RISKIENHALLINNAN JÄRJESTÄMINEN PUOLUSTUSVOIMISSA COSO ERM -MALLIN MUKAISESTI; ESIMERKKINÄ PUOLUSTUSVOIMIEN JOHTAMISJÄRJESTELMÄKESKUS

10. Turvallisuusjohdon
Koulutusohjelma

Teknillinen Korkeakoulu,
Koulutuskeskus Dipoli

Tutkielma 20.2.2010

Jari Oinonen

TEKNILLINEN KORKEAKOULU

Kurssi

Turvallisuusjohdon koulutusohjelma 10

Tekijä

Jari Oinonen

Tutkimustyön nimi

RISKIENHALLINNAN JÄRJESTÄMINEN PUOLUSTUSVOIMISSA COSO ERM -MALLIN MUKAISESTI; ESIMERKKINÄ PUOLUSTUSVOIMIEN JOHTAMIS-JÄRJESTELMÄKESKUS

Oppiaine, johon työ liittyy	Säilytyspaikka
Turvallisuusjohtaminen	Aalto-yliopiston elektroninen julkaisuarkisto
Aika Helmikuu 2010	Tekstisivuja 35 Liitesivuja 4

TIIVISTELMÄ

Opinnäytetyössä tarkastellaan kokonaisriskienhallintaan tähtäävää johtamismallia, COSO ERM:ia, puolustushallinnon (strateginen taso) alaisen tason eli puolustushaaran/joukko-osaston (taktinen taso) näkökulmasta. Tällä rajataan turvallisuuden laajempi konteksti, erilaiset kansainväliset ja valtiolliset uhkamallit, niiden määrittely ja keskinäinen riippuvuus, työn ulkopuolelle. ERM on suomennettuna yrityksen riskienhallinta, mutta tätä nimitystä mallista ei juurikaan käytetä. Yleisemmin malli tunnetaan joko sen englanninkielisellä lyhenteellä tai vain kokonais- tai yritysturvallisuutena.

Kokonaisturvallisuuden liittyminen puolustusvoimien riskienhallintaan on periaatteessa näkökulmakysymys; miten samaa turvallisuuden kokonaisuutta ja tehtäväkenttää voidaan tarkastella siten, että kaikilla osapuolilla on asiasta joukko-osastotasolla samankaltainen näkemys? Tässä työssä turvallisuuden näkemys kootaan puolustusvoimien turvallisuusstrategian ja yritysturvallisuuden mallin yhdistelmäksi tavoitteena mallintaa turvallisuuden eri osa-alueiden ymmärtäminen ja riskienhallinta, organisointi ja toteutus puolustusvoimien joukko-osastoissa yhdellä, mutta joukko-osastojen varioitavissa olevalla, tavalla.

Tutkimuskysymykset:

- Miten Puolustusvoimien Johtamisjärjestelmäkeskuksen (PVJJK) turvallisuusjärjestelmä tulee luoda kokonaisturvallisuuden mallin mukaisesti?
- Voidaanko esitettyä mallia soveltaa laajalti, ja millä poikkeuksilla, puolustusvoimien mui-

hin joukko-osastoihin?

Tutkimustuloksia:

Opinnäytetyössä esimerkkinä olleen Puolustusvoimien Johtamisjärjestelmäkeskuksen turvallisuus tulee rakentaa kokonaisturvallisuuden mallin mukaisesti siten, että kaikki ne osa-alueet, joissa keskuksella on toimintaa, tulee organisoida johdon asettamaan tavoitetilaan sitoen (operatiivisten tietojärjestelmien käytettävyys kaikissa tilanteissa). Osa-alueisiin tulee ryhmitellä puolustusvoimien normikokoelmasta ne menetelmät, joilla on joko hallinnollista tai toiminnallista käyttöä laitoksen riskienhallinnassa. Käytännössä tämä tarkoittaa sitä, että osa riskeistä tulee aluksi pitää, mutta tavoitteiden saavuttamisen (riskien laskemisen) myötä voidaan keskittyä nouseviin riskeihin tai jo prosesseista löydettyjen riskien laskemiseen. Riskienhallinnan saaminen osaksi koko organisaation prosesseja ja niiden johtamista johtaa myös riskitason yleiseen alenemaan. Tässä mallissa turvallisuusala tarjoaa tukiprosessina ydinprosesseille käsittely-/ajatusmallin, riskianalyysin sekä toimialansa riskienhallinnan menetelmiä. Menetelmiä löytyy myös muilta toimialoilta, kuten henkilöstöhallinnosta (mikä onkaan se kriittinen työvaihe, johon vaaditaan lisähenkilöstöä). Käytännössä tämä tarkoittaa toimintojen vastuuttamista mahdollisimman alas ja substanssiosaamisen merkityksen korostamista läpi koko organisaation.

Mallia voidaan soveltaa sellaisenaan kaikkiin puolustusvoimien organisaatioihin, mutta se vaatii organisaatiolta tavoitteen määrittelyä toiminnan eri tasoilla (mikä on olemassa olomme tavoite, johon koko organisaatio pyrkii), jossa riskit määrittävät tehtäviä päätöksiä. Näin toimittaessa saavutetaan riskien hallinnalla ja sisäisellä valvonnalla myös itsesääntelylle kokonaisuutena asetettuja tavoitteita, joita ovat muun muassa toiminnan tehokkuus, asiantuntevuus, asian nopea käsittely sekä mahdollisuus ennakkotietoon.

Työhön ei ole välittömästi liitettäviä jatkotutkimusvaihtoehtoja. Lähin tavoitteellinen muutos, jota opinnäytteen kautta voidaan lähteä soveltamaan, on ohjeistaa puolustushaarojen ja joukko-osastojen turvallisuustoiminnot organisoitavaksi kokonaisturvallisuuden mallin mukaisesti, jolloin joukkojen tehtäväkentät (ja tehtävänkuvaukset) sekä niitä vastaavat henkilöstömäärät saadaan toisiinsa nähden vertailukelpoisiksi. Jatkotyönä voidaan lähteä muuttamaan puolustusvoimien johtamista riskienhallinnan lähtökohdista sekä riskienhallinnan normittamista osaksi sisäistä valvontaa eli Corporate Governancea.

AVAINSANAT

COSO ERM (kokonaisturvallisuus), riskienhallinta, sisäinen valvonta, puolustusvoimat

RISKIENHALLINNAN JÄRJESTÄMINEN PUOLUSTUSVOIMISSA COSO ERM - MALLIN MUKAISESTI; ESIMERKKINÄ PUOLUSTUSVOIMIEN JOHTAMISJÄRJESTELMÄKESKUS

LIITTEET

KUVALUETTELO

RISKIENHALLINTA PUOLUSTUSVOIMISSA COSO ERM -MALLIN MUKAISESTI; ESIMERKKINÄ PUOLUSTUSVOIMIEN JOHTAMISJÄRJESTELMÄKESKUS

1. JOHDANTO

1.1 Aihealueesta

COSO (Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management) tuotti 1990-luvun alussa julkaisun 'Internal Control - Integrated Framework' (Sisäinen valvonta - kokonaisvaltainen ajatusmalli). "Julkaisun tarkoituksena oli auttaa yrityksiä ja muita yhteisöjä arvioimaan ja tehostamaan sisäisiä valvontajärjestelmiään. Siinä esitetystä mallista on sittemmin tullut osa strategioita, sääntöjä ja määräyksiä ja tuhannet organisaatiot soveltavat sitä pitääkseen toimintansa tavoitteidensa mukaisina." Maailman globalisoituessa, kilpailun kiristyessä ja yritysten verkottuessa on riskien tunnistaminen, arviointi ja hallinta saatava osaksi tätä "kiristyvää verkkoa". Tämän tavoitteen saavuttamiseksi "käynnisti COSO Price Water House Coopersin kanssa vuonna 2001 projektin luodakseen mallin, jolla johto voi helposti arvioida ja kehittää organisaationsa riskienhallintaa. Samanaikaisesti mallin kehittämistyön kanssa eri maita ravisteli joukko näyttäviä yritysskandaaleja ja -romahduksia, joissa sijoittajat, yritysten henkilökunta ja muut sidosryhmät kärsivät huomattavia menetyksiä. Kävi yhä tarpeellisemmaksi saada aikaan riskienhallinnan malli, jossa määritellään toiminnan keskeiset käsitteet ja periaatteet, yhteinen kieli ja selkeät toimintaohjeet." Vuonna 2004 julkaistu 'Enterprise Risk Management - Integrated Framework', tai tuttavallisemmin COSO ERM, on tällainen malli. Sen tarkoituksena ei ole syrjäyttää sisäisen valvonnan mallia vaan liittää se osaksi riskienhallintaa. "Organisaation johdon vaikeimpia haasteita onkin päättää, missä määrin se on valmis sietämään riskejä pyrkiessään arvon luomiseen."[1]

Käsitteenä Enterprise Risk Managementin levinneisyyttä voidaan todentaa helposti esimerkiksi internet –hakukoneilla, joista Google antoi hakusanalle 23.1.2010 tehdyssä kansainvälisessä haussa yhteensä 11,9 miljoonaa osumaa. Suomenkielisiltä sivuilta osumia löytyi "vain"

[1] Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management - Integrated Framework (Kokonaisvaltainen ajatusmalli organisaation riskienhallintaan), PDF-muotoinen nettijulkaisu ja siitä suomennos, syyskuu 2004, tiivistelmä, s. 3. COSO:n mukaan "Enterprise Risk Management - Integrated Framework käsittelee sisäistä valvontaa entistä kattavammin ja keskittyy aikaisempaa selkeämmin ja perusteellisemmin organisaatioiden riskienhallintaan.

28 500, joten ilmiö on selvästi kansainvälisesti painottunut. Enterprise Risk Management (jatkossa ERM) on suomennettuna 'yrityksen riskin hallinnointi ja/tai kokonaisturvallisuus', mutta näitä nimityksiä ilmiöstä ei kirjallisuudessa juurikaan käytetä. Syynä lienee kansainvälisestä kielenkäytöstä suomeenkin vakiintunut ja yhteisesti hyväksytty termi.

Suomeen ERM on rantautunut etenkin Elinkeinoelämän Keskusliiton, EK:n, kautta, joka on tutkinut mallia ja antanut siitä suosituksia yritysten käyttöön. EK käyttää mallista nimeä yritysturvallisuuden malli, mutta käytännössä kyse on ERM:n rinnalla kehitetystä kokonaisturvallisuuden "suomalaisesta" versiosta. EK:n yritysturvallisuuden malli sisältää taustat ja perusteet yritysturvallisuuden kehittämiselle, mallin johtavat periaatteet ja yksityiskohtaisen sisällön, itse mallin sekä sen soveltamisen erilaisissa organisaatioissa. Käytännössä kyseessä on "security ja safety risk management osana Corporate Governance -yrityskulttuuria". [2] EK:n mallia käsitellään tarkemmin jäljempänä kappaleessa 2.1., kokonaisturvallisuuden viitekehys.

1.2 Tutkimuskysymykset, näkökulma ja rajaukset

Tämän työn näkökulma on käytäntölähtöinen eli miten turvallisuusjohdon koulutusohjelmassa esitettyjä riskien hallinnan ja turvallisuusjohtamisen malleja tulisi saattaa osaksi puolustusvoimien käytännön johtamista. Tällä samalla rajataan muut teoreettiset tarkastelut tai johtamismallit tarkastelun ulkopuolelle. Tarkasteltaessa riskien hallintaa käytännössä joudutaan samalla linjauksella kuitenkin ottamaan tarkasteluun yritysten sisäinen valvonta eli Keskuskauppakamarin Suomessa ohjeistama malli yrityksen itsesääntelystä[3]. Itsesääntelyyn eli Corporate Governanceen liittyy yritystoiminnassa aina välittömästi raha, mutta tässä työssä talouden hallinta tai muu turvallisuustoimintaan välittömästi liittymätön toiminta rajataan tarkastelun ulkopuolelle, sillä muuten työ laajenisi liikaa. Käytännössä työssä "benchmarkataan" eli verrataan tavoitteellisesti kokonaisturvallisuuden, sisäinen valvonnan ja riskienhallinnan malleja puolustusvoimien turvallisuusstrategiaan ja riskienhallintaohjeeseen. Miten nämä lähestymistavaltaan toisistaan poikkeavat mallit voidaan, vai voidaanko, liittää yhteen ja millainen käytännössä sovellettava turvallisuuden hallintajärjestelmä täten saataisiin aikaan? Olisi-

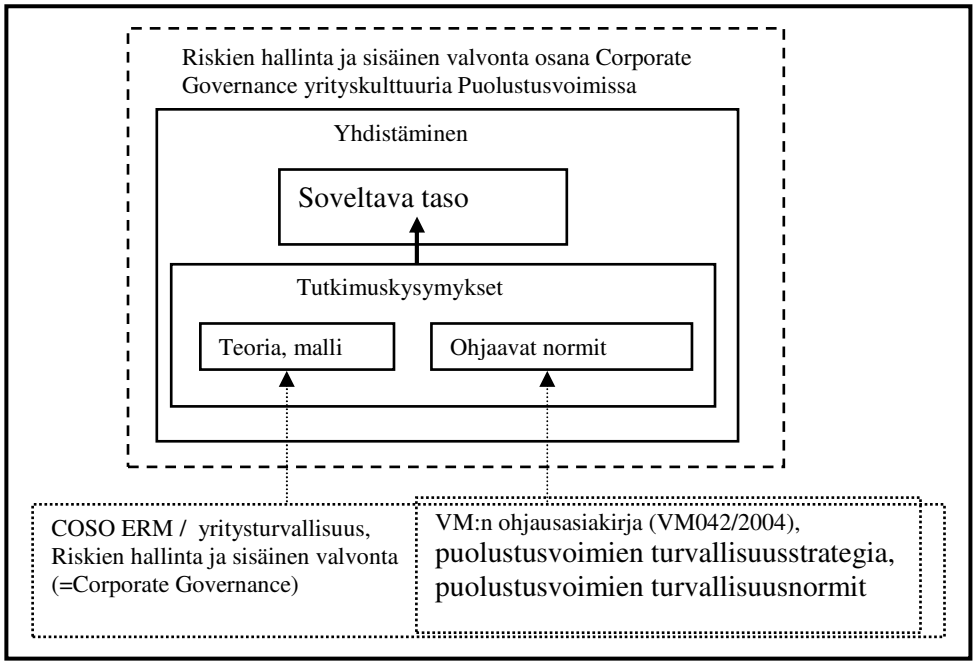
[2] Tiihonen, Kalevi: Yritysturvallisuuden malli, osa 1. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008. Tiihosen esityksen mukaan yritysturvallisuuden malli on "kehitetty ja otettu käyttöön vuonna 1986 EK:n jäsenyrityksissä sekä sidosryhmissä järjestelmän soveltuessa hyvin myös muihin kuin yritysorganisaatioihin". Mallin yhteneväisyys kurssilla opetettuun COSO ERM:in on hämmästyttävä, sillä edellä viiteen yksi mukaisesti ERM - kokonaisvaltainen ajatusmalli riskienhallintaan - on kehitetty maailmalla vasta vuosina 2001 - 2004. Kurssin sisällön perusteella on arvioitavissa, että mallit ovat muotouneet nykymuotoonsa rinnakkain, vaikkakin suomalainen yritysturvallisuuden ajattelu lienee ollut aikanaan aikaansa edellä kansainvälisestikin tarkasteltuna. Käsitystä puoltaa myös Tiihosen materiaalissaan esittämät yritysturvallisuutta koskevat väitöskirjat, joita on laadittu yhteensä viisi vuosina 1993 - 2007. Materiaali on tutkijan hallussa.

[3] Keskuskauppakamari (Joulukuu 2003): Suositus listayhtiöiden ja hallinnointi- ja ohjausjärjestelmistä (Corporate Governance).

ko se toimiva vai kenties toimiva, mutta liian raskas? Entä voidaanko sitä soveltaa laajalti siten, että sen pohjalta ajatus kokonaisvaltaisesta, riskeihin perustuvasta johtamisesta ja päätöksenteosta voitaisiin ottaa laajemmin käyttöön koko puolustusvoimissa; ensin joukko-osasto- ja puolustushaaratasalla ja myöhemmässä vaiheessa läpi koko organisaation? Näistä lähtökohdista työn tutkimuskysymyksiksi muotoutuivat seuraavanlaisiksi:

- Miten Puolustusvoimien Johtamisjärjestelmäkeskuksen (PVJJK) turvallisuusjärjestelmä tulee luoda kokonaisturvallisuuden mallin mukaisesti?
- Voidaanko esitettyä mallia soveltaa laajalti, ja millä poikkeuksilla, puolustusvoimien muihin joukko-osastoihin?

Tutkimuskysymykset on tarkoituksellisesti pidetty ”pieninä”, eikä lähdetty hakemaan laajoja teoreettisia kokonaisuuksia, joiden kautta turvallisuusjohtamisen malleja voitaisiin soveltaa myöhemmin määritettävällä tavalla taktisen tason toimijoihin. Tässä lähestymistavaksi valittiin täysin päinvastainen ajatus, jossa ensin sovelletaan mahdollista toteuttamista yhdessä puolustusvoimien joukko-osastossa ja sen perusteella esitetään pohdintaa, voidaanko ajatusmallia laajentaa koskemaan myös muita puolustusvoimien toimijoita. Työn lähestymistapa on siis yhtä aikaa sekä deskriptiivinen (kuvaileva) ja vahvasti generalisoiva (yleistävä)[4]. Opinnäytetyön viitekehys on mallitettu esitetyn mukaisesti alla olevaan kuvaan.



Kuva 1. Opinnäytetyön viitekehys.

[4] Niiniluoto, Ilkka: Johdatus tieteenfilosofiaan, Keuruu 1984, s. 26. Niiniluodon mukaan ”voidaan erottaa kaksi käytäntöön orientoitunutta tutkimusongelman tyyppiä: a) deskriptiivinen tutkimusasetelma, jossa pyritään kuvaamaan jonkin ”systeemin” nykyistä tilaa tai historiaa ja b) generalisoiva tutkimusasetelma, jossa kartoitetaan jotakin ”systeemiä” koskevia säännönmukaisuuksia, jotta voitaisiin tehdä luotettavia ennustuksia ja löydettäisiin tai parannettaisiin annettuun tavoitteeseen johtavia keinoja”.

Työn lähteinä on käytetty Turvallisuusjohdon koulutusohjelmassa jaettua materiaalia, puolustusvoimien soft law -tyyppistä ohjausasiakirjamateriaalia painopisteenään turvallisuusnormisto sekä muuta näitä täydentävää materiaalia. Työn kuvailevan luonteen vuoksi lähteiden reliabiliteettia ole tutkittu, sillä opinnäytteen ollessa kyseessä luotetaan siihen, että koulutusohjelmassa esitetyt mallit ja niiden ympärille rakennetut ohjeet ja säädökset ovat sellaisenaan riittäviä tämän työn perusteiksi. Kritiikkiä malleja kohtaan on käsitelty lyhyesti alaluvussa 2.3., mutta nämäkin perustuvat omakohtaisiin arvioihin mallien käytettävyydestä, eivätkä minkään tutkijayhteisön näkemyksiin mallien kehittämiseksi. Työn luettavuuden kannalta tarpeelliset lisätiedot on sijoitettu viitteisiin, jolloin lukija voi valita perehtymistarkkuuden ilman, että se vaikuttaa opinnäytetyön sisältöön. Viitteissä on myös käsitelty käytettyjen lähteiden luotettavuutta siltä osin, kuin se työn etenemisen kannalta on merkityksellistä. Tutkimusmenetelmänä on käytetty kirjallisuustutkimusta tavoitteena yleisten periaatteiden/mallien ja yksityiskohtien suhteen tasapainottaminen; liiallinen laajuus ja/tai yksityiskohtiin painottuminen voisi hämärtää työn päälinjaa eli soveltamista käytäntöön. Tehdyistä valinnoista johtuen työssä esitetyt tutkimusmenetelmät eivät sovellu sellaisenaan tämän tutkimusasetelman ulkopuolelle.

