



LAUREA
AMMATTIKORKEAKOULU

Uuden edellä

Riskienhallinta osaksi eduskunnan kanslian johtamista

Scherf, Anna

2012 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Riskienhallinta osaksi eduskunnan kanslian johtamista

Anna Scherf
Turvallisuusosaamisen
koulutusohjelma
Opinnäytetyö
Helmikuu, 2012

Anna Scherf

Riskienhallinta osaksi eduskunnan kanslian johtamista

Vuosi

2012

Sivumäärä

146

Eduskunnan turvallisuustoiminta nousee säännöllisin väliajoin julkisen kiinnostuksen kohteeksi ja kahden viimeisen vuoden aikana keskustelu eduskunnan turvallisuustoiminnan riittävydestä on ollut poikkeuksellisen vilkasta. Tämän tutkimuksellisen kehittämistyön tavoitteena on selvittää eduskunnan kanslian turvallisuustoiminnan kehittämistarpeet ja tutkia riskienhallinnan soveltamismahdollisuuksia turvallisuuden kehittämisessä. Tavoitteena on lisäksi tukea eduskunnan kanslian turvallisuusjohtajaa, riskienhallinnan asiantuntijaa ja virkamiesjohtoa organisaation kokonaisvaltaisessa kehittämisessä. Kehittämistyön toimeksiantaja on eduskunnan kanslian turvallisuusyksikkö.

Kohdeorganisaation kehittäminen jakautuu työssä kolmeen osaan. Teoreettinen viitekehys palvelee osaltaan eduskunnan kansliassa turvallisuuden ja riskienhallinnan parissa työskentelevien tiedontarvetta. Työn toisen osan muodostavat eduskunnan kanslian turvallisuustoiminnan nykytilaa, turvallisuusympäristön mahdollisia tulevaisuuden kehityssuuntia ja muiden eurooppalaisten parlamenttien riskienhallintaa käsittelevä luku. Sen tarkoituksena on yhtäältä osoittaa ja toisaalta perustella eduskunnan kanslian turvallisuustoiminnan kehittämistarpeet. Työn kolmas osa käsittelee eduskunnan kanslian riskienhallintatoiminnan käynnistämistä.

Tässä työssä riskienhallintaa käsitellään valtionhallinnon näkökulmasta ja sen soveltamismahdollisuuksia tutkitaan organisaatioturvallisuuden kehittämiseen sitoen. Viitekehys rakentuu organisaatioturvallisuuden, riskienhallinnan ja strategisen johtamisen teoriasta. Kehittämistyö toteutetaan tapaustutkimusta, tulevaisuudentutkimuksen skenaariotyöskentelyä ja konstruktivistista tutkimusta soveltaen. Tutkimusaineisto on kerätty haastatteluin, kyselyin, dokumenttianalyysin ja havainnoinnin avulla ja aineiston analyysimenetelminä käytetään kehittämistöille tyypillisesti sekä laadullisia että määrällisiä menetelmiä.

Johtopäätöksenä voidaan todeta, että eduskunnan turvallisuustoiminta ei nykyisessä muodossaan riitä vastaamaan turvallisuusympäristön alati koveneviin haasteisiin, jotka vaativat organisaatioturvallisuuden eri osa-alueiden kokonaisvaltaista hallintaa. Lisäksi voidaan osoittaa, että riskienhallintatoiminnan aloittaminen eduskunnan kansliassa tukee erinomaisesti organisaatioturvallisuuden pitkäjänteistä ja kokonaisvaltaista kehittämistä, resurssien tehokasta käyttöä ja turvallisuuskulttuurin rakentamista. Riskienhallintatoiminnalla voidaan myös kehittää eduskunnan kanslian johtamisjärjestelmää ja sisäistä viestintää sekä tukea kanslian maineenhallintaa ja kriisiviestintää.

Kehittämistyön tulokset on otettu hyvin vastaan eduskunnan kanslian turvallisuusyksikössä. Työ palvelee myös muita valtionhallinnon organisaatioita sillä siinä käsitellään organisaatioturvallisuuden ja riskienhallinnan suhdetta sekä turvallisuusympäristön tulevaisuuden mahdollisia kehityssuuntia julkisen sektorin näkökulmasta.

Asiasanat: eduskunnan kanslia, organisaatioturvallisuus, riskienhallinta, valtionhallinto, turvallisuusympäristö

Anna Scherf

Integrating Risk Management into the Finnish Parliamentary Office

Year	2012	Pages	146
------	------	-------	-----

The Parliament of Finland is regularly addressed in the national media and the sufficiency of Parliament's security has been of particular interest during the past two years. The purpose of this Master's thesis is to investigate the need for development of the security of Parliamentary Office as well as study the possibilities that risk management has to offer in terms of enhancing security within the organization. This thesis also aims at supporting the Director of Security, Risk Management expert and the Office's top management in developing their organization comprehensively. This research was commissioned by the Security Department of the Parliament Office.

This research-based development study can be divided into three parts. Firstly, the theoretical framework is meant to serve as background information for personnel involved with security and risk management in the Parliamentary Office. The second section studies the current capacity of the Office's Security Department, the possible future developments of the Parliament's security environment and the realization of risk management in other European Parliaments. The purpose of this second section is on one hand to point out and on the other hand validate the need for development in the organization's security. Finally the third section concentrates on suggestions on how to enhance the Office's security in applying risk management.

Risk management is approached from the point of view of state administration and its possibilities are studied in relation to organizational security. The framework is built on organizational security, risk management and strategic management theories. Research styles applied in the present study include case study, future studies' scenarios as well as constructive research. The research material is gathered using interviews, inquiries, document analysis and observation. Characteristically in a research-based development, analysis of the research material consists of both quantitative and qualitative methods.

The conclusions of this research indicate that the security in the Finnish Parliamentary Office at its current state does not meet the requirements set out by the security environment's development into an ever more challenging direction that require a more comprehensive approach on organizational security. Furthermore, the application of risk management within the Parliamentary Office enables the persevering and comprehensive development of security, the effective use of resources and construction of security culture within the organization. Risk management also contributes to the development of management system and internal communication and well as reputation management and crisis communication.

This research-based study development has been well received by the Security Department. In addition, the results concerning the synergies of organizational security and risk management as well as the scenarios of future security environment's possible developments can be applied within other public sector organizations.

Keywords: future studies, parliamentary office, state administration, risk management, organizational security

Sisällys

1	Johdanto	7
1.1	Eduskunnan kanslian tehtävät	8
1.2	Eduskunnan organisaatorakenteesta	9
1.3	Johtosuhteet ja henkilöstö	10
1.4	Lähtökohdat eduskunnan riskienhallinnan kehittämiseksi	11
2	Teoreettinen tausta	13
2.1	Keskeiset käsitteet	13
2.2	Riskienhallinta strategisen johtamisen tukena valtionhallinnossa	16
2.2.1	Strategisen johtamisen merkitys organisaation toiminnalle	17
2.2.2	Strategiatyön tarve valtionhallinnon organisaatioissa	18
2.3	Riskienhallinta	20
2.3.1	Riskienhallinnan tavoitteet	21
2.3.2	Riskienhallinnan johtaminen ja asiakirjat	23
2.3.3	Riskienhallintamenetelmät	27
2.4	Riskienhallinnan tarve ja toteutus valtionhallinnossa	29
2.4.1	Riskienhallinta ja organisaatioturvallisuus	31
2.4.2	Riskienhallinta ja sisäinen tarkastus	35
2.5	Kriisiviestintä osana riskienhallintaa	36
3	Kehittämistehtävän määrittely	39
3.1	Kehittämistyön tausta ja aikaisemmat tutkimukset	39
3.2	Kehittämistyön tavoitteet ja tutkimuskysymykset	43
3.3	Aiheen rajaus	45
4	Tutkimusmenetelmät	46
4.1	Kehittämistyö prosessina	46
4.1.1	Tapaustutkimus	48
4.1.2	Tulevaisuudentutkimus	49
4.1.3	Konstrukttiivinen tutkimus	50
4.2	Kehittämistyössä käytetyt aineistonkeruumenetelmät	51
4.2.1	Haastattelut ja kyselyt	51
4.2.2	Havainnointi ja dokumenttianalyysi	53
4.2.3	Parhaat käytänteet	55
4.2.4	Skenaariotyöskentely	55
4.3	Aineiston analysointi	58
5	Tutkimuksen tulokset	61
5.1	Eduskunnan kanslian riskienhallinnan nykytila	61
5.1.1	Eduskunnan kanslian strategia ja arvot	63
5.1.2	Turvallisuusjohtamisen painopisteet	66
5.1.3	Sisäinen tarkastus	69

5.1.4	Eduskunnan kanslian nelikenttäanalyysi	70
5.1.5	Eduskunnan kanslian ydintoimintoihin liittyvät riskit	73
5.2	Eduskunnan kanslian mahdolliset tulevaisuuden turvallisuusympäristöt	77
5.2.1	Valtionhallinnon turvallisuusympäristöä kuvaava tulevaisuustieto	78
5.2.2	Eduskunnan kanslian toimintaympäristön PESTE-analyysi	84
5.2.3	Eduskunnan kanslian turvallisuusympäristön ennakoititeemat	86
5.2.4	Skenaario 1: Kriittinen kotipesä	88
5.2.5	Skenaario 2: Teknokraattien anarkia	90
5.2.6	Skenaario 3: Viralliset valtarakenteet maalitauluina	91
5.2.7	Skenaario 4: Yhteiskuntarauha järkkyy	93
5.3	Riskienhallinnasta muissa eurooppalaisissa parlamenteissa	94
5.3.1	Määrällinen analyysi	94
5.3.2	Laadullinen analyysi	96
5.3.3	Vertailuaineiston yhteenveto ja johtopäätökset	100
6	Johtopäätökset	102
6.1	Eduskunnan kanslian turvallisuusympäristö muuttuu haasteellisemmaksi	102
6.2	Todellinen turvallisuus vaatii kokonaisvaltaista lähestymistapaa	102
6.3	Riskienhallinta tukee eduskunnan kanslian turvallisuuden kehittämistä	106
7	Riskienhallintatoiminnan käynnistäminen eduskunnan kansliassa	108
7.1	Riskienhallinnan tavoitteet eduskunnan kansliassa	109
7.2	Riskienhallinnan integrointi eduskunnan kanslian toimintaan	111
7.3	Turvallisuuskulttuuri ja riskitietoisuus	113
7.4	Kriisiviestintä ja poikkeustilanteiden johtaminen	116
8	Työn arviointi	119
8.1	Kehittämistyöhön liittyvät eettiset kysymykset	119
8.2	Tavoitteenasettelu ja tulokset	120
8.3	Teoreettinen viitekehys	121
8.4	Lähestymistavat	122
8.5	Aineistonkeruumenetelmät ja analyysi	123
8.6	Ehdotuksia jatkotutkimusten aiheiksi	124
	Lähteet	125
	Kuvat	131
	Kuviot	132
	Taulukot	133
	Liitteet	134

1 Johdanto

Riskienhallinnan sisällyttäminen osaksi eduskunnan kanslian johtamista on mahdollisuutena mielenkiintoinen ja aiheena ajankohtainen. Riskienhallinnan soveltamismahdollisuuksien tutkiminen valtionhallinnon organisaatiossa sopii hyvin turvallisuusosaamisen tieteenalalle ja sillä voi lisäksi olla yhteiskunnallista merkitystä. Valtionhallinnossa organisaatioturvallisuuden ja riskienhallinnan toteutus on aikaisemmissa tutkimuksissa (muun muassa Herrainsilta 2006) osoitettu tällä hetkellä olevan varsin vaihtelevalla tasolla. Valtionhallinnon toiminnan jatkuvuus vaikuttaa yhteiskunnan toimivuuteen ja kansalliseen päätöksentekoon ratkaisevasti. Näin ollen valtionhallinnon organisaatioiden turvallisuustoiminnan ja riskienhallinnan kehittämisen tulisikin olla aktiivista.

Eduskunnalla on ainutlaatuinen rooli valtionhallinnossa. Tämän opinnäytetyön johtojatukse-
na on, että riskienhallinnan soveltaminen eduskunnan kansliassa mahdollistaisi organisaatioturvallisuuden kokonaisvaltaisemman toteuttamisen, turvaisi tehokkaammin eduskunnan toiminnan jatkuvuuden sekä tukisi osaltaan eduskunnan kanslian strategista johtamista. Lisäksi sillä voi olla organisaation eri yksiköiden toimintaa yhdistävä ja lähentävä vaikutus, puhumattakaan eri yksiköiden ja osastojen erityisosaamisen tehokkaammasta hyödyntämisestä koko organisaation tasolla.

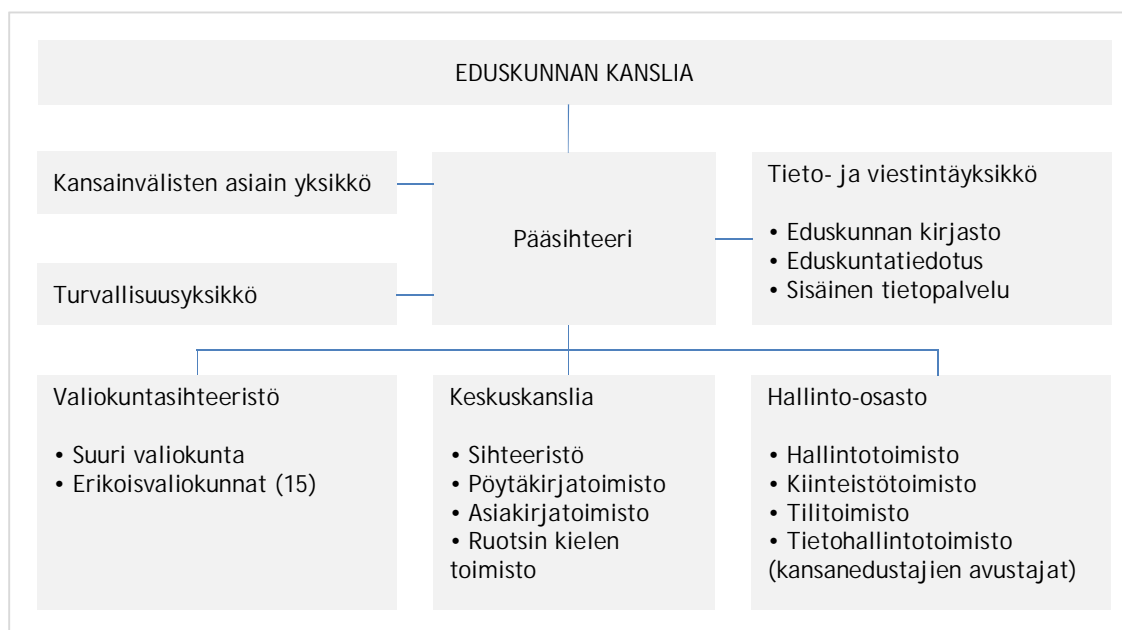
Tutkimustyön luovin osio on eduskunnan kanslian tulevaisuuden turvallisuusympäristön kehitystä käsittelevä luku, jossa hyödynnetään tulevaisuudentutkimuksen skenaariotyöskentelyä. Skenaariot rakennetaan eduskunnan kanslian turvallisuustoiminnan näkökulmasta, mutta niistä voi olla hyötyä myös muille valtionhallinnon organisaatioille valtionhallinnon näkökulman ja erityistarpeiden huomioiden osalta. Riskienhallintaan liittyvissä kysymyksissä tavoitteiltaan ja yhteiskunnalliselta rooliltaan yksityiseen sektoriin nähden erilaisen organisaation tarkastelu tuo lisää tietoa yksityisellä sektorilla yleisesti käytettyjen turvallisuuden ja riskienhallinnan ratkaisujen soveltamismahdollisuuksista julkisella sektorilla yleensä ja erityisesti valtionhallinnossa. Opinnäytetyön taustalla vaikuttaa vahva oletamus siitä, että eduskunnan kanslian turvallisuusympäristö kehittyy haastavampaan suuntaan yhteiskunnan ja kansainvälisen turvallisuustilanteen muutosten rinnalla.

Opinnäytetyön aihevalintaan on vaikuttanut osaltaan myös eduskunnan kansliassa työskentelyni aikana herännyt huoli organisaation kyvystä vastata tulevaisuuden turvallisuushaasteisiin. Johtopäätösten lisäksi opinnäytetyöhön onkin sisällytetty myös luku, jossa käsitellään riskienhallintatoiminnan käynnistämistä eduskunnan kansliassa.

1.1 Eduskunnan kanslian tehtävät

Eduskunnan tehtävänä on lakien säätäminen, valtion talousarviosta päättäminen, kansainvälisten sopimusten käsittely, maan hallituksen toimien valvominen ja pääministerin valitseminen. Eduskunnan keskeisiä tehtäviä toteuttavat elimet ovat päätösvaltaa käyttävä täysistunto, asioita valmistelevat valiokunnat sekä poliittista linjaa vetävät eduskuntaryhmät. (Eduskunta 2011.)

