinäiset väkivaltaiset välienselvittelyt ja niitä seuraavat kos-

toiskut voivat aiheuttaa vakavia vaaratilanteita sivullisille. Lisäksi ne heikentävät yleistä järjestystä ja turvallisuutta.

Sähköisten viestintä- ja tietojärjestelmien rakenteet mahdollistavat niiden käytön rikollisiin tarkoituksiin sekä vaikuttamisen yhteiskunnan elintärkeisiin toimintoihin myös maamme rajojen ulkopuolelta. Informaatio- ja tietoverkkosodankäynnin kohteina voivat olla päättäjät, kansalaiset, tiedotusvälineet, energialähteet, tietoverkot tai maanpuolustuksen keskeiset elementit.

Tietotekniikan avulla toteutetut rikokset lisääntyvät ja mahdollistavat rikoshyödyn nopean keräämisen sekä siirtämisen. Tietojärjestelmiin kohdistuvissa rikoksissa tekijä loukkaa tietojärjestelmän tiedon eheyttä, luottamuksellisuutta tai saatavuutta. Verkkoa käytetään muun muassa oikeudettomaan tiedon anastamiseen, tuhoamiseen tai käsittelyyn sekä laittoman sisällön välityskanavana, rikollisryhmien väliseen yhteydenpitoon rikosten valmistelussa, laittoman työvoiman rekrytointiin, omaisuusmassojen liikutteluun ja terroristisiin tarkoituksiin. Tietoverkkorikollisuuden seuraava kehitysvaihe tuo mukanaan erityisesti uusia asiakkaisiin kohdistuvia hyökkäystapoja, kuten sähköisten asiointipalvelujen sovellusistuntojen kaappaamisia ja massiivisessa määrin toteutettuja identiteettivarkauksia.

Suomeen kohdistuvien terroritekojen uhka on tällä hetkellä vähäinen, mutta uhka on viime vuosina lisääntynyt ja konkretisoitunut myös pohjoismaissa. Suomalaisia voi joutua terroritekojen kohteeksi myös ulkomailla muun muassa kriisinhallinta- tai muissa kansainvälisissä tehtävissä tai matkoilla. Teknologian kehitys lisää eivaltiollisten toimijoiden vaikuttamismahdollisuuksia. Yksittäisillä henkilöillä tai ryhmittymillä on entistä suuremmat tekniset mahdollisuudet aiheuttaa sellaista laajamittaista vahinkoa tai tuhoa, johon aiemmin pystyivät vain valtiot. Eivaltiolliset toimijat hyödyntävät erityisesti epäsymmetrisiä keinoja, jolloin valitaan haavoittuvimmat kohteet ja käytetään menetelmiä, joiden torjuntaan vastustaja ei ole riittävästi varautunut. Useimmat terrori-iskut tehdään edelleen omatekoisin räjähtein, mutta kemiallisten, biologisten, säteilevien tai muiden vaarallisten aineiden käyttömahdollisuus terroriteoissa on vakava uhka. Tieteen ja teknologian nopea kehitys luo uusia haasteita biologisten sekä kemiallisten aseiden leviämisen estämiselle.

Monipuolistuvat tehtävät kansainvälisissä kriisinhallintaoperaatioissa sekä niiden usein haastavat uhkaympäristöt lisäävät henkilöstöön kohdistuvia vaaroja. Tulevat kriisinhallintaoperaatiot toteutetaan todennäköisesti yhä vaikeammissa toimintaympäristöissä, joissa isäntämaatuki saattaa puuttua kokonaan ja kaluston kuluminen on nopeaa. Tapaturma-, onnettomuus- ja terveysvaarojen ohella saattaa operaatioalueella kehittyä myös merkittävä kriisinhallintatehtävissä palveleviin henkilöihin kohdistuva väkivallan uhka. Operaatioiden haastavuutta lisää se, että paikallinen väestö saattaa olla kriisinhallintajoukolle avoimen vihamielinen. Operaatioihin saattaa liittyä terrori-iskujen uhka myös Suomessa. Sodanomaiset olosuhteet ja niiden vaatimukset kriisinhallintaorganisaatioiden toiminnalle lisäävät myös joukkojen oman toiminnan aikaansaamien henkilötappioiden mahdollisuutta.

Suuronnettomuuksien tai poikkeuksellisten sääilmiöiden aiheuttamien luonnon-onnettomuuksien seurauksena on tavallisesti laajaa tu-

hoa tai vaaraa ihmisille, omaisuudelle tai ympäristölle. Nämä niin sanotut dynaamiset onnettomuudet tapahtuvat äkillisesti ja niiden vaikutusalue on aluksi paikallinen, mutta voi kasvaa jatkuvasti ajan kuluessa, ellei tehokasta pelastustoimintaa pystytä nopeasti organisoimaan.

Tartuntatautien leviämisen riskiä lisää ihmisten, eläinten ja elintarvikkeiden liikkuvuus. On odotettavissa, että aikaisemmin tuntemattomat tarttuvat taudit kuten SARS ja muuntuvat tunnetut taudinaiheuttajat, kuten influenssa A-virus, saattavat muuttua nopeasti väestöstä toiseen leviäviksi maailmanlaajuisiksi epidemioiksi. Tahallisesti levitettävät, mahdollisesti geenimuunnellut taudinaiheuttajat voivat tulevaisuudessa muodostaa nykyistä laaja-alaisemman uhkan.

Puolustushallinnon henkilöstön työkuorma kasvaa säästöpaineiden, henkilöstön vähentämisen ja jatkuvasti lisääntyvien normien sekä muiden vaatimusten myötä. Kasvava työkuorma saattaa heikentää henkilöstön työhyvinvointia, motivaatiota sekä huonontaa turvallisuuskulttuuria. Se voi myös heikentää sitoutuneisuutta työtehtäviin sekä lisätä tapaturmia ja lähtövaihtuvuutta. Heikko palvelus- ja työhyvinvointi vaikuttaa kielteisesti puolustushallinnon maineeseen ja haittaa uuden henkilöstön rekrytoimista. Huono työhyvinvointi kasvattaa myös eripuraa työpaikoilla ja väkivaltaisen purkautumisen mahdollisuuksia palvelus- ja työyhteisöissä.

Teknologian tuomat mahdollisuudet, organisaation tarpeet ja käyttäjien valmiudet eivät välttämättä kohtaa. Teknologiaa ei aina osata käyttää oikein eikä välttämättä ymmärretä, mihin käyttäjän tekemät virheet saattavat johtaa. Erilaisten viestivälineiden ja uusien sosiaalisten medioiden harkitsematon käyttö lisää tietovuotojen mahdollisuutta. Uuden teknologian mahdollistava liikkuva työskentely luo uudenlaisia vaatimuksia salassa pidettävän tiedon turvaamiselle niin ajan, paikan kuin käytettävyydenkin suhteen. Myös puolustushallinnon verkostoitumisen lisääntyminen muuhun yhteiskuntaan ja kansainvälisesti sekä uusien kumppanuuksien luominen jatkuu. Tämä lisää tarpeita luovuttaa salassa pidettävää tietoa hallinnonalan ulkopuolelle.

Kypsymätön turvallisuusjärjestelmä ja vastuiden tarkan määrittelyn puute kasvattavat osaltaan uhkien toteutumisen riskiä. Liian jäykkä turvallisuusjärjestelmä saattaa kasvattaa itsessään turvallisuusriskiä, koska tällöin reagointi nopeasti muuttuviin häiriötilanteisiin vaikeutuu.

Aukeaman kuvat: Kuvatoimisto Rodeo

Haasteellisemmaksi muuttuva vaatimusympäristö

Organisaatioiden turvallisuuden kehittämiseksi luodaan jatkuvasti uusia vaatimuksia ja vanhoja vaatimuksia ajanmukaistetaan. Tällaisia vaatimuksia ovat muun muassa kansainväliset ja kansalliset säädöstöt sekä yhteistoiminnassa sovitut menettelytavat. Vaatimuksia organisaatioiden turvallisuudelle asettavat myös erilaiset toimintaympäristöt ja niissä tapahtuvat muutokset.