Opinnäytetyön toinen pääluku esittelee kokonaisturvallisuuden sekä riskien hallinnan ja sisäinen valvonnan viitekehyksen, joihin tämän työn teoria nojaa. Käsittelyn painopiste on rakennettu riskienhallinnan ympärille, sillä lopulta sen onnistumisesta ja integroitumisesta osaksi organisaatiota ja sen johtamistoimintaa johtuu yrityksen riskien hallinta; kuinka syvälle prosesseihin riskiajattelu ja niiden analysoinnin kautta tehty vastuutettu hallinta on kyetty viemään. Tämän on sisäisen valvonnan perusta, kun taas kokonaisturvallisuuden malli käsittää turvallisuuden osa-alueet, joilla riskit voivat toteutua ja joiden hallinnan kautta niitä voidaan pienentää.

Tutkielman pääpaino on luvussa kolme, jossa teoriapohja liitetään osaksi puolustusvoimia ja edelleen Puolustusvoimien Johtamisjärjestelmäkeskus -nimistä yksittäistä toimijaa. Tarkastelu aloitetaan puolustusvoimien turvallisuusstrategiasta ja turvallisuusstrategialla johtamisesta; miten strategia luodaan ja miten sillä johdetaan? Tämän jälkeen tarkastellaan puolustusvoimien riskienhallinnan ja sisäisen valvonnan normeja ja liitetään ne luvun kaksi teoriapohjan kanssa Puolustusvoimien Johtamisjärjestelmäkeskuksen kokonaisturvallisuusjärjestelmäksi; millainen tämä yhdistelmä on ja voiko silla käytännössä hallita kokonaisuutta.

Lopulta luvussa neljä kootaan kokonaisuus yhteen ja esitetään näkemys siitä, vastasiko työ sille asetettuja tavoitteita.

1.3 Keskeiset käsitteet

Opinnäytetyöhön liittyvät keskeiset käsitteet[5] on jaettu toiminnan tasoja ja niihin liittyviä toimintatapoja sekä riskienhallintaa ja turvallisuutta käsitteleviin ryhmiin. Ryhmittelyllä on pyritty havainnollistamaan niitä eri aihealueita, joiden kokonaisuutta ja liittymäpintaa toisiinsa tutkimustyössä on selvitetty. Kunkin ryhmän ensimmäisenä on hierarkiassa laajin eli sellainen käsite, johon seuraava määritelmä liittyy (joko välittömästi tai välillisesti) ja/tai jolle se on alisteinen.

Toimintatasot ja niihin liittyvät toimintatavat:

- *Strategialla* tarkoitetaan keskushallintoviranomaisen parasta mahdollista toimintalinjaa käytettävissä olevissa resurssien puitteissa pitkän tähtäimen (6 – 20 vuotta) tavoitetilan saavuttamiseksi. Asetetut tavoitteet on oltava joko kyseisen viranomaisen päätettävissä tai hallinnassa, tai ainakin sen on kyettävä vaikuttamaan niihin.[6] Yrityksissä strategialla tarkoitetaan yleensä valittua toimintalinjaa lyhyen (3 kk:sta muutamaan vuoteen) tähtäimen tavoitteen saavuttamiseksi.
- *Strateginen taso*[7] tarkoittaa sitä viranomaistasoa, joka joko asettaa strategiset tavoitteet tai vaikuttaa niihin jo päätösten valmisteluvaiheessa. Tässä strateginen taso tarkoittaa lähinnä valtion ja puolustusvoimien ylintä johtoa. Operatiivisen tason muodostavat puolustusvoimien johto ja Pääesikunta.
- *Taktinen taso* tarkoittaa strategisen ja operatiivisen tason alapuolella olevia toimeenpanevia toimijoita, kuten puolustushaarat ja näiden alaiset joukot. PVJJK:n asema suoraan Pääesikunnan alaisena joukkona asettuu puolustushaara- eli taktiselle tasolle..
- *Strateginen johtaminen* on strategisen tason johtamana valmisteltu prosessi, joka tuottaa perusteet strategisten tavoitteiden asettamiselle. Strategisessa suunnittelussa hahmotellaan pitkän aikavälin tavoitteet ja kehittämisen peruslinjaukset, joita käytetään

[5] Niiniluoto (s. 167): ”Tieteessä pyritään määritelmien avulla mahdollisimman yksiselitteiseen kielenkäyttöön. Oman tutkimuksensa piirissä tiedemiehellä on velvollisuus pyrkiä täsmälliseen ja yksiselitteiseen käsitteistöön: uusia termejä määrittelemällä hän pyrkii toteuttamaan herra Humpty Dumptyn vaatimaa vapautta käyttää sanoja siten, että ne merkitsevät juuri sitä mitä hän haluaa, ei enempää, eikä vähempää.” Opinnäytetyössä keskeiset käsitteet on pyritty avaamaan lukijalle siten, että hän ymmärtää puolustusvoimien ja turvallisuuden termistöä sekä kirjoittajan tavan käyttää niitä.

[6] Kenttäohjesääntö, yleinen osa: Puolustusjärjestelmän toiminnan perusteet, Helsinki 2007, s. 58. Kenttäohjesäännön mukaan ”puolustusjärjestelmän ja puolustusvoimien toiminnan tavoitetilan määrittämisprosessissa käsitellään noin 10 – 20 vuoden aikajännettä”. Käytännön toiminnassa käsitellään pisimmillään TTS-kautta (viisivuotiskautta) eli nykyterminä TOSU eli toimintasuunnitelmakautta, jonka aikajänne on sama. Toimintasuunnitelmakausi jatkuu TA-kauden (talousarviokausi; yksi vuosi) yli siten, että tulostavoitteet pyritään antamaan viiden vuoden jaksolle entisen vuoden sijaan. PTS-kausi eli nykyterminä kehittämisohjelmakausi alkaa täten TOSU-kauden jälkeen eli kuuden vuoden kuluttua nykyhetkestä.

[7] Kenttäohjesääntö, s. 11. Kenttäohjesäännön mukaan ”sotilaallisen maanpuolustuksen johtamistasoja ovat strateginen, operatiivinen ja taktinen taso. Strateginen taso on jaettavissa poliittis- ja sotilasstrategisiin tasoihin. Strategisen tason toimijoita ovat valtion ja puolustusvoimien ylin johto. Puolustusvoimien johto ja Pääesikunta muodostavat operatiivisen johtamistason. Puolustushaarat ja niiden alajohtoportaat ovat taktisen tason toimijoita.

apuna/perustana puolustuspolitiikkaa valmisteltaessa. Strateginen suunnittelu sisältää yleensä erikseen valmisteltavat osastrategiat, joista kokonaisuus muotoutuu.

- *Strategialla johtaminen* tarkoittaa lyhyen ja/tai keskipitkän tähtäimen (1+4 vuotta) johtamista, jossa tulosohjauksen keinoin asetetaan tulostavoitteet ja annetaan niitä vastaavat resurssit. Tulosohjauksen keskeisiä käsitteitä ovat vaikuttavuus, taloudellisuus ja tuottavuus. Puolustusvoimien tulosohjaus toteutetaan hallintorakenteen johtosuhteiden mukaisesti eli PVJJK:n turvallisuusalan tavoitteet antaa Pääesikunnan operatiivinen osasto ja niitä voi täydentää Pääesikunnan Johtamisjärjestelmäosasto.

Turvallisuutta koskevat keskeiset käsitteet:

- *Corporate Governance tai sisäinen valvonta* tarkoittaa järjestelmää, jolla yritys pyrkii lainsäädännön lisäksi kontrolloimaan johtamista ja päätöksentekoa, ja täten varmistua käytettävissä olevan informaation luotettavuudesta. Sisäinen valvonta on siis osa yrityksen hyvää hallinto- ja johtamistapaa, johon liittyy kiinteästi riskienhallinta.[8]
- *Enterprise Risk Management* on kokonaisturvallisuuden johtamismalli, joka jakaa turvallisuuden kymmeneen osa-alueeseen, joista yrityksen on osallistuttava kaikkiin, joihin se osallistuu. Näillä suojataan maine, tiedot, henkilöt, ympäristö ja omaisuus.
- *Yrityritysturvallisuus* tarkoittaa johdon vastuulla olevaa päivittäistä yritystoimintaa, yrityksen turvallisuusasioiden (=lakisääteisen ja omaehtoisen turvallisuustoiminnan) kokonaisvaltaista toteutusta, joka on luonteva osa yrityksen riskienhallintaprosessia.[9]
- *Security* tarkoittaa yrityksen tai yhteisön toiminnan ja toimintojen suojaamista eli yritysturvallisuutta.
- *Safety* tarkoittaa yksilön ja hänen työskentely-ympäristönsä suojaamista lähinnä työturvallisuuden, mutta myös ympäristöturvallisuuden menetelmin.
- *Risk Management* eli riskienhallinta liittyy johtamiseen, ihmisten toimintaan ja tuotannon prosesseihin, valintaan ja päätöksentekoon. Keskeistä on ihmisten toimintatapojen muuttaminen.[10]

---

[8] Arvopaperimarkkinayhdistys: Corporate Governancen määritelmä, http://www.cgfinland.fi/content/blogcategory/15/42/lang,fi/... Ladattu 24.10.2010. Koska sisäisen valvonnan määritelmä ei ole yksiselitteinen on tähän määrittelyyn pyritty tiivistämään sen keskeinen sisältö tai ikään kuin johtoajatus opinnäytetyön kannalta.

[9] Tiihonen, Kalevi: Yritysturvallisuuden malli, osa 1. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008, kohta ”Mitä yritysturvallisuus on?”.

[10] Pisto Martti Herman: Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008 aiheesta ”Muuttuva yritys - turvallisuuden haasteet ja toteutus”, kohta ”Yritysturvallisuuspolitiikka, paikallisesti toteutettava. Tutkijan luennoitsijan esitysmateriaaliin täydentämät muistiinpanot. Materiaali tutkijan hallussa.

2. KOKONAISTURVALLISUUS JA RISKIENHALLINTA

Sanalle turvallisuus voidaan antaa useita erilaisia määritelmiä riippuen siitä, missä asiayhteydessä sitä tarkastellaan. Yksinkertaisimmillaan turvallisuus on yksilön harmoninen tunnetila. Maslowin tarvehierarkiassa[11] turvallisuus on yksi viidestä ihmisen tavalla tai toisella täytettävästä perustarpeesta. Tunteena turvattomuus liittyy yleensä tulevien tapahtumien ennustamattomuuteen eli epävarmuuteen. Yksilö tuntee siis olonsa turvattomaksi, jos lähitulevaisuuden uhkakuvat ovat vaikeasti ennustettavia tai ymmärrettäviä. Tämä sama pätee myös organisaatioon, mutta sen tapa käsitellä turvattomuutta on erilainen kuin yksilöllä. Päämäärä molemmilla on kuitenkin sama; lähitulevaisuuden hallinta. Turvallisuus on siis negatiivinen määre ja tarkoittaa vaaran tai riskin poissaoloa. Turvallisuus esiintyy tällöin ilmiönä kaikkialla, missä esiintyy jonkinlaista vaaraa tai vaaran tunnetta. Maailman monimutkaistuessa ja verkottuessa myös turvallisuus saa uusia piirteitä. Turvallisuus on usein absoluuttisesti mahdotonta, joten turvallisuus on suhteellinen määre.[12]

Kuten turvallisuuteen myös riskiin liittyy mahdollisuus negatiivisesta lopputuloksesta[13]. Sana riski tulee latinan kielen sanasta *risicare*, joka merkitsee karin tai karikon kiertämistä. Menestyvä liiketoiminta perustuu aina riskeihin, niiden ottamiseen ja valittujen riskien hallintaan. Riskienhallinta tarkoittaakin yritysmaailmassa laskelmoitujen riskien ottamista eli mahdollisuutta joko isompaan tai pienempään palautukseen/tulokseen. Yritysmaailmassa lopulta kaikki lasketaan rahassa.[14] Organisaatiolla, jonka tehtävä on tuottaa kustannustehokkain lopputulos määritettyyn tavoitetilaan annetulla kehyksellä voi kuitenkin olla erilainen käsitys niin riskeistä kuin riskienhallinnasta. Miten ensinnäkin määrittää tavoiteltava lopputulos, koska kehys ei sitä kuitenkaan mahdollista? Entä miten toteuttaa kaikki ne organisaation mahdollisesti ohjeistamat turvallisuustoimenpiteet, koska resurssit eivät niitä kuitenkaan mahdollista? Entä onko niitä kaikilta osin edes tarkoituksenmukaisia toteuttaa ts. haittaavatko ne kohtuuttomasti organisaation toimintaa? Mihin ja miten siis kohdentaa niukat resurssit tarkoituksenmukaisesti?

Niin tai näin, niin sekä yrityksessä että valtiollisella toimijalla on sama riskienhallinnan toimintaperiaate. Molemmilla on hallittavanaan riskejä, jotka tulee kaivaa organisaatiosta esille toimivan johdon tietoon riskivalintaa varten, ja edelleen vastuuttaa ydin- ja tukiprosessit riski-

---

[11] Wikipedia: Turvallisuuden tunne, http://fi.wikipedia.org/wiki/Turvallisuus ladattu 24.10.2010.
[12] Wikipedia: Turvallisuus, http://fi.wikipedia.org/wiki/Turvallisuus ladattu 24.10.2010.
[13] Tampereen Teknillinen Yliopisto: Riskienallintaa 1.10.2003, http://www.cs.tut.fi/~projekti/dokumentit/riskienhallintaa.pdf, ladattu 31.1.2010. Käsitystä riskistä kuvaavat useat siitä lausutut englanninkieliset ”pikkuviisaudet’, kuten ”risk = probability * penalty”, ”zero risk is a sign of poor management”, ”you can’t manage what you ignore” tai “if you don’t attack risks they will attack you”.
[14] Wikipedia: Riski, http://fi.wikipedia.org/wiki/Riski, ladattu 31.1.2010.

en haltuunottoon niiden hallitsemiseksi. Turvallisuustoimialan tehtäväksi jää tällöin riskienhallintaprosessin luominen, koulutusmateriaalin laadinta ja sen testaus, riskienhallinta valittuun toimijaan asti, riskikartan ja -analyysien teko sekä auditointien teko joko vuosittain tai jollekin muulle valitulle aikavälille. Tässä erinomaisena apuna on yritysturvallisuuden malli (ERM). Riskikartan laadinta on kuitenkin vasta toiminnan avaus, sillä toimivalle johdolle ja ydinprosesseista vastuullisille jää edelleen varsinaiset riskinhallintatoimenpiteet eli valittujen riskien minimointi ja hallinta. Ilman näitä toimenpiteitä koko työläs suunnitteluprosessi on turha.

2.1 Kokonaisturvallisuuden viitekehys, johtavat periaatteet ja sisältö[15, 16]

”Yritysturvallisuuden tarkoitus on parantaa tuottavuutta ja tukea yrityksen kilpailukykyä minimoimalla hallitsemattomia turvallisuusriskejä, parantamalla toimintavalmiuksia onnettomuus-, vaara-, vahinko- ja rikostilanteiden varalta, luomalla turvallisen ja häiriöttömän työskentely- ja asiointiympäristön sekä turvaamalla toiminnan jatkuvuuden kaikissa tilanteissa. Yhteiskunta- ja viranomaisvaatimusten lisäksi tavoitteita yritysturvallisuudelle asettavat/voivat asettaa yritysjohto, omistajat, asiakkaat, rahoittajat ja muut tärkeät sidosryhmät. Turvallisuusvaatimuksia tulee aiempaa enemmän myös sopimusvelvoitteina verkostoituneiden toimintaympäristöjen (mm. alihankinta, kehitys- ja yhteistyösopimukset) ja vakuutustoiminnan (vakuutussopimusten suojeluehdot ja -ohjeet) kautta.”

Tässä turvallisuutta eli lähitulevaisuuden hallintaa tarkastellaan organisaation näkökulmasta COSO ERM-mallin (Enterprise Risk Management) / EK:n eli Elinkeinoelämän Keskusliiton mallin mukaisesti. Mallilla pyritään yrityksen toimintavapauden ja valinnan mahdollisuuksien säilyttämiseen erilaisten turvallisuusuhkien vallitessa. Toisin sanottuna kyse on yrityksen toimintojen ”turvallistamisesta” analysoitujen riskien pohjalta ja tämän toiminnan saattamisesta osaksi organisaation jokapäiväistä johtamistoimintaa. EK:n merkittävyyttä Suomen elinkeinoelämässä kuvastaa hyvin sen 16 000 jäsenyritystä, joilla on noin 950 000 työntekijää ja yli 70 prosenttia maamme bruttokansantuotteesta. Yritysturvallisuuden ’rantapallo’ on esitetty jäljempänä luvussa 3.4 osana Puolustusvoimien Johtamisjärjestelmäkeskuksen turvallisuustoiminnan esittelyä. Yritysturvallisuuden perusajatuksenahan on, että yrityksen on otettava

[15] Tiihonen, Kalevi: Yritysturvallisuuden malli, osa 1. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008.
[16] Tiihonen, Kalevi: Sisäisen turvallisuuden ohjelman ja yritysturvallisuuden rajapinnat, osa 2. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008.

Viitteet 15 ja 16 muodostavat kokonaisturvallisuuden viitekehyksen rungon (yritysturvallisuuden johtavat periaatteet ja sisältö, malli ja soveltaminen), jota on täydennetty mallin eri osien osalta alan asiantuntijoiden sisältöesittelyillä Turvallisuusjohdon koulutusohjelman eri moduuleissa esiin tuotujen argumenttien pohjalta.

tavalla tai toisella huomioon kaikki yritysturvallisuuden kymmenen osa-aluetta, joiden kautta yrityksen turvallisuus on järjestetty.

Riittävän pienessä organisaatiossa kaikki osa-alueet on teoriassa mahdollista hoitaa yhden henkilön toimesta, mutta käytännössä kenenkään yksittäisen henkilön tieto-taito ei riitä kattamaan kaikkia osa-alueita riittävän yksityiskohtaisesti, mikä johtaa joko turvallisuusorganisaation laajentamiseen tai osaamisen ostamiseen ulkopuoliselta palveluntarjoajalta. Turvallisuuden ollessa tiivis osa yrityksen toimintaa on ostajankin tunnettava yrityksen ydin- ja tukiprosessit sekä turvallisuuden prosessit niin hyvin, että vähänkään isompi yritys ei selviä kokonaisuudesta omaa turvallisuusorganisaatiota. Turvallisuusorganisaation hallinnoimana iso osa palveluista voidaan kuitenkin tarkoin rajattuna (aika, paikka, toiminnan osa-alue tai projektin järjestäminen) ostaa alan palveluntarjoajilta. Tällä hetkellä vallalla olevan käsityksen mukaan yritys voi turvallisesti ulkoistaa/ostaa ulkoa vain sellaisia toimintoja, jotka se itse hallitsee.