Eduskunta laajana käsitteenä sisältää poliittisten toimijoiden (kansanedustajat, eduskuntaryhmät, puhemies, kansliatoimikunta) ja eduskunnan kanslian (virkamiehet) lisäksi myös eduskunnan yhteydessä toimivat kolme virastoa, jotka ovat eduskunnan oikeusasiamiehen kanslia, ulkopoliittinen instituutti (UPI) ja valtiontalouden tarkastusvirasto. Tämän kehittämistyön kohteena on eduskunnan kanslia ja työn toimeksiantajana eduskunnan kanslian turvallisuusyksikkö.



Kuvio 1: Eduskunnan kanslian organisaatiorakenne (Eduskunta 2011)

Eduskunnan kansliassa luodaan eduskunnalle edellytykset hoitaa sille valtioelimenä kuuluvat tehtävät. Kanslia koostuu kuudesta osastotasoisesta yksiköstä, jotka huolehtivat täysistunto-työn sujuvuudesta, valiokuntatyöstä, kansainvälisten suhteiden hoidosta, eduskunnan hallinnosta, kiinteistöistä, tiedonhankinnasta ja tiedottamisesta. Kanslian turvallisuusyksikkö vastaa eduskunnan turvallisuusjärjestelmän toimivuudesta kaikissa olosuhteissa, pelastustoiminnasta ja väestönsuojelusta. Sen vastuulla on myös turvallisuusjärjestelmän kehittäminen. (Eduskunta 2011.)

1.2 Eduskunnan organisaatorakenteesta

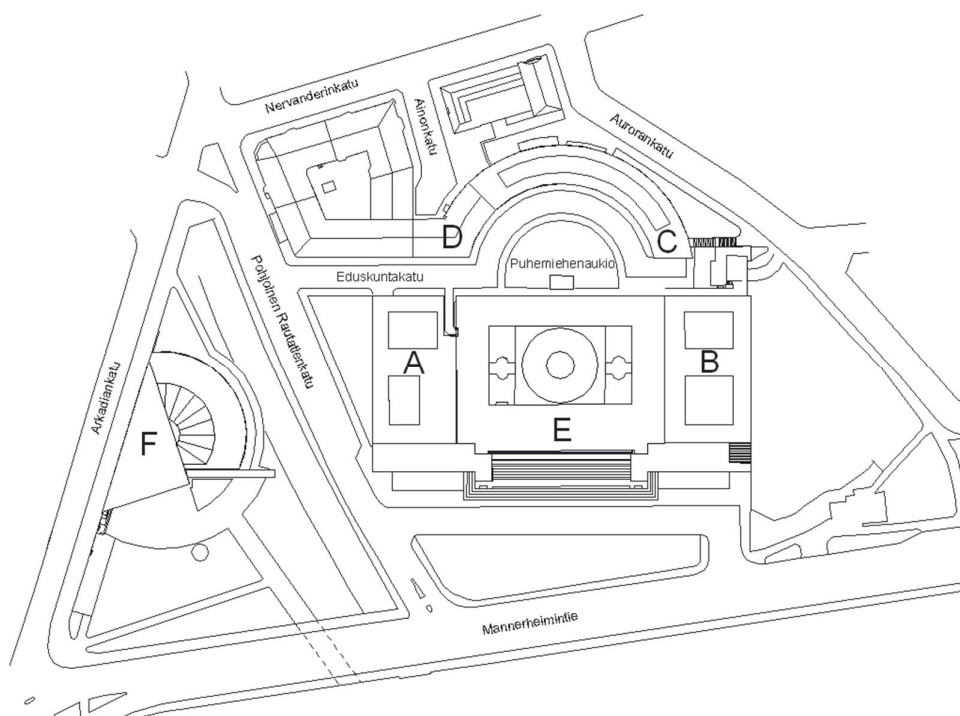
Keskuskansliassa huolehditaan eduskunnan täysistuntoihin liittyvistä valmistelu-, täytäntöönpano- ja palvelutehtävistä. Siellä laaditaan täysistuntojen pöytäkirjat, valmistetaan ja julkaistaan valtiopäiväasiakirjat ja rekisterit, käännetään keskeisten valtiopäiväasiakirjat ruotsin kielelle sekä huolehditaan asiakirjojen jakelusta ja arkistoinnista. Valiokuntasihteeristö vastaa valiokuntien kokousten valmisteluista ja käytännön järjestelyistä, käsiteltävien asioiden valmistelusta ja huolehtii asiakirjojen ja kokouspöytäkirjojen laatimisesta ja toimittamisesta. (Eduskunta 2011.)

Kansainvälisten asiain yksikkö hoitaa kansainvälisiä suhteita ja niihin liittyviä käytännön asioita. Se avustaa puhemiehiä, pääsihteerä sekä eduskunnan toimielimiä ja yksiköitä kansainvälisissä yhteyksissä pois lukien suhteet EU:n toimielimiin. Lisäksi yksikkö pitää yhteyttä muihin parlamentteihin, kansainvälisten järjestöjen sihteeristöihin ja ulkoasiainhallintoon ja toimii eduskunnan nimittämien valtuuskuntien sihteeristönä. (Eduskunta 2011.)

Eduskunnan tieto- ja viestintäyksikkö koostuu eduskunnan kirjastosta, sisäisestä tietopalvelusta sekä eduskuntatiedotuksesta. Eduskunnan kirjasto on kaikille avoin julkinen kirjasto, jonka asiantuntijuusalueet ovat oikeudellinen tieto, yhteiskuntatieto ja eduskuntatieto. Sisäisen tietopalvelun tehtävänä on kansanedustajien ja virkamiesten eduskuntatyössä tarvitseman tietoaineiston hankkiminen, EU-tietopalvelu, tv-ohjelmien videopalvelu, verkkotietopalvelujen tarjoaminen ja muun muassa verkkolähteiden käyttökoulutus. Eduskuntatiedotus vastaa mediaviestinnästä, verkkoviestinnästä ja kansalaisten tiedotuspalvelusta. Tiedotuksen tehtäviin kuuluu lisäksi opastettujen vierailujen järjestäminen, kansalaiskyselyihin vastaaminen ja kansalaisinfon toiminnasta vastaaminen. (Eduskunta 2011.)

Eduskunnan kuusi yksikköä sijaitsevat kolmessa eri rakennuksessa ja yhteensä seitsemässä siivessä Antinkatu mukaan luettuna (Kuva 1). Työhuoneita eduskunnassa on Antinkadun toimitot mukaan lukien hieman yli 800 (Eduskunnan kiinteistötoimisto 2011a). Käynnissä oleva peruskorjaus vaikuttaa valmistuessaan myös tilaratkaisuihin.

Eduskunnan päärakennus valmistui vuonna 1931. Eduskuntatalon sijainti Arkadianmäellä ei ollut kaupunkisuunnittelijoiden eikä arkkitehdin tarkoitus – eduskuntatalon eteen suunnitellut julkisten rakennusten ryhmä ja Itsenäisyyden aukio jäivät ajan saatossa alkuperäisistä suunnitelmista poiketen rakentamatta. Kuriositeettina kerrottakoon lisäksi, että eduskuntatalon 48:stä askelmasta koostuvien pääportaiden yhteenlaskettu pituus on huikeat kaksi kilometriä. (Eduskunta 2011, Eduskunnan kiinteistötoimisto 2011a.)



Kuva 1: Eduskuntaan kuuluvat rakennukset ja henkilöstön työskentelytilat (A–F) pois lukien Antinkatu (Eduskunnan kiinteistötoimisto 2011b)

1.3 Johtosuhteet ja henkilöstö

Pääsihteeri on eduskunnan kanslian päällikkö tehtävänänsä johtaa ja valvoo eduskunnan kanslian toimintaa toimien itse kansliatoimikunnan alaisuudessa. Käytännössä se tarkoittaa huolehtimista muun muassa kanslian työskentelyn vaatimasta toimintavalmiudesta, kanslian toiminnan tehokkaasta suunnittelusta ja johtamisesta sekä henkilökunnan tarkoituksenmukaisesta sijoittamisesta ja käytöstä. Pääsihteeri tekee kansliatoimikunnalle tarpeelliseksi katsomiansa esityksiä kanslian toiminnan kehittämiseksi ja valvoo erityisesti kansliaa koskevien lainsäädäntö- ja muiden tärkeimpien asioiden valmistelua. (Eduskunnan kanslia 1987.)

Eduskunnan hallituksen asemassa toimii kansliatoimikunta, johon kuuluvat eduskunnan puhemies, varapuhemiehet sekä neljä eduskunnan keskuudestaan valitsemaa kansanedustajaa ja heidän varajäsenensä. Kansliatoimikunta päättää muun muassa eduskunnan vuotuisesta talousarvioehdotuksesta, nimittää eduskunnan keskeisimmät virkamiehet, sopii virkamiesten palvelussuhteen ehdoista, eduskunnan tilojen käytöstä ja merkittävistä hankinnoista. (Eduskunta 2011.)

Eduskunnan kansliassa toimii lisäksi virkamiesjohdon jäsenistä koostuva johtoryhmä. Eduskunnan kanslian johtoryhmästä ei ole säädetty erikseen, mutta se vastaa toimintaperiaatteiltaan ja asemaltaan ministeriöiden johtoryhmiä sillä erotuksella, että kansliatoimikunta tekee myös

lopullisia päätöksiä. Eduskunnan kanslian johtoryhmä on viimeisen vuoden aikana käsitellyt pääosin hallinnon kehittämishanketta, kanslian työaikajärjestelyitä, uutta palkkausjärjestelmää, koulutusasioita sekä tulos- ja taloussuunnittelua. (PNE 1/2010 vp.)

Johdettavia eduskunnan kansliassa oli vuoden 2010 lopussa yhteensä 655, joista vakinaisessa virassa toimi kaksi kolmasosaa (Eduskunnan kanslia 2010b, 17). Eduskunnan kanslian henkilöstön keski-ikä saman vuonna oli noin 44,9 vuotta ja vähintään 45-vuotiaiden osuus oli 52,8 prosenttia. Alle 35 -vuotiaita henkilöstöstä oli 26 prosenttia, joista naisten osuus 64 prosenttia. Henkilöstön pysyvyys on korkea, sillä lähes 40 prosentilla henkilöstöstä on takanaan vähintään 15 vuoden palvelus. Alle viisi vuotta palvelleita henkilöstöstä on 22 prosenttia. Ylemmän korkeakoulutason tutkinnon suorittaneita oli vuoden 2010 loppuun mennessä 32,8 prosenttia henkilöstöstä ja lähes 60 prosenttia näistä tutkinnoista kaupallisia tai yhteiskuntatieteellisiä. (Eduskunnan kanslian hallintotoimisto 2011. Tulevina vuosina eduskunnan kansliaan palkataan yksi uusi virkamies kahta eläkkeelle siirtyvää virkamiestä kohden.

1.4 Lähtökohdat eduskunnan riskienhallinnan kehittämiseksi

Tutkijan esittely lienee sekin paikallaan sikäli, että tutkijan ja kehitettävän kohteen välinen suhde vaikuttaa osaltaan työn arviointiin ja esitettyjen argumenttien uskottavuuteen. Aloittaessani opinnäytetyön kirjoittamisen olin ehtinyt työskennellä eduskunnan kansliassa yhteensä puolitoista vuotta valiokuntasihteeristöön sijoittuvassa määräaikaisessa virassa. Toimenkuvani ei suoranaisesti sisällä turvallisuusvastuuta päivittäisiä tieto- ja toimitilaturvallisuuteen liittyviä yleisiä velvollisuuksia lukuun ottamatta.

Työyhteisöä innostavasti kehittävän työn tuottaminen edellyttää aktiivista ja ennakkoluulotonta yhteistyötä sen jäsenten kanssa. Turvallisuusyksikön lisäksi yhteistyö sisäisen tarkastuksen, teknisestä tietoturvallisuudesta vastaavan henkilön, kriisiviestinnän parissa työskentelevän henkilön sekä virkamiesjohdon kanssa on perusedellytys organisaation turvallisuustoiminnan kokonaisvaltaiselle ymmärtämiselle ja toisaalta turvallisuuden eri osa-alueiden parissa toimivien tahojen kehitystoiveiden selvittämiseksi. Turvallisuuden ja riskienhallinnan kehittämiseen liittyvä verkostoituminen eduskunnan kansliassa aloitettiin heti turvallisuusosamisen opintojen alkuvaiheessa koulutusohjelmaan kuuluvien kurssitöiden yhteydessä.

Kohdeorganisaation kokonaisvaltaista ymmärrystä lisää myös osallisuuteni kanslian erilaisissa kehittämisprojekteissa (strategialuonnoksen kommentointi, tietohallintouudistus, valiokuntasihteeristön sisäiset kehitysprojektit, työyksikön kehittämistyöt), joiden kautta tutustuin myös oman yksikköni ulkopuolella työskenteleviin virkamiehiin. Valiokuntasihteeristön näkökulmaa laajensivat puolestaan sen eri kanslioissa tekemäni sijaisuudet. Vaikka edellä mainitut tekijät eivät suoranaisesti liity turvallisuuteen tai riskienhallintaan, auttoivat ne minua ym-

märtämään eduskunnan kanslian virallisen ja epävirallisen toiminnan suhdetta ja päätöksentekoprosesseja. Virallisen tiedon lisäksi saatavillani on edellä mainituista syistä ollut myös eduskunnan kansliassa vuosikymmeniä työskennelleiden virkamiesten kautta saatua niin kutsuttua hiljaista tietoa.

Opinnäytetyönä suoritettavan kehittämistyön aiheen muotoutuminen alkoi turvallisuusosaamisen koulutusohjelmaan kuuluvien tutkimusessoiden ja kehittämistöiden myötä. Kurssitehtävien kirjoittamisen yhteydessä alkoi myös aineistonkeruu eduskunnan kanslian henkilöstöä ja johtoa haastatteleamalla. Kurssitehtävien aihevalinnat ohjautuivat pitkälti opinnäytetyön tiedontarpeiden perusteella.

2 Teoreettinen tausta

Opinnäytetyön teoreettinen viitekehys käsittelee riskienhallintaa ja sen suhdetta strategiseen johtamiseen, organisaatioturvallisuuteen ja kriisiviestintään. Teoriatietoa hyödynnetään opinnäytetyössä eduskunnan kanslian turvallisuustoiminnan nykytilan kartoittamisessa, sen tavoitetilaa määriteltäessä sekä toimenpidesuosituksia laadittaessa ja perusteltaessa. Toisaalta teoriaosion on tarkoitus myös sellaisenaan palvella eduskunnan kanslian johtoa jäsentämällä ja arvioimalla riskienhallinnan käytänteitä.

2.1 Keskeiset käsitteet

Valtionhallinto koostuu Suomessa keskushallinnosta ja aluehallinnosta. Suomen eduskunta kuuluu virallisesti valtion ylimpiin toimielimiin, mutta tässä kehittämistyössä käytetään valtionhallinnon käsitettä eduskunnan kanslian organisatorisena yläkäsitteenä vaihteluvälillä yksityinen sektori–julkisen sektori. Valtionhallinto kuvaa tutkijan mielestä paremmin eduskunnan kansliaa kuin vaihtoehtoiset termit julkinen sektori tai julkishallinto.

Eduskunnan kanslia tarkoittaa eduskunnan ei-poliittista osaa. Se koostuu virkamiehistöstä, jonka tehtävänä on huolehtia eduskunnan poliittisen osan tekemän lainsäädäntötyön sujuvuudesta ja eduskunnan hallinnosta. Kansliaa johtaa eduskunnan pääsihteeri yhdessä kanslian virkamiesjohtajista koostuvan johtoryhmän kanssa. Eduskunnan kansliaa koskevat suuremmat päätökset on kuitenkin hyväksyttävä eduskunnan poliittista puolta edustavassa kansliatoimikunnassa. Poliittisen ja ei-poliittisen osan välisiä suhteita ja valtarakenteita käsitellään syvällisesti Hertta Niemen väitöskirjassa ”Managing in the ‘Golden Cage’”. Eduskunnan kansliaan on vaikea viitata yleisillä termeillä, sillä se ei suoranaisesti sovi valtionhallinnon organisaatioksi erityisluontoisten tehtäviensä ja niistä syntyvän ainutlaatuisen asemansa vuoksi. Kokonaisvaltaisesta palvelurakenteesta huolimatta termit virasto tai laitos tuntuvat nekin epäsopiivilta, vaikkakin Niemen väitöskirjassa kanslia luokitellaan julkiseksi instituutioksi (Niemi 2010, 199).