Toimintaympäristö kehittyy

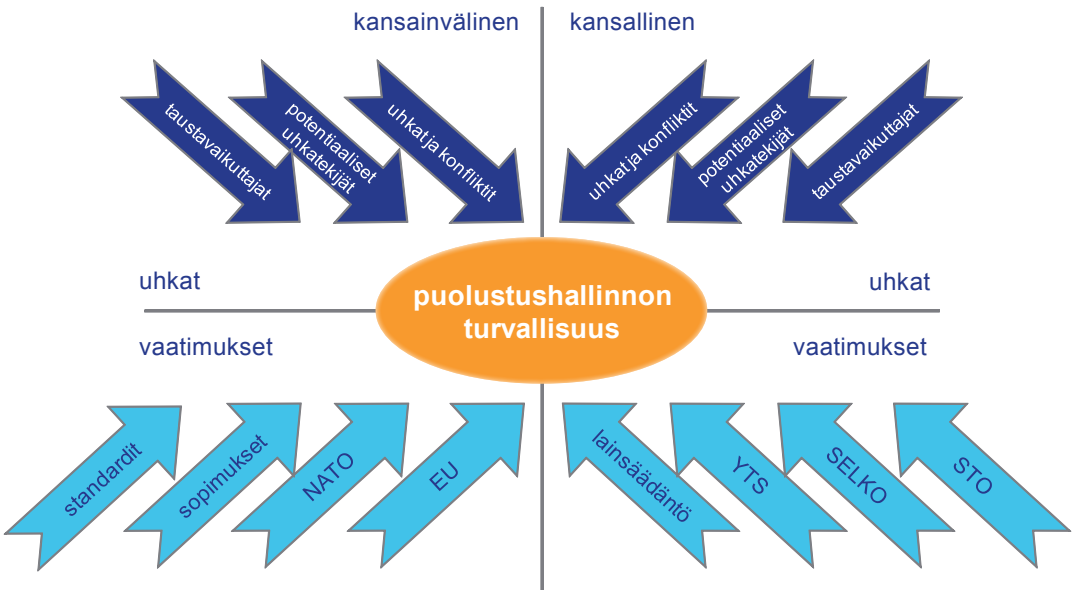
Palvelut, prosessit, tuotantoketjut ja järjestelmät automatisoituvat, monimutkaistuvat, integroituvat ja verkottuvat voimakkaasti.

Tietojen yhteiskäyttö laajenee ja automatisoituu.

Palvelut hankitaan usean toimittajan palveluverkostolta.

Palveluketjujen omistussuhteissa sekä sopimusvastuissa tulee tapahtumaan jatkuvasti muutoksia eivätkä omistajuus ja vastuut ole aina yksiselitteisiä.

Kansainvälisen yhteistoiminnan ja ohjauksen merkitys kasvaa voimakkaasti.



Kuva 1. Puolustushallinnon uhka- ja vaatimusympäristö

Laaja-alaisiin uhkiin varaudutaan osana eurooppalaisia ja maailmanlaajuisia yhteistyörakenteita ja järjestöjä, joiden kautta voidaan muun muassa poliittisella, taloudellisella, sotilaallisella sekä tieteellisellä ja teknologisella yhteistyöllä vahvistaa kansallisia kykyjä.

Euroopan unionissa tapahtuva integraatio tullee syvenemään jatkossa ja EU-maat muodostanevat yhä tiiviimmän yhteisön. EU:n turvallisuus- ja puolustuspolitiikka tulee kattamaan EU-maiden yhteisen varautumisen laajan turvallisuuskäsitteen uhkiin. Tällöin myös turvallisuuden toimintatavat yhtenäistyvät entisestään ja turvallisuusasioita hoidetaan yhä enemmän EU-johtoisesti. Kansallinen sopeutuminen EU:n turvallisuussäännöstöön edesauttaa sopeutumista myös Naton turvallisuussäännöstöön.

EU:n neuvoston ja komission yhdessä jäsenmaiden kanssa valmistelema turvallisuussäännöstö otettiin käyttöön vuonna 2001. Säännöstö velvoittaa jäsenmaita erityisesti tiedon suojaamisessa EU:n sisäisessä kanssakäymisessä, muttei jäsenmaiden omistamaan tietoon kohdistuvassa keskinäisessä tiedonvaihdossa. Säännöstö koskee erityisesti EU:n sotilasesikunnan välityksellä myös puolustusyhteistyötä ja sitä kautta kansallista turvallisuussuunnittelua.

Nato säilyy merkittävänä toimijana Euroopan turvallisuudessa jatkossakin. Nato on myös turvallisuuden osalta yksi standardien ja säännöstöjen luojista. Nato edellyttää rauhankumppaneilta toimivia turvallisuusjärjestelyjä, joita se myös aktiivisesti valvoo yhteistyössä kansallisten turvallisuusviranomaisten kanssa.

Suomi liittyi 2005 monikansalliseen yhteisöturvallisuustyöryhmään (Multinational Industrial Security Working Group, MISWG), jonka Nato-maat ovat perustaneet käytännön syistä Nato-organisaation ulkopuolelle. MISWG antaa työnsä tuloksena suosituksia ja konkreettisia toimintatapamalleja. MISWG-dokumentteihin perustuvat ohjeet liittyvät erityisesti puolustusmateriaalihankkeisiin sekä materiaalikuljetuksiin maasta toiseen.

Kansallisesti puolustushallinnon turvallisuutta ohjaa voimassaoleva lainsäädäntö, joka luo oikeudellisen perustan organisaatioiden turvallisuusjärjestelyille sekä asettaa turvallisuusjärjestelyille vähimmäisvaatimukset. Lainsäädännön lisäksi puolustushallinnon turvallisuutta ohjaavat kansalliset strategiset linjaukset.

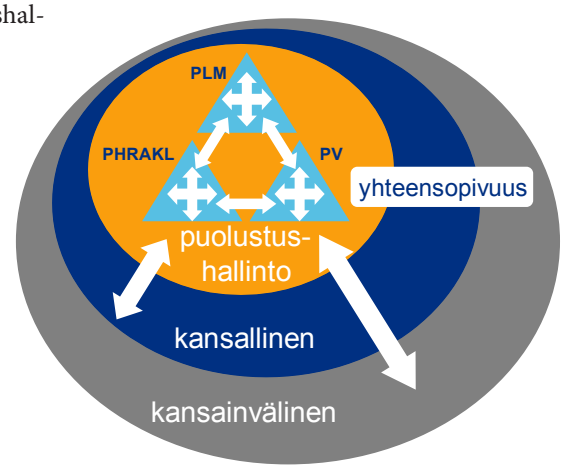
Tavoitetila

Tavoitetilassa puolustushallinnon päätehtävien häiriötön toteuttaminen ja kriittisten toimintojen jatkuvuus turvataan kaikissa tilanteissa siten, etteivät turvallisuusuhkat aiheuta ydintehtäville merkittävää haittaa. Jos haittaa aiheutuu, sen vaikutukset rajataan mahdollisimman pieniksi ja lyhytaikaisiksi. Tavoitetilassa puolustushallinnolla on kyky vastata olemassa oleviin turvallisuusuhkiin, osallistua kansalliseen ja kansainväliseen virka-apuun ja yhteistoimintaan, turvallisuutta koskevien vaatimusten hallintaan, turvallisuuden tilannekuvan muodostamiseen sekä turvalliseen kansainväliseen kriisinhallintaan.

Turvaamisen painopiste on ennakoivassa toiminnassa, jolla havaitaan, tunnistetaan ja torjutaan puolustusministeriön hallinnonalan toimintaa uhkaavat tekijät ja varaudutaan uhkaavien tekijöiden hallintaan. Puolustushallinnolla on myös kyky vastata nopeasti muuttuviin vaaratilanteisiin, häiriötilanteiden hallintaan sekä haittavaikutusten lieventämiseen ja niistä toipumiseen hallitusti. Turvaamiseen sisältyvät kaikki toiminnan osa-alueet, joilla tähdätään puolustusministeriön hallinnonalalla tärkeiden arvojen, kuten sen henkilöstön, tiedon, materiaalin, teknisen infrastruktuurin ja ympäristön turvaamiseen. Puolustushallinto pitää huolen henkilöstöstään, tiedoistaan sekä käyttämästään materiaalista ja infrastruktuurista niiden elinkaaren ajan. Mainittujen arvojen onnistunut turvaaminen vaikuttaa myönteisesti puolustushallinnon uskottavuuteen ja julkisuuskuvaan.

Tavoitetilassa valitut toimenpiteet kohdistuvat ydintehtävien kannalta kriittisimpien toimintojen ja muiden arvojen turvaamiseen. Puolustushallinnon päätehtävien turvaamisessa onnistuminen perustuu organisaatioiden turvallisuuteen liittyvien riskien ja haavoittuvuuksien analysointiin sekä organisaatioiden turvallisuuden tilannekuvan perusteella tehtävään päätöksentekoon. Näiden perusteella hallinnonalan turvallisuusriskejä hallitaan, turvattavat kohteet ja toiminnot priorisoidaan sekä käytettävissä olevat voimavarat mitoitetaan sekä kohdennetaan tarkoituksenmukaisimmalla tavalla.