Yritysturvallisuuden malli jakautuu seuraaviin osa-alueisiin (huomioi erotella security ja safety osa-alueet): 1) Henkilöturvallisuus, 2) Työturvallisuus, 3) Tietoturvallisuus, 4) Tuotannon ja toiminnan turvallisuus, 5) Kiinteistö- ja toimitilaturvallisuus, 6) Pelastustoiminta, 7) Valmiussuunnittelu (riskienhallinta), 8) Ympäristöturvallisuus, 9) Rikosturvallisuus ja 10) Ulkomaantoimintojen turvallisuus. Osa-alueilla pyritään suojaamaan joko yrityksen mainetta, tietoja, henkilöstöä, omaisuutta tai ympäristöä tai näiden muodostamaa kokonaisuutta. Käytännössä yrityksen toimiala ohjaa eri osa-alueiden merkitystä siten, että eri yrityksissä painottuvat eri kokonaisuudet ja joissakin on tarkoituksenmukaista kattaa vaikkapa vain puolet eri osa-alueista. Yrityskoon kasvaessa osa-alueiden ja niissä olevien toimintojen määrä pääsääntöisesti kasvaa. Osa-alueet menevät joiltain osin päällekkäin, jolloin kaikille osa-alueille yhteisistä niin sanotuista yleisistä asioista voidaan laatia yrityskohtainen toimintamalli tai käsikirja. Yleiset asiat käsittävät turvallisuuspolitiikan tai toimintaperiaatteen, ohjaavan lainsäädännön, viranomaisten valvonnan, ohjaavat standardit, yrityksen sisäisen ohjeiston, organisaation, riskiarviot, vakuuttamisen, toimintaohjelman (tavoitteet ml. koulutus, menetelmät, vastuut, mittarit, tilastot, benchmarking, aikataulu, seuranta ja valvonta), analyysit, ennalta ehkäisevät toimenpiteet, yhteistyökumppanit ja sidosryhmät. Kaikkien toimintaohjelmien tulisi puolestaan perustua riskiarvioon.

1) Henkilöturvallisuus: työntekijöiden suojaaminen rikoksilta ja onnettomuuksilta, liiketoiminnan suojaaminen estämällä rikollisen aineksen soluttautuminen yritykseen, avainhenkilöiden suojaaminen ja liiketoiminnalle kriittisten henkilöresurssien varmentaminen. Menetelmiä

ovat asiakkaiden turvallisuus, yrityksen henkilöiden turvallisuus, kodin ja perheen turvallisuus, matkustusturvallisuus, henkilösuojaus erityistapauksissa, tavoitettavuus- ja hälytysjärjestelyt, varamiesjärjestelyt ja luotettavuusmenettelyt (turvallisuusselvitykset, huumeostot, koeostotoiminta).

2) Työturvallisuus (työterveydenhuolto ja työsuojelu): työterveys- ja työturvallisuustason jatkuva parantaminen, toimintatapojen, työolosuhteiden ja työvälineiden kehittäminen, yhteistyökumppaneiden sitouttaminen, työmaatoiminnan kehittäminen, työkyvyn ja työympäristön parantaminen ennakoivan terveydenhuollon avulla, turvallisuustietoisuuden lisääminen. Menetelmiä ovat työturvallisuus työpaikalla, koneiden ja työvälineiden turvallisuus, työpaikan sisäinen liikenne, fysikaaliset tekijät, vaarallisten aineiden käsittely, henkilösuojaimet, välivallan kohtaaminen työssä, yksintyöskentely ja turvallisuus, työterveyshuolto, työturvallisuus työpaikalla, jossa toimii useita yrityksiä. Ohjaavana työturvallisuuslainsäädäntö ja työsuojelun valvontalaki sekä erilaiset ohjaavat standardit.

3) Tietoturvallisuus: tietojen merkityksen arviointi organisaatiolle, luottamuksellisuus, yrityksen tiedon luottamuksellisuuden, käytettävyyden ja eheyden takaaminen, liiketoiminnan jatkuvuuden turvaaminen, asiakkaan tietojen turvaaminen, tietoturvallisuuden menetelmien jatkuva seuraaminen ja omien toimenpiteiden jatkuva parantaminen. Menetelmiä: tietojen luokittelu ja käsittely eri luottamuksellisuusluokissa, hallinnollinen tietoturvallisuus, turvallisuusselvitykset, salassapitosopimukset, tietosuoja, henkilötietojen käsittely, yksityisyyden suoja työelämässä, yksityisyyden suoja sähköisessä viestinnässä, tietotekninen turvallisuus, palomuuri-, virus- ja haittaohjelmatorjunta, roskaposti, tiedonsiirron suojaus, laitteistoturvallisuus, ohjelmistoturvallisuus, varmuuskopiointi, fyysinen turvallisuus, käyttöturvallisuus, tietosodankäynti (tietojen ja -järjestelmien laajamittainen sabotointi ja toiminnan lamaannuttaminen), tietojärjestelmien toiminnan jatkuvuuden varmistaminen ja tietojenkäsittelyn ulkoistaminen ja tietoturvallisuus sopimusasiana.

4) Tuotannon ja toiminnan turvallisuus: tavoitteena häiriötön tuotanto ja/tai toiminta, nopea toipuminen häiriön jälkeen sekä turvalliset tuotteet. Menetelminä ovat jatkuvuussuunnittelu riskienarvioinnin perusteella[17], liiketoimintariskien arviointi ja vaihtoehtoissuunnittelu, tuotevastuu- ja turvallisuus, varastointi ja kuljetukset, palvelujen turvallisuus, logistiikkaturvalli-

[17] Koivisto, Raija: Tulevaisuuden uhkiin varautuminen; uudenlaiset riskit -tutkimus. Luento Turvallisuusjohdon koulutusohjelmassa TTK Dipolissa 10.2.2009. Koivisto toimii tutkimusprofessorina VTT:llä. Koiviston mukaan tulevaisuuden uhkiin varautumisen ketju on seuraava: ”jatkuvuussuunnittelu (hallintatoimenpiteiden suunnittelu), ennakoiva varautuminen (ennakoinnin ja riskienhallinnan yhdistäminen), vuorovaikutusketjujen tunnistaminen, heikkojen signaalien tunnistaminen ja riskienhallintatoimenpiteiden toteutus (hallintatoimenpiteiden täytäntöönpano)”.

suus, maksuliikenteen turvallisuus, arvo-omaisuuden säilytys, sopimusten (tieto)turvallisuus, alihankkijat ja palvelutoimittajat, vakuuttaminen (tuotevastuu-, omaisuus-, kuljetus-, projektivakuutukset).

5) Kiinteistö- ja toimitilaturvallisuus: yrityksen toimipaikkojen ja -tilojen riskiarvioon perustuva, kustannustehokas suojaaminen, joka perustuu kehäajatteluun tavoitteena turvata häiriötön työskentely ja estää yritykselle arvokkaan tiedon tai materiaalin anastaminen. Menetelmiä: toimitilaturvallisuusluokitus ja luokituksen mukainen suojaus sekä rakenteellinen turvallisuus (estetään vapaa pääsy, hidastetaan tunkeutumista ja voitetaan aikaa: rakennusten runko- ja seinärakenteet, ovet, ikkunat, luukut, aidat, portit, ajo-esteet, lukot, kalterit, valaistus ja kiinteistötekniikka), turvallisuusvalvonta (tehdään havaintoja, saadaan taltiointia ja välitetään hälytys tapahtumasta eteenpäin) sisältäen teknisen valvonnan (kamera-, kulunvalvonta-, rikos-, paloilmoitin ja kuulutusjärjestelmät) ja turvallisuuspalvelut (tarvittava vaste saadaan yleensä tehokkaimmin vartiointiliikkeeltä), kokousten ja neuvottelujen turvallisuus (neuvottelutilojen sijoittelu ja rakenne), sopimushallinta ja ulkoistaminen sekä järjestelmien ylläpito- ja huoltosopimukset sekä tarkastukset (tekniseen valvontaan tarkoitetut laitteet on monimutkaisuudestaan johtuen syytä ottaa osaksi systemaattista huoltotoimintaa).[18]

6) Pelastustoiminta: tulipalojen ja muiden onnettomuuksien ennalta ehkäisy ja nopea sekä oikea vaste onnettomuustilanteissa, koulutus ja valistustyö, onnettomuuksiin liittyvien riskien hallinta ennakoimalla, poistamalla, minimoimalla ja vakuuttamalla, henkilöstön yleisten kansalaistaitojen kehittäminen mm. ensiapukoulutuksen ja alkusammutuksen osalta sekä kumppanuussopimukset viranomaisten kanssa. Menetelmiä: yrityksen varautumis- ja suunnitelmavelvoitteet, pelastussuunnitelma, työpaikkakohtaiset järjestelyt rakennuksissa, rakenteelliset toimenpiteet, toiminnan edellyttämä materiaali, toimenpiteet uhkien torjumiseksi (vartiointi ja kulunvalvonta, sammutus ja pelastaminen, ensiapu, korjaus ja raivaus), varautuminen suuronnettomuuksiin, rakennusten paloturvallisuus (paloluokittelu, kantavat rakenteet, palo-osastointi, pelastus- ja sammutusjärjestelyt, tuhopolttojen torjunta), teknillinen turvallisuustaso (alkusammutuskalusto, automaattinen paloilmoitin, automaattinen sammutuslaitteisto, savunpoisto, turva- ja merkkivalaistus, turvallisuusopasteet), tulitöiden turvallisuus, pelastusalan laitteiden määräaikaistarkastukset, kunnossapito-ohjelmat ja huolto.

[18] Mikkonen, Jarmo: Toimitilaturvallisuus ja turvallisuusvalvonta. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 13.10.2009. Koivisto työskentelee Securitas Oy:n toimitusjohtajana. Materiaali on tutkijan hallussa. Mikkosen materiaali täydentää EK:n esitystä etenkin menetelmien määrittelyn osalta, jotka EK:n jakomateriaalista puuttuivat. Mikkoselta lainatut osiot ovat tekstissä suluissa.

7) Valmiussuunnittelu (sekä poikkeusolojen riskiarvioinnit): tavoitteena on puolustustaloudellisen suunnittelun ja huoltovarmuuden turvaaminen sekä näitä koskevien valmiusvelvoitteiden täyttäminen ja kriisiajan toiminnan turvaaminen (koskee erityisesti tärkeysluokiteltuja valmiusyrityksiä). Menetelmiä: varautuminen poikkeusoloihin, tuotannon ja toiminnan suunnittelu, riskiarvioinnin tarkistaminen poikkeusoloihin soveltuvina, energiahuolto, raaka-aineet, koneet ja laitteet, korjaus- ja huoltotoiminta, varaosat, materiaalivarastointi, alihankinta- ja muut palvelutyöt, henkilövaraukset (VAP-menettely). Ohjaavana valmiuslainsäädäntö.

8) Ympäristöturvallisuus: ekologisen kestävyyden huomiointi, asiakkaiden ja yhteiskunnan ympäristöodotusten ennakointi, prosessien ja parhaiden käytäntöjen kehittäminen, vastuun ottaminen ympäristöstä, henkilöstön tietoisuuden lisääminen, avoin tiedottaminen, sitoutuminen standardien periaatteisiin. Menetelminä ovat elinkaariajattelu, ekotase, ympäristövaikutusten arviointi, ilmoitus- ja lupamenettely, vaarallisten aineiden käsittely ja säilytys, ympäristönsuojelun hallintajärjestelmä ja toimintaohjelma, ilmansuojelu ja päästökauppa, vesien ja maaperän suojelu, meluntorjunta ja maisemansuojelu, kemikaalivalvonta ja jätehuolto. Ohjaavana kansainvälinen ja kansallinen lainsäädäntö sekä erilaiset standardit (mm. ISO14001).

9) Rikosturvallisuus: yrityksen toimintaan, henkilöstöön ja omaisuuteen kohdistuvien rikosten ennaltaehkäisy, tapahtuneiden rikosten selvittäminen ja rikostilanteen seuranta sekä yrityksen sisältä että ulkopuolelta uhkaavan rikollisuuden osalta. Menetelmiä: rikosriskien hallintakeinot (ennalta ehkäisevät toimenpiteet, toimenpiteet rikosten ilmisaamiseksi) ja toiminta rikostapauksissa (esikuntaan johtavat ja muut esiselvitykset, asianomistajarikokset, virallisen syytteen alaiset rikokset, huumetestaus työelämässä, teknisten laitteiden huolto ja kunnossapito sekä yhteistoiminta viranomaisten kanssa).

10) Ulkomaantoimintojen turvallisuus: henkilöstön turvallisuustason takaaminen heidän ollessaan ulkomailla vailla kotimaansa palveluja tavoitteena kohdemaan korkean riskitason vaikutusten poistaminen tai pienentäminen. Menetelmiä: maiden riskiluokitus (riskiluokituksen mukaiset ohjeet, valmistautuminen, evakuointisuunnitelma, matkustaminen, majoittuminen, oleskelu, erityistilanteiden hoitaminen), matkustajan status (liikematkustaja, komennushenkilö, expatriaatti) ja yleiset ohjeet (matkustusasiakirjat, terveydenhuolto, työturvallisuus, rahaasiat, verotus, yleinen matkustus-, liikenne- ja majoitusturvallisuus, kodin ja perheen turvallisuus, kulttuurit ja uskonnot, rikollisuus, matkavakuutukset (sotariskimaat)).

2.2 Riskienhallinta ja sisäinen valvonta[19]

Yrityksen sisäinen valvonta on osa yrityksen Corporate Governancea eli hyvää hallinto- ja johtamistapaa. Corporate Governancelle ei ole olemassa yksiselitteistä määritelmää. Yksinkertaistettuna Corporate Governancella tarkoitetaan järjestelmää, jonka avulla yritystoimintaa johdetaan ja kontrolloidaan. Corporate Governance -suosituksilla pyritään siten täydentämään lakisääteisiä menettelytapoja eli kyseessä on yrityksen itsesääntely. Keskuskauppakamarin antaman asialuettelon mukaan sisäisen valvonnan ja riskienhallinnan tavoitteena on varmistaa, että yhtiön toiminta on tehokasta ja tuloksellista, informaatio luotettavaa ja että säännöksiä ja toimintaperiaatteita noudatetaan. Sisäisen valvonnan suositusten (49 - 51) mukaan yhtiön on määriteltävä sisäisen valvonnan toimintaperiaatteet sekä selostettava periaatteet, jonka mukaan riskienhallinta on järjestetty, minkä lisäksi yhtiön on selostettava, miten sisäisen tarkastuksen toiminto on järjestetty. Toiminta on dokumentoitava.

Valtiovarainministeriön internet-sivuilla ohjeistetaan yksityiskohtaisemmin viraston sisäinen valvonta. Sen mukaisesti ”sisäinen valvonta tarkoittaa viraston ohjaus- ja toimintaprosesseihin sisältyviä menettelyitä, organisaatioratkaisuja ja toimintatapoja, joiden avulla voidaan saada kohtuullinen varmuus 1) toiminnan lainmukaisuudesta, 2) varojen turvaamisesta, 3) toiminnan tuloksellisuudesta sekä 4) taloutta ja tuloksellisuutta koskevien oikeiden ja riittävien tietojen tuottamisesta. Talousarviolain 24 b §:n mukaan viraston ja laitoksen on huolehdittava siitä, että sisäinen valvonta on asianmukaisesti järjestetty sen omassa toiminnassa sekä toiminnassa, josta virasto tai laitos vastaa. Riskienhallinnalla tunnistetaan, arvioidaan ja hallitaan yllä mainittuihin neljään luokkaan sisältyvien tavoitteiden saavuttamista uhkaavia tekijöitä. Riskienhallinnalla on samat tavoitteet kuin sisäisellä valvonnalla. Parhaimmillaan sisäisen valvonnan ja riskienhallinnan menettelyt on upotettu osaksi viraston tavanomaisia suunnittelu-, johtamis- ja toimintaprosesseja.” Ministeriö viittaa sivustollaan 20.12.2005 julkaistuun asiakirjaan VM 042/2004[20], jossa ohjeistetaan sisäisen valvonnan ja riskienhallinnan arviointikehikko. Kehikko on tarkoitettu käytettäväksi ”pienissä virastoissa tai virastoissa, jotka haluavat aloittaa sisäisen valvonnan minimivaatimusten täyttämisellä”. Kehikko perustuu löyhästi COSO ERM:in. [21]

---

[19] Arvopaperimarkkinayhdistys: Corporate Governancesta yleisesti, http://www.cgfinland.fi/content/blogcategory/15/42/lang,fi/... Ladattu 24.10.2010. Tämän työn perimmäinen tavoite ei ole tarkastella sisäistä valvontaa, mutta sen ollessa varsin kiinteä osa riskienhallintaa ja kokonaisturvallisuutta (COSO ERM) on tähän tiivistetty sisäisen valvonnan keskeinen sisältö. Sisäisen valvonnan järjestämistä ei kuitenkaan käsitellä opinnäytetyön soveltavassa osiossa, jossa paneudutaan lähemmin Puolustusvoimien Johtamisjärjestelmäkeskuksen turvallisuusjärjestelyihin ja riskienhallinnan toteuttamismahdollisuuksiin.

[20] Valtiovarainministeriö (VM 042/00/2004): Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta (valtionhallinnon hyvä käytäntö ja sen toteutumisen arviointi), 20.12.2005.

[21] Valtiovarainministeriö: Sisäinen valvonta ja riskienhallinta/viraston sisäinen valvonta ja riskienhallinta/vastuu sisäisen valvonnan järjestämisestä/sisäisen valvonnan arviointi/arviointikehikko,

Sisäinen valvonta ja siihen kiinteästi liittyvä riskienhallinta ovat jatkuvaa toimintaa, joiden avulla yritys pyrkii varmistamaan tavoitteidensa saavuttamisen. Tästä syystä sisäistä valvontaa ei voi eriyttää muusta tavoitteiden saavuttamiseen tähtäävästä toiminnasta, vaan se on olennainen osa toiminnan ohjausta ja sen järjestämistä ja siitä on oltava vastuussa jokainen toiminta-alueen ja/tai vastuualueen toimiva johto. Itsesääntelyn avulla yritykset etsivät tarkoituksenmukaisimman tavan ongelmiensa selvittämiseksi, joten yhtä ja ainoaa oikeaa tapaa itsesääntelyyn, kuten ei myöskään sisäiseen valvontaan, voida antaa. Ollakseen tehokas, tulisi yrityksen tai viraston laatiman sisäisen valvonnan ohjeen sisältää ainakin seuraavia osa-alueita: 1) Johtamisjärjestelmä yleensä (strategiaperusta, johtamisen organisointi, hyvä hallinto- ja johtamistapa, riskienhallinta), 2) Toimivalta ja vastuut, 3) Valvontajärjestelmä (sekä sisäinen että ulkoinen valvonta rajapinnan tiedostamiseksi), 4) Sisäinen valvonta (tavoitteet, osa-alueet, päätöksentekojärjestelmä), 5) Päätöksentekoprosessin sisäinen valvonta, 6) Henkilöstöasioiden sisäinen valvonta, 7) Talous- ja strategiaprosessin sisäinen valvonta, 8) Kirjanpidon ja maksuliikenteen sisäinen valvonta, 9) Omistajapolitiikka ja sisäinen valvonta, 10) Tietohallinnon, tietoturvan ja tietosuojan sisäinen valvonta, 11) Sopimuskäytäntö (hankinnat) ja valvonta sekä 12) Väärinkäytösten ehkäisy (sanktiointi tms).