Riski tarkoittaa tässä opinnäytetyössä sellaista tapahtumaa tai ilmiötä, jolla on toteutuessaan negatiivinen vaikutus eduskunnan kanslian toimintaan. Riskin merkittävyteen vaikuttavat yhtäältä riskin toteutumisesta seuraavat vaikutukset ja toisaalta riskin toteutumisen todennäköisyys. Opinnäytetyössä korostuvat organisaatioturvallisuuden näkökulman vuoksi strategiset, operatiiviset ja vahinkoriskit. Taloudelliset riskit jäävät vähemmälle huomiolle (Taulukko 1).

Strategiset riskit	Operatiiviset riskit	Vahinkoriskit	Taloudelliset riskit
<ul style="list-style-type: none"> • toiminnan kehitykseen liittyvät riskit • toimintaympäristöön liittyvät riskit • teknologiariskit • poliittisen, taloudellisen ja kulttuuriseen kehityksen riskit • globaaleista ilmiöistä johtuvat riskit • viestintäriskit 	<ul style="list-style-type: none"> • organisaatioon ja johtamiseen liittyvät riskit • informaatioteknologiaan liittyvät riskit • tietoturvallisuusriskit • toimintaprosesseihin ja tehokkuuteen liittyvät riskit • toiminnan keskeytysriskit • kriisitilanteisiin liittyvät riskit • rikosriskit 	<ul style="list-style-type: none"> • työterveysriskit • työturvallisuusriskit • henkilöstöriskit • ympäristöriskit • vahingoittumisriskit • luonnonkatastrofeihin liittyvät riskit • toimitilaturvallisuuden riskit 	<ul style="list-style-type: none"> • likviditeettiriskit • korkoriskit • valuuttariskit • vastapuoliriskit • maariskit • sopimusriskit • veroriskit • kirjanpidon ja talousraportoinnin riskit • pääomarakenteen riskit

Taulukko 1: Riskilajit Ilmonen, Kallio, Koskinen & Rajamäki mukaillen (2010, 71)

Riskienhallinta tarkoittaa riskien tunnistamista ja arvioimista sekä riskeihin liittyvien päätösten tekemistä ja näiden päätösten toimeenpanoa (Juvonen, Korhonen, Ojala, Salonen & Vuori 2005, 18). Riskienhallintaprosessin avulla voidaan torjua organisaatioita uhkaavia vaaroja ja toisaalta myös minimoida niiden mahdollisesta toteutumisesta aiheutuvia menetyksiä riskien kokonaiskustannukset optimoiden (Juvonen ym. 2005, 20; Suominen 2003, 27).

Riskienhallintaa lähestytään tässä opinnäytetyössä defensiivisesti: oman toiminnan suojausta korostaen. Kokonaisvaltainen riskienhallinta-ajatus, joka painottaa riskien sisältämän liike-toiminnallisen mahdollisuuden hyödyntämistä, jää tässä työssä sen sijaan vähemmälle huomiolle eduskunnan toiminnan tavoitteiden vuoksi, pois lukien toiminnan tehostumisen mukanaan tuomat, organisaation sisäiset mahdollisuudet.

Tässä kehittämistyössä riskienhallintaa tarkastellaan organisaatioturvallisuuden näkökulmasta. Riskienhallinnan aloittamiseksi ehdotetut toimenpiteet liittyvät näin ollen organisaatioturvallisuuden eri osa-alueisiin, jotka tosin voidaan jakaa myös eri riskilajeihin (Taulukko 2).

Strategiset riskit	Operatiiviset riskit	Vahinkoriskit
<ul style="list-style-type: none"> • henkilöturvallisuus • valmiussuunnittelu • tietoturvallisuus • pelastustoiminta • (kriisiviestintä) • (turvallisuusjohtaminen) 	<ul style="list-style-type: none"> • tietoturvallisuus • valmiussuunnittelu • pelastustoiminta • ulkomaantoimintojen turvallisuus • rikosturvallisuus • tuotannon ja toiminnan turvallisuus 	<ul style="list-style-type: none"> • henkilöturvallisuus • työturvallisuus • kiinteistö- ja toimitilaturvallisuus • ympäristöturvallisuus • pelastustoiminta • ulkomaantoimintojen turvallisuus

Taulukko 2: Organisaatioturvallisuuden osa-alueet eri riskilajeihin jaoteltuna

Kehittämistyössä käytettävät riskienhallintaan liittyvät käsitteet määritellään seuraavasti

- riski termi tarkoittaa ei-toivotun, organisaatioturvallisuuden eri osa-alueisiin kuuluvan tapahtuman toteutumisen mahdollisuutta
- riskienhallinta tarkoittaa riskien tunnistamista ja arvioimista sekä riskeihin liittyvien päätösten tekemistä ja tehtyjen päätösten järjestelmällistä toimeenpanoa (Juvonen, Korhonen, Ojala, Salonen & Vuori 2005, 18)
- riskienhallinta nähdään organisaation strategista johtamista tukevana elementtinä ja organisaatioturvallisuuden kaikki osa-alueet kattavana (mukaan lukien turvallisuusjohtaminen) toimintana.

Organisaatioturvallisuus käsitteenä vastaa sisällöllisesti yritysturvallisuutta. Termin organisaatioturvallisuus käyttö perustellaan tässä kehittämistyössä valtionhallinnon näkökulman vuoksi kuitenkin yritysturvallisuus -termiä tarkoituksenmukaisempaan, sillä se sallii paremmin julkisen sektorin turvallisuustoiminnan osittain yksityisestä sektorista poikkeavia painotuksia. Lisäksi termin yritysturvallisuus käyttäminen eduskunnan kansliaa käsittelevässä kehittämistyössä tuntuu lähtökohtaisesti ristiriitaiselta. Organisaatioturvallisuus määritellään tässä kehittämistyössä siitä huolimatta Yritysturvallisuus EK:n (2009) käyttämän jaon mukaisesti (Kuvio 6). Organisaatioturvallisuuden eri osa-alueiden sisältö on avattu liitteessä yksi.

Turvallisuusympäristö tarkoittaa toimintaympäristön ilmiöitä, joilla on kohdeorganisaation turvallisuuden kannalta merkitystä joko jo olemassa olevan uhkan tai uhkan mahdollisuuden muodossa. Turvallisuusympäristöä tarkasteltaessa otetaan huomioon yhteiskunnan kaikki tasot, toimijat ja tapahtumat. Esimerkkejä tämän kehittämistyön kohdeorganisaation kannalta merkittävistä turvallisuusympäristön ilmiöistä ovat

- väestörakenteen muutokset, syrjäytyminen
- teknologiariippuvuuden lisääntyminen, energihuollon ja -varmuuden muutokset
- valtaetäisyyden muuttuminen, yksilötason vaikuttamismahdollisuuksien lisääntyminen

- poliittisen järjestelmän kriisi (kansalaisten luottamus), sisäpoliittisten erimielisyyksien purkautuminen väkivallantekoihin
- kansainvälinen terrorismin lisääntyminen, asymmetrinen sodankäynti
- epidemiat ja pandemiat.

Riskitietoisuus voidaan määritellä kyvyksi tunnistaa ja tiedostaa riskit ja uhkat, jotka syntyvät ja kohdistuvat henkilöön, yhteisöön, toimintaan, olosuhteisiin tai asemaan. Yksilötason riskitietoisuus on edellytys organisaation riskienhallintatoiminnan kestäväälle toteuttamiselle sekä turvallisuuskulttuurin syntymiselle. Hopkinin mukaan riskitietoinen organisaatiokulttuuri edellyttää, että henkilökunta tunnustaa ja hyväksyy riskienhallintatoiminnan tärkeyden. Lisäksi organisaatiojohdon ja työntekijöiden on ymmärrettävä oma roolinsa riskienhallinnassa ja myös sitouduttava toimimaan sen edellyttämällä tavalla. (2010, 298.) Riskitietoisuus kehittyy koulutuksen, tiedotuksen, mutta myös kokemusten myötä. Riskitietoisuus koskee kaikkea toimintaa, joka sisältää päätöksentekoa. Riskitietoisuuden merkitys korostuu monimutkaisissa ja eriasteisista riippuvuussuhteista rakentuissa toimintaympäristöissä.

2.2 Riskienhallinta strategisen johtamisen tukena valtionhallinnossa

Kehittämistyö ei suoranaisesti kohdistu eduskunnan kanslian strategiseen johtamiseen. Organisaatioturvallisuus ja riskienhallinta ovat kuitenkin strategisen tason kysymyksiä ja siten organisaation ylimmän johdon vastuulla. Vastuunkantamisen lisäksi riskienhallinnan onnistunut toteutus vaatii ylimmältä johdolta sitoutumista ja osallistumista.

Analysit muodostavat strategisen johtamisen kivijalan, sillä ne luovat perusteet toiminnan johtamiselle ja kehittämiselle, syventävät ulkoisen ja sisäisen toimintaympäristön tuntemusta, kehittävät henkilöstön analysointitaitoja ja luovat edellytykset organisaation yhteisen näkemyksen syntymiselle (Kamensky 2000, 102). Riskienhallintaan liittyvät analysit ja riskiraportointi tuovat läpinäkyvyyttä, auttavat tunnistamaan, analysoimaan ja arvioimaan organisaation rajapintoihin liittyviä ongelmia sekä kehittämään niihin ratkaisuja. Johdon näkökulmasta riskienhallinnan painoarvo riippuu sen systemaattisuudesta ja liittymäpinnasta strategiseen suunnitteluun (Ilmonen ym. 2010, 19; Suominen 2003, 28). Käytännössä siis riskienhallinnan sisällyttäminen strategiatyön kaikkiin vaiheisiin on välttämätöntä, jotta sen avulla saatava tieto vastaa strategisen johtamisen kannalta oleellisiin kysymyksiin.

Riskienhallinta tukee strategian toteutusta myös siltä osin, että strategiatyöhön liittyvässä riskianalysissä tulisi pohtia myös strategian itsensä mahdollisia heikkouksia (Kamensky 2000, 268). Kun organisaation strategia- ja vuosisuunnitteluprosessiin on sisällytetty kattava ja kokonaisvaltainen riskienhallintaprosessi, ovat strategian ja suunnitelmien täytäntöön panemi-

sen lähtökohdat sekä tavoitteiden saavuttamisen mahdollisuudet hyvät (Ilmonen ym. 2010, 194).

Seuraavissa osaluvuissa käydään läpi strategisen johtamisen, organisaatioturvallisuuden ja riskienhallinnan teoriaa valtionhallinnon näkökulmasta. Strategista johtamista käsitellään siksi, että se auttaa hahmottamaan riskienhallintaan liittyviä organisaatiotason tavoitteita ja edelleen näiden tavoitteiden yhteyttä organisaation johtamiseen. Myös organisaatioturvallisuuden ja riskienhallinnan keskinäistä suhdetta on syytä käsitellä yhtäältä synergiaetujen huomioimiseksi ja toisaalta tarpeettomien vastakkainasetteluiden välttämiseksi.

2.2.1 Strategisen johtamisen merkitys organisaation toiminnalle

Strategiakäsitteestä on olemassa erilaisista näkökulmista käsin laadittuja määritelmiä. Mika Kamenskyn (2008) kolmijakoinen määritelmä sopii erinomaisesti kuvaamaan kaikenlaisten organisaatioiden strategiaa. Kamenskyn mukaan

- strategia on organisaation tietoinen keskeisten tavoitteiden ja toiminnan suuntaviivojen valinta muuttuvassa maailmassa
- strategian avulla organisaatio hallitsee ympäristöä
- strategian avulla organisaatio hallitsee tietoisesti ulkoisia ja sisäisiä tekijöitä sekä niiden välisiä vuorovaikutussuhteita siten, että organisaatiolle asetetut kannattavuus-, jatkuvuus- ja kehittämistavoitteet pystytään saavuttamaan (2008,19).

Kilpailutilanteessa toimivalle organisaatiolle strategia on olemassaolon ehto, joka mahdollistaa kyvyn erottautua kilpailijoista. Kilpailun puuttuminen muuttaa kyllä organisaation strategian luonnetta, mutta ei suinkaan tee strategiatyöskentelystä tarpeetonta. Strategialla varmistetaan tällöin huomion kohdistaminen oikeisiin tarpeisiin ja asiakkaisiin, muutostarpeiden havaitseminen ja resurssien oikea kohdentaminen. (Kamensky 2008, 17–18.)

Strategisia suuntauksia on useita erilaisia. Viimeaikoina on korostettu erityisesti strategista ketteryyttä (strategic agility), jolla viitataan organisaation joustavuuteen sekä kykyyn ja haluun reagoida muuttuvaan toimintaympäristöön. Kamenskyn (2008, 21–22) mukaan organisaatioiden muutosherkyys kuitenkin vaihtelee suuresti. Kamenskyn viitaten organisaation reagoititapaa voidaan tarkastella muutoksen havainnoinnin, muutoksen merkityksen ymmärtämisen ja muutoksen ymmärrystä seuraavan toiminnan perusteella. Pahimmillaan muutos on tapahtunut ja organisaatiokin huomannut muutoksen ymmärtäen sen vaikutukset osaamatta tai haluamatta kuitenkaan kehittyä. Parhaimmillaan organisaatio havaitsee omaan toimintaansa kohdistuvat muutospainet ennakkoon ja kykenee näin ollen kääntämään mahdollisuudet tai mahdolliset uhat omaksi edukseen. (Kamensky 2008, 21–22.)

Strategiaprosessin päävaiheet ovat tietojen keruun ja analysoinnin vaihe, strategian määrittelyvaihe, strategisten projektien suunnitteluvaihe, strategian toteuttamisvaihe sekä seurannan, arvioinnin ja päivityksen vaihe (Ojasalo 2010). Strategisessa työssä joudutaan tekemään valintoja useiden hyvien vaihtoehtojen välillä. Johdon tehtävä onkin priorisoida niistä organisaatiolle parhaiten sopivat. (Doz & Kosonen 2008, 72–77.) Lecklinin mukaan strategiset valinnat saattavat sisältää tilanteita, joissa organisaatio joutuu valitsemaan laadun ja kustannustehokkuuden välillä. Pitkällä tähtäimellä laatu ja tehokkuus kuitenkin tukevat toisiaan, joten menestyvä organisaatio panostaa laatuun. (Lecklin 2002, 50–51.)

Vaikka strategia pohjautuu organisaation ylimmän johdon yhteiseen tahtotilaan, koskettaa se muitakin organisaatiotasoja toimiessaan ohjeena asetettujen tavoitteiden saavuttamiseksi. Tämän vuoksi on tärkeää myös, että päätöksentekoprosessiin osallistuu henkilöitä organisaation kaikilta johtamistasoilta, jotta eri osastojen vahvuudet ja näkökulmat voidaan ottaa huomioon kokonaisratkaisua haettaessa (Kamensky 2000, 17; Doz & Kosonen 2008, 80–82). Strategiseen suunnitteluun osallistuminen lisää myös henkilöstön sitoutumista suunnitelmien toteuttamiseen. (Lecklin 2002, 50).

2.2.2 Strategiatyön tarve valtionhallinnon organisaatioissa

Valtionhallinnon organisaatioiden tehtävät ja toimintaperiaatteet poikkeavat toisistaan ja siksi myös niiden strategioissa on eroja. Strategiatyön yhtenä tarkoituksena on määrittää arvot, joiden mukaan organisaation toimintaa ohjataan.

Valtionhallinnon organisaatioiden huomio kohdistunee toiminnan sisäiseen suorituskykyyn, sillä ne eivät kohtaa ulkoisia kilpailukykyyn liittyviä haasteita yksityisen sektorin organisaatioiden mittakaavassa. Toisaalta myös valtionhallinnon organisaatioiden toiminta on muuttunut enemmän yksityistä sektoria muistuttavaksi esimerkiksi johtamisen suhteen ja siltä osin myös sidosryhmien tarpeiden huomioiminen on noussut aikaisempaa merkittävämpään rooliin toiminnan kehittämisessä. Hallinnollisen ajattelun uudistumisen (New Public Management) myötä 1990-luvulla valtionhallinnossa otettiin käyttöön tulosohejaus ja tulosjohtaminen. Samalla myös riskienhallinnan merkitys valtionhallinnon toiminnassa ja johtamisessa korostui (Herrain-silta 2006, 39).

Valtioneuvoston mukaan valtionhallinnon arvoperustan muodostavat toiminnan tuloksellisuus, luottamus, tasa-arvo, puolueettomuus, riippumattomuus, vastuullisuus, palveluperiaate, avoimuus sekä laatu ja vahva asiantuntemus (Valtioneuvosto 2001, 3–4). Tähän arvoperustaan sisältyvät luottamuksen, tasa-arvon, puolueettomuuden ja riippumattomuuden tulisi olla korostuneita arvoja valtionhallinnon organisaatioissa, joiden toiminnan perusta on kansalaisten luottamus ja toiminnan legitimitetti.