Organisaatioiden turvallisuuden ylläpito ja kehittäminen vaatii tulevaisuudessa entistä laajempaa organisaatioiden välistä verkottumista ja tiiviimpää yhteistyötä. Tavoitetilassa turvallisuuden rakentamiseksi ja kehittämiseksi tehtävä yhteistyö puolustushallinnon organisaatioiden sisällä, organisaatioiden välillä ja ulkoisten organisaatioiden kanssa on sujuvaa. Puolustushallinnon organisaatioiden yhteistyö kansainvälisesti ja kansallisesti perustuu viranomaisten sekä muiden sidosryhmien kanssa yhdessä sovittujen turvallisten, luotettavien ja luottamuksellisten toimintatapojen noudattamiseen. Puolustushallinnon turvallisuuden toimintatavat ovat yhteensopivia kansainvälisten ja kansallisten yhteistoimintaosapuolten kanssa.



Kuva 2.
Turvallisuuden yhteistoiminnan kenttä

Tavoitetilassa turvallinen toiminta on luonnollinen osa kaikkea toimintaa organisaation kaikilla tasoilla. Turvallisuus on integroitu organisaatioiden prosesseihin, toimintamalleihin, hankkeisiin, projekteihin ja käytäntöihin. Turvallisuuden toteutuminen on osa organisaatioiden riskienhallintaa. Se on otettu huomioon toiminnan suunnittelussa, ja turvallisuuteen liittyvä toiminta on integroitu täysin normaaliin suunnittelujärjestelmään.

Tavoitetilassa puolustushallinto on vastannut informaatio- ja tietoverkkosodankäynnin uhkiin kehittämällä kyvyn, jolla muodostetaan ajantasainen tilannekuva, suojataan omat järjestelmät, minimoidaan uhkista ja niiden mahdollisesta toteutumisesta aiheutuvat haitat sekä mahdollistetaan viiveetön toipuminen ja oman toiminnan jatkuvuus.

Tavoitetilassa puolustushallinto täyttää lakien, asetusten ja kansainvälisten turvallisuusvelvoitteiden turvallisuusmääräykset osana jokapäiväistä toimintaansa ja toimintaympäristöään ja on edellä mainittujen perusteilla toimeenpannut perus-, korotetun- ja korkean tietoturvallisuustason tietoteknisissä järjestelyissään.

Organisaatioiden henkilöstö toimii ja työskentelee viihtyisässä toiminta- ja työympäristössä turvallisissa työskentelyolosuhteissa, joissa henkilöstö ei ylikuormitu toimintaa ja muita turvattavia arvoja vaarantavalla tavalla. Henkilöstöllä on käytössään työtehtäviä helpottavat työvälineet ja materiaali, joiden käyttö ei aiheuta vaaraa eikä toiminnassa tarvittava muu materiaali aiheuta hallitsematonta riskiä organisaatioille.

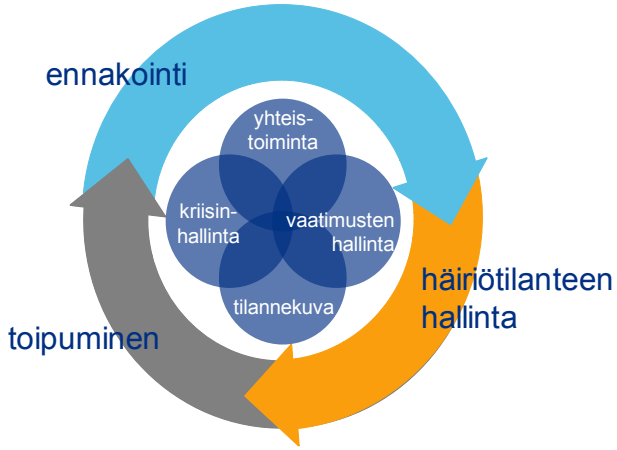
Tavoitetilassa henkilöstön työhyvinvointi tukee työssä jaksamista ja tuloksellista toimintaa. Henkilöstö asennoituu turvallisuuteen myönteisesti ja tahtoo tehdä työnsä turvallisesti oikein. Henkilöstö tekee päivittäin työssään ja työympäristössään turvallisia ratkaisuja ja tekee aina parhaansa turvallisuuden ylläpitämiseksi ja edistämiseksi.

Puolustushallinnon työyhteisössä arvostetaan henkilöstöä, tietoa ja taitoa sekä huolehditaan materiaalista. Henkilöstö arvostaa omaa ja toisen työtä sekä kokee itsensä ja työnsä tärkeäksi. Organisaatioiden henkilöstö ymmärtää turvallisen toiminnan periaatteet ja turvallisuuden merkityksen itselleen, muulle henkilöstölle, koko väestölle, muille turvattaville arvoille ja koko organisaatiolle.

Organisaatioiden oppiminen turvallisuuteensa liittyen on jatkuvaa, ja oppiminen perustuu henkilöstön kokemukseen, palautteeseen sekä helposti hankittavaan uuteen tietoon. Motivoitunut ja osaava henkilöstö osaa ratkaista arkipäiväiset turvallisuushaasteet turvallisuuden asiantuntijahenkilöstön keskittyessä turvallisuutta koskeviin erityishaasteisiin. Turvallisuuden johtaminen on luonnollinen osa ammattimaista esimiestaitoa.

Tavoitetilassa puolustushallinnon organisaatioissa vallitsee hyvä turvallisuuskulttuuri, joka muodostuu johdon ja muun henkilöstön sitoutumisesta, riittävästä ammattitaitoisesta ja motivoituneesta henkilöstöstä, tarkoituksenmukaisista taloudellisista ja ajallisista resursseista, ajantasaisesta normistosta sekä vaatimukset täyttävästä toiminnasta ja teknologiasta.

Turvallisuuden rakentamisen kyvyt



Kuva 3.
Puolustushallinnon turvallisuuden ylläpidon ja kehittämisen kyvyt

1. Kyky virka-apuun ja yhteistoimintaan muiden turvallisuusviranomaisten sekä sidosryhmien kanssa kansallisesti ja kansainvälisesti

Yhteistoiminta on edellytys hallinnonalan turvallisuustoiminnan onnistumiselle. Yhteistoiminta säästää resursseja, jotka ovat kohdennettavissa kehittämiseen. Organisaatioiden välinen yhteistoimintakyky riippuu oleellisesti henkilöstön osaamisesta ja vuorovaikutustaidoista eli tiedoista, taidoista ja yhteistyökyvystä. Rekrytoinnista alkaen on tärkeää löytää tarvittavan osaamisen ja oikean asenteen omaava henkilö oikeaan tehtävään, oikeanpituiseksi ajaksi. Soveltuvuus korostuu turvallisuustehtävissä palvelevien osalta, sillä heidän luotettavuuteensa ja oikeudenmukaisuuteensa kohdistuu muita enemmän odotuksia.

Puolustushallinnon tulee kyetä yhteiskunnan elintärkeiden kohteiden turvaamiseen ja virka-avun antamiseen muille viranomaisille. Tämä edellyttää ennakoivaa ja viranomaisten yhteistyössä tekemää säädösvalmistelutyötä, kansallisten tavoitteiden ja strategioiden laadintaa, koordinoivia toimia yhteistyöhön osallistuvien hallintojen eri tasoilla, koulutusta, harjoittelua, yhteistoiminnan arviointia ja tarpeeseen perustuvaa kehittämistä.

Puolustushallinnossa on oltava kyky sekä kansalliseen että kansainväliseen turvallisuusyhteistyöhön. Muiden viranomaisten ja elinkeinoelämän kanssa tehtävässä kansallisessa yhteistyössä on tärkeää saada vaikuttavuutta hallinnonalan näkemyksille ja tarpeille. Erityistä merkittävyyttä tällä on säädösvalmistelun ja kansallisen turvallisuuden asioissa. Kansainvälisessä yhteistyössä on tärkeää kyetä osoittamaan maan luotettavuus ja tarjoamaan yhteistyötahoille parhaita turvallisuuskäytänteitä. Siten voidaan odottaa niiden suhteen vastavuoroisuutta.

Puolustushallinnon alalla korostuu erilaisten turvallisuusluokiteltujen hankkeiden myötä kiinteä yhteistyö elinkeinoelämän kanssa myös turvallisuusasioissa. On pyrittävä saumattomaan ja molemminpuoliseen luottamukseen perustuvaan yhteistyöhön. Tätä edesauttavat kansallisesti hyväksytyt turvallisuuskriteerit.