2.3 Kritiikkiä turvallisuuden hallinnan malleja kohtaan

Turvallisuuden käsitteen yksi suurimpia haasteita on sen laajuus. Yksi ja sama termi tarkoittaa monta erilaista asiaa ja asiakokonaisuutta riippuen siitä, keneltä kysyt ja mihin turvallisuus halutaan liittää. Esimerkiksi Sisäisen turvallisuuden ohjelma[22], jossa ohjelman tavoitteeksi on kirjattu ”Suomi on Euroopan turvallisin maa vuonna 2015”. Tässä turvallisuuden käsitteellä ymmärretään väkivaltaa, alkoholin käyttöä, onnettomuuksien ja tapaturmien määrän kasvua, järjestäytynyttä rikollisuutta, terrorismia, monikulttuurisuutta, ihmiskauppaa ja niin edelleen. On siis vaikea antaa turvallisuuden käsitteille suoraa jatkumoa tai liittymäpintaa asioiden välillä. Mihin vedetään raja? Liittyykö kaikki toiminta turvallisuuteen? Turvallisuusjohdon koulutusohjelmassa EK:n esityksessä oleva yritysturvallisuuden malli jakaa turvallisuuden osa-aluekaavioon, jonka mukaan ”turvallisuusjohtaminen ohjaa kaikkea yrityksen toimintaa”. Onkohan asia nyt kuitenkaan näin? Ainakin asian esittäminen tällä tavoin yritysjohdolle voi helposti saada aikaan kielteisen reaktion ainakin henkilöillä, joiden näkökulmasta turvallisuus on vain välttämätön kuluerä. Eivätkö benchmarking, laatujohtaminen tai julkishallintoa välittömästi koskeva New Public Management olekaan mitään? Tällaisilla laajoilla käsitteillä on

---

http://www.vm.fi/vm/fi/09_valtiontalous/045_tuloksellisuus/03_sisainen_valvonta_ja_riskienhall/index.jsp (ladattu 13.2.2010)

[22] Viljanen Ritva: Luento Turvallisuusjohdon koulutusohjelmassa 15.10.2008 aiheena ”Sisäisen turvallisuuden ohjelma ja sisäisen turvallisuuden strategia”. Viljanen työskentelee Sisäasiainministeriön kansliapäällikkönä. Materiaali on tutkijan hallussa.

helposti tapa sekoittua osaksi ihmisen aiempia elämänkokemuksia. Malli pitääkin mielestäni ottaa käyttöön yrityksissä vaivihkaa ohjaamalla yrityksen turvallisuustoimintoja omatoimisesti kohti EK:n mallia ja osaksi yritysjohtajien paljon paremmin tuntevaa Corporate Governancea eli omaehtoista sisäistä valvontaa, joka jo sinällään vaatii riskienhallinnan toimiakseen.

Vastaavan tuntuinen käsitteiden epäselvyys tuntuu vaivaavan myös kokonaisturvallisuuden (ERM) ja yritysturvallisuuden käsitteitä ja/tai malleja. Turvallisuusjohdon koulutusohjelmassa käytetyn materiaalin perusteella näyttää siltä, että kaksi eri organisaatiota pyrkii ottamaan mallista kunnian itselleen, mutta kuka mitäkin mallia käyttää tai sanoo käyttävänsä riippuu lopulta sattumasta; onko hienompaa linkittää itsensä kansainväliseen COSO-organisaatioon ja maksaa riittävän osaamisen käytöstä lisenssimaksut vai kotimaiseen Elinkeinoelämän Keskusliittoon ja saada sama oppi käyttöönsä ilmaiseksi? Paljon varmaan riippuu kyseessä olevan yrityksen asiakaskunnasta ja heidän vaatimistaan referensseistä. Kunhan tuotanto- ja palveluketjujen riskienhallinta ja niitä vastaavat hallintamenetelmät ovat kunnossa voi yrityksen tarkastaa mikä tahansa auditointiyritys ja myöntää sille tarvittavat sertifikaatit asiakkaan vaatimusten täyttämiseksi.

Käyttipä yritys toimintansa mallintamiseen ja ymmärryksen lisäämiseen mitä tahansa yksityiskohtaisempaa turvallisuusjärjestelmää (esimerkiksi ISO-sarja), niin niillä kaikilla tuntuu olevan sama maksullisuuden ongelma. Niistä saa lähinnä markkinointitietoja, joissa perustellaan järjestelmän, opintokokonaisuuden ja/tai myönnettävän sertifikaatin merkitystä yritykselle, yritysjohdolle, markkinoinnille ja lopulta yrityksen tulokselle. Poikkeuksena näistä kaikista on Elinkeinoelämän Keskusliiton, Sisäasiainministeriön ja Puolustusministeriön 20.11.2009 yhdessä julkaisema Kansallinen turvallisuusauditointikriteeristö[23], jossa niin turvallisuuden tavoitteet kuin niiden yksityiskohtainen soveltaminenkin ovat julkisia ja pääosiltaan kaikkien saatavilla olevia. Valitettavasti kriteeristöä ei ole rakennettu ERM:n ja/tai Yritysturvallisuuden Neuvottelukunnan omissa esitysmateriaaleissaan käyttämän yritysturvallisuuden osa-alueiden ympärille. Osa-alueista on katettu vain kolme kymmenestä, mutta positiivista kriteeristössä on se, että siinä selkeästi ohjeistetaan ja vastuutetaan yritysjohto (mitä, kuka, milloin, miten) turvallisuushallintoon ja -johtamiseen. Käytetty rakenne täyttää jo varsin hyvin Keskuskauppakamarin ohjeistuksen sisäisen valvonnan ja riskienhallinnan järjestämiseksi. Kansallisella turvallisuusauditointikriteeristöllä on kuitenkin sama haaste edessään kuin muillakin turvallisuusjohtamisen malleilla; monimutkaisuus. Mallissa esitetään turvallisuuden välitön ja välillinen linkittyminen kaikkeen yrityksen johtamistoimintaan, mutta ennen tälle tasolle pää-

[23] Elinkeinoelämän Keskusliitto, Sisäasiainministeriö, Puolustusministeriö (20.11.2009): Kansallinen turvallisuusauditointikriteeristö (KATAKRI). Sisäisen turvallisuuden ohjelman toisen vaiheen toimenpide 6.4. tp 2.

syä on yritysjohto kyettävä vakuuttamaan mallin tärkeydestä. Tällaisten mallien käyttöönotto vaatii vuosia ennen kuin ne ovat oikeasti osa yritysten todellista päätöksentekoprosessia. Pitäisikö siis ekonomeille ja diplomi-insinööreille opettaakin projekti- ja rahoitusjohtamisen sijasta turvallisuusjohtamista?

2.4 Johtopäätökset

Yritysturvallisuus on osa työelämän pelisääntöjä, joiden mukaisesti yrityksissä tehdään tuotteet, palvelut ja lopulta koko liiketoiminnan tulos. Kyse on toiminnan riskitason asettamista omaehtoisesti osaksi yrityksen liiketoimintamalleja, palveluketjuja ja johtamista. Toimittaessa yritysturvallisuuden perusteiden ja suositusten mukaan kyetään yritykselle laatimaan sellainen turvallisuusohjelma, että sillä voidaan mallintaa vaiheittain sekä yrityksen yritysturvallisuuden nykytila, suositukset tavoitetilaksi että lähteä kehittämään yrityksen toimintaa kohti johdon valitsemaa tavoitetilaa. Kaikkea ei tarvitse, eikä resurssien puitteissa yleensä kyetäkään tekemään kerralla, mutta se mitä tehdään, kannattaa tehdä järjestelmällisesti ja koko yrityksen toimintaa ohjaavasti.

Yritysturvallisuus liittyy välittömästi yrityksen sisäiseen valvontaan. Molempien jopa määritellään olevan ”johdon vastuulla olevaa päivittäistä yritystoimintaa, yrityksen turvallisuusasioiden (=lakisääteisen ja omaehtoisen turvallisuustoiminnan) kokonaisvaltaista toteutusta sekä osa yrityksen riskienhallintaprosessia”. Sisäisen valvonnan voitaneen katsoa jatkavan siitä, mihin yritysturvallisuuden työskentelyvalikoimalla päästään, eli johtamistoiminnan ja päätöksenteon valvontaan. Hyvään lopputulokseen vaaditaan molempia eli kumpikaan ei tule toimeen ilman toista. Riskienhallintaa voidaan tietysti toteuttaa ilman sisäistä valvontaakin, mutta tämä jättää riskienhallinnan vaikuttavuuden ’puolitiehen’ eli senkin toteutusta on valvottava ja toimintaa kehitettävä tehtyjen havaintojen pohjalta. On siis löydettävä nousevat ja laskevat riskit, joihin vaikutetaan. Turvallisuus toimialana kykenee tarjoamaan organisaatiolle menetelmiä, joilla turvallisuus kyetään saattamaan tietylle tasolle, mutta tukitoiminto ei yksinään kykene nostamaan yrityksen turvallisuutta tänä päivänä yrityksiltä vaadittavalle tasolle. Siinä vaaditaan kaikkia; johtoa, ydin- ja tukiprosesseista vastuullisia sekä turvallisuustoimialaa menetelmien tarjoajana. Tällaisessa ympäristössä turvallisuustoimijat kykenevät vähitellen virittämään ’oman prosessikoneistonsa’ sellaiseen tilaan, että sillä voidaan saavuttaa EK:n mallin mukainen tavoitetila. Tämä vaatii kuitenkin riittävät resurssit ja useita työvuosia. Tällaista toimintaa on myös mielekästä valvoa ja kehittää sisäisen valvonnan keinoin. Sisäinen valvonta ei kuitenkaan voi olla turvallisuustoimialan prosessi. Se on sellaista yrityksen omaehtoisen toiminnan kehittämistä, jonka kokonaisuuden hallinta ja ohjaus on kuuluttava toimintaa kehit-

tävälle organisaatiolle yritysjohdon välittömässä alaisuudessa. Sisäisessä valvonnassa turvallisuustoimiala on vain yksi valvottavista prosesseista.

Niin tehokasta kuin tällainen johtaminen onkin, on sen saattaminen osaksi organisaation johtamista etenkin toiminnan alkuvaiheessa erittäin työlästä. Tämä vaatii kaikilta osapuolilta sellaista sitoutumista oman työnsä kehittämiseen, ettei se kestä ainakaan alussa prosessien ja organisaatiorakenteen voimakkaita muutoksia. Toiminnan ylösajon eli käytännössä usean toimintavuoden jälkeen toimintojen muutokset ovat kuitenkin helpompia kaikkien tietäessä omat vastuunsa ja kyetessä tekemään päätöksiä riskienhallinnan kautta. Tällöin organisaatio todella ohjaa itse itseään kohti turvallisempia tuotteita, palveluita ja koko liiketoimintaa.

3. PUOLUSTUSVOIMIEN TURVALLISUUSJOHTAMINEN

Turvallisuusjohtaminen puolustusvoimissa. Mitä se on? Hallitaanko sillä yritysturvallisuuden mallin mukaisesti mainetta, tietoa, omaisuutta, henkilöstöä ja ympäristöä? Entä johdetaanko sillä näiden osa-alueiden hallintaa? Vai johdetaanko niitä jostain aivan muualta kuin turvallisuustoimialalta?

Tässä luvussa haetaan näkökulmaa siihen, onko puolustusvoimilla turvallisuusstrategiaa, millainen se on ja millaisen prosessin kautta sen vaikuttavuus syntyy. Vai jääkö koko strategia toimivien joukkojen näkökulmasta katsottuna vain ”kuolleeksi kirjaimeksi”? Eli käytännössä esitetään näkemys siitä, onko puolustusvoimien turvallisuusjohto riittävän lähellä ylintä strategisen ja operatiivisen tason päätöksentekoa saadakseen vietyä turvallisuutta eteenpäin yritysturvallisuuden mallin mukaisesti, ja edelleen jaettua puolustusvoimien turvallisuuspolitiikkaa vuotuisine toimintaohjelmineen taktisen tason toimijoille. Ymmärrämmekö me toisiamme ja pyrimmekö me kohti samaa tavoitetta? Miten tämä on kyetty järjestämään puolustusvoimien kaltaisessa ”johtamistasojen maailmassa”; jossa strategiat eivät välity toimijoille sellaisenaan läpi organisaation, kuten yritysmaailmassa[24].

3.1 Puolustusvoimien turvallisuusstrategia ja turvallisuusstrategialla johtaminen

Strateginen näkökulma asioihin on katsoa kokonaisuutta ylhäältä (top down) eli tarkastella asioiden kytkeytymistä toisiinsa. Liiketalous- ja sotateorioissa strategianäkemykset niihin liittyvine käsitteineen poikkeavat kuitenkin lähes täysin toisistaan. Liiketaloudessa esimerkik-

[24] Laaksonen, Marko: Luento strategian perusteista EUK60:lle, 12.9.2007. Komentajakapteeni Laaksonen valmistelee väitöskirjaa Maanpuolustuskorkeakoulun johtamisen laitoksella aiheenaan strategia ja siihen liittyvä käsitteistö. Materiaali on tutkijan hallussa.

si taktinen taso on operatiivisen tason yläpuolella. Valtiohallinnon tasoajattelun mukaan valtion johto (tasavallan presidentti, valtioneuvosto, ministeriöt, UTVA, TPAK) ja puolustusvoimien ylin johto (puolustusvoimain komentaja, pääesikunnan päällikkö, henkilöstöpäällikkö, operaatiopäällikkö, materiaalipäällikkö, puolustushaarakomentajat ja Maanpuolustuskorkeakoulun rehtori) johtavat, virkamiehet suunnittelevat ja toteuttamista tapahtuu eri tasoilla. Yhteistä strategioille on kuitenkin se, että niillä haetaan tavoiteltavaa lopputilaa.[25]

Perusteet puolustushallinnon kehittämiselle tulevat hallitusohjelmasta, valtioneuvoston johtamasta turvallisuus- ja puolustuspoliittisesta selonteosta ja muista strategisen tason ohjausasiakirjoista. Puolustushallinnon strategisena ohjaajana ja ohjausvastuussa olevana keskushallintoviranomaisena toimii Puolustusministeriö. Puolustusministeriön keskeisenä strategisen suunnittelun tuotteena on strateginen suunnitelma tavoitteenaan hallinnonalan pitkäjänteinen kehittäminen. Pitkäjänteisyydellä tarkoitetaan 6 – 20 vuoden aikajännettä, jolloin kehittämiseen vaikuttavat muutokset käsitellään eriasteisina emergensseinä. Valtioneuvoston selonteon neljän vuoden aikajännettä voidaan pitää pitkän tähtäimen kehittämisohjelmissa emergenssinä, kuten myös hallitusohjelman ja suunnitellun määrärahakehyksen muutoksia. Vaikutukset voivat olla resurssien osalta joko positiivisia tai negatiivisia riippuen hallinnonalojen välisistä ja sisäisistä painotuksista. Puolustusministeriön strateginen ohjaus toteutetaan:[26]

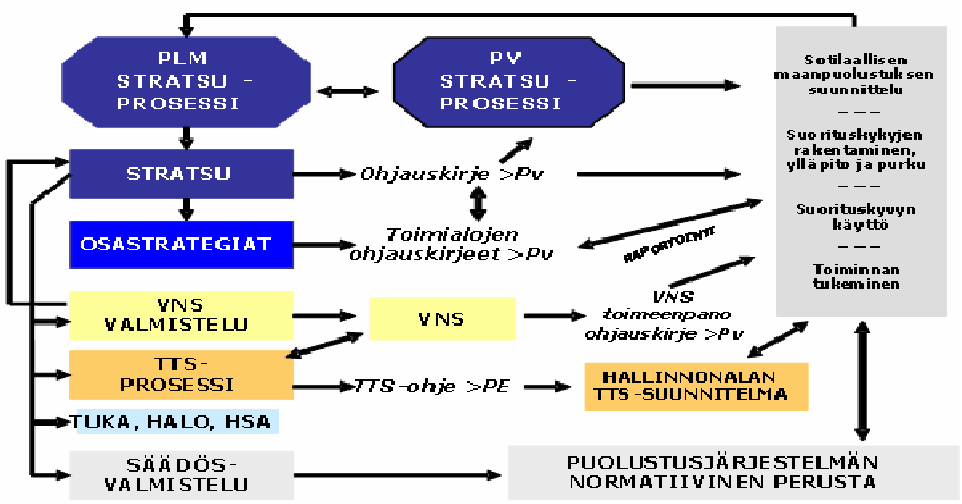
- Strategisella suunnitelmalla, jossa määritetään hallinnonalan tavoitetila ja kehittämislinjaukset sekä näitä palvelevissa toimialakohtaisissa osastrategioissa ja niihin perustuvissa ohjauskirjeissä
- Tarkentamalla turvallisuus- ja puolustuspoliittisen selonteon linjauksia aina yksittäisiksi tehtäviksi saakka ohjauskirjein ja muin vastaavin järjestelyin
- Ohjaamalla puolustusvoimien strategista suunnittelua
- Tulosohjauksella

Puolustusvoimien strategia- ja suunnittelutyön keskeisenä ohjaavana asiakirjana on Puolustusministeriön strategia-asiakirja, josta puolustusvoimat rakentaa strategisen suunnittelun ohjeen operatiivisen ja taktisen tason noudatettavaksi. Puolustusvoimien strategia- ja suunnitteluprosessi ovatkin toisilleen rinnakkaisia ja/tai päällekkäisiä toiminnan ohjaukseen liittyviä rakenteita, joilla tuotetaan sekä perusteet maanpuolustuksen kehittämiselle että kohdennetaan niihin käytettävät resurssit. Suunnitteluprosessin voidaan katsoa olevan strategiaprosessille kuitenkin siinä mielessä alisteinen, että se jatkuvana prosessina tuottaa strategiaprosessin tar-

[25] Aalto, Mika: Luento 'strategiasta kriittisesti' EUK60:lle, 12.12.2007. Materiaali on tutkijan hallussa.
[26] Kenttäohjesääntö, yleinen osa, s. 25.

vitsemaa valmistelutietoa operatiivisella ja jopa taktisella tasolla. Puolustusvoimien strategisen suunnittelun tuotteet ovat:

- Puolustusjärjestelmän ja puolustusvoimien toiminnan tavoitetila
- Puolustusvoimien kehittämisohjelma
- Puolustusvoimien tutkimusohjelma[27]



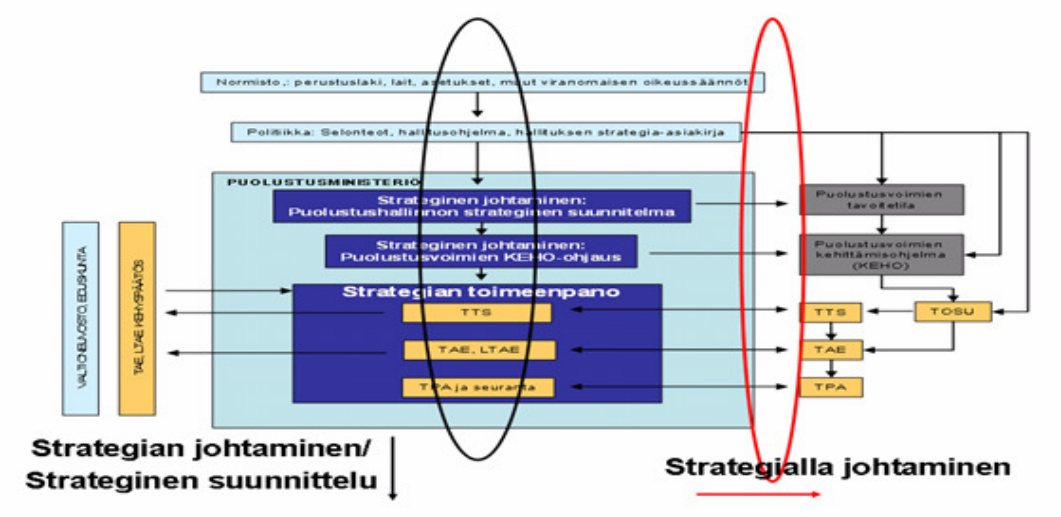
Kuva 2: Puolustusministeriö hallinnonalansa strategisen suunnittelun ohjaajana[28]

Nykyinen, olemassa oleva suorituskyky ei vastaa voimassa olevaa strategiaa, sillä strategialla valmistellaan suorituskykyä 20 vuoden päähän. Täten puolustusvoimien on strategiatyössään lähdettävä ajatuksesta, jossa Valtioneuvosto ohjaa selonteoillaan puolustusvoimia asteittain kohti muuttuvaa tavoitetilaa. Johtamisen järjestys tarkoittaa tällöin sitä, että virkamiesten tehtävänä on suunnitella ja antaa syötteitä resurssipoliittiseen järjestelmään poliitikkojen tehdessä päätökset. Puolustusvoimien osalta analogiaa voidaan jatkaa siten, että käytännössä strategiasuunnittelussa tehdään lähinnä perusteita TRSS- eli täytäntöönpanoprosessille TTS/TOSU –kaudelle.[29] Suunnittelun jatkuvuus puolustusvoimissa voidaan tiivistää seuraavasti:

- YETTS / kokonaismaanpuolustus
- Strateginen suunnitteluprosessi (strateginen johtaminen) / PLM
- PTS (12 v), PVKEHO (4 v), TAE (1 v) (strategialla johtaminen) / Eduskunta
- **VNS (emergenssi, järjestelmään kuulumattomuus) / mm. selonteot**
- OPSU, TOSU / Pv:n suorituskyky (strategialla johtaminen) / Pv
- Hankkeet / Pv
- PTL / Pv

[27] Kenttäohjesääntö, yleinen osa, s. 58.
[28] Puolustusministeriö: Puolustusministeriön strateginen suunnittelu, käsikirja, Helsinki 2007, s. 5.
[29] Laaksonen Marko: Palaute strategisen suunnittelun etätehtävistä EUK60:lle, 15.10.2007. Komentajakapteeni Laaksonen valmistelee väitöskirjaa Maanpuolustuskorkeakoulun johtamisen laitoksella aiheenaan strategia ja siihen liittyvä käsitteistö. Materiaali on tutkijan hallussa.