Yhteiskunnallinen vaikuttavuus ja toiminnallinen tuloksellisuus ovat peruskriteerit, joita valti-onhallinnossa käytetään tulostavoitteiden asettamisessa ja tuloksellisuutta koskevassa rapor-toinnissa. Valtionhallinnon organisaatioiden oma panos on tärkeää erityisesti toiminnallisten tulostavoitteiden saavuttamisen osalta perustanaan tehokkuus ja laadun ja henkisten voima-varojen hallinta. (Valtiovarainministeriö 2005a, 24). Valtion- ja julkishallinnon organisaatioi-den on lisäksi lunastettava olemassaolon oikeutuksensa palvelukyvyllään ja puoleensavetä-vyydellään (Santalainen & Huttunen 1993, 31). Lisäksi valtioneuvosto pitää tärkeänä, että val-tio on esimerkillinen työnantaja. Valtion henkilöstöpolitiikan mukaan tuloksellisuudelle ja palvelukyvyille luodaan edellytykset muun muassa hyvällä työnantaja- ja henkilöstöpolitiikalla sekä hyvällä johtamisella. (Valtioneuvosto 2001, 3–4.)

Aktiivinen strategiatyö ei vielä kovin pitkään ole ollut osa julkisten organisaatioiden tai valti-onhallinnon organisaatioiden toiminnanohjausta. Santalainen ja Huttunen (1993, 48) ehdotta-vat julkisten organisaatioiden kehittämistarpeiden kartoittamista seuraavista näkökulmista

- onko johtamisen kriittisin kehitystarve suunnitelmien laatimisessa vai toteutusvoiman lisäämisessä?
- syntykö johdon lisäarvo järjestelmiä vai ajattelua ja substanssia kehittämällä?
- löytykö toiminnan optimaalinen lopputulos asiakkaiden tarpeita tutkimalla vai ra-kentamalla tulevaisuutta oman ydinosaamisen varaan?
- onko tarvetta uudelle käsitteistölle vai pitääkö keskittyä nykykäsitteistön selkeyden ja keskinäisten suhteidenvarmistamiseen?

Organisaatioturvallisuus ja strateginen johtaminen liittyvät oleellisesti toisiinsa. Organisaation toimintaa ohjaavat strategiatyössä määritetyt arvot, joita turvallisuustoiminnalla puolestaan pyritään suojaamaan. Suojattavat arvot sen sijaan - ihmiset, omaisuus, tieto, toiminta, maine ja ympäristö - ovat organisaatiosta riippumatta samat, niiden suojauksen painotus vain vaihtelee toimialakohtaisesti. Tärkeimmät suojattavat arvot ovat kuitenkin aina ihmisten terveys ja turvallisuus. Turvallisuustoiminta mahdollistaa onnistuessaan organisaation johdon uhkista ja riskeistä tietoisien päätöksenteon. (Kerko 2001, 21; Mäkinen 2007, 155; Yritysturvallisuus EK 2009.) Nämä reunaehdot eivät muutu, oli tarkastelun kohteena sitten julkisen tai yksityisen sektorin organisaatio.

Myös riskienhallintaan liittyviä päätöksiä tulee organisaatiosta riippumatta tarkastella strate-gisina kysymyksinä. Riskienhallinta tuottaa tietoa, jota johto tarvitsee päätöksenteon tueksi sekä toimenpiteiden priorisoimiseksi ja läpiviemiseksi (Juvonen ym. 2005, 19; Kuusela & Olli-kainen 2005, 136, 158). Riskienhallinta pohjautuu aina organisaation visioon, arvoihin ja stra-tegiaan, jolloin sen tuottama tieto ei rajoitu tukemaan ainoastaan riskinottoon tai riskien välttämiseen liittyvää päätöksentekoa. Kokonaisvaltainen riskienhallinta helpottaa kohdista-

maan toiminnan painopisteet yhtenäisesti laaditun strategian mukaisiksi osoittamalla organisaation kehityskohteet. (Ilmonen ym. 2010, 21; Lanne 2007, 31).

Laatu on Santalaisen ja Huttusen mukaan keskeisessä asemassa myös valtionhallinnon strategiatyön kehittämisessä. Virastot joutuvat kehittämään tuottavuuttaan ja toiminnan laatua soveltamalla uusia toimintatapoja. Pitkän aikavälin elinvoimaisuuteen liittyville pohdinnoille tulisi olla avoin, vaikka makrotason strategisten haasteiden kanssa on samanaikaisesti ratkaistava tulosityksikkökohtaisia ongelmia. (1993, 46–47.)

Strateginen johtaminen on tärkeää julkisen sektorin organisaatioissa ja sen laatuun liittyvät vaatimukset tulevat lisääntymään tulevaisuudessa. Riskienhallinta-ajattelu korostuu vuosi vuodelta maailmalla ja suomalaisessa yhteiskunnassa, ei vähiten yleisen turvattomuudentunteen lisääntymisen vuoksi. Riskienhallinnalla on suuri merkitys organisaation strategisen johtamisen tukijana. Kehittämistyö kannattaa käynnistää nyt, kun arki ja teoria tarjoavat erinomaisia perusteluja sen tarpeellisuudelle ilman, että vielä olisi liian myöhäistä aloittaa.

2.3 Riskienhallinta

Riskienhallinta on tukiprosessi, joka tukee strategia- ja vuosisuunnittelun pääprosessia. Riskienhallinnan kytkeminen ajallisesti ja prosessuaalisesti organisaation suunnitteluprosessiin on tärkeää. Riskien tunnistamisen paras ajankohta on silloin, kun strategiset tai vuositavoitteet on jo luonnosteltu, koska riskit arvioidaan niiden pohjalta. Riskienhallintaprosessia ei kuitenkaan kannata jättää niin myöhäiseen vaiheeseen strategia- tai vuosisuunnitteluprosessia, ettei siinä tehtyjä havaintoja ehditä ottaa huomioon lopullisia strategiavaihtoehtoja valittaessa. (Ilmonen ym. 2010, 80.)

Riskienhallintaprosessi voidaan jakaa toisiaan seuraaviin vaiheisiin

- riskien tunnistaminen
- riskien arvottaminen (toteutumistodennäköisyys ja vaikutukset)
- merkittävimpien riskien hallintakeinoista päättäminen
- riskienhallintakeinojen resursointi
- poikkeustilanteiden hallinnan suunnittelu ja toiminnan jatkuvuuden suunnittelu
- raportointi ja valvonta
- riskienhallintajärjestelmän arviointi (Hopkin 2010, 39).

Moderni riskienhallinta kattaa organisaation kaikki riskit (Taulukko 3), vaikka riskienhallinnan juuret ovatkin pääasiassa vahinkoriskien hallinnassa. Riskienhallinta, toiminnan laatu ja toimintavarmuus ovat osittain päällekkäisiä ja tukevat toisiaan. (Hopkin 2010; Suominen 2003, 27, 153.)

Strategiset riskit	Operatiiviset riskit	Vahinkoriskit	Taloudelliset riskit
<ul style="list-style-type: none"> • toiminnan kehitykseen liittyvät riskit • toimintaympäristöön liittyvät riskit • teknologiariskit • poliittisen, taloudellisen ja kulttuuriseen kehityksen riskit • globaaleista ilmiöistä johtuvat riskit • viestintäriskit 	<ul style="list-style-type: none"> • organisaatioon ja johtamiseen liittyvät riskit • informaatioteknologiaan liittyvät riskit • tietoturvallisuusriskit • toimintaprosesseihin ja tehokkuuteen liittyvät riskit • toiminnan keskeytysriskit • kriisitilanteisiin liittyvät riskit • rikosriskit 	<ul style="list-style-type: none"> • työterveysriskit • työturvallisuusriskit • henkilöstöriskit • ympäristöriskit • vahingoittumisriskit • luonnonkatastrofeihin liittyvät riskit • toimitilaturvallisuuden riskit 	<ul style="list-style-type: none"> • likviditeettiriskit • korkoriskit • valuuttariskit • vastapuoliriskit • maariskit • sopimusriskit • veroriskit • kirjanpidon ja talousraportoinnin riskit • pääomarakenteen riskit

Taulukko 3: Riskienhallinta kattaa organisaation kaikki riskit (Ilmonen ym. 2010, 71)

Yksityisellä sektorilla organisaation toimiala vaikuttaa riskien erilaiseen painottumiseen. Valtionhallinnossa tähän painottumiseen vaikuttaa pääasiassa organisaation tehtävä. Valtionhallinnon näkökulmasta katsottuna riskienhallinta ei yleisellä tasolla kuitenkaan eroa merkittävästi yksityisen sektorin suhteen: valtionhallinnossakin sillä tarkoitetaan organisaation ja sen toimintayksikköjen riskien ja niiden todennäköisyyksien järjestelmällistä tunnistamista, arviointia ja hallintaa. (Herrainsilta 2006, 42–43, 76; Valtiovarainministeriö 2005b, 8–11.)

Riskienhallintatyöskentelyn käytännön toteutus on syytä suunnitella huolella toimialasta ja sektorista riippumatta. Työtä käynnistettäessä vastataan ainakin kysymyksiin mitä (tavoite), miksi (motiivit), miten (toiminta ja keinot), millä eväin (resurssit), milloin (aikataulu) ja ketkä (osallistujat). (Juvonen ym. 2005, 23).

2.3.1 Riskienhallinnan tavoitteet

Asiantuntevasti toteutettu riskienhallinta tuottaa hyötyä organisaatiolle organisaation sektorista, toimialasta, koosta tai iästä riippumatta. Riskienhallintaa käsittelevässä teoksessaan Paul Hopkin (2010) toteaa näitä hyötyjä olevan muun muassa

- organisaation toiminnan vaatimustenmukaisuus (compliance)
- vakuus riskien tunnistamisesta ja niiden hallinnasta organisaatiojohdolle (board assurance)
- päätöksentekoa tukevan tiedon tuottaminen (decisions)
- toimintaprosessien vaikuttavuus (effective processes)
- operatiivisten toimintojen tehokkuus (efficient operations)

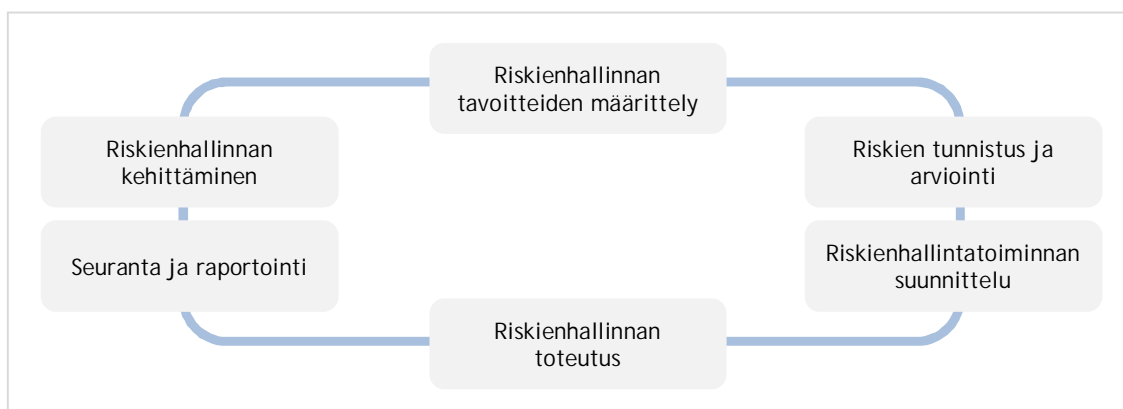
- valittujen toimintastrategioiden tarkoituksenmukaisuus (efficacious strategy).

Riskienhallinnan päätavoitteeksi voidaan myös määritellä toiminnan jatkuvuuden varmistaminen kaikissa olosuhteissa riskikustannukset optimoiden ja organisaation toimintamahdollisuuksien hyödyntäminen (Juvonen, Korhonen, Ojala, Salonen & Vuori 2005, 20). Riskienhallinnalla on lisäksi tärkeä rooli organisaation päätöksenteon tukijana sikäli, että hyvin hoidettu riskienhallinta parantaa organisaation kykyä kohdata uusia ja ennen kaikkea tuntemattomia riskejä (Ilmonen ym. 2010, 12; Kuusela & Ollikainen 2005, 158).

Kokonaisvaltaisen riskienhallinnan ideologia ei rajoitu negatiivisilta riskeiltä suojaavaan lähestymistapaan vaan se sisältää lisäksi liiketoiminnan mahdollisuuksien hyödyntämisen (Ilmonen, Kallio, Koskinen & Rajamäki 2010, 17; Lanne 2007, 31; Mäkinen 2007, 155). Mahdollisuuksia on riskilajeista selvästi eniten strategisten riskien alueella, kun taas vahinkoriskeissä niitä ei ole koskaan. Operatiivisissakin riskeissä mahdollisuudet liittyvät usein kannattavuuden parantamiseen, eli käytännössä säästöihin ja toiminnan tehostamiseen. (Ilmonen ym. 2010, 18.)

Riskienhallinnan voidaan katsoa olevan myös käytettyjen resurssien, pääomien ja kustannusten optimoimista suhteessa tavoiteltaviin hyötyihin (Ilmonen ym. 2010, 19). Elinkenoelämän keskusliiton (2006) mukaan riskienhallinnan tehtävänä on arvioida ja hallinnoida organisaation toiminnassa esiintyviä mahdollisuuksia, uhkia ja riskejä asetettujen tavoitteiden saavuttamiseksi ja toiminnan jatkuvuuden varmistamiseksi. Riskien ja liiketoimintamahdollisuuksien tunnistamiseen ja arviointiin onkin mahdollista käyttää samoja työkaluja, sillä molempien todennäköisyyttä voidaan arvioida kutakuinkin samanlaisella asteikolla (Ilmonen ym. 2010, 18).

Riskienhallintaprosessin (Kuvio 2) vaiheet tuottavat toimintaan organisaatioturvallisuuttakin painottaessaan järjestelmällisyyttä, säännöllisyyttä, aktiivista arviointia, johdon informointia ja henkilöstön osallistamista.



Kuvio 2: Riskienhallintaprosessi Ilmonen ym. mukailten (2010, 93)

Riskienhallinnassa yhdistyvät turvallisuusajattelu ja liiketoiminnan näkökulmat. Riski määritellään uhkan tai mahdollisuuden toteutumisen todennäköisyyden ja seurannaisvaikutuksen mukaan. Riskien arviointi ja riskikartoitukset toimivat pohjana organisaation kaikille suojaustoimenpiteille ja turvallisuustoiminnalle. (Yritysturvallisuus EK 2009.) Systemaattisesti hoide-
 tun riskienhallinnan turvin organisaatiolla on paremmat lähtökohdat kohdata paitsi tavanomaisia niin erityisesti myös uusia ja tuntemattomia riskejä (Kuusela & Ollikainen 2005, 158).

Riskienhallinnan ansiosta organisaation johto voi tehdä merkittävät päätöksensä riskikuvasta tietoisena. Tämä tietenkin edellyttää riskikuvan säännöllistä päivittämistä sekä johdolta ymmärrystä organisaation riskinkantokyvystä. Kiinnostuksen kohteena eivät päätöksentekotilanteissa niinkään ole yksittäiset riskit vaan merkittävimpien riskien muodostama kokonaisuus. (Ilmonen ym. 2010, 12.) Herrainsillan (2006, 80) referoiman tutkimuksen mukaan suomalais-
 ten suuryritysten johtajien mielestä kokonaisvaltaisen riskienhallinnan etuja ovatkin juuri epävarmuuden parempi hallinta, tappioiden minimointi, organisaation tavoitteiden saavuttaminen, maineen ylläpitäminen ja prosessien tehostaminen.

Toteutuneet riskit muuttavat yleensä asenteita ja nopeuttavat päätöksentekoa. Riskienhallintaprosessi ei kuitenkaan itsessään toimi organisaation suojana vaan riskiltä suojautumisen onnistumiseksi on tehtävä mahdollisimman oikeaan osuvia päätöksiä. On lisäksi muistettava, että paraskaan suojauspäätös ei auta organisaatiota, jota vahinko on jo kohdannut. (Suomi-
 nen 2003, 147–148.)

2.3.2 Riskienhallinnan johtaminen ja asiakirjat

Vastuun riskienhallinnasta tulee olla tarpeeksi ylhäällä organisaatiossa ja riskienhallinnan kehittämistä vastaavalla henkilöllä pitäisi olla asiantuntemusta ja tarpeeksi valtaa viedä kehittämiseen liittyviä asioita eteenpäin organisaatiossa (Kuusela & Ollikainen 2005, 129).