2. Kyky turvallisuutta koskevien vaatimusten hallintaan

Turvallisuuden perusta on henkilöstön turvallinen ja oikea toiminta. Lait ja asetukset sekä eri hallinnonalojen ohjeet ja määräykset luovat oikeudellisen perustan organisaatioiden turvallisuusjärjestelyille sekä asettavat turvallisuudelle vähimmäisvaatimukset ja siten velvoittavat määrätyn turvallisuustason saavuttamisen. Hallitusohjelma, hallituksen periaatepäätökset, yhteiskunnan turvallisuusstrategia ja sisäisen turvallisuuden ohjelma asettavat myös vaatimuksia turvallisuudelle. Lisäksi Suomen solmimista kansainvälisistä, sekä kahdenvälisistä että monenkeskisistä, turvallisuussopimuksista muodostuu velvoitteita ja vaatimuksia. Jälkimmäisestä on esimerkkinä EU:n jäsenvaltioiden hallitusten välinen tietoturvallisuussopimus sekä EU:n neuvoston päätös EU:n turvaluokiteltujen tietojen suojaamiseksi.

Turvallisuutta koskevien vaatimusten tunnistaminen edellyttää perusteellista kartoittamista, joka on ensi askel vaatimusten hallintaan. Tässäkin suhteessa on korostettava kiinteää yhteyttä kansallisiin edustajiin erityisesti EU:ssa ja Natossa, joiden hankkeet asettavat suoria vaatimuksia turvallisuudelle.

Turvallisuus kuuluu kaikkiin prosesseihin. Hyvin järjestetty toiminta organisaatioketjussa ja prosessien välillä sekä laatutietoisesti valitut järjestelmät, laitteet ja toimitilat vähentävät turvallisuutta vaarantavia tekijöitä.

3. Kyky osallistua turvallisuuden tilannekuvan muodostamiseen hallinnonalana

Turvallisuuden tilannekuvan tarkoituksena on mahdollistaa puolustushallinnon turvallisuustoiminnan mukauttaminen turvallisuusuhkaan ja turvallisuusympäristön muutoksiin. Puolustushallinnolla tulee olla kyky tuottaa Valtioneuvoston yhteiseen tilannekuvaan hallinnonalan turvallisuuden kokonaistilannekuva, joka perustuu puolustushallinnon organisaatioiden turvallisuudesta saatuihin tietoihin. Toiminnan kannalta tämä tarkoittaa, että hallinnonalalle kuuluu kattavan toimintaympäristön ja turvallisuuden kehityssuuntien sekä lyhytviiveisen tilannekuvan ja ennakoivan analyysin tuottaminen, seuranta ja arviointi.

4. Kyky ennakointiin

Kyvyllä ennakoida ymmärretään kaikkia niitä toimenpiteitä, joilla tähdätään uhkien hallitsemiseen ja niiden toteutumisen todennäköisyyden ja haittavaikutusten vähentämiseen.

Ennakoivat toimenpiteet edellyttävät uhkien tunnistamisen etukäteen. Turvallisen toiminnan painopiste on ennaltaehkäisevässä toiminnassa. Tämän lisäksi on oltava kyky vastatoimiin tunnistettujen uhkien hallitsemiseksi sekä varautumiseen häiriötilanteiden varalle. Organisaation tulee kannustaa henkilöstöä valppauteen riskien suhteen ja oikeisiin toimintatapoihin. Periaatteellisesti yksilön väärin tekemän toimenpiteen sanktioimisen sijasta tulisi siirtyä palkitsemaan henkilöstöä siitä, että riskit eivät ole toteutuneet.

5. Kyky häiriötilanteiden hallintaan

Häiriötilanteen mahdollisuutta ei voida koskaan täysin poistaa, joten organisaation on varauduttava häiriötilanteen hallintaan. Jos häiriötilannetta ei kyetä ennakoimaan, korostuu kyky tilanteen hallintaan. Häiriötilanteessa tulee organisaatiolla olla kyky pelastaa turvattavat arvot eli henkilöstö, tiedot, materiaali ja tekninen infrastruktuuri sekä ympäristö. Sen myötä sillä on mahdollisuus säilyttää omaamansa julkisuuskuva. Henkilöstön turvaaminen on kaikissa tilanteissa etusijalla.

Henkilöstön toimintakyvyn säilymisellä varmistetaan organisaation toiminnan jatkuminen ja turvataan avainhenkilöiden päätöksentekokyky. Tämä korostuu häiriön vakavuuden lisääntyessä. Tiedon luottamuksellisuuden, saatavuuden ja eheyden säilymisen merkitys kasvaa häiriötilanteessa, jolloin mahdollisuus virheisiin on entisestään minimoitava. Tekninen infrastruktuuri luo edellytykset organisaation ja sen työntekijöiden toiminnalle. Se sisältää mm. tilat, järjestelmät, verkot, laitteet ja välineet. Niiden saumaton liittyminen toisiinsa ja järjestelmien hyvä vikasietokyky mahdollistavat toiminnan häiriötilanteenkin aikana.

Häiriötilanne on aina poikkeama normaalista toiminnasta. Se edellyttää henkilöstöltä osaamista, jonka voidaan ajatella jakautuvan koko henkilöstöltä vaadittavaan tietoon ja taitoon sekä häiriön tuntevien asiantuntijoiden erityisosaamiseen. Organisaation on kyettävä mm. koulutuksella varmistumaan osaamisen hallinnasta erilaisissa häiriötilanteissa. Häiriötilanteen haittavaikutukset on pyrittävä rajoittamaan mahdollisimman pieniksi. Mitä kriittisempi järjestelmä tai asia on, sitä paremmin haittavaikutukset on kyettävä rajaamaan. Kriittisten toimintojen häiriöiden hallintaohjeet tulee olla laadittu, koulutettu ja toiminta harjoiteltu. Lisäksi häiriötilanteiden synnystä sekä niiden hallinnan onnistumisesta kerätään tietoja, joiden perusteella kyetään edelleen parantamaan organisaation toimintamalleja.

6. Kyky toipumiseen

Organisaatiolla on oltava kyky hallittuun häiriöstä toipumiseen. Toipuminen on toiminnan jatkamista kohti normaalia olotilaa. Kyse on jatkuvuuden hallinnasta, joka on osa normaalia johtamista, suunnittelua ja toimintaa. Sen tulee kattaa kumppanit ja keskeiset mediaverkostot.

Tietoyhteiskunnassa korostuu kyky palauttaa turvallisuuden kannalta kriittisten järjestelmien toimintakyky. Niiden toimintakyvyn palauttaminen tulee tapahtua mahdollisimman nopeasti, jottei turvallisuudelle ehdi aiheutua vakavaa haittaa. Raportointi erityisesti tietojärjestelmien osalta on pyrittävä automatisoimaan mahdollisimman pitkälle, jotta analysointi voidaan aloittaa hyvin lyhyellä viipeellä. Perusteellisesti tehty analysointi yhdessä koulutuksen kanssa, joka tähtää vastaavan tilanteen ennaltaehkäisyyn, ovat keskeisessä roolissa häiriötilanteesta oppimisessa.

7. Kyky turvalliseen kansainväliseen kriisinhallintaan

Sotilaalliseen kriisinhallintaan osallistuminen perustuu laaja-alaiseen kansainväliseen yhteistyöhön. Sotilas- ja siviilikriisinhallinnan muodostamassa kokonaisuudessa varaudutaan erityisesti vaativiin ja pitkäkestoisiin kriisinhallintaoperaatioihin. Kansallisella tasolla tavoitteena on rakentaa sellaiset sotilaalliset kriisinhallinnan toimintaedellytykset, yleisjärjestelyt ja keskeiset toimintaperiaatteet, jotka mahdollistavat Suomen joukkojen ja henkilöstön turvallisen osallistumisen kriisinhallintaan.

Kansainvälisen sotilaallisen kriisinhallinnan arvioidaan muuttuvan lähitulevaisuudessa yhä haasteellisemmaksi vaativampien, nopeammin käynnistettävien ja kauempana olevien operaatioiden myötä. Tämä edellyttää puolustushallinnolta voimakasta panostamista operaatioturvallisuuteen mm. järjestelmällisellä riskienhallinnan kehittämisellä ja koulutuksella osana kriisinhallintaoperaatioiden suunnittelua, harjoittelua, toimeenpanoa ja purkamista. Lisäksi on varmistettava joukkojen omasuojan riittävä taso.