- Joukkotuotanto pv:n suorituskyvyn mukaan / Pv
    - Toimintojen priorisointi resurssien mukaan



Kuva 3: Strateginen johtaminen ja strategialla johtaminen puolustusvoimissa[30]

Puolustusvoimien tavoitetilan (turvaluokitukseltaan erittäin salainen, joten tässä tarkastellaan ainoastaan tavoitetilan määrittelyprosessia) ja sitä vastaavan puolustusvoimien kehittämisohjelman määrittelyn jälkeen voidaan aloittaa varsinainen kehitystyö Puolustusministeriön määrittämin kehyksin[31]. Strategiaprosessin liittyminen puolustusvoimien prosesseihin on esitetty seuraavassa kuvassa:

Kuva 4: Puolustusvoimien toimintatapa prosesseina[32]

[30] Laaksonen, palaute etätehtävistä EUK60:lle.
[31] Pääesikunnan operatiivisen osaston ohje R2/11.2/D/I/19.1.2004: Strateginen suunnittelu puolustusvoimissa normaaliaikana, s. 7 – 8.
[32] Kenttäohjesääntö, yleinen osa, s. 34.

Kokonaisuutena puolustusvoimien suunnittelujärjestelmä on varsin massiivinen. Haasteena tämäntyyppisessä suunnittelussa on yritysmaailmaan verrattuna se, että sotilasorganisaation strategisessa suunnitteluprosessissa määrittämät tulostavoitteet toimivat tasoina, kun yritysmaailmassa sama strategia viestitään sellaisenaan läpi koko organisaation[33]. Toiseksi haasteeksi muodostuu strategian käytettävyys, sillä ollakseen tehokas, tulee strategian olla toimiva ja koko ajan käytettävissä[34]. Turvallisuusjohtamisen kannalta merkittävää on 'turvallisuusprosessin' puuttuminen koko prosessikartasta. Luonteeltaan kyse olisi koko organisaation leikkaavasta tukiprosessista, jolloin turvallisuusprosessin tulisi olla omana tukiprosessinaan kohdassa neljä. Sisäiselle tarkastukselle tukiprosessin rooli on annettu prosessina 4.5.

Entä mitä toteaa turvallisuusstrategiasta Pääesikunnan turvallisuusosaston pysyväisasiakirja 01:02 'Puolustusvoimien turvallisuustoiminnan strategia'? Sen mukaan "puolustusvoimien turvallisuustoiminnan strategia perustuu puolustusvoimien pitkän aikavälin suunnitteluun, mutta aikajänne ei rajaudu tarkkaan määriteltyihin vuosiin. Strategia on perusteena toiminnan ja resurssien sekä ohjeistuksen yksilöidympään suunnitteluun ja kehittämiseen, joka toteutetaan mm. kehittämisohjelmina. Puolustusvoimien turvallisuustoiminnan strategia päivitetään osana Puolustusvoimien strategista suunnittelua ja siinä otetaan huomioon yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (Valtioneuvoston periaatepäätös 27.11.2003) ja Suomea velvoittavat kansainväliset sopimukset ja ohjeistus." Edelleen sama asiakirja määrittää organisaation turvallisuuden asiaintilaksi, jossa riskit ovat hallinnassa.[35]

Tämän tarkastelun perusteella voisi olettaa, ettei turvallisuusjohtaminen ole saanut vastaavaa statusta puolustusvoimien uusitussa organisaatiossa kuin mikä sillä oli omana turvallisuusosastonaan vuoteen 2005 saakka. Myös ohjeistus on jäänyt turvallisuusosaston lakkauttamisen jälkeen osittain jälkeen muun yhteiskunnan turvallisuuskehityksestä. Uusilla turvallisuustoimijoilla, Pääesikunnan operatiivisen osaston turvallisuussektorilla ja Pääesikunnan tutkintaosastolla, onkin melkoinen työ kiriä takaisin turvallisuusosaston aikanaan alullepanema voimakas turvallisuustoimialan kehitys puolustusvoimissa. Tämäkään ei vielä takaa johdon sitoutumista turvallisuustoimintaan eikä riskienhallinnan saamista osaksi päätöksentekoprosessia. Riskienhallinnan voidaankin katsoa kattavan tänä päivänä paljon laajemman toimintaympäristön kuin vielä voimassa olevan pysyväisasiakirjan PETURVOS PAK 01:02 (julkaisuajankohta 2004) mukaan: "turvallisuusjohtaminen perustuu riskien hallintaan, jonka tärkeimpänä tavoitteena on onnettomuuksien ja rikosten ennaltaehkäisy".

---

[33] Laaksonen, luento.
[34] Aalto.
[35] Pääesikunnan turvallisuusosaston pysyväisasiakirja 01:02: Puolustusvoimien turvallisuustoiminnan strategia, esipuhe, johdanto sekä päämäärä ja sisältö. Asiakirjasta ei ole tietojärjestelmävaihdoksesta johtuen luettavissa julkaisuajankohtaa, mutta tekstin sisällön perusteella sen voidaan olettaa olevan vuodelta 2004.

Miten sitten määritellä ”haluttava lopputulos”, jollei voimassa oleva strategia määritäkään omistajan turvallisuuspolitiikkaa (jollei normeja katsota tällaiseksi) eikä ylimmältä johdolta saada suunnitteluprosessissa vuotuista toimintaohjelmaa muutoin kuin periaatteella ’jatketaan’ toimintoja ja/tai tehtäviä sekä niihin osallistumista? Turvallisuusjohtamisen tavoitetilan määrittely jää tällöin alatason (turvallisuus)johdolle, jolloin turvallisuusnormit muuttuvatkin menetelmiksi ja keinoiksi (katso liite yksi: Puolustusvoimien Täydennyskoulutuskeskuksen opetusmateriaalia otsikolla ’puolustusvoimien turvallisuusstrategia’), joiden toteuttamiseksi on suunniteltava (paikallisesti) tietty määrä resursseja. Näiden lisäksi puolustusvoimat toteuttavat laajempia turvallisuushankkeita (mm TUVA, turvallisuusvalvomohanke sekä TUVE, turvallisuusverkkohanke), joihin paikalliset toimijat liittyvät resurssiensa puitteissa ja/tai käsketysti. Turvallisuusjohtaminen onkin tällä hetkellä enemmän normeja ja menetelmiä kuin turvallisuusstrategialla johtamista. Tulisiko siis riskejäkin alkaa hallita pyrkimällä integroimaan riskienhallinta osaksi taktisen tason ydin- ja tukiprosesseja sekä kehittämiskeskusteluja. Jäljempänä luvussa 3.4 tarkastellaan Puolustusvoimien Johtamisjärjestelmäkeskuksen turvallisuusjärjestelmää ja siihen suunniteltua riskienhallintajärjestelmää tästä lähtökohdasta.

3.2 Riskienhallinta ja sisäinen valvonta puolustusvoimissa

Puolustusvoimien normitietokannasta löytyi 13.2.2010 tehdyssä haussa kuusi sisäisen valvonnan voimassa olevaa ohjetta[36, 37, 38, 39, 40, 41], joiden tulisi perustua puolustusvoimien Pääesikunnan suunnitteluosaston asiakirjaan HD522, sisäinen valvonta puolustusvoimissa (luonnos), vuodelta 2008. Luonnosasiakirjaa tietokannasta ei löytynyt, vain poistettu etulehti[42]. Laajennettaessa hakua hakusanalla ’sisäinen valvonta’ löytyi normitietokannasta 99 asiakirjaa, mutta näiden sisällössä on varsin suuria poikkeavuuksia toisistaan. Näistä vain muutamaan on kirjattu sisäisen valvonnan tarkoitus Corporate Governance -hengessä ja suuressa osassa normeja käsitellään materiaalitarkastuksia, henkilöstön työjärjestystä, hankintoja ja niin edelleen. Painotus on monessa lakien noudattaminen, ei päätöksenteon omaehtoinen oh-

[36] Merivoimien sisäisen valvonnan ohje, HF691/28.5.2009
[37] Pääesikunnan kanslian sisäisen valvonnan ohje, HE519/19.5.2008
[38] Sisäinen valvonta reserviupseerikoulussa, HE1143/29.9.2008
[39] Viestirykmentin sisäisen valvonnan ohje, HE1159/2.10.2008
[40] Ilmavoimien Esikunnan huolto-osaston materiaalitoimintojen valvonta, Cf4346/9.3.2009
[41] Kainuun Prikaatin sisäisen valvonnan ohje, HE1365/3.12.2008

Esitettyjen ohjeiden lisäksi vastaavia ohjeita löytyy asiakirjahallintajärjestelmän eri osista enemmänkin, mutta niiden viitekentässä ei ole ilmeisesti viitattu suoraan Pääesikunnan sisäisen valvonnan ohjeen luonnokseen, jolloin tässä käytetty tietokantaohjelma ei tällaisia asiakirjoja löytänyt. Oletettavasti vastaavia ohjeita, mutta hieman eri referenssikehykseen laadittuna, löytyy kaikista puolustusvoimien joukko-osastoista.
[42] Pääesikunnan suunnitteluosaston asiakirja PVHSM003 (28.10.2009): Sisäinen valvonta puolustusvoimissa. Asiakirjakortti poistettu 18.1.2010. Asiakirjassa on runkona VM042/2004 antama sisäisen valvonnan tarkastelukehikko, jonka mukaisesti asiakirjalla oli tarkoitus ohjeistaa sisäisen valvonnan toteutus puolustusvoimissa.

jaaminen. Ajatuksellisesti kysehän on ’johtamisen laadunvalvonnasta’ eikä sitä voi tehdä kukaan muu kuin toimiva organisaatio itse.

Nopeasti tarkasteltuna muutamat puolustusvoimien normitietokannan ohjeista on laadittu linjaan Valtionvarainministeriön sisäisen valvonnan tarkastelukehikon (VM 042/2004) kanssa ja merivoimat jopa viittaa ohjeessaan tähän asiakirjaan. Merivoimat on kuvannut 14-sivuisessa ohjeessaan sisäisen valvonnan ohjeen tarkoituksen, vastuut, valvontaympäristön, riskienhallinnan ja sen liittymisen välittömästi tehtyihin päätöksiin sekä johtamiseen, valvontamenetelmät, sisäisen valvonnan seurannan ja raportoinnin ja lopulta toimenpiteet havaittaessa väärinkäytöksiä. Merivoimat kuvaa ohjeessaan sisäisen valvonnan seurantaa seuraavasti: ”Sisäisen valvonnan toimivuutta tulee seurata jatkuvasti. Johdon ja esimiesten tulee varmistua sen toimivuudesta ja riittävyydestä osana päivittäistä johtamista. Lisäksi sisäisen valvonnan tilaa arvioidaan itsearviointien avulla vuosittain. Tulos- ja vuosiraporttiin sisältyvänä osana hallintoyksikön johto antaa lausunnon sisäisen valvonnan ja riskienhallinnan tilasta sekä mahdollisista kehittämistarpeista niissä.” Lausunnossa on selvitettävä muun muassa sisäisen valvonnan painopisteet, valvonnalliset toimenpiteet, sisäisen valvonnan havainnot, syyt poikkeamiin, valvonnan onnistuminen ja tulokset, sisäisen valvonnan kokonaistilanne ja kehittämistarpeet aikatauluineen. Merivoimien ohjeen mukaan VM042/2004 ”-arviointikehikko on tarkoitettu johdon työvälineeksi sisäisen valvonnan ja riskienhallinnan asianmukaisuuden ja riittävyyden arviointiin sekä olennaisimpien kehittämistarpeiden tunnistamiseen”.

Entä miten merivoimat on onnistunut toteuttamaan sisäisen valvonnan ohjeessa asettamansa tavoitteet? Tätä voidaan tarkastella merivoimien vuoden 2009 vuosiraportista[43], johon on laadittu oma liitteensä sisäisestä valvonnasta. Vuosiraportin sisäistä valvontaa käsittelevä osio keskittyy hankintojen lainmukaisuuteen ja rahoituksen tarkastukseen. Johtamista, sitä tukevaa päätöksentekoa ja sisäisen valvonnan pohjalta tehtyä prosessiohjausta ei merivoimat kykene raportissaan esittämään. Merivoimien sisäinen valvonta ei siis kykene antamaan vastausta edellisessä kappaleessa esiteltyyn merivoimien sisäisen valvonnan normin vaatimuksiin, minkä perusteella voidaan päätellä, ettei ohjetta ole otettu merivoimissa käyttöön. Näin siis toimintansa yksityiskohtaisimmin ohjeistaneen puolustusvoimien tulosyksikön osalta.

Sisäisen valvonnan toimintojen ja vastuiden luominen puolustusvoimien organisaation on edellä esitetyn perusteella kesken, mutta entä välittömästi liittyvä riskienhallinta? Riskienhallinta on ohjeistettu puolustusvoimissa 22.12.2004 päivätyllä asiakirjalla ’Riskienhallinta puo-

[43] Merivoimien Esikunnan asiakirja DG605 (4.2.2010): Merivoimien vuosiraportti, kohta sisäinen valvonta.

lustusvoimissa[44]'. Ohje sisältää riskienhallinnan periaatteet (johdanto, uhkat ja riskit, riskienhallinta on johtamista, riskienhallinnan velvoitteet, kokonaisturvallisuuden kehittäminen, mistä riskit aiheutuvat, riskin muodostumisen luonne, mihin uhka voi kohdistua, riskin suuruus, kuinka riskejä hallitaan, riski- ja vahinkokustannukset, riskien analysointi, riskianalyysimenetelmiä) ja käytännön toteutuksen (riskienhallinta - mukana kaikissa toiminnoissa, riskianalyysin tekeminen, toimintojen kartoitus, riskianalyysin suunnittelu, analyysiryhmän perustaminen, uhkien tunnistaminen, riskin suuruuden arviointi, riskien luokittelu, toimenpiteiden määrittely ja toteuttaminen, seuranta ja kehittäminen, riskianalyysistä tiedottaminen ja raportointi). Verrattaessa ohjetta turvallisuusjohdon koulutusohjelmassa käsiteltyyn riskienhallinta-aineistoon voidaan todeta, että pysyväisasiakirja sisältää kaikki keskeiset riskienhallinnan perusteet, se on laadittu helposti toimintaan sovellettavaksi kokonaisuudeksi ja on pääosiltaan edelleen ajantasainen. Mutta sovelletaanko sitä puolustusvoimien johtamistoiminnassa siten kuin ohjetta laadittaessa on ollut tarkoitus? Vuosi 2009 nimettiin Pääesikunnan turvallisuustoimialan toimesta 'riskienhalllinan teemavuodeksi[45]', joten tilannetta voidaan tarkastella Pääesikunnan operatiivisen osaston tekemän riskienhallintakartoituksen kautta.