Riskienhallinnasta vastaavat toimitusjohtaja ja hallitus. Hallituksen on varmistettava, että organisaatiolla on tarkoituksenmukainen ja toimiva prosessi riskien tunnistamiseksi. Hallitus määrittelee organisaation riskinottohalun, vastaa riskienhallinnan tulosten ja toimenpiteiden seurannasta sekä riskienhallintaprosessien toimivuuden arvioinnista. Ylimmän johdon tulee osaltaan edellyttää toimivalta johdolta riskianalyysien tekoa ja riskienhallintaa. (Ilmonen y. 2010, 57; Koivu, Ranta-aho & Vuoti 2010, 95; Kuusela & Ollikainen 2005, 130.)

Riskienhallinnan päätökset ovat organisaation koosta riippumatta strategisia kysymyksiä. Riskienhallinnan johtamiseen liittyy päätösten tekemisen ja niiden toimeenpanon lisäksi toimeenpanon seuranta ja tulosten raportointi. Johdon tulee ottaa kantaa organisaatiolle ominaiset riskit sisältävän riskikartoituksen tekemiseen sekä hallintatoimenpiteiden valintaan ja

niiden riittävyyden arviointiin. Toimiva riskienhallinta edellyttää yritykseltä sekä pitkäaikaista sitoutumista että valmiutta ryhtyä riskienhallintaa edistäviin toimenpiteisiin. (Juvonen ym. 2005, 18–19, 192; Suominen 2003, 32, 97.)

Organisaatiot nimeävät usein itselleen riskienhallintajohtajan, joka raportoi toimitusjohtajalle tai talousjohtajalle. Riskienhallintajohtaja vastaa riskienhallinnan viitekehyksen kehittämisestä ja käyttöönotosta sekä organisaation hallitukselle raportoinnista, parhaassa tapauksessa johdon kuukausiraportointiin yhdistettynä. (Koivu ym. 2010, 95; Kuusela & Ollikainen 2005, 129.) Suurempiin organisaatioihin voidaan lisäksi perustaa riskienhallinnan ohjausryhmä, johon kuuluvat yrityksen ylin johto, operatiivinen johto sekä riskienhallinnasta vastuulliset tahot (Ilmonen ym. 2010, 57).

Linjajohdon on tarpeellista omaksua riskienhallinnan toimintamallit ja vielä niitä edelleen alemmille organisaatiotasoilta, sillä riskienhallinta ei toimi riittävän tehokkaasti, jos se jätetään pelkästään riskienhallinnan ammattilaisten hoidettavaksi. (Ilmonen ym. 2010, 23; Kuusela & Ollikainen 2005, 126–127; Koivu ym. 2010, 95; Suominen 2003, 28). Liiketoimintayksiköiden johto vastaa osaltaan riskienhallinnan toteuttamisen organisoinnista, henkilöstön sitouttamisesta, riskienhallintasuunnitelmien laatimisesta ja riskien seurannasta. Lisäksi yksiköt raportoivat säännöllisesti oman liiketoimintayksikkönsä riskeistä. (Kuusela & Ollikainen 2005, 130).

Riskienhallinnan vastualueiden on oltava selvät koko organisaatiossa. Yksittäisen työntekijän rooli riskienhallinnassa on merkittävä. Henkilöstö toteuttaa käytännön riskienhallintaa yhtäältä noudattamalla annettuja ohjeita ja määräyksiä ja toisaalta puuttumalla havaitsemiinsa epäkohtiin. Lisäksi aktiivinen kommunikointi ja koordinointi eri yksiköiden välillä ovat tärkeitä riskienhallinnan onnistumisen edellytyksiä. (Ilmonen ym. 2010, 58.) Eduskunnan kanslian turvallisuusyksikön toiminta koskee kaikkia yksiköitä ja kansanedustajia. Yksikkönä se on kuitenkin tasavertainen muiden rinnalla, eikä sillä ole varsinaista johtosuhdetta muihin yksiköihin nähden. Riskienhallinta on kuitenkin kaikkien organisaatiotasojen toimintaa ja siihen liittyvistä johtosuhteista olisi linjattava eduskunnan kansliassa laadittavissa riskienhallintaa koskevissa asiakirjoissa. Sisäinen tarkastus täydentää turvallisuusyksikköä ja riskienhallintaa, toimien kuitenkin niistä erillään ja kohdistuen puolueettoman tarkastustoimintansa myös niihin. Riskienhallinnan mahdollista sijoittumista eduskunnan kanslian organisaatiossa on havainnollistettu liitteessä seitsemän.

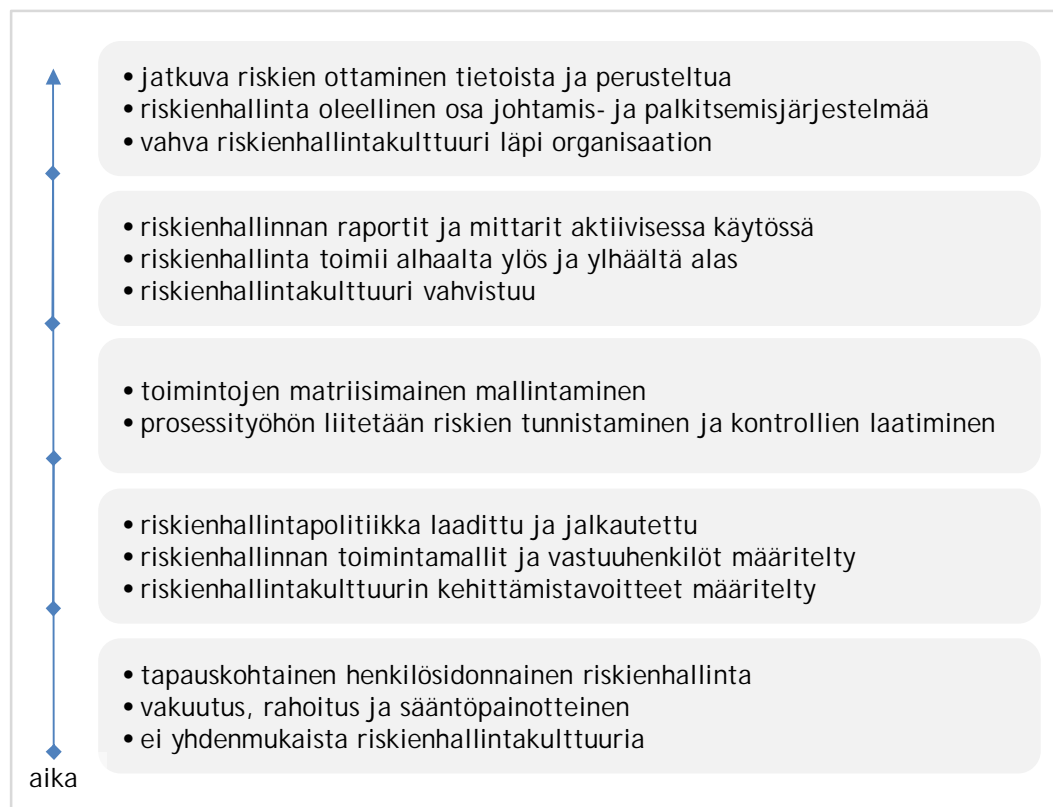
On syytä pohtia riskienhallintatyöskentelyn organisointia ja sitä, keiden tulisi työskentelyyn osallistua. Suositeltavaa on keskittyä yhteen osastoon tai yksikköön kerrallaan, jolloin työskentely on helpompi pitää fokuksituneena ja tehokkaana. Kun kaikkien osastojen ja toimintojen riskit on tunnistettu ja analysoitu ja niiden hallintatoimet on suunniteltu, yhdistetään

nämä riskikuvat organisaation yhteiseksi riskikuvaksi, joka tarjoaa kattavan kuvan koko organisaation merkittävimmistä riskeistä. (Ilmonen ym. 2010, 78–79.)

Tähän liittyy myös riskienhallintatyöskentelyn vaiheistaminen. Riskienhallintatyöhön on perusteltua ottaa mukaan keskeisimmät toimijat ja sellaiset henkilöt, jotka ymmärtävät erinomaisesti organisaation tavoitteet, prosessit, tuotteet, asiakkaat, kilpailijat, henkilöstön kuin työssä tarvittavat järjestelmät ja sovelluksetkin. Aloitus on hyvä tehdä osallistujien perehdyttämällä riskienhallinnan metodologiaan, työkaluihin ja työskentelyvaiheisiin. Osallistujien on hyvä listata omalla vastualueellaan havaitsemiaan organisaation tavoitteiden kannalta keskeisiä riskejä ennen yhteisen riskienhallintatyöskentelyn alkua. Työpajan tulokset on käytävä läpi organisaation ylimmän johdon kanssa, mikäli siihen ovat osallistuneet muut kuin kohdeorganisaation ylimpään johtoon kuuluvat. (Ilmonen ym. 2010, 78–79, 81.)

Organisaation riskienhallintastrategia konkretisoituu siinä, miten tunnettuihin riskienhallintakeinoihin suhtaudutaan ja miten tunnistettujen riskien varalta suojaudutaan. Riskienhallintastrategioiden karkea erottelu perustuu riskienhallinnan asteeseen (korkea–alhainen) sekä riskienhallintastrategian asemaan; se voi olla organisaatiossa joko tarkkaan puntaroitu tai täysin taka-alalla (Suominen 2003, 160).

Ilmosen mukaan riskienhallinnan kehittämistä voidaan kuvata kypsyyssasteittain (Kuvio 3). Riskienhallinnan kehittämisen tavoitteena on, että riskienhallinta integroituu organisaation muihin toimintaprosesseihin. (Ilmonen ym. 2010, 93.) Riskienhallinnan perustaso saavutetaan suojaamalla organisaatio sen keskeisten riskien varalta sekä täyttämällä lakisääteiset ja viranomaisten asettamat vaatimukset (Suominen 2003, 32, 150).



Kuvio 3: Riskienhallinnan kypsyyssasteet Ilmonen ym. mukailleen (2010, 94)

Riskienhallinnan edistämisen saatetaan joskus ajatella kilpailevan ideologisella tasolla muiden organisaation johtamiseen liittyvien tukitoimien kanssa, kuten esimerkiksi henkilöstöhallinto, projektitoimisto tai laatutoimisto. Vastakkainasetteluja voidaan välttää osallistamalla edellä mainittujen osa-alueiden johto riskienhallintaa koskevaan suunnittelutyöhön ja asettamalla tavoitteeksi kaikkia palvelevien toimintamallien löytäminen. (Ilmonen ym. 2010, 81–82.)

Riskienhallinnan ohjeistus ja muu dokumentaatio koostuu riskienhallintapolitiikasta, riskienhallinnan periaatteista ja toimintapolitiikoista (Kuusela & Ollikainen 2005, 128). Organisaation strategiaan saatetaan kirjata riskienhallinnan tavoitteita ja konkreettisemmat riskienhallinnan tavoitteet kirjataan organisaation toimintasuunnitelmiin ja eri politiikkoihin. Riskienhallinnassa ei ole olemassa yhtä ainoa oikeaa toteutustapaa – kunkin organisaation on sovellettava riskienhallintaa itselleen parhaiten soveltuvalla tavalla. (Ilmonen ym. 2010, 22, 67; Hopkin 2010).

Riskienhallintapolitiikka on muutaman sivun pituinen dokumentti, jonka tulisi sisältää ainakin seuraavat asiat

- riskienhallinnan periaatteiden ja tavoitteiden kuvaus
- riskienhallintapolitiikan kattavuus ja riskien määrittely

- riskienhallinnan merkitys eduskunnan kanslian strategisten tavoitteiden suhteen sekä
- riskienhallintaan osallistuvien tahojen roolien ja velvollisuuksien määrittely. (Kuusela & Ollikainen 2005, 128.)

Riskienhallinnan periaatteet tulee kirjata tarkemmin erilliseen dokumenttiin. Sen tulee sisältää ainakin seuraavat asiat

- riskienhallinnan strategiat ja tarkemmat tavoitteet
- riskienhallintaprosessin (riskien tunnistaminen ja arviointi, hallintakeinot, riskien ja riskienhallinnan seuranta ja raportointi) toteutus käytännössä
- merkittävimmät riskialueet
- yksityiskohtaiset organisatoriset vastuut (riskien omistajat seuranta ja raportointi)
- menetelmät, joilla riskienhallinnan onnistumista mitataan
- miten johto varmistuu riskienhallinnan prosessien ja toimenpiteiden tehokkuudesta ja riittävydestä. (Kuusela & Ollikainen 2005, 128.)

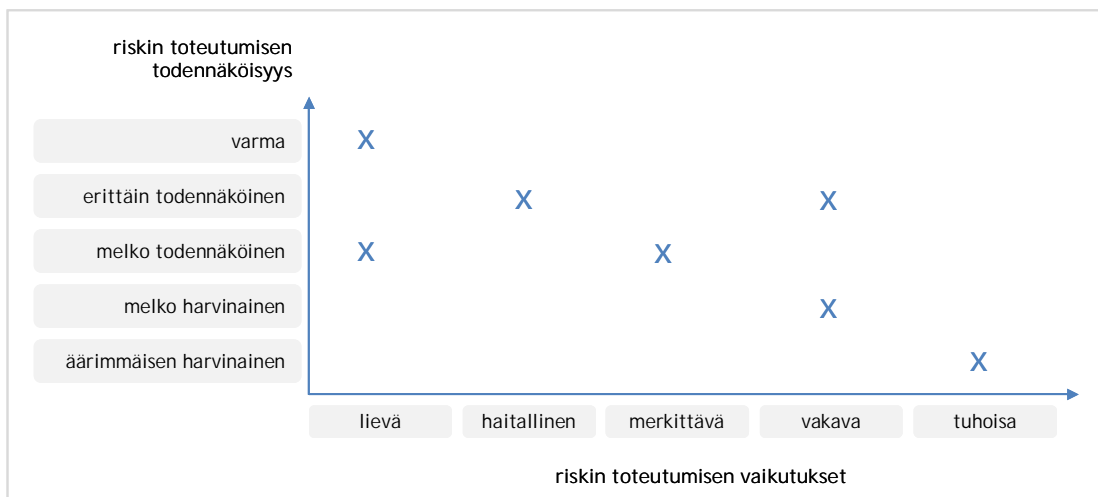
2.3.3 Riskienhallintamenetelmät

Riskienhallinnan ollessa kypsyysslaji (Kuvio 3), kannattaa toiminta aloittaa yksinkertaisella mallilla. Riskienhallintaa laajennetaan ja syvennetään organisaation riskienhallinnallisen osaamisen ja kokemuksen kasvamisen myötä. (Ilmonen ym. 2010, 80.)

Ensimmäiseksi päätetään tavoitteet, joita vasten riskit pyritään tunnistamaan ja analysoidaan. Tällaisia tavoitteita voivat olla esimerkiksi organisaation strategiset ja vuositavoitteet. Niiden saavuttamista uhkaavien riskien fokus on paikallaan, kun organisaatiossa aloitetaan systemaattinen riskienhallintatyö, jonka tarkoitus on yleisesti tukea johtamista ja tavoitteiden saavuttamista. (Ilmonen ym. 2010, 77–78.)

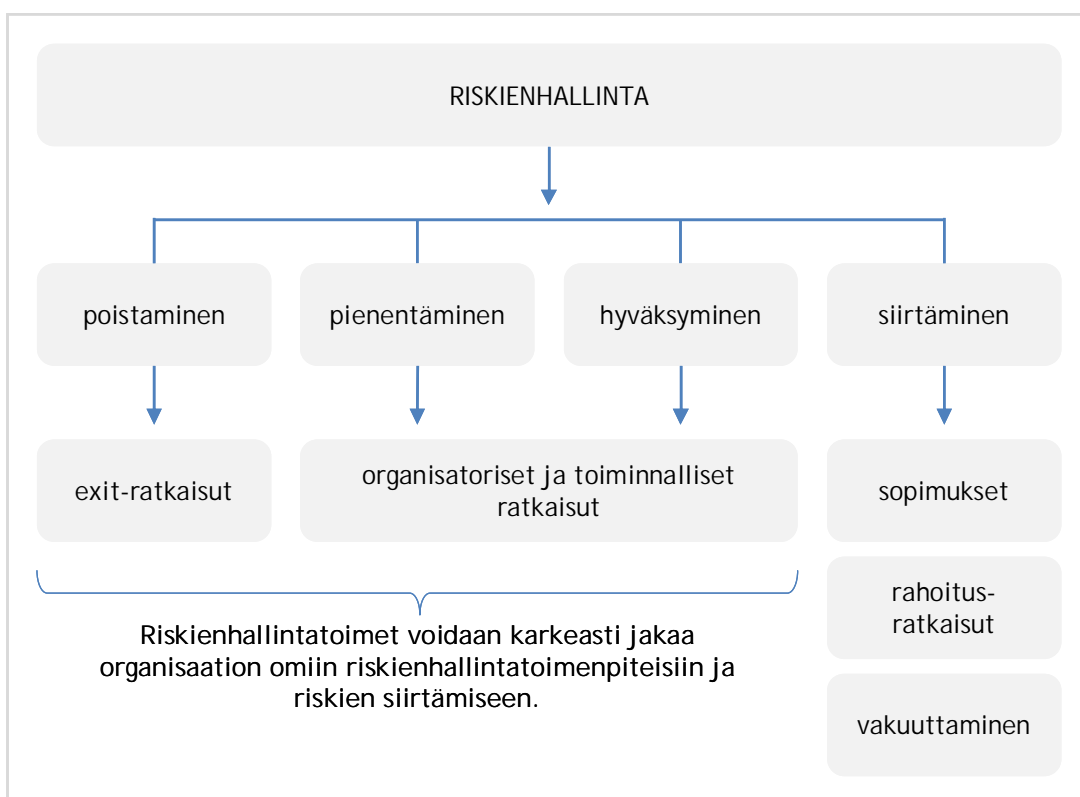
Riskienhallintaprosessi käynnistyy yksinkertaisen riskien tunnistamista ja arviointia helpottavan perusmallin pohjalta. Organisaation on syytä tarkastella itselleen ominaisia riskejä, käydä läpi esimerkiksi tiedostetut ja tiedostamattomat riskit sekä arvioida havaittuihin riskeihin liittyvä hallintatoimenpiteet ja niiden riittävyys. (Suominen 2003, 32.)