Kuva: Puolustusministeriö

Strategian toimeenpano

Turvallisuuden rakentaminen riskienhallinnan periaattein

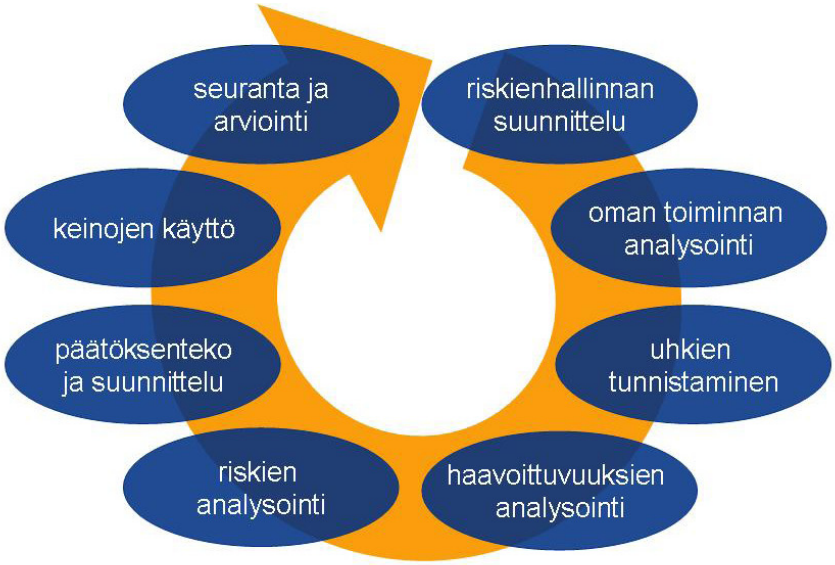
Organisaatioturvallisuuteen sisältyvät turvallisuuden kaikki osa-alueet, joilla tähdätään puolustusministeriön hallinnonalalla toiminnan, henkilöstön, tiedon, materiaalin, teknisen infrastruktuurin ja ympäristön turvaamiseen. Näistä asioista huolehtiminen ylläpitää hallinnonalan uskottavaa ja positiivista julkisuuskuvaa sekä kansalaisten maanpuolustustahtoa.

Organisaation turvallisuuden tavoitteet saavutetaan noudattamalla riskienhallinnan periaatteita. Turvallisuusriskienhallinnalla tarkoitetaan järjestelmällistä tapaa taata hallinnonalan toimintojen turvallinen toteutuminen kaikissa olosuhteissa. Turvallisuusriskienhallinta on osa organisaation kokonaisriskienhallintaa.

Turvallisuusriskienhallinta on jatkuvaa toimintaa, jolla pyritään turvaamaan hallinnonalan organisaatioiden voimavarat ja suorituskyvyt siten, että riskien toteutumisen todennäköisyys ja kokonaisvaikutukset ovat optimaalisesti mahdollisimman pienet ja organisaation toiminnan tavoitteet voidaan saavuttaa. Riskienhallinta liittyy kiinteästi tilanteen arviointiin ja siinä otetaan huomioon voimavarat, suorituskyky ja vallitsevien olosuhteiden vaikutukset.

Puolustushallinnossa riskienhallinnalla vähennetään toimintaan vaikuttavien häiriöiden syntymistä ja niistä aiheutuvia seurauksia pitkäjänteisesti ja suunnitelmallisesti kaikessa toiminnassa rauhan aikana mukaan lukien osallistuminen kansainvälisiin kriisinhallintaoperaatioihin sekä valmiutta kohotettaessa ja sodan aikana. Riskien vaikutukset otetaan huomioon kaikessa toiminnassa ja organisaatioiden kaikilla tasoilla.

Jokainen puolustushallinnon työntekijä ottaa huomioon riskienhallinnan periaatteet omassa



Kuva 4.
Turvallisuusriskienhallinnan prosessi

toiminnassaan. Esimiehet vastaavat organisaationsa riskienhallinnasta. Johdon sitoutuminen on ensimmäinen ja keskeinen askel kohti järjestelmällistä riskienhallintaa. Johdon sitoutuminen ilmenee käytännön toimenpiteissä, kuten turvallisuuteen vaikuttavien voimavarojen järjestämisessä, turvallisuuden tavoitteiden asettamisessa ja toteutettujen toimenpiteiden vaikuttavuuden seuraamisessa.

Onnistuneen riskienhallinnan perusteita ovat oman toiminnan analysointi, turvattavien arvojen määrittäminen, uhkien ja haavoittuvuuksien tunnistaminen ja turvallisuusriskien analysointi. Näitä riskienhallinnan perusteita tarvitaan kykyjen ja voimavarojen käyttöä koskevien perusteltujen päätösten tekemiseksi. Lisäksi tarvitaan tarkoituksenmukaiset menetelmät riskien hallitsemiseksi ja mahdollisilta uhkien toteutumisen haittavaikutuksilta toipumiseksi.

Organisaation oman toiminnan analysointi luo perustan turvattavien arvojen määrittämiselle ja siten auttaa kohdistamaan uhkien tunnistamisen ja riskien hallinnan toimenpiteet tarkoituksenmukaisimpiin kohteisiin. Oman toiminnan analysointi mahdollistaa myös omasta toiminnasta syntyvien uhkien tunnistamisen.

Uhkien tunnistamisen tarkoituksena on löytää tekijät, jotka voivat vaikuttaa haitallisesti organisaation turvattaviin arvoihin sekä toiminnan tavoitteiden saavuttamiseen. Koska organisaatioon kohdistuvat uhat ovat muuttuvia, on uhkien kartoitusta tehtävä jatkuvasti riskienhallintasuunnitelman mukaisesti. Haavoittuvuuksien tunnistaminen auttaa selvittämään turvattavien arvojen ja niitä turvaavien toimenpiteiden alttiudet häiriötilanteiden haittavaikutuksille.

Riskien analysoinnin tarkoituksena on tutkia organisaatiota uhkaavien tekijöiden mahdollisuuksia vaikuttaa haitallisesti organisaation toimintaan sekä haittavaikutusten vakavuutta ja turvallisuusjärjestelyjen riittävyyttä. Huolellinen riskien analysointi vaatii yleensä avointa ideointia ja ryhmätyöskentelyä. Riskianalyysien avulla löydetyt kehittämiskohteet siirretään organisaation toiminnan ja resurssien suunnittelujärjestelmään.

Järjestelmälliseen riskienhallintaan tulosyksiköt tarvitsevat riskienhallintasuunnitelman, jota ylläpidetään ja päivitetään säännöllisesti. Suunnitelma perustuu organisaation toiminnan ja talouden suunniteluun sekä riskienhallinnan periaatteisiin ja ohjeisiin. Riskienhallintasuunnitelmassa määritetään riskienhallinnan tavoitteet, tehtävät ja voimavarat. Toiminnasta, kohteesta tai hankkeesta vastaava johto päättää resursseista ja toteutettavista toimenpiteistä, joilla riskeihin vaikutetaan.

Riskien hallintaan tarvittavat voimavarat käytetään tarkoituksenmukaisesti ja mitoitetaan siten, että tunnistettujen uhkien muodostamien riskien hallintaan käytetään riittävästi resursseja kuitenkaan ylimitoittamatta niitä. Myös yllättävien häiriötilanteiden hallintaan ja haittavaikutuksista toipumiseen varataan tarkoituksenmukaisia voimavaroja.

Kykyjen käyttö

Merkittävän osan puolustushallinnon organisaatioiden turvallisuuden rakentumisesta muodostavat ammattitaitoiset, turvallisuuden johtamisen hallitsevat esimiehet ja henkilöstö, joka osaa toimia tehtävissään turvallisesti ja ymmärtää turvallisen toiminnan periaatteet ja tavoitteet. Henkilöstön riittävä osaaminen saavutetaan ylläpitämällä ja kehittämällä henkilöstön turvallisuustietoutta, perehdyttämällä uudet työntekijät työpaikkansa turvallisuusjärjestelyihin, toteuttamalla turvallisuuteen liittyviä tietoiskuja organisaation muun viestinnän ohella sekä täydennyskouluttamalla.

Lait ja asetukset luovat oikeudellisen perustan organisaatioiden turvallisuusjärjestelyille sekä vähimmäisvaatimukset organisaatioiden turvallisuudelle. Näiden lisäksi puolustushallinnon organisaatioiden toiminnan ominaispiirteistä johtuen ohjataan organisaatioiden toimintaa myös hallinnollisilla normeilla. Hallinnollisten normien laatimisessa noudatetaan tarveharkintaa ja niitä ylläpidetään suunnitelmallisesti. Puolustushallinnon kansainvälisessä toiminnassa otetaan huomioon myös kansainväliset ja kohdemaan kansalliset normit.

Teknologisin ratkaisuin mahdollistetaan henkilöstön sijoittaminen turvallisuuden kannalta merkittävimpiin tehtäviin ja täydennetään mahdollisuuksia valvoa tilannetta ja tapahtumia alueilla ja kohteissa, joihin henkilöstöä ei ole tarkoituksenmukaista sijoittaa. Teknisiä turvallisuusjärjestelmiä ylläpidetään ja kehitetään suunnitelmallisesti. Uusien järjestelmien hankinnoilla on kyettävä perustellusti pienentämään esille tulleita riskejä.