17.3.2009 aloitetun riskienhallintakartoituksen lähtökohta määriteltiin siten, että "riskienhallinta tarkoittaa tunnistettujen uhkien vaikutuksen arviointia omaa toimintaa kohtaan, riskien pienentämiseen tähtäävien toimenpiteiden suunnittelua ja toteutusta sekä niiden vaikuttavuuden arviointia. Jokainen toimiala tai toiminto Puolustusvoimissa on vastuussa oman toimintansa riskienhallinnasta. Turvallisuustoimiala arvioi ensisijaisesti turvallisuuteen liittyviä riskejä oman toimialansa asiantuntemuksen puitteissa." Kartoituksen puitteissa oli tarkoitus saada selvyys turvallisuuden (ei siis ydin- ja tukiprosessien) riskienhallintasuunnitelmien laajuudesta, ajantasaisuudesta ja vaikuttavuudesta. Tämän perusteella "pyritään vuoden kuluessa päivittämään riskienhallinnan normi koordinoiden se muiden toimialojen riskienhallinnan ohjeistuksen kanssa sekä aloittamaan Puolustusvoimien erityispiirteet paremmin huomioivan turvallisuuden riskienarviointimenetelmän kehittäminen."[46]

Riskienhallinnan teemavuoden kartoituksen lopputulemana oli asiakirja AF20764/8.10.2009, jossa "pyrittiin selvittämään turvallisuuteen liittyvän riskienhallinnan tilaa, mutta käsitteistön yleisestä luonteesta johtuen osa vastauksista käsitteli riskienhallintaa muun kuin turvallisuu-

[44] Pääesikunnan turvallisuusosasto: PETURVOS PAK 01:04, Riskienhallinta puolustusvoimissa, 22.12.2004.
[45] Pääesikunnan operatiivisen osaston asiakirja AF1386 (17.3.2009): Turvallisuuden riskienhallinnan nykytilan kartoitus ja teemavuosi 2009. Asiakirjan mukaan "teemavuoden tarkoitus on kartoittaa riskienhallinnan tilanne ja laatia riskikartoitukset organisaatioissa, joissa niitä ei ole tehty, sekä päivittää vanhat suunnitelmat. Vuoden kuluessa pyritään päivittämään riskienhallinnan normi koordinoiden se muiden toimialojen riskienhallinnan ohjeistuksen kanssa sekä aloittamaan Puolustusvoimien erityispiirteet paremmin huomioivan turvallisuuden riskienarviointimenetelmän kehittäminen."
[46] Sama.

den näkökulmasta". Riskienhallinnan vastuista todettiin, että "riskienhallinnan vastuut on kirjattu työjärjestykseen karkeasti puolessa vastaajista, mutta koska riskienhallinta on osa kaikkeen johtamiseen liittyvää toimintaa, sitä ei ole erikseen aina työjärjestyksiin kirjattu. Joukkojen käytännön riskienhallintatyön myötä tehdyt kehittämiskohteet ovat olleet rakenteellisia parannuksia sekä koulutuksen ja ohjeistuksen kehittämisen kautta tehty palvelus- ja työturvallisuuden kehittäminen. Työllä on saavutettu merkittäviä parannuksia turvallisuuteen." Lopulta todettiin, että riskienarviointityö jää usein irralliseksi tapahtumaksi, eikä johda parantamistoimiin, mikä johtuu suunnitelmien jäämisestä TRSS-prosessin (toiminnan ja resurssien suunnittelu ja seuranta) ulkopuolelle, jolloin niistä ei muodostu TOSU:n (toimintasuunnitelma nelivuotiskaudeksi) tavoitteita ja tehtäviä, eikä niihin allokoida tarpeellisia resursseja. Tulevaisuudesta todettiin, että "turvallisuustoiminnan riskianalyysien pohjana tulee olla tutkintaosaston ja tiedustelun tuottamat uhka-arviot", vaikka "todellinen riskienhallinta tai hallitsemattomuus ilmentyy viimekädessä kuitenkin kaikessa johtamistoiminnassa kautta linjaorganisaation". Lisäksi "turvallisuustoiminnan kehittämisen on vastattava sotilaallisen toiminnan aiheuttamaan uhkaan". Tästä johtuen "Puolustusvoimien ja yritysten riskienhallinnan vertailu ja mallien kopioiminen ei ole automaattisesti toimiva ratkaisu, koska riskienhallinnan painopiste yrityksillä on taloudellisten riskien hallinnassa ja lisäksi tärkeänä riskinsiirtokeinona niillä on käytettävissä vakuuttaminen". Asiakirjassa katsottiin ensimmäisen riskienhallintakeinon olevan turvallisuusmääräysten täyttäminen ja näiden valvominen sisäisin ja ulkopuolisin tarkistuksin. Kokonaisuutena riskikartoitusten katsottiin olevan kunnossa.[47]

Pääesikunnan tarkastusyksikkö laati edellisen asiakirjan rinnalla omaa asiakirjaansa puolustusvoimien riskienhallinnasta. Sen tavoitteena oli arvioida puolustusvoimien riskienhallinnan periaatteita, käytäntöjä ja riskienhallinnan nykytilaa. Menetelminä oli arvioida riskienhallintaohjeistus, riskienhallinnalle asetetut tavoitteet ja riskikartoitusten perusteet (oliko arvioitu oikeita asioita). Arviointikriteereinä tarkastusyksikkö käytti valtionhallinnon sisäisen valvonnan ja riskienhallinnan suosituksen arviointikehikkoa vuodelta 2005. Vastaako puolustusvoimien riskienhallinta näitä suosituksia? Loppuanalyysinä riskienhallinnasta oli "riskien tunnistamisen ja arvioinnin perustuminen pääosin vahinkoriskien kartoitukseen, joka perustui puolustusvoimien riskienhalllintaohjeeseen". Kokonaisuutena kehittämistä vaatisi prosessin pitäminen mahdollisimman yksinkertaisena ja sen painopisteen siirtäminen tuloksellisuus- ja prosessiriskien arviointiin. Turvallisuus toimialana kykenee tämän näkemyksen mukaan tarjoamaan kokonaisuudelle 1) näkökulman turvallisuuskartoituksen tekemiseen prosessinomistajien vastatessa riskienhallinnasta ja 2) menetelmiä valittujen riskien hallintaan henkilöiden,

[47] Pääesikunnan operatiivisen osaston asiakirja AF20764 (8.10.2009): Kooste turvallisuuden riskienhallinnan kartoituksesta.

maineen, ympäristön, omaisuuden ja tiedon suojaamiseksi. Tällöinkin on prosessinomistajan vastattava riskin määrittelemisestä ja hallinnasta. Sitä ei voi tehdä kukaan muu.[48]

Kokonaisuutena voidaan todeta, että sekä sisäinen valvonta että riskienhallinta ovat puolustusvoimissa vielä voimakkaassa käymistilassa ja lopputulos riippuu siitä, mihin kokonaisuutta halutaan viedä. Jäädäänkö toimimaan normien varassa, joihin kirjataan ohjeet siitä, miten tulisi toimia, vai päästäänkö puolustusvoimissa todelliseen tulos- ja tehtäväjohtamiseen, johon on liitetty ydin- ja tukiprosessien vakiinnuttaminen ja sisäisen valvonta sekä tähän kokonaisuuteen liitetty riskienhallinta. Riskienhallinnan jäädessä toiminnasta irralliseksi turvallisuustoimialan, tai jonkun muun toimialan vastuulle, ei siitä koskaan saada irti sitä, mitä Valtiovarainministeriö on tarkastelukehikollaan tarkoittanut.

3.3 Puolustusvoimien Johtamisjärjestelmäkeskuksen esittely

”Puolustusvoimien Johtamisjärjestelmäkeskus kuuluu Pääesikunnan alaisiin laitoksiin ja on osa Suomen puolustusta. Sen tehtävänä on luoda puolustushaaroille ja aselajeille niiden tarvitsemat johtamisedellytykset valmiuden eri vaiheissa. PVJJK toimii kolmellakymmenellä paikkakunnalla ja sen palveluksessa on yli 800 työntekijää. Keskuksen johto, hallinto-osasto ja tuotanto-osaston keskitetyt osat toimivat Jyväskylässä ja kehitysosasto Espoossa. Palvelutuotanto toteutetaan neljässä alueellisessa johtamisjärjestelmäkeskuksessa (Oulu, Mikkeli, Hämeenlinna, Turku) ja Tietopalvelukeskuksessa (TPK) Tampereella ja Mikkelissä. Tietopalvelukeskus tuottaa tietojärjestelmien tukipalveluita puolustushallinnolle ja muulle valtionhallinnolle. Puolustusvoimien Johtamisjärjestelmäkeskus tarjoaa monipuolisia ja haastavia johtamisjärjestelmäalan tehtäviä niin siviileille kuin sotilaillekin järjestelmien ylläpidosta alan kehittämistehtäviin.” [49]

Lukuina PVJJK:ta voidaan hahmottaa seuraavasti[50]:

- Palkattu henkilöstö, noin 830
- Miehitettyjä toimipisteitä 30 paikkakuntaa, joissa noin 80 kohdetta
- Viestiasemia 700 - 800 ryhmittelytavasta riippuen (yhdessä

[48] Pääesikunnan tarkastusyksikön asiakirja AF366 (23.4.2009): Puolustusvoimien riskienhallinta.
[49] Puolustusvoimien Johtamisjärjestelmäkeskus: Puolustusvoimien Johtamisjärjestelmäkeskus, http://www.mil.fi/laitokset/pvjjk/index.dsp, ladattu 31.1.2010.
[50] Puolustusvoimien Johtamisjärjestelmäkeskus: PVJJK esittely, http://www.mil.fi/laitokset/pvjjk/aineistot_esitysmateriaalit.dsp ladattu 31.1.2010. Puolustusvoimien Johtamisjärjestelmäkeskus esittäytyy varsin avoimesti internet -verkossa, joten tässä työssä on käytetty PVJJK:n yleisesittelyyn vain julkista aineistoa. Muutamia tietoja on tarkennettu opinnäytetyöntekijän yksityiskohtaisemman tietämyksen pohjalta. Näitä ei ole kuitenkaan yleisesittelyyn lähdetty viitteistämään esimerkiksi virallisten asiakirjojen ja/tai haastattelujen pohjalta, sillä se ei ole työn sisällön kannalta merkittävää.

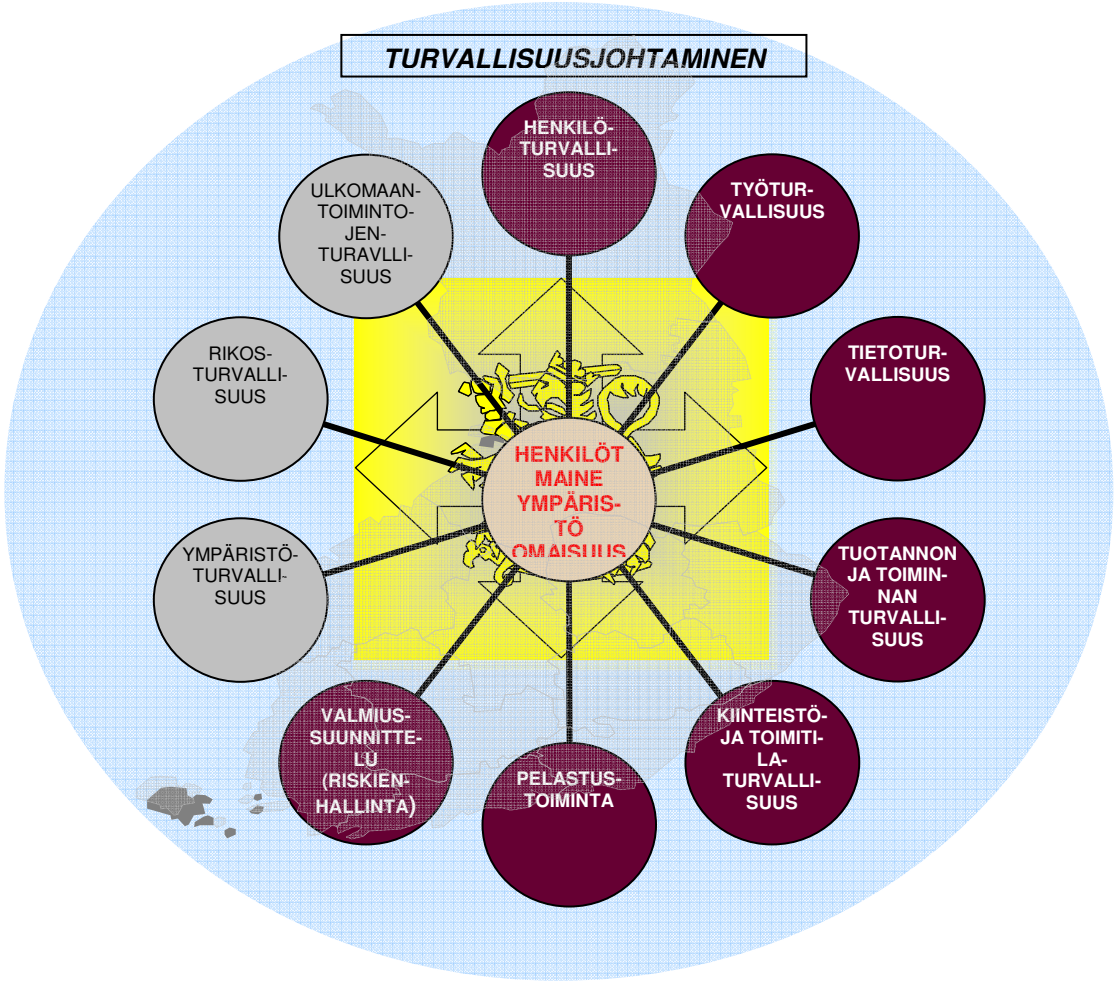
	kohteessa voi olla useita viestiasemia); kasvussa
• ATK-konesaleja, noin	30 eri puolilla Suomea
• Puhelinliittymiä, noin	20 000 (joista pääosa langattomia)
• Erilaisia tietojärjestelmiä, noin	300, mutta joiden määrää pyritään määrätietoisesti supistamaan erilaisilla kehitysohjelmilla, jotka tähtäävät toimintojen vakiointiin (siirto- ja dataverkkotoimintojen uudenlaisella hallinnoinnilla kyetään erottamaan entistä paremmin hallinnolliset ja operatiiviset tietojärjestelmät sekä siirtoverkot toisistaan)
• Asiakkaita	Puolustusvoimat, Puolustusministeriö, Puolustushallinnon Rakennuslaitos, Rajavartiolaitos, Poliisi, Tulli, Merenkulkulaitos, Ilmailulaitos, Senaattikiinteistöt, kaikki Suomessa toimivat teleoperaattorit jne. Valtiovarainministeriön johdolla etenevän turvallisuusverkko -hankkeen (TUVE) myötä asiakkaiden ja hallinnoitavien viestiasemien määrä on nopeassa kasvussa.

Puolustusvoimien Johtamisjärjestelmäkeskuksen rooli poikkeaa muista puolustushallinnon taktisen tason toimijoista siinä, että sen tehtävänä on toimia mahdollistajana muiden joukkojen tiedustelun, valvonnan ja johtamisen eli tiedon pohjalta tehdyn päätöksenteon prosessissa. Laitos ei itsessään tuota varsinaista suorituskykyä tai siis tulivoimaa valittuun maaliin asejärjestelmän muodossa. Nykyisin tosin käsite ’asejärjestelmä’ ja sen myötä myös tuhovoima ovat muuttuneet tai muuttumassa. Esimerkiksi vaikutuskyky vastustajan valtiolliseen päätöksentekoon esimerkiksi tiedustelun, virheellisen informaation antamisen, haitanteon tai muun sellaisen muodossa voi olla tietyissä tilanteissa jopa suurempaa kuin asevaikutus kohteessa. Kaikki tämä tapahtuu mahdollisessa kriisitilanteessa tietysti molempien osapuolten toimintana, mutta sen perusteet luodaan jo syvän rauhan aikana. Tältä perustalta tarkasteltuna Puolustusvoimien Johtamisjärjestelmäkeskuksen riskienhallinta liittyy sekä rauhan aikana tarjottavaan tuotantotoimintaan että vastustajan rauhan aikana tekemien valmistelujen huomioimisena järjestelmä- ja prosessiriskeissä. Suurimpana haasteena tällaiselle kriisiorganisaatiolle onkin omien valmistelutoimien ja järjestelmien kyvykkyyden todellinen testaaminen; se ei liene mahdollista muutoin kuin kriisin eskaloituessa äärimmilleen eli sodaksi. Sotaakin voi tietysti olla useassa eri muodossa ja nykyään jo joillakin yksityisillä, ja mahdollisesti valtioiden salaisesti tukemilla, järjestöillä voi olla sellaista suorituskykyä, että sillä kyetään vaikuttamaan jopa supervaltojen päätöksentekoon. Miten siis tällaisessa kehyksessä niinkin pieni toimija

kuin Puolustusvoimien Johtamisjärjestelmäkeskus voi varautua erilaisiin yksittäisiin ja verkostoriskeihin? Sopivaa toimintamallia pyritään hahmottelemaan seuraavassa luvussa.

3.4 Puolustusvoimien Johtamisjärjestelmäkeskuksen kokonaisturvallisuuden mukainen turvallisuusjärjestelmä

Luotaessa Puolustusvoimien Johtamisjärjestelmäkeskukselle yritysturvallisuuden mallin mukaista turvallisuusjärjestelmää on aivan aluksi hahmotettava se toimintakenttä, jossa PVJJK toimii. Tätä voitaneen hahmottaa sekä liitteen yksi mukaisella turvallisuustoimintojen ryhmittelyllä että puolustusvoimien turvallisuusnormikokoelmalla. Mitkä näistä toiminnoista ja normeista koskevat välittömästi johtamisjärjestelmäkeskusta? Liitteessä yksi käytetty turvallisuusmenetelmien ryhmittely on jo varsin lähellä Elinkeinoelämän Keskusliiton käyttämää yritysturvallisuuden toimintojen ryhmittelyä, joten sen mukaisesti PVJJK:n turvalllisuustoimintojen osa-alueet (joihin keskus päivittäisessä työssään välittömästi osallistuu) ovat:



Kuva 5. ERM-kokonaisturvallisuuden osa-alueet ja niiden toteuttaminen PVJJK:ssa

Käytännössä ryhmittely tarkoittaa sitä, että keskuksen turvallisuusjohtamisen kokonaisuus muodostuu kokonaisuuden johtamisesta, henkilöturvallisuudesta (lupahallinto, turvallisuusselvitykset), työturvallisuudesta (safety; ryhmitetty nykytilassa turvallisuustoimistosta erikseen painottuen työhyvinvointiin), tietoturvallisuudesta jakautuen hallinnolliseen ja järjestelmien tietoturvallisuuteen, tuotannon ja toiminnan turvallisuuteen (sopimuskumppaneiden ja muiden sidosryhmien turvallisuuden järjestäminen), kiinteistö- ja toimitilaturvallisuudesta (PVJJK:n miehitettyjen ja miehittämättömien kohteiden, joita on valtakunnassa yhteensä noin 800 - 900 laskentatavasta riippuen, turvallisuus- ja turvajärjestelmien rakentaminen LVIST-KA-auditointien[51] perusteella), pelastustoiminnasta (lakisääteinen velvoite, jossa keskus toissijaiseksi tukeutuu kunnallisiin palo- ja pelastusviranomaisiin sekä muihin puolustusvoimien alueellisiin toimijoihin) ja valmiussuunnittelusta (ydin- ja tukiprosessien jatkuvuussuunnittelu riskienhallinnan, toimintojen vastuuttamisen ja tehtäväjohtamisen/kehityskeskustelujen keinoin tavoitetilana ottaa järjestelmä käyttöön osana keskuksen organisaatiomuutosta 1.1.2012). Muilla turvallisuusjohtamisen osa-alueilla eli ympäristö-, rikos- ja ulkomaantoimintojen turvallisuus, turvaudutaan joko ylemmän johtoportaan tai muiden viranomaisten tarjoamiin viranomaispalveluihin. Esimerkiksi ulkomailla osana rauhanturvaoperaatioita olevien viestiasemien turvallisuuden järjestelyt kuuluvat kohteella toimivan joukon vastuulle ja matkustusturvallisuus järjestetään Puolustusvoimien Kansainvälisen Keskuksen ohjeiden mukaan. Tämän toimintamallin mukaisesti ryhmitetyt ja käytössä olevat puolustusvoimien normit on ryhmitelty osa-alueittain liitteeseen kaksi ja tätä toimintamallia vastaava turvallisuusorganisaatio on liitteenä kolme.

Puolustusvoimien Johtamisjärjestelmäkeskuksen ollessa nuori, vasta 1.1.2007 perustettu, organisaatio ovat myös monet hallinnolliset ja toimintaa kehittävät mallit vielä työn alla. Turvallisuusorganisaation osalta tämä tarkoittaa sitä, että monet toiminnot on vielä ryhmitelty organisaation sisälle osin turvallisuusorganisaation ulkopuolelle, jolloin myös niiden johtaminen ei ole kokonaisuutena turvallisuuspäällikön johdossa. Järjestelmien tietoturvallisuuden osalta tämä on ollut tietoinen päätös, sillä keskuksen luonteen huomioiden tietojärjestelmäturvallisuus on kiinteä osa sen ydinprosesseja, jolloin se on organisoitu osaksi tuotantotoimintaa. Suurimpana haasteena keskuksella onkin nykytilassaan järjestää yhteiset hallinnolliset menettelytapansa siten, että niilläkin pyritään kohti keskuksen johtajan määrittämää toiminnan tavoitetilaa, joka on ”operatiivisten tietojärjestelmien käytettävyys kaikissa tilanteissa”. Operatiivista kokonaisuutta ei luonnollisesti kannata täysin irrottaa hallinnollisista tietojärjestelmäpalveluista, sillä esimerkiksi järjestelmiin pääsy, henkilöstön luotettavuusarvioinnit, koulutus,

[51] Nikupeteri, Jukka: Tietoteknisten laitetilojen kokonaisturvallisuuden arviointi -tutkielma 17.9.2008, Teknillinen Korkeakoulu, Dipoli.