Riskienarvioinnin aikana riskit tunnistetaan ja niiden todennäköisyys ja vakavuus analysoidaan. Riskin vaikutuksia arvioitaessa tulisi taloudellisten arvon lisäksi huomioida henkilö- ja ympäristövaikutukset sekä vaikutukset organisaation maineeseen. Riskien toteutumisen vaikutusten arviointi euroissa puolestaan auttaa luokittelemaa riskit suhteessa toisiinsa. Riskien vaikutus voidaan määrittellä esimerkiksi asteikolla lievä–tuhoisa. Riskien toteutumisen todennäköisyyttä voidaan arvioida esimerkiksi asteikolla äärimmäisen harvinainen–varma (Kuvio 4). (Ilmonen ym. 2010, 95–95, 99.)



Kuvio 4: Riskienarvioinnin perusmalli Ilmonen ym. mukaillen (2010, 99)

Riskien tunnistamisen jälkeen niiden käsittelyyn on määritelty vaihtoehtoisia toimintatapoja. Näistä yleisimpiä ovat riskien pienentäminen tai siirtäminen, riskien hyväksyminen niiden vaikutuksia rajoittamalla tai riskien ottaminen tietoisesti omalle vastuulle. (Kuusela & Ollikainen 2005, 150; Ilmonen ym. 2010, 12; Juvonen ym. 2005, 19.)



Kuvio 5: Riskienhallintamenetelmät Ilmonen ym. mukaillen (2010, 124)

Riskienhallintatoimintaa voidaan kehittää tehokkaasti ainoastaan tunnistettuja ja arvioituja riskejä vastaan. Lähtökohtana on, että organisaation riskit pyritään hallitsemaan organisaation omilla riskienhallintakeinoilla. Niiden avulla pyritään pienentämään riskien todennäköisyyttä ja toteutuneen riskin seurausta. Osa riskeistä voidaan ulkoistaa siltä osin, kun organisaation omat toimet eivät riitä niihin vastaamaan. (Ilmonen ym. 2010, 124–126.)

2.4 Riskienhallinnan tarve ja toteutus valtionhallinnossa

Kuten aikaisemmin jo tuotiin esiin, ovat valtionhallinnon tulostavoitteiden asettamisen ja tuloksellisuutta koskevan raportoinnin peruskriteereitä yhteiskunnallinen vaikuttavuus ja toiminnallinen tuloksellisuus. Julkisten organisaatioiden oman panoksen merkitys korostuu erityisesti toiminnallisten tulostavoitteiden saavuttamisessa, jonka perustana puolestaan ovat tehokkuus sekä laadun ja henkisten voimavarojen hallinta. (Valtiovarainministeriö 2005a, 24).

Riskien perinteinen jako vahinko- ja liikeriskeihin ei suoraan sovellu valtionhallinnon organisaatioihin, koska niiden toiminta ei ensisijaisesti liity voiton tavoitteluun. Valtionhallinnossa riskit liittyvät sen sijaan erityisesti tuloksellisuuteen, jotka jaetaan edelleen valtion vastuulla olevien varojen ja omaisuuden turvaamiseen, lain ja talousarvion noudattamiseen sekä hyvän hallinnon periaatteiden ja arvojen toteuttamiseen. Lisäksi henkilöstö- ja osaamisriskien, tietoriskien sekä erityisesti maineriskien hallinta ovat tärkeässä asemassa. (Herrainsilta 2006, 42–43, 76–78, 81; Valtiovarainministeriö 2005b, 8–11.) Yksittäisten riskilajien tasolla julkishallinnossa parannettavaa olisi tutkimusten mukaan erityisesti omaisuus-, keskeytys- ja vahinkoriskien tunnistamisessa sekä riskikustannustietoisuuden kehittämisessä. (Herrainsilta 2006, 77–78, 81.)

Informaatio ja tieto sekä henkiset voimavarat (henkilöstö, osaaminen, työmotivaatio ja työhyvinvointi) ovat tulevaisuuden kannalta yhä tärkeämpiä valtionhallinnon voimavaroja ja toimintaedellytyksiä. Suurimmat haasteet valtionhallinnossa kohdistuvat lähitulevaisuudessa juuri henkilöstöön henkilöstövähennysten ja suurten ikäluokkien eläköitymisen myötä. (Herrainsilta 2006, 42, 53; Valtiovarainministeriö 2005b, 11.) Ikävä kyllä toiminnan tuloksellisuuden korostuminen heijastuu usein erityisesti henkilöstön hyvinvointiin.

Työkyvyn säilyttäminen ja työhyvinvointi ovat valtionhallinnossa tunnistetun henkilöriskien hallinnan tärkeimpiä osa-alueita. Valtionhallinnossa työskentelevä henkilöstö on tutkimusten perusteella (Herrainsilta 2006, 54) pitänyt tärkeimpinä työpaikan säilymistä, palkan lisäämistä sekä johtamistapojen parantamista. Erilaisista painotusehdotuksista huolimatta on kuitenkin muistettava, että turvallisuus syntyy ainoastaan mahdollisimman kattavan ja kokonaisuuksien suojaamiseen tähtäävän toiminnan tuloksena (Kuusela & Ollikainen 2005, 164).

Valtiovarainministeriön selvityksen (2004) mukaan riskienhallintaa toteutettiin valtionhallinnossa varsin vaihtelevasti vielä 2000-luvun puolessavälissä. Valtionhallinnon riskienhallinnan tilaa on kritisoitu muun muassa toimintatapojen hajanaisuudesta, riskienhallinnan tarkoituksen epäselvyydestä ja käsitteistön epäyhtenäisyydestä sekä riskienhallinnan eriyttämisestä omaksi toiminnokseen integraation sijaan. Tämä siitäkkin huolimatta, että tutkimuksen mukaan valtionhallinnon organisaatioiden johto pitää riskienhallinnan erityispiirteensä runsasta ohjeistusta ja sääntelyä. (Valtiovarainministeriö 2004; Herrainsilta 2006, 77–78, 81).

Riskienhallinnan vaihteleva tila valtionhallinnossa johtuu eräiltä osin henkilöstöryhmien erilaisista odotuksista riskienhallinnan suhteen. Johdon näkökulmasta riskienhallinnalla tavoitellaan erityisesti taloudellisuutta ja tuottavuutta, laatua sekä turvallisuuden edistämistä. Työntekijöiden lähestymistapa on kuitenkin käytännönläheisempi; heidän mielestään tavoitteena on ennen muuta työnteon sujuvuus sekä asiakaspalvelun laadun ja työilmapiirin parantaminen. (Herrainsilta 2006, 77–78.) Haasteena voidaan myös pitää riskienhallintakeinojen käyttömahdollisuuksia ja niiden painotuksen poikkeavuutta yksityiseen sektoriin verrattuna, sillä riskien tietoinen välttäminen tai poistaminen voi julkishallinnossa pahimmillaan tarkoittaa ongelmien siirtämistä tulevaisuudessa kohdattaviksi. (Herrainsilta 2006, 77–78, 81.)

Riskienhallinnan toteuttamista valtionhallinnon organisaatioissa vaikeuttaa muun muassa se, että riskeistä ja niiden toteutumisesta ole systemaattista tietoa, riskienhallinnalle asetettavia vaatimuksia ei ole riittävän järjestelmällisesti linjattu ja osassa toimintaa myös riskien näkökulma on uusi tai sitä ei ole sovellettu. (Valtiovarainministeriö 2004.) Yksityisellä sektorilla näitä linjauksia on sen sijaan runsaasti, mutta niiden sovellettavuus valtionhallinnossa voidaan kokea haasteelliseksi.

Valtionhallinnon organisaatiossa riskienhallintaa ja organisaatioturvallisuutta kehittävän on työssään hyvä huomioida ja arvioida ainakin seuraavien lähteiden soveltamismahdollisuudet

- valmiuslaki (22.7.1991/1080)
- pelastuslaki (29.4.2011/379)
- laki kansainvälisistä tietoturvallisuusvelvoitteista (24.6.2004/588)
- laki viranomaisten toiminnan julkisuudesta (21.5.1999/621)
- valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (1.7.2010/681)
- ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VM VAHTI 2/2010)
- asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (12.11.1999/1030)
- asetus valtion talousarviosta (11.12.1992/1243)
- Suomen turvallisuus- ja puolustuspolitiikka 2009, valtioneuvoston selonteko (VNK 11/2009)

- yhteiskunnan turvallisuusstrategia, YTS (valtioneuvoston periaatepäätös 16.12.2010)
- valtionhallinnon viestintä kriisitilanteissa ja poikkeusoloissa (VNK 15/2007)
- valtionkonttorin kehittämä riskienhallintatyökalu Kaiku-Luotain
- paikallisen turvallisuustyön kehittäminen, sisäinen turvallisuus (SM 19/2006).

Eduskunnan kanslian riskienhallinnan kehittämisessä on lisäksi huomioitava seuraavat lähteet

- laki turvatoimista eduskunnassa (30.5.2008/364)
- laki eduskunnan virkamiehistä (19.12.2003/1197).

Valtiovarainministeriön ja valtiokonttorin internet-sivuilla löytyy yksityiskohtaisia ohjeita ja suosituksia riskienhallinnan käytännön toteutuksesta. Lisäksi sisäisen tarkastuksen vaatimus on ollut lakiin perustuen voimassa vuodesta 2005 ja sen voidaan myös katsoa liittyvän julkisen organisaation riskienhallintaan ja turvallisuustoimintaan.

Riskienhallintaa ja organisaatioturvallisuutta koskevat kansalliset ja kansainväliset standardit ovat nekin hyviä lähteitä. Niitä ei tosin varsinaisesti ole laadittu valtionhallinnon tai julkisen sektorin tarpeita palvelemaan. Ammattitaitoinen riskienhallinnan asiantuntija osaa kuitenkin hyödyntää niitä myös soveltuvin osin ja omaa organisaatiota parhaiten palvelevalla tavalla.

Riskienhallintaan ja turvallisuuteen liittyviä standardeja ovat muun muassa

- Committee of Sponsoring Organizations of the Treadway Commission (COSO):
COSO ERM Enterprise Risk Management – Integrated Framework 2004
- Institute of Risk Management (IRM): A Risk Management Standard 2002
- International Organization for Standardization: ISO 31000:2009 (riskienhallinta), ISO 27001:2005 ja ISO 27005:2008 (tietoturvallisuus)
- British Standard: BS 31100 (riskienhallinta) ja BS 2599 (jatkuvuussuunnittelu)
- Kansallinen turvallisuusauditointikriteeristö (KATAKRI)
- Canadian Institute of Chartered Accountants: Criteria of Control (CoCo) 1995 (Hopkin 2010).

Standardit ja parhaat käytänteet on hyvä valtionhallinnon organisaatioiden toimintaa kehitettäessä mieltää sovellettavaksi materiaaliksi, ideoiden lähteiksi ja suunnittelua tukeviksi julkaisuksi. Valmiiden mallien hyödyntäminen ei saa korvata organisaatiokohtaista ajatustyötä ja siten myös oppimista. Ratkaisujen täytyy palvella kohdeorganisaation todellisia riskienhallintaan ja turvallisuuteen liittyviä tarpeita ja tavoitteita.

2.4.1 Riskienhallinta ja organisaatioturvallisuus

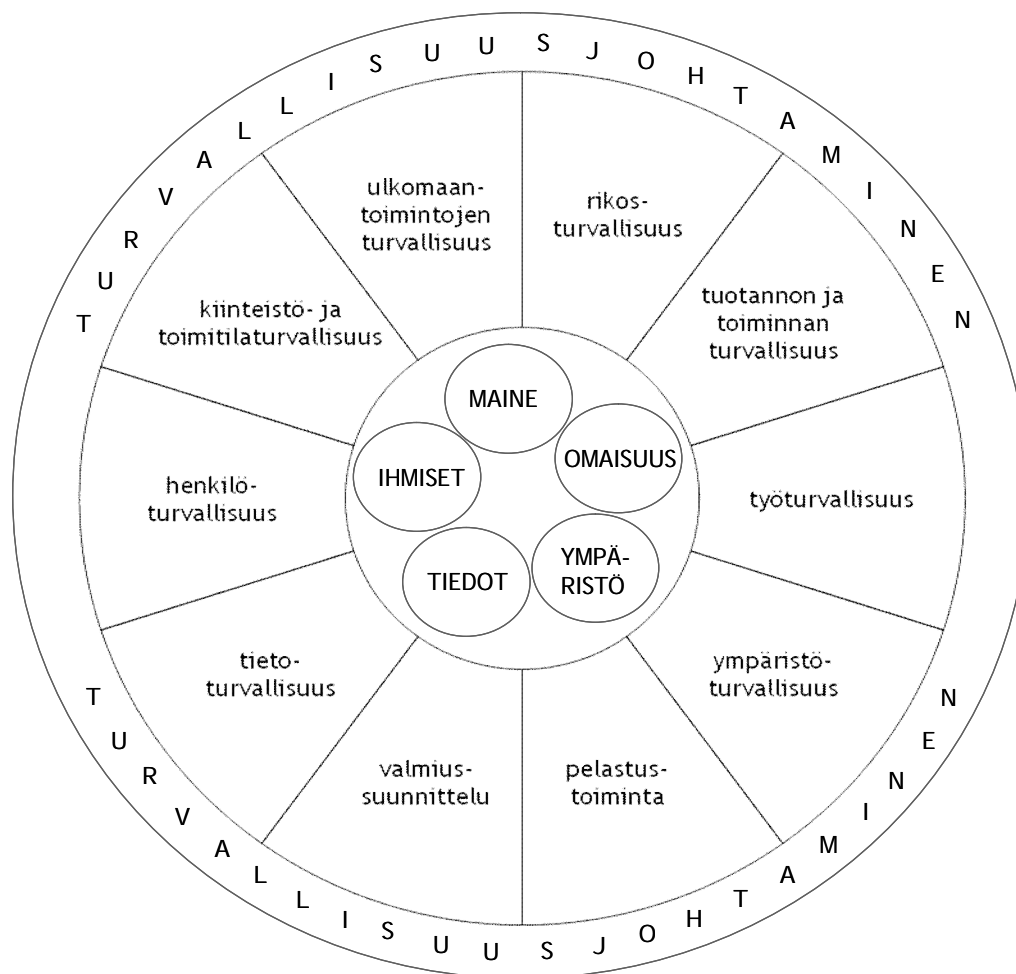
Organisaatioturvallisuutta ja riskienhallintaa voidaan tarkastella näkökulmasta riippuen toinen toisensa yläkäsitteenä, mutta staattista hierarkkista suhdetta ei niiden välille ole tarkoituk-

senmukaista muodostaa. Molempien osalta käsitteen väljyys ja yleisluontoinen määrittely vaikeuttavat osaltaan niiden keskinäisen suhteen ymmärtämistä ja kuvaamista. (Suominen 2003, 163–164, 165; Lanne 2007, 30–31.) Käytännössä riskienhallinnan ja organisaatioturvallisuuden synergiaedut ovatkin keskinäistä hierarkiaa tai käsitteellistä jaottelua tärkeämpiä. Käytännön tarpeista riippuen ja toiminnan organisoiminnan kannalta on kuitenkin tärkeää, että nämä käsitteet ja niiden keskinäinen suhde on selvästi määritelty ja viestitty. Tähän on pyritty myös riskienhallintaa ja organisaatioturvallisuutta käsittelevässä kirjallisuudessa.