Puolustushallinnolla on yhteistoiminnassa muiden viranomaisten kanssa oltava kaikissa tilanteissa kyky luoda ja ylläpitää turvallisuuden tilannetietoisuutta, jossa korostuu tieto organisaatioon vaikuttavista uhkaavista ilmiöistä ja tekijöistä sekä ymmärrys omasta suorituskyvystä ja mahdollisuuksista vastata turvallisuutta vaarantaviin tekijöihin. Tosiasioihin perustuva tilannetietoisuus mahdollistaa turvallisuuden ylläpidon ja kehittämisen kannalta perustellun ja oikea-aikaisen päätöksenteon ja voimavarojen tarkoituksenmukaisen käytön. Turvallisuuden osa-alueista ohjausvastuussa olevat toimijat ylläpitävät tilannetietoisuuttaan osa-alueensa turvallisuudesta.

Puolustushallinnon organisaatioiden on kyettävä vastaamaan nopeasti muuttuviin uhkakuviin yhteistoiminnassa muiden viranomaisten kanssa ja nostamaan joustavasti turvallisuustasoaan uhkan aiheuttamien vaatimusten mukaisesti. Turvallisuustason kehittämisen kannalta on tärkeää myös seurata toimenpiteiden toteutusta ja käytännön vaikutuksia. Raportoinnilla on tärkeä merkitys riskienhallinnan jatkuvan kehittämisen kannalta.

Turvallisuuden tuottamiseen tarvittavat kyvyt ja keinot ovat osin päällekkäisiä ja jakautuvat turvallisuuden eri osa-alueille. On aikaisempaa selvemmin ymmärrettävä puolustushallinnon ulkopuolisten toimijoiden mahdollisuudet tukea hallinnonalan turvallisuuden tavoitteiden saavuttamista. Tarkoituksenmukaisinta voimavarojen käytön suunnittelussa on selvittää ja päättää, mitkä tavoitteet voidaan saavuttaa vain hallinnonalan voimavaroin, missä voidaan tehdä yhteistyötä muiden toimijoiden kanssa ja milloin joidenkin turvallisuuden tavoitteiden saavuttamiseen voidaan osaaminen ja muut voimavarat hankkia puolustushallinnon ulkopuolelta. Tukeuduttaessa muiden toimijoiden voimavaroihin on otettava huomioon, että valmiuden kohottamisen yhteydessä muiden viranomaisten ja sidosryhmien voimavarat sitoutuvat yhteiskunnan muiden toimintojen turvaamiseen.

Riskien hallintaa ja uhkien ennaltaehkäisemistä täydentävät toiminnan jatkuvuuden suunnittelu ja toipumissuunnittelu.

Puolustushallinnon turvallisuusjärjestelyjen kehittämiseksi tehdään tutkimustoimintaa. Se kohdistuu uhkien muodostumiseen, niiden taustavaikuttajiin, toteutettuihin turvallisuusjärjestelyihin sekä uusiin tarkoituksenmukaisiin ja kustannustehokkaisiin mahdollisuuksiin. Hallinnonalan turvallisuusjärjestelyjen kehittäminen tulee edellyttämään hallinnonalalta aktiivista osallistumista toimintamallien, teknisten ratkaisujen ja lainsäädännön kehittämiseen niin kansallisesti kuin kansainvälisestikin verkostoitumalla.

Strategian toteutumisen seuranta, arviointi ja ohjaus

Puolustushallinnon turvallisuuden strategian toteutumista seurataan, sitä arvioidaan ja tarvittaessa ohjataan tavoitetilan saavuttamiseksi. Seuranta perustuu tämän strategian liitteessä 1 esitettyihin tarkastuspisteisiin, joilla tarkoitetaan ajallisia ja toiminnallisia kriteerejä, joihin strategian toteutumista verrataan. Hallinnonalan organisaatiot asettavat näiden perusteella omat tavoitteensa, suunnittelevat turvallisuuteensa liittyvän toiminnan (TRSS) ja seuraavat tavoitteidensa toteutumista, joka raportoidaan kuten muu toiminta (VURA). Seuranta sisältää mm. asetuksen tietoturvallisuus valtionhallinnossa (681/2010) siirtymäaikojen toteutumisen valvonnan.

Turvallisen toiminnan arviointiin organisaatiot käyttävät Kansallista turvallisuusauditointikriteeristöä (KATAKRI). Sitä käytetään niin puolustushallinnon sisäiseen kuin ulkopuolisen toimijan turvallisuusauditointiin. Organisaatiot käyttävät myös puolustushallinnon sisäisiä kriteerejä täydentämään kansallisen turvallisuusauditoinnin kriteeristöä hallinnonalan erityispiirteiden osalta (esim. tekninen turvallisuus, varomääräykset). Arvioinnin, jossa otetaan huomioon salassa pidettävää aineistoa koskeva ohjeistus, tulee perustua tosiasioihin ja sen tulee olla läpinäkyvää ja osallistavaa.

Puolustushallinnon turvallisuuden strategian toteutumista arvioidaan vuosittain puolustusministeriön kokoon kutsumassa vuorovaikutteisessa seminaarissa, jossa puolustushallinnon organisaatiot esittävät omat arvionsa saavutetuista tuloksista.

Kuva: Puolustusvoimat

Kriittiset menestystekijät

Kriittisillä menestystekijöillä tarkoitetaan tässä strategiassa niitä tekijöitä, joiden täytyy onnistua, jotta puolustushallinnon turvallisuuden strategia toteutuu ja organisaatiot saavuttavat turvallisuutensa tavoitetilan. Tässä strategiassa kriittisiä menestystekijöitä ovat motivaatio, osaaminen, voimavarat ja johtajuus. Jokainen näistä on merkittävä, sillä yhdessä kriittisessä menestystekijässä epäonnistuminen estää organisaatiota saavuttamasta asetettua turvallisuuden tavoitetilaa tai ainakin hidastaa sen saavuttamista.

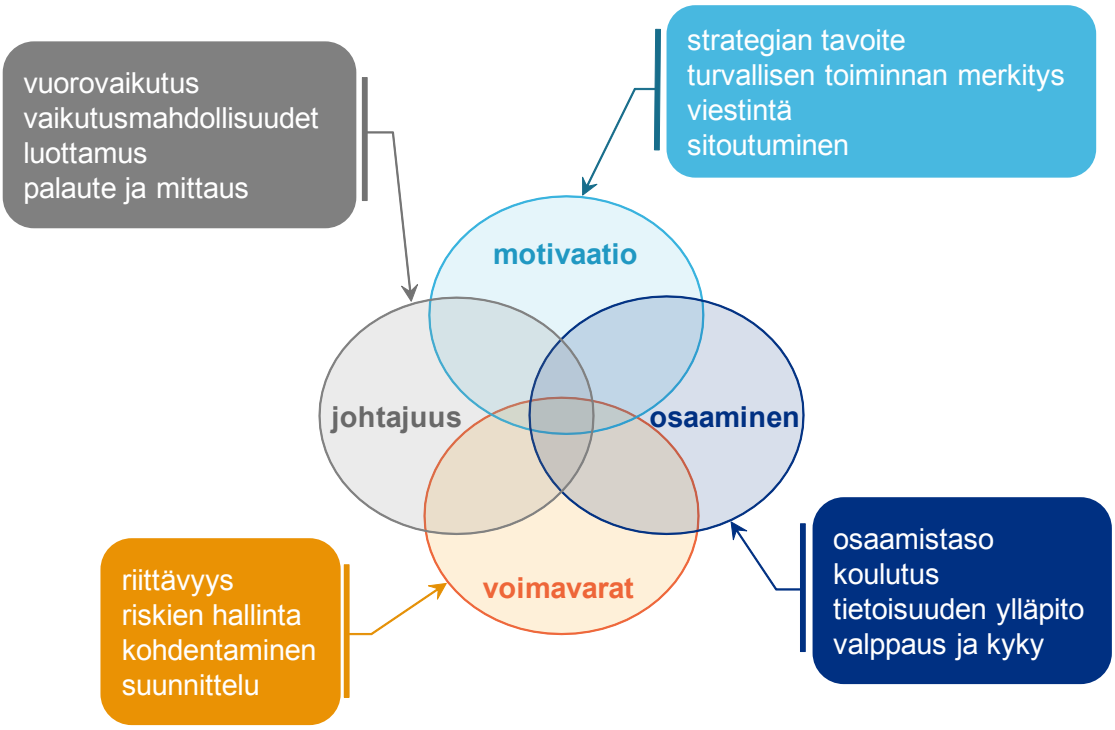
Henkilöstön, johto mukaan lukien, motivaatio perustuu ymmärrykselle siitä, mihin turvallisuuden strategialla tähdätään, miksi työtehtävissä tulee toimia turvallisesti ja mikä on kunkin toimijan merkitys oman toimintansa ja organisaationsa turvallisuuden tavoitteiden saavuttamisessa. Ymmärrys saavutetaan turvallisuuden strategiaan perustuvalla koko henkilöstön tavoittavalla viestinnällä. Hyvä motivaatio on hyvän turvallisuuskulttuurin yksi ilmenemä, joka luodaan usealla keinolla. Näitä ovat hyvä turvallisuuden johtaminen, osaamisen kehittäminen ja hallinta sekä viestintä. Motivaatio näkyy koko henkilöstön sitoutumisessa turvallisten ratkaisujen toteuttamiseen.