PKI-korttituotanto ja jakelu kannattaa järjestää yhtenä prosessina. Mutta miten tällaisessa osittain julkisessa toimintaympäristössä kyetään takaamaan toimintojen jatkuvuus?

Toistaiseksi keskus on pyrkinyt järjestämään turvallisuustoimintojaan noudattamalla puolustusvoimien normeja siinä laajuudessa kuin se on ollut olemassa olevilla resursseilla mahdollista, mutta jo asioiden esittäminen EK:n mallin mukaan on johtanut siihen, että keskukseen on palkattu keskitettyjen osien turvallisuusrakenteista vastaava turvallisuusupseeri ja vuosien 2009/2010 vaihtuessa keskukseen palkattiin kaksi sopimusauditoijaa, jotka ovat ottamassa vastuulleen keskuksen sidosryhmien turvajärjestelyiden tarkastamisen. Tämä kokonaisuus tukee myös alueellisten johtamisjärjestelmäkeskusten turvallisuusupseereita rakentamaan alueellisen lupahallinnon, tietoturvallisuuden ja fyysiset kohteet siten, että ne palvelevat tavoitetilaa. Turvaorganisaation täydellinen keskittäminen on kuitenkin mahdotonta paikallistuntemusvaatimusten vuoksi.

Kuten alaluvuista 3.1 ja 3.2 voi päätellä, suurimpana haasteena Puolustusvoimien Johtamisjärjestelmäkeskukselle on järjestää riskienhallintansa siten, että se palvelee jatkuvuussuunnittelua. Yksiselitteistä mallia toiminnan järjestämiseksi ei puolustusvoimat -tasolla ole, mutta tarve saattaa riskienhallinta osaksi johtamisprosessia on varsin suuri. Muussa tapauksessa on vaara, että rajallisia resursseja kohdennetaan tehottomasti sellaisiin kohteisiin, jotka voitaisiin turvata tehokkaammin toimimalla toisin (esimerkiksi henkilöstöhallinnon toimenpitein). Turvallisuus ei voi toimialana tarjota muita kuin turvallisuuden menetelmiä prosessinomistajien käyttöön. Toistaiseksi haasteena on prosessinomistajien keskittyminen osaprosessien hallintaan, jolloin prosesseja ja niiden liittymäpintoja toisiinsa ei tarkastella kokonaisuutena.

Ydin- ja tukiprosessien riskienhallinnan järjestäminen siten, että se vastaa olemassa olevia uhkia ei voi perustua edellä esitetyn mukaisesti ”tutkintaosaston ja tiedustelun tuottamiin uhka-arvioihin”, sillä ne eivät vastaa prosessienomistajien käsitystä kriittisistä riskeistä. Puolustuspoliittisissa selonteoissa linjatut uhka-arviot ovat liian laajakantaisia prosessiuhkien poistamiseksi tai minimoimiseksi, mutta ne tulee huomioida osana laajempaa kokonaisuutta, kuten puolustusvoimien kehittämishankkeita. PVJJK:n turvallisuusalan näkemyksen mukaan ydin- ja tukiprosesseista vastuulliset on saatava organisaatioroolinsa mukaisesti vastuuseen myös riskienhallinnasta. Tavoitteeseen pääsemiseksi ollaan keskukselle kuvaamassa riskienhallintapäällikön tehtävää, joka käytännössä toteuttaa riskienhallinnan suunnittelun turvallisuuspäällikön määrittämässä kehyksessä (miten alas organisaatioon riskienhallinta viedään), kouluttaa prosessien omistajat ERM:in mukaiseen tarkastelumalliin (seitsemän kohtaa, joihin PVJJK osallistuu) sekä osallistuu prosessien tarkasteluun (osa toimintoketjussa, uhka, seura-

ukset, nykyinen suojautuminen, toimenpide-ehdotukset, riskiluku ja riskianalyysi) ja osaprosessien riskien kokoamiseen. Turvallisuusala tarjoaa siis menetelmiä riskienhallintaan sekä hallinnoi kokonaisuutta.

Riskienhallintaa tullaan tarkastelemaan tiettyyn tavoitetilaan sitoen, joka PVJJK:lla tullee olemaan ”operatiivisen verkon käytettävyys kaikissa tilanteissa”. Keskeytysriskit tullaan siis irrottamaan yritysmaailman käyttämästä talouteen perustuvasta tarkastelusta ja painotetaan operatiivisia sekä vahinkoriskejä. Keskeytysriskejä arvioidaan lähinnä tuotannon ja toiminnan turvallisuuteen eli sidosryhmiin liittyen. Käytännössä tämä tarkoittaa sitä, että myös ydin- ja tukiprosessien johtaminen voitaisiin perustaa tiedostettuihin riskeihin, riskianalyyseihin, riskivalintaan ja johtamisen sekä turvallisuuden keinoja käyttäen riskien minimointiin. Riskienhallinnan tuotteena saadaan tällöin eri toimintatasojen (johto, tuotanto, tukitoiminnot) riskit ja pullonkaulat. Kukin riski analysoidaan (mitä on tehtävä, jotta…) ja luokitellaan (prioriteettilista). Kullekin tasolle määritetään luokittelun perusteella suurimmat riskit (2-4 kpl) ja vastuuhenkilö (kuka). Tavoitteet asetetaan (implementointi) osana vuosittaisia kehityskeskusteluja, jolloin tiedot tehdyistä suojautumisista saadaan vuosittain tehtävässä tarkastelussa. Tämän perusteella kyetään määrittämään PVJJK:lle ns. nousevat ja laskevat riskit sekä niin sanotut TOP10 riskit ja niiden sijoittautuminen organisaatioon. Ensivaiheessa riskejä arvioidaan listattavan PVJJK:lla noin 350 (23 organisaatiotasoa * 15 riskiä). Riskit ovat organisaation eri osissa oletetusti erilaisia, jolloin riskienhallinnalla saadaan sekä riskejä esille että myöhemmässä vaiheessa vakioitua toimintaa.[52]

PVJJK:n riskienhallinta alkaa suunnitellusti vuoden 2011 toisella kvartaalilla ja/tai erikseen määritettävänä ajankohtana, riippuen keskuksen uuden NATO-organisaation käyttöönoton aikataulusta. Nykyiseen organisaatioon ei riskienhallinnan rakentamisen aloittamista katsota nykyresursseilla tarkoituksenmukaiseksi, vaikka siitä saataisiinkin perusteita uuden organisaation johtamisprosesseille. Ne poikennevat nykytila kuitenkin niin paljon, että koko työ jouduttaisiin kuitenkin rakentamaan uudelleen. Oletusarvoisesti riskikartan suunnittelu, hyväksyttäminen PVJJK:n johdolla, koulutusmateriaalien laadinta sekä riskienhallinnan järjestelyjen testaus (johto) kestää vuoden 2011 loppuun, jolloin varsinainen riskienhallinta tuotantoorganisaatiolla kyetään aloittamaan vuonna 2012. Implementointi kyetään tällöin huomioimaan kehityskeskusteluissa vuonna 2013, jollei organisaatio ala saatujen tulosten pohjalta toteuttamaan oma-aloitteisesti riskienhallintaa.

[52] Puolustusvoimien Johtamisjärjestelmäkeskuksen asiakirja AF7626 (8.4.2009): Puolustusvoimien Johtamisjärjestelmäkeskuksen riskienhallinta.

3.5 Johtopäätökset

Puolustusvoimien turvallisuustoiminnot sekä siihen välittömästi liittyvät riskienhallinta ja sisäinen valvonta eivät ole tämän tutkimuksen perusteella sillä tasolla kuin mikä yleinen mielikuva asiasta mahdollisesti on. Toimintaan näyttää tulleen taantuma vuodesta 2005 alkaen, jossa haasteina näyttäisivät olevan sekä turvallisuusorganisaation alaspainettu asema entiseen verrattuna (nykyisin toimialan ylin toimija on Pääesikunnan operatiivisen osaston turvallisuussektorin johtaja, eikä NSA:n roolissa oleva puolustusvoimien turvallisuusjohtaja/-päällikkö), pääosan turvallisuusosaston tehtävistä (mm. normit, DSA:n tehtävät, yritysten turvallisuusauditoinnit) vastaanottanut Pääesikunnan tutkintaosasto, jolla ei ole ollut riittäviä resursseja ylläpitää toimintaa aiemmalla tasolla sekä turvallisuusstrategian ja strategialla johtamisen sekä tehtäväjohtamisen puutteet. Jonkinlainen turvallisuustoimialan esiintulo riskienhallinnan integroimisessa osaksi päätöksentekoa voisi viedä toimialan tavoitteita eteenpäin nopeammin kuin mihin nykymallilla pystytään.

Analysoitaessa riskienhallintaa Pääesikunnan operatiivisen osaston ja tarkastusyksikön asiakirjojen pohjalta näyttää siltä, ettei ohjaavalla johtoportaalla ole toistaiseksi yhtenäistä linjaa siitä, miten ohjeistaa riskienhallintaa. Pääesikunnan tarkastusyksikkö on asiakirjallaan liittynyt Valtionvarainministeriön tarkastelukehikon kannattajaksi, kuten myös suunnitteluosasto tietokannasta poistetulla HD522 -asiakirjallaan. Sen sijaan operatiivisen osaston turvallisuustoimiala lähestyy asiaa turvallisuusnäkökulmasta. Kokonaisuus on selvästi vielä jäsentymätön. Kyettäessä luomaan malli, jossa tavoitteet, organisaatio ja tehtävät ovat linjassa ylhäältä alas asti, saataneen toimintaa tehostettua nykyisestä vielä huomattavasti.

4. YHDISTELMÄ

Kaikilla hankkeilla tulee olla kasvollinen omistaja, joka antaa niille tavoitteet sidottuna henkilöön ja aikaan; ”Virtanen, esikuntarakennuksen kamera on oltava asennettuna tänään kello 12.00!” Vain saamalla ylätason ’liihottelutavoitteet’ koko organisaation ja kaikkien sen prosessien läpi yksilöityinä tavoitteina toteuttajalle asti on johtaminen onnistunutta. Tämän opinnäytetyön tuloksena on esitetty haasteita, joita turvallisuustoimialalla on puolustusvoimissa tämän ketjun toteuttamisessa ja miten toimintaa voitaisiin kehittää. Miten siis laatia tavoitteet, mihin tavoitetilaan ne tulee laatia ja millaisella organisaatiolla niihin kyetään vastaamaan? Puhtaimmillaan koko johtamisessahan on kyse viestintäsuunnitelman laatimisesta, sen noudattamisesta ja jonkinlaisesta takaisinkytkennästä. Tämän tavoitteen saavuttamiseen jokainen

ketjun toimija tarvitsee kolme viestiä: 1) Mitä uutta teen?, 2) Mitä lakkaan tekemästä ja 3) Mitä alan tehdä eri tavalla? Pelkällä normeeraamisella tai normijohtamisella ei tähän päästä.[53]

Kun prosesseja ryhdytään rakentamaan, niin turvallisuusarkkitehtuurin tulee olla mukana suunnittelussa alusta alkaen. Tällaisen proaktiivisen suunnittelun kautta päätöksen teon tullessa ajankohtaiseksi ollaan uuteen tilanteeseen valmentauduttu, kuten tilanne olisi jo koettu. Jos tietoisuutta turvallisuusriskeistä ei ole, niin silloin riskin realisoitumisen vaara on paljon suurempi kuin proaktiivisessa toimintamallissa. Aika monet erilaisista riskeistä toteutuvatkin vain siksi, ettei niihin ole varauduttu; ei ole riittävästi mietitty toimintojen seurauksia. Arkirutiineissa nämä riskit eivät yleensä näyttäydy, jolloin niihin valmistautuminen vaatii huolellista oman toiminnan ja prosessien tarkastelua. Vietäessä tällä tavoin laadittu riskikartta yritysjohdolle päätöksentekoa varten, niin heille samalla annetaan todellinen mahdollisuus tehdä sitä strategista pohdiskelua yrityksen riskikentästä, josta he ovat vastuussa. Nollatoleranssi on riskien suhteen mahdotonta; ilman riskiä ei ole voittoa. On siis tunnistettava riskien paikat ja tehtävä valinta riskeihin varautumisesta. Tärkeintä on tilannetietoisuus.[54]

Turvallisuusjohdon tehtävänä on tässä mallissa miettiä valmiiksi, miten aktualisoituneeseen riskiin kyetään reagoimaan olemassa olevilla resursseilla. Nämä kyvyt tulee antaa ylimmän johdon tietoon, sillä se tekee lopulta ratkaisut käytettävistä menetelmistä. Tällöin tarjolla on yleensä vain huonoja vaihtoehtoja ja aikaa todella vähän, joten ennakkovalmistautumisen merkitys korostuu. Turvallisuusjohdon onkin analysoitava työtään siten, että ”teemmekö oikeita asioita” ja ”mihin/miten me aikamme käytämme”. Pienet, mutta moninaiset riskit, joiden vaikuttavuus on vähäinen, kannattaa yleensä pitää. Tärkeintä on saada prosessin omistaja/t mukaan kehittämään oman toimintansa hallintaa.[55, 56]

Opinnäytetyössä esimerkkinä olleen Puolustusvoimien Johtamisjärjestelmäkeskuksen turvallisuus tulee rakentaa kokonaisturvallisuuden mallin mukaisesti siten, että kaikki ne osa-alueet, joissa keskuksella on toimintaa, tulee organisoida johdon asettamaan tavoitetilaan sitoen (operatiivisten tietojärjestelmien käytettävyys kaikissa tilanteissa). Osa-alueisiin tulee ryhmitellä puolustusvoimien normikokoelmasta ne menetelmät, joilla on joko hallinnollista tai toimin-

[53] Huuskonen, Visa: Muutoksen johtamisen hyvät käytännöt. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 16.2.2010. Huuskonen on koulutukseltaan kauppatieteiden tohtori ja Leaderment Oy:n toimitusjohtaja.
[54] Aho, Esko: Yritysturvallisuus, johdon odotukset. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 17.2.2010, tutkijan muistiinpanot. Aho on entinen pääministeri ja nykyinen Nokian kokonaisturvallisuudesta vastaava johtaja. Materiaali tutkijan hallussa.
[55] Sama.
[56] Nyström, Tommi: Turvallisuuden kehittäminen yhteistyökumppanien avulla. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 17.2.2010. Nyström toimii Otso Oy:n konsernitoimintojen johtajana. Materiaali tutkijan hallussa.

nallista käyttöä laitoksen riskienhallinnassa. Käytännössä tämä tarkoittaa sitä, että osa riskeistä tulee aluksi pitää, mutta tavoitteiden saavuttamisen (riskien laskemisen) myötä voidaan keskittyä nouseviin riskeihin tai jo prosesseista löydettyjen riskien laskemiseen. Riskienhallinnan saaminen osaksi koko organisaation prosesseja ja niiden johtamista johtaa myös riskitason yleiseen alenemaan. Tässä mallissa turvallisuusala tarjoaa tukiprosessina ydinprosesseille käsittely-/ajatusmallin, riskianalyysin sekä toimialansa riskienhallinnan menetelmiä. Menetelmiä löytyy myös muilta toimialoilta, kuten henkilöstöhallinnosta (mikä onkaan se kriittinen työvaihe, johon vaaditaan lisähenkilöstöä). Käytännössä tämä tarkoittaa toimintojen vastuuttamista mahdollisimman alas ja substanssiosaamisen merkityksen korostamista läpi koko organisaation.

Mikä lopulta sitten yhdistää yritysturvallisuutta ja sisäistä valvontaa? ”Sisäinen valvonta on prosessi, johon vaikuttavat organisaation hallintoelimet, johto ja henkilöstö ja joka on tarkoitettu kohtuullisessa määrin varmistamaan, että toiminta on tehokasta ja tarkoituksenmukaista, raportointi on luotettavaa ja lakeja ja ohjeita noudatetaan. Riskienhallinta sisältää toimintatavat, prosessit ja rakenteet, joilla tunnistetaan, arvioidaan ja hallitaan tavoitteita uhkaavia riskejä. Molemmat sisältävät ajatuksen epävarmuuden hallinnasta. Sisäisen valvonnan osa-alueet ovat COSO:n mukaan 1) johtamistapa ja valvontakulttuuri, 2) riskien arviointi, 3) päivittäisvalvonta ja tehtävien eriyttäminen, 4) seuranta ja tarkastus sekä 5) tiedonkulku ja raportointi.”[57] Valtiovarainministeriön tästä kehittämää sisäisen valvonnan mallia (VM042/2004) voidaankin soveltaa sellaisenaan kaikkiin puolustusvoimien organisaatioihin, mutta sen käyttöönotto vaatii organisaatiolta ponnisteluja, joihin ainakaan tämän tutkimuksen perusteella ei ole vielä löytynyt tarvittavaa motivaatiota. ”Vapaus hyvä, kontrolli paras[58]”.

Kokonaisturvallisuutta, puolustusvoimien turvallisuusstrategiaa ja puolustusvoimien turvallisuuden normiohjausta on käsitelty tässä työssä holistisesti eli kokonaisuutena tai toisiinsa liittyvinä kokonaisuuksina. Joku voisikin sanoa, että empiria on muodostettu reduktionistisesti, eli työssä on liitetty toisistaan irrallisia osia yhteen kokonaisturvallisuuden oppien mukaan. Turvallisuuden ollessa kiinteä osa kaikkia puolustusvoimien toimintoja voidaan siitä tällöin käsitellä myös tiettyjä, valittuja osa-alueita. Tässä työssä on käsitelty turvallisuuden itsensä kannalta keskeistä johtamisen ketjua, josta kokonaisuus muodostuu tai on muodostumatta. Tutkimus on toistettavissa käytetyin menetelmin puolustushallinnon sisällä, minkä lisäksi sitä

[57] Vuoti, Helge: Corporate Governance - mikä on sallittua, mikä kiellettyä, miten torjua väärinkäytökset? Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 10.11.2009. Vuoti työskentelee Tuokko Tilintarkastus Oy:ssä. Materiaali on tutkijan hallussa.

[58] Pisto Martti Herman: Muuttuva yritys - turvallisuuden haasteet ja toteutus, kohta turvallisuuden haasteita. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008. Tutkijan luennoitsijan esitysmateriaaliin täydentämät muistiinpanot. Materiaali tutkijan hallussa.

voidaan laajentaa myös muihin valtionhallinnon aloihin (yleistettävyys). Täten tulosten validiteetin ja reliabiliteetin arvioidaan vastaavan asetettuja tutkimustavoitteita [59].

Työhön ei ole välittömästi liitettäviä jatkotutkimusvaihtoehtoja. Lähin tavoitteellinen muutos, jota opinnäytteen kautta voidaan lähteä soveltamaan, on ohjeistaa puolustushaarojen ja joukko-osastojen turvallisuustoiminnot organisoitavaksi kokonaisturvallisuuden mallin mukaisesti, jolloin joukkojen tehtäväkentät (ja tehtävänkuvaukset) sekä niitä vastaavat henkilöstömäärät saadaan toisiinsa nähden vertailukelpoisiksi. Jatkotyönä voidaan lähteä pohtimaan puolustusvoimien johtamista riskienhallinnan lähtökohdista sekä riskienhallinnan normittamista osaksi sisäistä valvontaa eli Corporate Governancea.