Suomisen mukaan turvallisuutta voidaan käsitteenä pitää riskienhallintaa laajempänä. Organisaatioturvallisuus ja riskienhallinta ovat kuitenkin molemmat keskeisiä prosesseja organisaation kokonaisturvallisuuden saavuttamiseksi. Organisaation riskienhallinnan lähtökohdat muodostetaan strategisesta johtamisesta ja se ohjaa riskinottoon liittyvää päätöksentekoa, mutta myös turvallisuuden tavoitetaso on strateginen. (Suominen 2003, 163–164; Lanne 2007, 30–31.) Turvallisuuden käsite on saanut enemmän huomiota kuin riskienhallinta, koska turvallisuus käsitteenä liittyy liiketoiminnan lisäksi laajemmin ihmiskunnan edesottamuksiin kuten sodankäynti, politiikka ja vaikkapa subjektiivinen käsitys elämän mielekkyydestä.

Yritysturvallisuus EK:n mukaan organisaatioturvallisuuden johtaminen mielletään turvallisuuden kaikki osa-alueet kattavana ja niiden toteutumista ohjaavana tekijänä (2011). Turvallisuusosalalla on käytössä myös sellaisia yritysturvallisuuden määritelmiä ja yritysturvallisuutta visualisoivia kuvioita, joissa turvallisuusjohtaminen on laskettu yhdeksi osa-alueeksi muiden yritysturvallisuuden osa-alueiden rinnalle. Oleellista ei kuitenkaan ole se, miten osa-alueet määritellään vaan sen oivaltaminen, että turvallisuusjohtamisen tulee joka tapauksessa koskea kaikkia turvallisuuden osa-alueita ja toimia samalla myös eri osa-alueita yhdistävänä tekijänä.

Kuvion kuusi keskelle on kirjattu organisaation turvallisuustoiminnalla suojattavat arvot (Yritysturvallisuus EK 2011). Alkuperäislähteessä arvot ovat sijoiteltu mahdollisimman lähelle nimikkeeltään vastaavaa turvallisuuden osa-aluetta (esimerkiksi tieto lähelle tietoturvallisuutta), mutta turvallisuuden kokonaisvaltainen toteutuminen on riippuvainen kaikkien osa-alueiden tarkoituksenmukaisesta soveltamisesta. Tarkoituksenmukainen soveltaminen puolestaan tarkoittaa sitä, että organisaation toimialan ja toiminnan tavoitteiden vaikutukset turvallisuuden eri osa-alueiden painottumiseen on huomioitava (Yritysturvallisuus EK 2011).



Kuvio 6: Yritysturvallisuuden osa-alueet Yritysturvallisuus EK:ta mukaillen (2011)

Kokonaisturvallisuuteen kuuluu kuitenkin uhkista ja riskeistä tietoinen päätöksenteko sekä niiden seuraamusten ja seurannaisvaikutusten hallitseminen. Toiminnan jatkuvuuden varmistamisen lisäksi kokonaisturvallisuuden tavoitteena on lisäksi toimintamahdollisuuksien hyödyntäminen, sillä uhkien ja riskien tunnistaminen auttaa näkemään niissä piilevän positiivisen potentiaalin. Kokonaisturvallisuuden optimitaso löytyy uhkien ja riskien todennäköisyyden, niihin varautumisesta aiheutuvien kustannusten sekä saavutettavien toimintamahdollisuuksien ja päätöksenteon varmuuden väliltä. (Ilmonen ym. 2010, 19; Mäkinen 2007, 155.)

Organisaation turvallisuustoiminnan ollessa hyvin organisoitu ja järjestelmällistä on myös sen eri osa-alueiden yksityiskohtaisempi tarkastelu säännöllistä. Turvallisuuden eri osa-alueiden tarkasteluun liittyvät puolestaan uhka- ja riskianalyysit, joiden huolellinen ja säännöllinen laatiminen mahdollistaa paremmin hiljaisten signaalien havaitsemisen ja siten myös niiden hyödyntämisen. Näin ollen riskienhallinnankin perimmäinen tavoite on yhteneväinen turvalli-

suusjohtamisen tavoitteen kanssa; organisaation vastuullisen ja tosiasioihin perustuvan päätöksenteon mahdollistaminen organisaation koosta ja toimialasta riippumatta.

Yritysturvallisuuden neuvottelukunnan näkemyksen mukaan riskienhallintatoimet kohdistetaan yritysturvallisuuden osa-alueisiin. Riskienhallintaa voidaan tarkastella turvallisuusjohtamisen tukena; turvallisuutta koskevan ylemmän päätöksenteon tulisi perustua riskienhallintaperiaatteeseen riskienarvioinnin ollessa lähes ainoa hyväksyttävissä oleva pohja yritysturvallisuuden osa-alueisiin liittyvissä päätöksissä. (Suominen 2003, 163–164,165; Kerko 2001, 57; Lanne 2007, 30–31.) Kokonaisturvallisuus on osaltaan riskienhallintaa ja toisaalta riskien tunnistaminen, analysointi sekä riskienhallintakeinojen käyttö vaikuttavat osaltaan kokonaisturvallisuuden optimointiin. Riskienhallinnan menettelytapoja ja käytäntöjä (mm. riskien arviointi tai riskianalyysi) voidaan hyödyntää yhtenä turvallisuusjohtamisen työkaluina. (Ilmonen ym. 2010, 49–50; Lanne 2007, 31).

Riskienhallinnan kannalta katsottaessa turvallisuusjohtamisen keinot puolestaan auttavat riskien pienentämisessä, eli niiden todennäköisyyden ja seurausten vähentämisessä. Turvallisuustoiminnan avulla organisaatioon onkin joskus sitä tiedostamatta saatettu järjestää ainakin osittain toimiva riskienhallintajärjestelmä. (Ilmonen ym. 2010, 49–50; Lanne 2007, 31; Mäkinen 2007, 155.)

Turvallisuusjohtamisen ja riskienhallinnan yhteys on selkeä myös valtionhallinnon organisaatioiden toiminnassa. Vaikka riskilajit ja turvallisuustoiminnan painotukset siellä poikkeavatkin yksityisen sektorin vastaavista, ovat turvallisuusjohtamisen ja riskienhallinnan tavoitteet, johtaminen ja käytettävät työkalut samat. Julkisen sektorin erityispiirteiden huomioiminen vaatii kuitenkin vastuuhenkilöiltä ammattitaitoa ja oikeanlaista asennetta seurata myös alan yleistä kehitystä.

Organisaation turvallisuustoiminta kehittyy Miettisen mukaan vaiheittain lähtötasosta kohti ylivoimaista suojaustasoa (2002, 21). Vähimmäissuojaustaso saavutetaan, kun organisaation johto sitoutuu turvallisuuden kehittämiseen. Perussuojaustasolla turvallisuus on integroitunut osaksi organisaation toimintaprosesseja. Edistyksellinen suojaustaso vaatii jo sen, että turvallisuudesta on tullut osa organisaatiokulttuuria - ylivoimainen suojaustaso on saavutettu, kun organisaation turvallisuustoiminta tuottaa sille selvää kilpailuetua. (Miettinen 2002, 21.) Miettinen muistuttaakin, että turvallisuuden kehittämisen askeleiden pituus on yleensä suoraan verrannollinen organisaation kokoon nähden (2002, 21). Tämä ja erityisesti jäykät byrokraattiset rakenteet huomioiden julkisen sektorin turvallisuustoimintaa kehitettäessä on tärkeää olla kärsivällinen.

Turvallisuusjohtaminen ja riskienhallinta vaikuttavat valtionhallinnossa myös organisaation sisäiseen yhteistyöhön esimerkiksi viestinnän ja auditoinnin osalta sekä ulkoisten sidosryhmien kanssa toimimiseen erityisesti pelastustoimen ja väestönsuojelun osalta. Selkeä vastuunjako niiden välillä helpottaa normaaliolosuhteissa tapahtuvaa suunnittelutyötä ja erityisesti toteutuneiden uhkien tilannejohtamista.

Organisaatioturvallisuutta ja riskienhallintaa tai niiden painoarvoa ei siis ole tarkoituksenmukaista asettaa vastakkain. Molempien käytännön toteutus riippuu pitkälti organisaation tehtävästä ja toimialasta ja ennen kaikkea strategisella tasolla tehdyistä turvallisuustoimintaan ja riskienhallintaan liittyvistä päätöksistä. Johtoasemassa toimivien henkilöiden vastuulla onkin kullekin organisaatiolle optimaalisen turvallisuuden ja riskienhallinnan kokonaisratkaisun rakentaminen.

2.4.2 Riskienhallinta ja sisäinen tarkastus

Hyvä hallintotapa (corporate governance) tarkoittaa organisaation kestävästä ja laadukasta johtamista ja sen toiminnan valvontaa. Terminä se usein liitetään tilivelvollisuuteen, mutta käytännössä hyvä hallintotapa vaatii riskienhallintaa, turvallisuuden vaalimista, tilintarkastusta ja yrityksen sisäisiä tarkastus- ja raportointikäytäntöjä. 2000-luvun puolestavälistä alkaen maailmalla käyty keskustelu hyvästä hallintotavasta on painottanut sisäisen valvonnan ja riskienhallinnan merkitystä. (Kuusela & Ollikainen 2005, 124, 164.)

Sisäinen tarkastus on tärkeä osa organisaation riskien menestyksekkästä hallintaa. Sisäisen tarkastuksen menetelmät, prosessit ja tarkastustoimenpiteet tähtäävät siihen, että organisaatio saavuttaa asetetut tavoitteet. (Hopkin 2010, 291.) Sisäisen tarkastuksen ansiosta organisaatiota voidaan johtaa luottavaisina niin hyvinä kuin vaikeinakin aikoina. Sisäisen tarkastuksen toiminnan tärkeimmät tavoitteet ovat

- organisaation varallisuuden varjelu ja suojeleminen
- virheettömän kirjanpidon varmistaminen
- organisaation operationaalisen tehokkuuden ja vaikuttavuuden edistäminen
- toimintapolitiikkojen ja työjärjestyksien, mukaan lukien tarkastusproseduurien, noudattaminen
- sisäisen ja ulkoisen raportoinnin luotettavuuden edistäminen
- organisaation toiminnan lain- ja säädöstenmukaisuuden varmistaminen
- sidosryhmien etujen turvaaminen (Hopkin 2010, 292).

Valtiohallinnossa on jo vuodesta 2005 alkaen pitänyt laatia niin sanottu sisäisen valvonnan arviointi- ja vahvistuslausuma (Asetus valtion talousarviosta, 65 §). Sisäinen tarkastus on riskianalyysien ja riskienhallintamenettelyjen asiantuntija, mutta sillä on omat erilliset tehtävän-

sä, eikä sen tule vastata yrityksen riskienhallinnasta. Sisäinen tarkastus arvioi riskienhallintaa ehdottoman riippumattomana osapuolena. (Koivu, Ranta-aho & Vuoti 2010, 95, 102; Ilmonen ym. 2010, 50).

Sisäinen tarkastus on osa yrityksen strategista suunnittelua ja riskienhallinta puolestaan on osa sisäistä valvontaa. Organisaatiojohdon on näin ollen huolehdittava, että myös riskienhallinta on asianmukaisesti järjestetty. (Koivu ym. 2010, 76–77; Kuusela & Ollikainen 2005, 125.) Sisäinen valvonta ja riskienhallinta parantavat toimintayksikön tuloksia tukemalla oikeaan tietoon perustuvaa suunnittelua ja päätöksentekoa ja varmistamalla toiminnan laillisuuden ja resurssien tehokkaan käytön (Valtiovarainministeriö 2005b, 8).

Sisäinen tarkastus voi toimia organisaatiossa riskianalyyysien ja riskienhallintamenettelyjen asiantuntijana (Koivu ym. 2010, 95), mutta sen ei kuitenkaan tule vastata operatiivisesta riskienhallinnasta. Sen sijaan tavoitteen on tarjota riippumatonta ja objektiivista arviointi-, varmistus- ja konsultointitoimintaa (Kuusela & Ollikainen 2005, 129). Sisäinen tarkastus valvoo riskienhallintaprosessin toimivuutta esimerkiksi arvioimalla, miten johto varmistuu riskienhallinnan osa-alueiden tehokkuudesta ja riittävydestä (Kuusela & Ollikainen 2005, 131).

Yhteistyö riskienhallinnan ja sisäisen tarkastuksen välillä on siis tärkeää. Niillä on toisistaan erilliset tehtävät, jotka kuitenkin tukevat yhteisen tavoitteen – hyvän hallintotavan, riskitietoisuuden johtamisen, tehokkaan toiminnan ja turvallisen työympäristön mahdollistaminen.

2.5 Kriisiviestintä osana riskienhallintaa

Riskien ja uhkien toteutumisesta seuraavat poikkeustilanteet vaativat vahvaa johtamista. Viestintä puolestaan on keskeinen osa johtamista, oli kyse normaalioloista tai poikkeustilanteesta. Epäonnistunut viestintä merkitsee johtamisen epäonnistumista. Onnistunut johtaminen ja viestintä vaativat puolestaan ajantasaista tilannetietoa. (Seeck 2008, 6; Seeck, Laventa & Hakala 2009, 7.) Johtamisessa tilannetieto toimii päätöksenteon perustana ja viestinnän tehtävänä on puolestaan jakaa edelleen tehdyt päätökset. Toisaalta on muistettava, että sekä johtaminen että viestintä muuttavat itsekin tilannekuvaa vaikuttaessaan osaltaan tilanteen kehittymiseen. Riskienhallinnan ja organisaatioturvallisuuden järjestelmällisen ja suunnitelmallisen toteutuksen myötä kasvavat myös poikkeustilanteissa käytettävissä olevan tiedon määrä ja ennen kaikkea laatu.

Viestinnän ja kriisiviestinnän ammattitaitoinen hoitaminen on tärkeää kriisitilanteista toipumisen ja organisaation toiminnan tulevaisuuden vuoksi. Kriisiviestinnän ja -johtamisen suunnittelulla voidaan oleellisesti parantaa organisaation toimintakykyä ja toiminnan tulosta kriisi-

tilanteissa ja normaaliolojen poikkeustilanteiden hoidossa. Ennakkoon varautuminen helpottaa myös yksilötasolla vastuutehtävissä toimivien asemaa.

Toimiva sisäinen viestintä yhtenäistää ulkoista viestintää. Lisäksi se voi parhaimmillaan rajoittaa vahinkoja esimerkiksi henkilöstön pelastautumista vaativissa tilanteissa. Viestintä on helppompaa, kun siitä vastuussa olevalla on tarvittavat tiedot ja kun viestintävastuut ja -kanavat ovat selvät ja ennalta harjoitellut. Riskienhallinta tukee kriisiviestintää ja poikkeustilanteiden hallintaa, sillä sen soveltaminen normaalioloissakin vaatii viestintä-, raportointiväylien sekä johtosuhteiden ja -vastuiden määrittelyä ja toimeenpanoa.

Perusteet johtamisen ja viestinnän yhteen kytkemiselle luodaan organisaation normaaliolojen aikaisessa toiminnassa. Myös valtionhallinnon kriisijohtamisessa korostetaan periaatetta, jonka mukaan viranomaisten ja toimielinten vastuujako ja toimintamallit säilytetään mahdollisimman pitkään normaaliolojen kaltaisina. (Valtioneuvoston kanslia 2007, 11–12.)

Viranomaisviestintä voidaan jakaa poliittiseen ja hallinnolliseen viestintään. Hallinnosta vastaava viranomainen toimii virkavastuulla ja perustaa viestinnän faktoihin. Poliittisella vastuulla toimiva voi helpommin kertoa arvioita, näkemyksiä ja vahvistamattomiakin huonoja uutisia. (Huhtala & Hakala 2007; Seeck ym. 2008, 128.)

Viestintää käytetään tiedonsiirtoon, sanoman levittämiseen ja yhteisyyden rakentamiseen (Seeck ym. 2008, 25). Kriisiviestintään kohdistuu kovia laatuvaatimuksia, sillä siinä korostuu tiedonsiirron lisäksi erityisesti yhteisyyden rakentaminen: se, miten asiat kerrotaan ja ilmaistaan on vähintään yhtä tärkeää kuin viestin varsinainen sisältö. Viestinnän laatu lopulta ratkaisee, onko siitä hyötyä vai haittaa organisaatiolle poikkeustilanteen hoitamisessa. Näin ollen kriisiviestintä voi onnistua silloinkin, jos huonoista puitteista tai puutteellisesta ennakkosuunnittelusta huolimatta viestinnän sisältö on laadullisesti hyvää. Kriisiviestinnän laatu puolestaan vaikuttaa osaltaan myös organisaation maineeseen. Seeck muistuttaakin, että viranomaisten huonosti hoitama kriisi voi johtaa kansalaisten luottamuksen menettämiseen (2009, 7).