Henkilöstön osaaminen osaltaan mahdollistaa strategian onnistumisen. Osaaminen perustuu kunkin toimijan työtehtävissään tarvitsemiin tiedollisiin ja taidollisiin vaatimuksiin. Organisaation turvallisuuden osaamisen ylläpitoon ja mahdollisiin puutteisiin osaamisessa vastataan kartoittamalla olemassa oleva osaamistaso, kouluttamalla tarvittaessa henkilöstöä ja pitämällä ennakoivasti yllä henkilöstön tietoisuutta turvallisuuteen liittyvistä tekijöistä sekä mahdollisista muutoksista. Henkilöstön osaaminen näkyy turvallisena toimintana sekä valppautena ja kykynä ryhtyä toimenpiteisiin erilaisten häiriöiden hallitsemiseksi.

Turvallisuuden tavoitetilan saavuttaakseen organisaatio tarvitsee motivoituneen ja osaavan henkilöstön lisäksi tarkoituksenmukaiset ja riittävät voimavarat. Riskienhallinnan periaattein selvitetään millä osa-alueella organisaatio tarvitsee enemmän resursseja turvallisuutensa ylläpitoon ja kehittämiseen sekä miltä osa-alueelta voidaan tarvittaessa resursseja kohdentaa ja muuttaa joustavasti voimavarojen käytön painopistettä. Organisaation turvallisuuden ylläpitämiseksi ja kehittämiseksi tarvittavien voimavarojen riittävyyteen vaikutetaan järjestelmällisellä ja todellisiin tarpeisiin perustuvalla suunnittelulla.

Turvallisuuden johtaminen on jokapäiväinen ja luonnollinen osa puolustushallinnon organisaatioiden yleisjohtamista. Turvallisuuden strategian tavoitteiden saavuttamiseksi on organisaation henkilöstöä ja voimavarojen käyttöä johdettava vuorovaikutteisesti, siten että myös työntekijöillä on todelliset mahdollisuudet vaikuttaa työnsä turvallisuuden ylläpitoon ja kehittämiseen. Luottamus johdon tahtoon ja kykyyn saada organisaatio saavuttamaan turvallisuuden tavoitetila perustuu avoimeen palautteen antamiseen ja saamiseen. Mittaamalla turvalliselle toiminnalle asetettujen tavoitteiden saavuttamista ja organisaation suorituskykyä selvitetään mihin suuntaan organisaation turvallisuus on kehittymässä ja miten turvallisuuden strategian toteuttamisessa on onnistuttu.

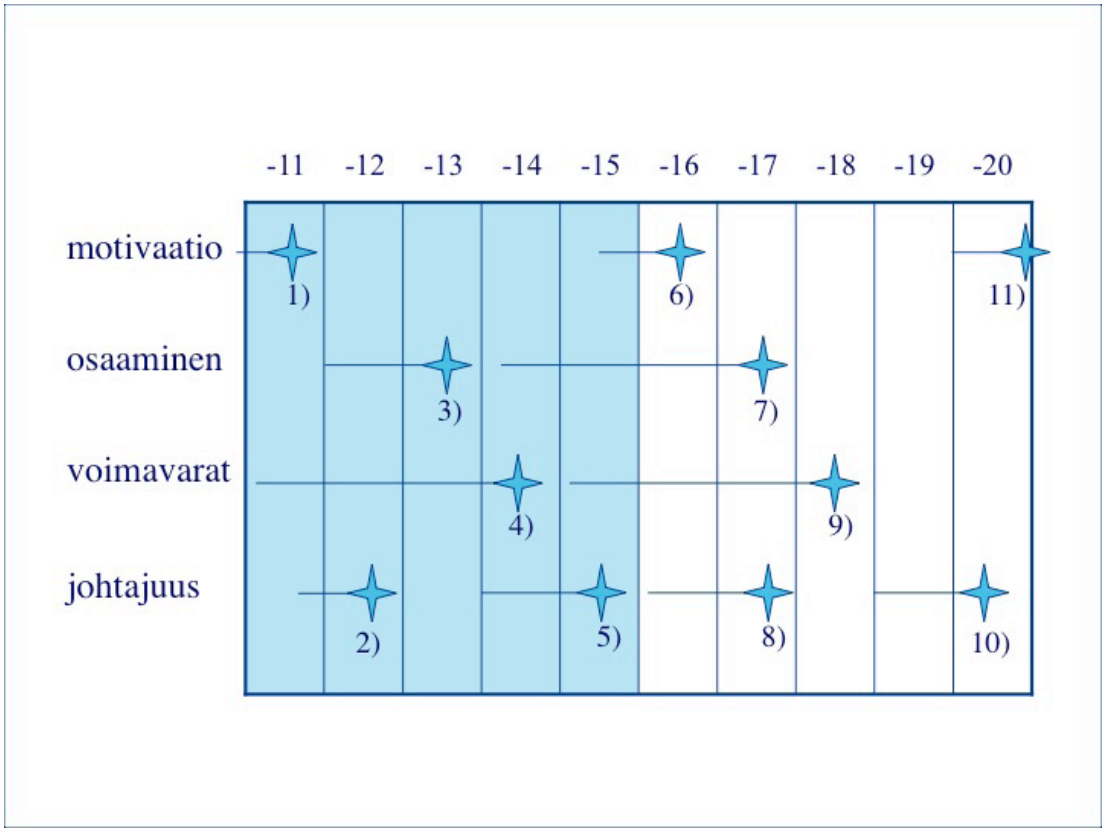
Kuva 5. Kriittiset menestystekijät



Liite 1

Osatavoitteet ja tarkastuspisteet

1. puolustushallinnon turvallisuuden strategian tarkoituksen ja toteutuksen periaatteiden viestiminen organisaatioissa
2. turvallisuuden tilannetietoisuuden mallin kehittäminen ja testaaminen
3. organisaatioiden koko henkilöstön turvallisuuteen liittyvän osaamistarpeen sekä olemassa olevan osaamisen kartoittaminen
4. hallinnonalan yhteisen riskienhallintamallin kehittäminen ja testaaminen; organisaatioiden turvallisuuteen tarvittavien voimavarojen kartoittaminen
5. puolustushallinnon turvallisuuden strategian päivittäminen
6. puolustushallinnon turvallisuuden päivitetyn strategian tarkoituksen ja toteutuksen periaatteiden viestiminen organisaatioissa
7. osaamiskartoitusta ja koulutustarvetta vastaavan täydennyskoulutusjärjestelmän kehittäminen
8. väärinkäytösten hallinnan menettelyjen kehittäminen
9. hallinnonalan organisaatioiden riskienhallintajärjestelmän kehittäminen johtamisen eri tasoille
10. puolustushallinnon turvallisuuden strategian päivittäminen
11. puolustushallinnon turvallisuuden päivitetyn strategian tarkoituksen ja t oteutuksen periaatteiden viestiminen organisaatioissa


-11
-12
-13
-14
-15
-16
-17
-18
-19
-20
motivaatio
osaaminen
voimavarat
johtajuus
1)
2)
3)
4)
5)
6)
7)
8)
9)
10)
11)

Liite 2 Keskeisiä määritelmiä

Akkreditointi (accreditation)
Akkreditointi eli hyväksyntä on prosessi, jonka päätteeksi hyväksyvä viranomainen antaa virallisen lausunnon siitä, että esim. tietojärjestelmä on hyväksytty käytettäväksi määritellyssä turvallisuusluokassa tiettyä turvallisuuden takaavaa toimintatapaa noudattaen käyttöympäristössään ja hyväksyttävällä riskitasolla sen pohjalta, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvallisuustoimenpiteet on toteutettu.

Auditointi (audit)
Kohteen ja sen toiminnan tarkastus ennalta asetettujen ja hyväksyttyjen arviointiperusteiden mukaan.

Fyysinen turvallisuus (physical security)
Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten suojaustoimenpiteiden toteuttamista niin, että estetään tuhot ja vahingot henkilöitä, laitteita, aineistoja sekä kiinteistöjä vastaan. Sen keskeinen osa on tilaturvallisuus, jota tuetaan vartioinnilla.