[59] Tuomi, Jouni, Sarajärvi, Anneli: Laadullinen tutkimus ja sisältöanalyysi, Jyväskylä 2006, s. 66 – 68, 101 – 102 ja 133. ”Koska kaikessa tutkimustoiminnassa pyritään välttämään virheitä, on yksittäisessä tutkimuksessa arvioitava tehdyn tutkimuksen luotettavuutta. Metodikirjallisuudessa tutkimusmenetelmien luotettavuutta käsitellään yleisesti validiteetin (tutkimuksessa on tutkittu sitä, mitä on luvattu) ja reliabiliteetin (tutkimustulosten toistettavuus / yleistettävyys) käsittein.” Nämä käsitteet ovat syntyneet kvantitatiivisen tutkimuksen parissa, jolloin yhdistettäessä ihmistieteellinen tutkimus luonnontieteelliseen menetelmään on tutkimuksen validiteettia ja reliabiliteettia arvioitava menetelmänsä eli toistettavuuden ja tutkittavan kohteen kautta.

LÄHTEET

1. JULKAISEMATTOMAT LÄHTEET

Aalto, Mika: Luento ’strategiasta kriittisesti’ EUK60:lle, 12.12.2007
Aho, Esko: Yritysturvallisuus, johdon odotukset. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 17.2.2010
Huuskonen, Visa: Muutoksen johtamisen hyvät käytännöt. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 16.2.2010
Koivisto, Raija: Tulevaisuuden uhkiin varautuminen; uudenlaiset riskit -tutkimus. Luento Turvallisuusjohdon koulutusohjelmassa TTK Dipolissa 10.2.2009
Laaksonen, Marko: Luento strategian perusteista EUK60:lle, 12.9.2007
Laaksonen Marko: Palaute strategisen suunnittelun etätehtävistä EUK60:lle, 15.10.2007
Mikkonen, Jarmo: Toimitilaturvallisuus ja turvallisuusvalvonta. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 13.10.2009
Nyström, Tommi: Turvallisuuden kehittäminen yhteistyökumppanien avulla. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 17.2.2010
Pisto Martti Herman: Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008 aiheesta ”Muuttuva yritys - turvallisuuden haasteet ja toteutus”
Porras Ville: Fyysisen turvallisuuden kurssin koulutusmateriaalia vuodelta 2009 aiheena ”puolustusvoimien turvallisuusstrategia”
Tiihonen, Kalevi: Yritysturvallisuuden malli, osa 1. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008
Tiihonen, Kalevi: Sisäisen turvallisuuden ohjelman ja yritysturvallisuuden rajapinnat, osa 2. Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 15.10.2008
Viljanen Ritva: Luento Turvallisuusjohdon koulutusohjelmassa 15.10.2008 aiheena ”Sisäisen turvallisuuden ohjelma ja sisäisen turvallisuuden strategia”
Vuoti, Helge: Corporate Governance - mikä on sallittua, mikä kiellettyä, miten torjua väärinkäytökset? Luento Turvallisuusjohdon koulutusohjelmassa TKK Dipolissa 10.11.2009

2. JULKAISTUT LÄHTEET

Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management - Integrated Framework, syyskuu 2004 (nettijulkaisu)

Elinkeinoelämän Keskusliitto, Sisäasiainministeriö, Puolustusministeriö (20.11.2009): Kansallinen turvallisuusauditointikriteeristö (KATAKRI). Sisäisen turvallisuuden ohjelman toisen vaiheen toimenpide 6.4. tp 2

Kenttäohjesääntö, yleinen osa: Puolustusjärjestelmän toiminnan perusteet, Helsinki 2007

Niiniluoto, Ilkka: Johdatus tieteenfilosofiaan, Keuruu 1984

Keskuskauppakamari: Suositus listayhtiöiden ja hallinnointi- ja ohjausjärjestelmistä (Corporate Governance), joulukuu 2003 (nettijulkaisu)

Nikupeteri, Jukka: Tietoteknisten laitetilojen kokonaisturvallisuuden arviointi -tutkielma 17.9.2008, Teknillinen Korkeakoulu, Dipoli

Oinonen Jari: New Public Management ja puolustusvoimien uudistaminen -tutkimustyö, huhtikuu 2008

Puolustusministeriö: Puolustusministeriön strateginen suunnittelu, käsikirja, Helsinki 2007

Tuomi, Jouni, Sarajärvi, Anneli: Laadullinen tutkimus ja sisältöanalyysi, Jyväskylä 2006

Valtiovarainministeriö (VM 042/00/2004): Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta (valtionhallinnon hyvä käytäntö ja sen toteutumisen arviointi), 20.12.2005

3. INTERNET

Arvopaperimarkkinayhdistys: Corporate Governancen määritelmä, http://www.cgfinland.fi/content/blogcategory/15/42/lang,fi/... Ladattu 24.10.2010

Arvopaperimarkkinayhdistys: Corporate Governancesta yleisesti, http://www.cgfinland.fi/content/blogcategory/15/42/lang,fi/... Ladattu 24.10.2010

Puolustusvoimien Johtamisjärjestelmäkeskus: Puolustusvoimien Johtamisjärjestelmäkeskus, http://www.mil.fi/laitokset/pvjjk/index.dsp, ladattu 31.1.2010

Puolustusvoimien Johtamisjärjestelmäkeskus: PVJJK esittely, http://www.mil.fi/laitokset/pvjjk/aineistot_esitysmateriaalit.dsp ladattu 31.1.2010

Tampereen Teknillinen Yliopisto: Riskienallintaa 1.10.2003, http://www.cs.tut.fi/~projekti/dokumentit/riskienhallintaa.pdf, ladattu 31.1.2010

Valtiovarainministeriö: Sisäinen valvonta ja riskienhallinta/viraston sisäinen valvonta ja riskienhallinta/vastuu sisäisen valvonnan järjestämisestä/sisäisen valvonnan arviointi/arviointikehikko http://www.vm.fi/vm/fi/09_valtiontalous/045_tuloksellisuus/03_sisainen_valvonta_ja_riskienhall/index.jsp (ladattu 13.2.2010)

Wikipedia: Riski, http://fi.wikipedia.org/wiki/Riski, ladattu 31.1.2010.

Wikipedia: Turvallisuuden tunne, http://fi.wikipedia.org/wiki/Turvallisuus ladattu 24.10.2010.

Wikipedia: Turvallisuus, http://fi.wikipedia.org/wiki/Turvallisuus ladattu 24.10.2010.

4. MUUT LÄHTEET

4.1 Puolustusvoimien pysyväisasiakirjat / hallinnolliset normit

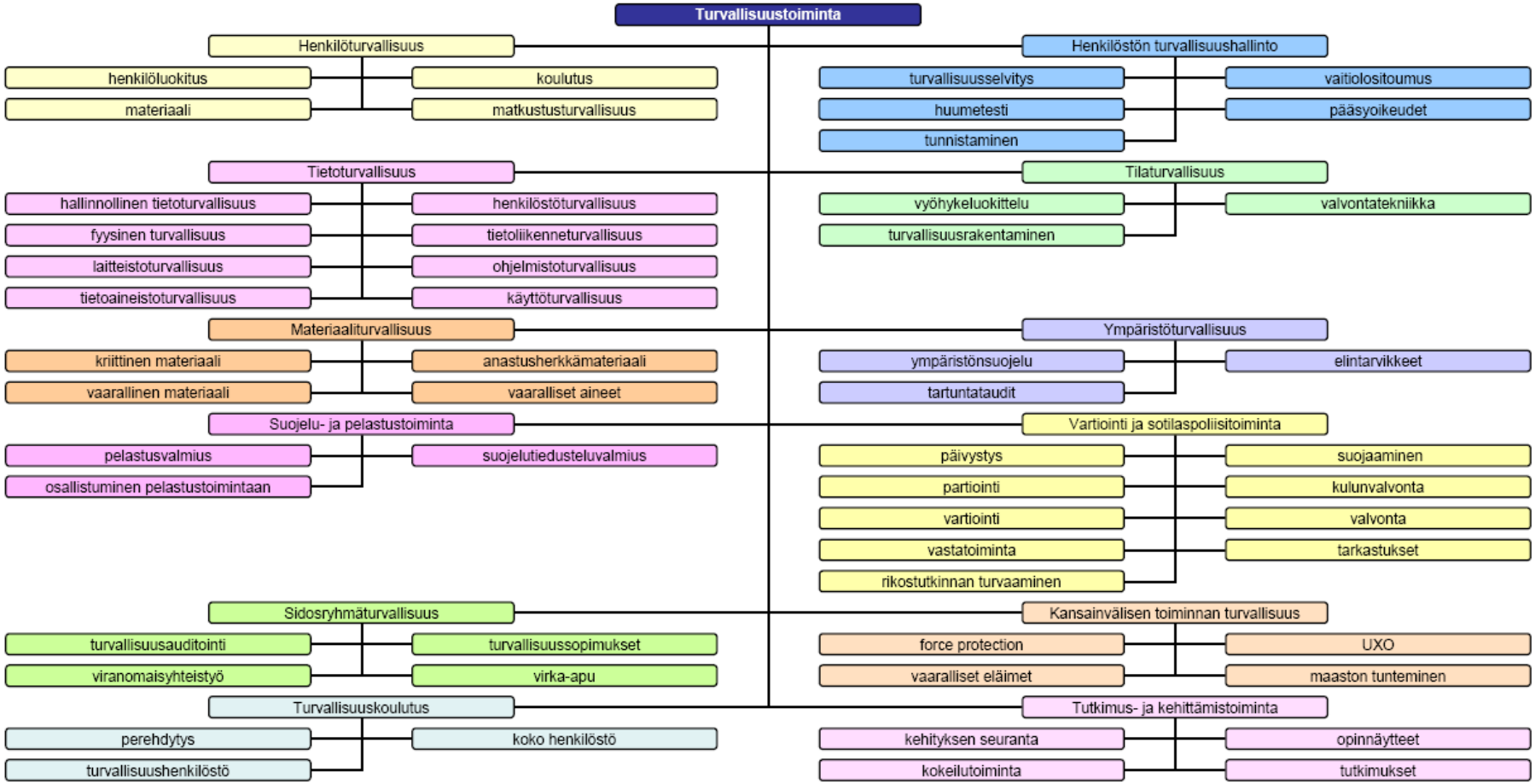
Ilmavoimien Esikunnan huolto-osaston materiaalitoimintojen valvonta, Cf4346/9.3.2009
Kainuun Prikaatin sisäisen valvonnan ohje, HE1365/3.12.2008
Merivoimien sisäisen valvonnan ohje, HF691/28.5.2009
Pääesikunnan kanslian sisäisen valvonnan ohje, HE519/19.5.2008
Pääesikunnan operatiivisen osaston ohje R2/11.2/D/I/19.1.2004: Strateginen suunnittelu puolustusvoimissa normaaliaikana
Pääesikunnan suunnitteluosaston asiakirja PVHSM003 (28.10.2009): Sisäinen valvonta puolustusvoimissa
Pääesikunnan turvallisuusosasto: PETURVOS PAK pysyväisasiakirja 01:02: Puolustusvoimien turvallisuustoiminnan strategia
Pääesikunnan turvallisuusosasto: PETURVOS PAK 01:04, Riskienhallinta puolustusvoimissa, 22.12.2004
Pääesikunnan turvallisuusosasto: PETURVOS PAK 02:02, Hankintojen ja ostopalvelujen turvallisuus
Pääesikunnan turvallisuusosasto: PETURVOS PAK 03:01, Pääsy ja liikkuminen sotilaskohteissa
Pääesikunnan turvallisuusosasto: PETURVOS PAK 03:02, Puolustusvoimien henkilötodistukset
Pääesikunnan turvallisuusosasto: PETURVOS PAK 03:05, Turvallisuusselvitykset
Pääesikunnan turvallisuusosasto: PETURVOS PAK 03:07, Käyttöoikeuksien hallinta
Pääesikunnan turvallisuusosasto: PETURVOS PAK 03:08, Käyttöoikeuksien myöntämisen perusteet
Pääesikunnan turvallisuusosasto: PETURVOS PAK 03:09, Puolustusvoimien henkilöstöturvallisuus
Pääesikunnan turvallisuusosasto: PETURVOS PAK 04:02, Puolustusvoimien tietoturvallisuus
Pääesikunnan turvallisuusosasto: PETURVOS PAK 04:03, Asiakirjojen luokittelu ja tietoturvallisuusmerkinnät
Pääesikunnan turvallisuusosasto: PETURVOS PAK 04:05, Turvallisuusluokiteltujen asiakirjojen käsittely

Pääesikunnan turvallisuusosasto: PETURVOS PAK 04:10, NATO:n turvaluokiteltujen asiakirjojen käsittely
Pääesikunnan turvallisuusosasto: PETURVOS PAK 04:12, Salassa pidettävien asiakirjojen katoamiset ja tuhoutumiset
Pääesikunnan turvallisuusosasto: PETURVOS PAK 04:13, Valtionhallinnon tietoturvaohjeiston käyttö
Pääesikunnan turvallisuusosasto: PETURVOS PAK 04:15, Käyttäjän tietoturvaohje
Pääesikunnan turvallisuusosasto: PETURVOS PAK 05:01, Sotilaskohteiden turvallisuusvyöhykkeet
Pääesikunnan turvallisuusosasto: PETURVOS PAK 05:02, Tilaturvallisuus
Pääesikunnan turvallisuusosasto: PETURVOS PAK 05:03, Puolustusvoimien alueiden merkitseminen
Pääesikunnan turvallisuusosasto: PETURVOS PAK 05:11, Sotilaskohteiden ja maanpuolustustiedon julkisuus paikkatiedossa
Pääesikunnan turvallisuusosasto: PETURVOS PAK 06:02, Suojelu- ja pelastustoiminnan yleisohje
Pääesikunnan turvallisuusosasto: PETURVOS PAK 07:01:Sidosryhmäturvallisuus
Pääesikunnan turvallisuusosasto: PETURVOS PAK 07:02, Turvallisuusauditointi (20.11.2009 KATAKRI)
Pääesikunnan turvallisuusosasto: PETURVOS PAK 07:03, Turvallisuus ulkoistamisessa
Sisäinen valvonta reserviupseerikoulussa, HE1143/29.9.2008
Viestirykmentin sisäisen valvonnan ohje, HE1159/2.10.2008

4.2 Puolustusvoimien (julkiset) asiakirjat

Merivoimien Esikunnan asiakirja DG605 (4.2.2010): Merivoimien vuosiraportti
Puolustusvoimien Johtamisjärjestelmäkeskuksen asiakirja AF7626 (8.4.2009): Puolustusvoimien Johtamisjärjestelmäkeskuksen riskienhallinta
Pääesikunnan operatiivisen osaston asiakirja AF1386 (17.3.2009): Turvallisuuden riskienhallinnan nykytilan kartoitus ja teemavuosi 2009
Pääesikunnan operatiivisen osaston asiakirja AF20764 (8.10.2009): Kooste turvallisuuden riskienhallinnan kartoituksesta
Pääesikunnan tarkastusyksikön asiakirja AF366 (23.4.2009): Puolustusvoimien riskienhallinta

PUOLUSTUSVOIMIEN TURVALLISUUSSTRATEGIA[60]



[60] Porras Ville: Fyysisen turvallisuuden kurssin koulutusmateriaalia vuodelta 2009. Majuri Porras toimii Puolustusvoimien Täydennyskoulutuskeskuksessa turvallisuusalan pääopettajana

PUOLUSTUSVOIMIEN TURVALLISUUSNORMIKOKONAISUUS
PUOLUSTUSVOIMIEN JOHTAMISJÄRJESTELMÄKESKUKSESSA[61]

Hallinnollinen turvallisuus, yhteinen kaikille osa-alueille:

- PETURVOS PAK 01:02 Turvallisuusstrategia

1. Henkilöstöturvallisuus:

- PETURVOS PAK 03:01 Pääsy ja liikkuminen sotilaskohteissa
- PETURVOS PAK 03:02 Puolustusvoimien henkilötodistukset
- PETURVOS PAK 03:05 Turvallisuusselvitykset
- PETURVOS PAK 03:09 Puolustusvoimien henkilöstöturvallisuus

2. Työturvallisuus:

- Oma toimialansa, jolla omat norminsa ja joiden pohjalta PVJJK:lle on laadittu työsuojelun toimintaohjelma. Turvallisuustoimiala toimii osaltaan työsuojelun hankintojen rahoittajana, muttei muutoin osallistu tavoitteiden ja/tai ohjeiden laadintaan.

3 Tietoturvallisuus:

- PETURVOS PAK 03:07 Käyttöoikeuksien hallinta
- PETURVOS PAK 03:08 Käyttöoikeuksien myöntämisen perusteet
- PETURVOS PAK 04:02 Puolustusvoimien tietoturvallisuus
- PETURVOS PAK 04:03 Asiakirjojen luokittelu ja tietoturvallisuusmerkinnät
- PETURVOS PAK 04:05 Turvallisuusluokiteltujen asiakirjojen käsittely
- PETURVOS PAK 04:10 NATO:n turvaluokiteltujen asiakirjojen käsittely
- PETURVOS PAK 04:12 Salassa pidettävien asiakirjojen katoamiset ja tuhoutumiset
- PETURVOS PAK 04:13 Valtionhallinnon tietoturvaohjeiston käyttö
- PETURVOS PAK 04:15 Käyttäjän tietoturvaohje

4. Tuotannon ja toiminnan turvallisuus:

- PETURVOS PAK 01:04 Riskien hallinta

[61] Puolustusvoimien normitietokanta, josta on koottu keskeiset eri normit ryhmiteltynä yritysturvallisuuden malliin siten, kuin Puolustusvoimien Johtamisjärjestelmäkeskus normeja tutkielman tekohetkellä käyttää.

- PETURVOS PAK 02:02 Hankintojen ja ostopalvelujen turvallisuus
- PETURVOS PAK 07:01 Sidosryhmäturvallisuus
- PETURVOS PAK 07:02 Turvallisuusauditointi (20.11.2009 KATAKRI)
- PETURVOS PAK 07:03 Turvallisuus ulkoistamisessa

5. Kiinteistö- ja toimitilaturvallisuus:

- PETURVOS PAK 05:01 Sotilaskohteiden turvallisuusvyöhykkeet
- PETURVOS PAK 05:02 Tilaturvallisuus
- PETURVOS PAK 05:03 Puolustusvoimien alueiden merkitseminen
- PETURVOS PAK 05:11 Sotilaskohteiden ja maanpuolustustiedon Julkisuus paikkatiedossa

6. Pelastustoiminta:

- PETURVOS PAK 06:02 Suojelu- ja pelastustoiminnan yleisohje

7. Valmiussuunnittelu:

- PETURVOS PAK 01:04 Riskien hallinta

8. Ympäristöturvallisuus, rikosturvallisuus ja ulkomaantoimintojen turvallisuus ovat ilman ylemmän johtoportaan turvallisuusnormeja

- Puolustusvoimien Johtamisjärjestelmäkeskus turvautuu näiden toimintojen osalta joko ylemmän johtoportaan tarjoamiin virastopalveluihin tai muihin viranomaispalveluihin.

PVJJK:n TURVALLISUUSORGANISAATIO JA -RAKENTEET RYHMITELTYNÄ COSO ERM-MALLIN MUKAISESTI