Haavoittuvuusanalyysi (vulnerability analysis)
Haavoittuvuusanalyysillä selvitetään olemassa oleva turvallisuustaso ts. kuinka haavoittuva turvattava kohde on.

Hallinnollinen turvallisuus (administrative security)
Hallinnollisella turvallisuudella tarkoitetaan turvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta.

Henkilöstön turvallisuushallinto (personnel security administration)
Henkilöstön turvallisuushallinto käsittää taustatarkastukset, toimenkuvien ja sijaisuuksien määrittelyn, pääsyoikeuksien määrittelyn, hallinnoinnin ja valvonnan kohteisiin ja tietoihin sekä näihin liittyvän koulutuksen.

Henkilöstöturvallisuus (personnel safety and security)
Henkilöstöturvallisuudella tarkoitetaan henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen järjestelyihin liittyvien turvallisuustekijöiden hoitamista.

Henkilöturvallisuus (personal safety and security)
Henkilöturvallisuus käsittää ne toimenpiteet, joilla puolustushallinnon henkilöstön turvallisuudesta huolehditaan.

Laaja-alaiset turvallisuusuhkat (extensive security threats)
Uhkia, jotka aiheuttavat merkittävää vaaraa väestölle tai vakavaa tai merkittävää haittaa yhteiskunnan elintärkeille toiminnoille. Ne ovat joko ihmisten aktiivista toimintaa (esim. tietoverkkojen haittaohjelmat tai terrorismi) tahattomia tapahtumia (esim. sähköverkon laajat toimintahäiriöt ja ydinvoimalaonnettomuus) tai luonnon ääri-ilmiöt. Näille usein valtion rajat ylittäville uhkille on tyypillistä arvaamattomuus, ennakoimisen ja paikallistamisen vaikeus sekä lyhyet varoitusajat. Ne ovat usein sidoksissa sotilaallisiin uhkiin tai osa niitä.

Lupahallinto (permission administration)

Turvallisuuden lupahallinto käsittää toimenpiteet, joilla annetaan turvallisuuteen kuuluvia oikeuksia. Esim. oikeutetuille henkilöille annetaan pääsyoikeus sotilaskohteeseen, perehtymisoikeudet tietoihin, käsittelyoikeus tietojärjestelmään tai materiaaliin.

Omistaja (owner)

Oikeushenkilö, joka on päätösvaltainen esim. tietoa, materiaalia tai kohdetta koskevissa kysymyksissä. Liittyy usein päätösvaltaan ja allekirjoitusoikeuteen.

Organisaatioturvallisuus (organisational security)

Organisaatioturvallisuus sisältää kaikki ne keinot, joilla turvataan organisaation henkilöstö, tiedot, materiaali ja tekninen infrastruktuuri sekä ympäristö. Organisaatioturvallisuudella varmistetaan organisaation toiminnan jatkuvuus kaikissa tilanteissa.

Riski (risk)

Riski on vahingon mahdollisuus. Riski muodostuu, kun uhkalle arvioidaan todennäköisyys ja vaikutus. Riskin toteutumiseen vaikuttaa se, kuinka hyvin olemme varautuneet riskien taustalla olevia uhkia vastaan. Riskiä voidaan pitää siedettävänä, jos sitä on vähennetty sellaiselle tasolle, jonka organisaatio voi sallia ottaen huomioon lakisääteiset velvoitteensa ja omat turvallisuudelle asettamansa tavoitteet.

Riskianalyysi (risk analysis)

Etukäteen laadittujen suunnitelmien ja täsmällisten menetelmien mukaisesti tehtävä uhkien sekä niiden toteutumisen todennäköisyyksien ja aiheuttaman vahingon suuruuden selvitys ja analysointi. Analyysiin sisältyy usein toimenpide-ehdotuksia. Usein virheellisesti käsitetään synonyymiksi käsitteille uhka-analyysi ja haavoittuvuustutkimus.

Riskienhallinta (risk management)

Järjestelmällinen tapa turvata voimavarat ja toiminta siten, että riskien kokonaisvaikutukset ovat optimaalisesti mahdollisimman pienet ja asetetut tavoitteet voidaan saavuttaa. Riskienhallinnan vaiheita ovat esim. oman toiminnan kartoitus, uhkien kartoitus, riskien tunnistaminen, riskien analysointi, riskienhallintamenetelmän valinta, riskien poistaminen, pienentäminen, siirtäminen, pitäminen omalla vastuulla ja riskienhallinnan organisointi.

Tietoturvallisuus (information security)

Tietoturvallisuudella tarkoitetaan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä.

Turvaaminen (securing)

Turvaaminen on toimintaa, jolla pyritään säilyttämään arvokkaana pidetyt asiat, valmistaudutaan vaaranaiheuttajien ehkäisemiseen ja torjuntaan, vapaudutaan uhkista sekä tuotetaan levollisuutta, varmuutta ja tunne tilanteen ennustettavuudesta.

Turvallisuus (security and safety)
Turvallisuus on olotila, jossa ei ole tosiasiallista uhkaa tai tiedossa olevat uhat eivät aiheuta merkittävää riskiä. Mahdolliset turvallisuutta heikentävät riskit ovat hallinnassa hyväksyttävällä tasolla ja uhkien ehkäisemiseksi sekä torjumiseksi on olemassa riittävät edellytykset. Lisäksi olotila koetaan turvalliseksi ja pysyväksi.

Turvallisuuspolitiikka (security policy)
Organisaation turvallisuuspolitiikka on niiden päätösten kokonaisuus, joilla vaikutetaan turvallisuuden muodostumiseen ja kehitykseen. Organisaation valitsema turvallisuusperiaatteiden soveltamistapa. Organisaation johdon hyväksymä periaatteellinen näkemys turvallisuuskäytännöistä, jotka otetaan huomioon kaikessa toiminnassa.

Turvallisuustoiminta (security)
Kaikkeen toimintaan ja jokapäiväiseen työhön liittyvät toimenpiteet, joilla pyritään takaamaan puolustushallinnon tehtävien mahdollisimman häiriötön toteuttaminen sekä estämään kaikenlainen puolustushallintoon tai sen kohteisiin suunnattu vahingollinen toiminta.

Turvallisuusvalvonta (security surveillance)
Kohteen, alueen, tilan tai järjestelmän turvallisuustilanteen tarkkailu ja tapahtumista ilmoittaminen sekä tilannekuvan muodostaminen.

Työhyvinvointi (occupational welfare)
Työhyvinvointi on työorganisaation, työyhteisön, fyysisen ympäristön, työn ja työntekijän ominaisuuksien ja voimavarojen muodostama vuorovaikutteinen kokonaisuus. Työhyvinvointi tukee työssä jaksamista, työkyvyn säilymistä ja ehkäisee ennenaikaista siirtymistä pois työelämästä.

Työ- ja palvelusturvallisuus (occupational and in-service safety)
Työ- ja palvelusturvallisuus käsitetään olosuhteina ja tekijöinä, jotka vaikuttavat organisaation henkilöstön ja tilapäisten työntekijöiden, urakoitsijana toimivan henkilöstön, vierailijoiden tai kenen tahansa henkilön hyvinvointiin työpaikalla. Työ- ja palvelusturvallisuutta voidaan arvioida vaarojen tunnistamisen ja niiden aiheuttaman riskin perusteella.

Työ- ja palvelusturvallisuustoiminta (occupational and in-service safety management)
Työ- ja palvelusturvallisuustoiminta on osana henkilöturvallisuutta joukon ja yksilön suorituskykyä sekä sodan ajan taistelukelpoisuutta edistävää ja toiminnan häiriöttömyyttä varmistavaa toimintaa. Se käsittää ne puolustushallinnon huolehtimisvelvoitteiden (työturvallisuuslainsäädäntö yms.) mukaiset toimenpiteet, jotka ovat tarpeen joukkojen ja henkilöstön suorituskyvyn (taistelukelpoisuuden ja työkyvyn) varmistamiseksi.

Uhka (threat)
Uhka on vahingollisen tapahtuman tuottava tekijä ja se on usein vaikeasti määriteltävä kokonaisuus, joka tapahtuessaan voi aiheuttaa turvattaville arvoille haittaa tai muuta ei-toivottua.

Uhka-analyysi (threat analysis)
Sisäisten ja ulkoisten uhkien tunnistamiseen ja riskien arvioinnin pohjaksi tehtävä analyysi. Tavoitteena on kartoittaa uhat ja analysoida uhkien sisältöä ja laatua.

Puolustusministeriö
Försvarsministeriet
Ministry of Defence