Ihmisten kriisitilanteessa tuntema epävarmuus ja turvattomuus vaativat viestinnältä ihmisten kohtaamista, joka käytännössä tarkoittaa kuulluksi ja ymmärretyksi tulemista ja tiedontarpeen täyttymistä. Kriisiviestinnästä vastuussa olevan henkilön tulisi olla luottamusta herättävä persoona ja omata kyky esiintyä julkisuudessa. Se, että asiasta ei tiedetä sen enempää kuin jo julkisuudessa on ilmaistu, tulee myös pysytää välittämään aidosti ja luottamusta herättävästi. (Seeck ym. 2008, 59, 95.)

Kriisijohtamisen ensisijaisena päämääränä on yleisen turvallisuuden takaaminen, jolloin organisaation maineenhallintaan ja taloudellisiin seuraamuksiin liittyvät toimet ovat aina toissijaisia. Kriisien hoidosta seuraa verkostoyhteiskunnassa haittaa maineelle erityisesti silloin, kun kriisi hoidetaan huonosti. Maineriski toteutuu käytännössä sidosryhmien vuoropuhelussa ja vuorovaikutuksessa, jota käydään viestinnän spontaaneilla persoonallisilla areenoilla ja muodollisilla institutionaalisilla areenoilla. Mainekriisissä oleva organisaatio pyrkii haastamaan huonon maineensa ja saamansa julkisen tuomion. (Seeck 2009, 6, 16, 59–60, 63.)

Maineenhallinta vaatii siis jo normaalioloissa vahvaa ja johdonmukaista viestintää. Kriisijohtamisen ja maineenhallinnan näkökulmasta onnistunut kriisiviestintä voi vaikuttaa organisaation selviytymiseen pitkällä aikavälillä. Vakavastakin tapahtumasta voidaan selvitä ilman kollektiivista vihaa ja sitä mahdollisesti seuraavia organisaation monimuotoista boikotointia, mikäli kriisin akuutissa vaiheessa voidaan osoittaa, että yhtiö vastuutaho ottaa tapahtumat vakavasti ja tekee aktiivisesti töitä tilanteen ratkaisemiseksi. Myös vastuun julkinen tunnustaminen vaikuttaa organisaatiolle lopulta lankeavaan yhteisölliseen tuomioon.

3 Kehittämistehtävän määrittely

Ammattikorkeakouluissa tehtävillä opinnäytetöillä on erityinen, työelämän kehittämiseen tähtäävä tarkoitus. Valtioneuvoston mukaan työelämän ongelmien erittelyn ja ratkaisemisen lisäksi opinnäytetyön tavoitteena on osoittaa tutkijan valmius itsenäiseen vaativaan asiantuntijatyöhön. (Valtioneuvoston asetus 423/2005.)

Laurea-ammattikorkeakoulu painottaa ongelmien ratkaisua opinnäytetyöprosessin aikana syntyneen tiedon avulla, uusien ratkaisujen, menetelmien ja mallien kehittämistä sekä uuden osaamisen luomista. Ylemmän ammattikorkeakoulututkintoon tähtäävän on opinnäytetyössään osoitettava hallitsevansa prosessinomainen, soveltava sekä uuteen tietoon ja innovaatioihin tähtäävä työskentely. (Laurea-ammattikorkeakoulu 2008, 3.)

Kohdeorganisaatioiden kehittämistavoitteet liittyvät Ojasalo, Moilanen & Ritalahtea mukaillen toiminnan kannattavuuden parantamiseen, henkilöstön motivoimiseen, tulevaisuuden toimintaan vaikuttavien tekijöiden ennakoimiseen, toiminnan tehostamiseen sekä organisaatiossa ilmenneiden ongelmien ratkaisemiseen (2010, 12). Mitä isompi organisaatio, sitä suurempi haaste on ohjata sisäiset organisaatorajat ylittävää yhteistyötä ja sitä tärkeämpää on panostaa asioiden kehittämiseen koko organisaation tasolla (Ilmonen ym. 2010, 19; Miettinen 2002, 19).

3.1 Kehittämistyön tausta ja aikaisemmat tutkimukset

Opinnäytetyön toimeksianto juontaa vuoden 2010 kevääseen, jolloin lähestyin eduskunnan kanslian turvallisuusjohtajaa kysyäkseni mahdollisista tutkimustarpeista turvallisuusyksikön toimintaan liittyen. Olin aloittamassa opintoja alalta, joka ei suoranaisesti liittynyt toimenkuvaani eduskunnassa – opinnot vaatisivat osan huomiostani ja poissaoloja työpaikalta, joten oli tärkeä osoittaa anomuksiani käsittelevälle johdolle, että opinnoistani olisi hyötyä myös työnantajalleni.

Alun perin oli tarkoitus, että tutkisin eduskunnan kanslian turvallisuusyksikön kehittämismahdollisuuksia tulevia vuosikymmeniä silmällä pitäen. Organisaatioturvallisuuden näkökulmasta toimeksianto muutettiin koskemaan riskienhallintaa yhtäältä tutkijan opintojen etenemisen ja toisaalta eduskunnan kansliassa tapahtuneiden organisaatiomuutosten seurauksena. Kokonaisvaltainen turvallisuus vaatii organisaation kaikkien tasojen osallistumista, joten riskienhallinnan ja strategisen johtamisen näkökulma tuntui muodostavan hyvän lähtökohdan myös organisaatioturvallisuuden kestäväälle ja pitkäjänteiselle kehittämiselle.

Eduskunnan kanslian kaltaisessa organisaatiossakaan turvallisuutta ei sen käytännön toteuttamisen osalta ole tarkoituksenmukaista eristää vain turvallisuusyksikön vastuulle, vaan koko henkilöstön tulisi omalta osaltaan osallistua turvallisuuden ylläpitoon ja kehittämiseen. Riskienhallinnan näkökulma korostaa koko organisaation osallistumista ja ylimmän johdon aktiivisuutta. Lisäksi turvallisuustoiminnan merkityksen ymmärtäminen talouden ja toiminnan kannattavuuden näkökulmasta voi osaltaan vaikuttaa turvallisuuden eteen tehtävän työn arvostukseen ja edelleen sen kehittämismahdollisuuksiin. Näistäkin syistä riskienhallinnan soveltaminen eduskunnan kanslian organisaatioturvallisuuden kehittämiseen on perusteltua.

Eduskuntaa on tutkittu aiemmin niin turvallisuuden kuin johtamisenkin näkökulmasta. Kokonaisvaltaisen riskienhallinnan toteutuksen hyödyistä valtionhallinnon organisaation strategisen johtamisen tukena sen sijaan ei löytynyt suomalaisia tutkimuksia. Valtionhallinnossa toteutettavaan riskienhallintaan liittyviä suosituksia on laadittu valtiovarainministeriössä ja erityisesti valtionhallinnon organisaatioita varten kehitetyn riskienhallintatyökalun (Kaiku-Luotain) käyttöönottoa on arvioitu Juha Herrainsillan toimesta (2006). Edellä mainittujen lisäksi eduskunnan kansliaa koskevia tai tätä kehittämistyötä muuten tukevia aikaisempia tutkimuksia ovat

- Juuso Rönholmin Pro Gradu -tutkielma "Mikä hiippari on eduskunta-avustaja? Tutkielma suomalaisista kansanedustajien avustajista" (Turun yliopisto, 2011)
- Teemu Isoahon opinnäytetyö "Poliittisten luottamushenkilöiden turvallisuus" (Laurea-ammattikorkeakoulu, 2011)
- Heli Kestin lopputyö "Eduskunnan kanslian kriisiviestintäohjeisto" (Infor Oy, 2011)
- Hertta Niemen väitöskirja "Managing in the Golden Cage" (Hanken, 2010)
- J-P Schroderuksen lopputyö "Eduskunnan turvallisuustoiminnan kehittäminen 2003–2008" (TKK Dipoli, 2008).

Kehittämistyöni kannalta tärkeimpiä edellä mainituista ovat J-P Schroderuksen, Teemu Isoahon ja Hertta Niemen työt. Lyhyt esittely kustakin työstä lienee paikallaan, jotta niiden merkitystä tämän kehittämistyön kannalta on helpompi hahmottaa.

Eduskunnan puhemies asetti vuonna 2003 turvallisuusasioita selvittäneen työryhmän (ETKT), jonka sihteerinä toimi Jukka-Pekka Schroderus. Schroderuksen vuonna 2008 valmistunut lopputyö käsittelee vuonna 2003 alkanutta eduskunnan turvallisuustoiminnan kehittämisprojektia, tuon projektin loppuraporttia ja eduskunnan turvallisuuden eri osa-alueiden sen hetkistä tilaa (Schroderus 2008).

Schroderuksen kehittämisprojektin yhtenä tavoitteena oli liittää projektin aikana syntyneet uudet turvallisuuteen liittyvät näkemykset osaksi eduskunnan toimintaa. Toimintatutkimuksen muodossa tehty ja sosiotekniseen näkökulmaan perustuva lopputyön tutkimuskysymykset liittyivät turvallisuustoiminnan kehittämisen tarpeisiin ja tavoitteisiin, ETKT:n työskentelyn arvi-

ointiin ja ETKT:n laatiman loppuraportin kehitysesitysten toteutumiseen. Schroderuksen mukaan nämä tavoitteet saavutettiin hyvin. (Schroderus 2008, 45–46.)

Työryhmän loppuraportin ehdotuksen mukaisesti päätös erillisestä turvallisuusyksiköstä eduskunnan kansliaan perustettavasta tehtiin vuoden 2004 lopulla. Päätöksen myötä muutoksia tehtiin lisäksi eduskunnan virkamieslakiin ja eduskunnan kanslian ohjesääntöön. ETKT:n työskentelyä kuvattiin haasteelliseksi – siinä oli kyettävä yhtäältä yhdistämään poliittinen tahto, virkamiesten näkemykset ja eri viranomaisten kokemukset sekä toisaalta teoria ja käytäntö. Työryhmän loppuraportissa esitetyt kehitysehdotukset olivat kaikki valmistelussa tai valmistuneet vuoden 2008 kuluessa. Schroderus esitti jatkotutkimusaiheiksi johdonmukaisen ja ymmärrettävän viestintätavan löytämisen turvallisuustoiminnan kehittämistarpeiden välittämiseksi poliittisille johdolle ja turvallisuustoiminnan jalkauttamisen työntekijätasolle. (Schroderus 2008, 29, 46.)

Teemu Isoahon vuonna 2011 valmistuneessa opinnäytetyössä kartoitettiin kyselytutkimuksen keinoin poliittisten luottamushenkilöiden kokemuksia turvallisuudesta, heidän arvioitaan tulevaisuuden turvallisuudesta ja näkemyksiä turvallisuuden tunteen parantamiseksi. Tutkimuksen tuloksista mainittakoon luottamushenkilöiden huoli erityisesti läheisten turvallisuudesta, yksityisyyden suojasta, sanallista uhkauksista ja tietoturvaan liittyvistä riskeistä sekä maine-riskit, häiritsevän käytöksen lisääntyminen ja suoran väkivallan pelko (Isoaho 2011, 30–39).

Luottamushenkilöiden mukaan turvallisuutta voitaisiin parantaa viranomaisten ja turvallisuustoimijoiden tarjoaman avun ja teknisen avun saatavuuden parantamisella sekä muun muassa politiikan julkisuuskuvan parantumisella (Isoaho 2011, 41). Yleisesti ottaen poliittiset luottamushenkilöt ovat erittäin tyytyväisiä työhön liittyvään turvallisuuteensa. Kehittämiskohteiksi ehdotetaan kuitenkin riskitietoisuuden lisäämistä, henkilökohtaisen riskiprofiilin laatimista luottamushenkilöistä, turvallisuusasioista keskustelemista ja selkeää ohjeistusta uhkatilanteissa toimimiseen. Jatkohankkeiksi Isoaho ehdottaa kyselytutkimuksen uusimista vertailuaineiston saamiseksi sekä eri turvallisuustoimijoiden yhteistyön kehittämisen arviointia. (Isoaho 2011, 47–56.)

Hertta Niemen väitöskirja tutkii etnografisin menetelmin eduskunnan johtamiskulttuuria, tassa-arvoa ja valtarakenteita. Vaikka väitöskirja ei suoranaisesti käsittele riskienhallintaa, on siitä löydettävissä muun muassa maineriskeihin liittyviä elementtejä. Niemi nostaa lisäksi esiin riskienhallinnan toteuttamisen kannalta mielenkiintoisia kysymyksiä, kuten eduskunnan poliittisen osan ja hallinnon välinen suhde sekä yksilön tahdon ja kollektiivisen tahdon ristiriidan aiheuttamat organisaatiokulttuuriset ongelmat. Asiajohtamisen ja ihmisten johtamisen erottaminen toisistaan tai niiden epätasapainoinen painottaminen on lyhytnäköistä, sillä ih-

misten johtamisen laatu on kriittinen tekijä henkilöstön työhyvinvoinnin ja työnteon tehokkuuden kannalta.

Niemen väitöskirjan suurin merkitys tämän opinnäytetyön kannalta on eduskunnan epävirallisen organisaatiokulttuurin avaamisella, epävirallisten valtarakenteiden käsittelyllä sekä päätöksentekoprosessien erittelyllä. Yksi Niemen ehdottamista jatkotutkimuskohteesta liittyy kysymykseen eduskunnan hallinnollisen ja poliittisen osan suhteesta; onko poliittinen puoli hallinnon asiakas vai tuleeko kansanedustajiin suhtautua kollegoina. Tämä kysymys on tärkeä myös riskienhallintaa ja turvallisuustoimintaa kehitettäessä. Turvallisuus koskee kaikkia ja on sen tulisi olla yhteinen tavoite, jolloin myös turvallisuusohjeiston tulisi olla koko organisaation hyväksymä ja noudattama.

Julkisen sektorin ja valtionhallinnon turvallisuustoimintaa käsitellään muun muassa ulkoasiainhallinnon turvallisuuskoulutuksen tarvetta (Tammi 2006), taloushallintopalvelun turvallisuustietoisuutta (Saarinen 2007), valtionhallinnon henkilöturvallisuutta (Lauttamus 2010) ja viestintäviraston riskienhallintaa (Arnell 2010) käsittelevissä Laurea-ammattikorkeakoulun opinnäytetöissä. Valtionhallinnon riskienhallintaa ja valtiokonttorin riskienhallintamenetelmän käyttöönottoa tutkitaan Tampereen Yliopistoon tehdystä pro-gradu tutkielmassa (Herrainsilta 2006). Edellä mainituista töistä löytyy paljon yleisesti valtionhallintoa koskevaa tietoa. Syvemmän tutkimuksen tekeminen ja erityisesti julkisen sektorin organisaatioiden käytännön kehittäminen vaatii kuitenkin aina organisaatiokohtaista lähestymistapaa.

Eduskunnan kanslian vuoden 2010 sisäisen tarkastukset arviointi- ja vahvistuslausuma sisältää riskienhallinnan ja organisaatioturvallisuuden kehittämisen kannalta lupaavia kannanottoja. Lausuma pohjautuu sisäisen tarkastuksen tammikuussa 2011 toteuttamaan eduskunnan kanslian johdolle suunnattuun kyselyyn. Kyselyyn vastanneiden mielestä riskienhallinta kuuluu kanslian vastuulliseen johtamiseen, sillä sen avulla lisätään luottamusta kanslian toimintaan ja talouteen. (Eduskunnan kanslia 2010c.)

Edellä mainitusta kyselystä poimituista avoimista vastauksista voidaan todeta, että tarve riskienhallinnan ja turvallisuuden kehittämiseksi on tunnustettu myös eduskunnan kanslian johdossa. Huomion kiinnittäminen riskienhallintaan saa johdolta yksimielisen tuen, ja riskienhallinnan tilan arvioinnilla pyritään vahvistamaan avoimuutta, vuorovaikutusta ja hyvää hallintoa eduskunnan kansliassa. Tavoitteena on, että kanslian johto kiinnittää huomioita riskeihin niin, että toimintayksikön johtavat virkamiehet tuntevat vastuunsa oman yksikkönsä hallinnon ja talouden oikeellisuudesta kanslian tiliohjesäännön edellyttämällä tavalla. (Eduskunnan kanslia 2010c.)

Kyselyyn vastanneet esittivät lisäksi kehittämisehdotuksia muun muassa kokonaisvaltaiseen organisaatioturvallisuuteen ja riskienhallintaan liittyen

- esimiehille pitäisi järjestää koulutustilaisuus riskienhallinnasta tai se tulisi sisällyttää yhteiseen esimieskoulutukseen
- esimiehille tulisi laatia tiivistetty opas riskienhallinnan käytännön toteuttamiseen
- riskienhallinnan teoretisoimisen välttäminen ja käsitteiden avaaminen
- turvallisuustoiminta tulisi suunnitella riskikartoituksen pohjalta
- riskienhallintatoiminta tulisi liittää turvallisuusyksikön yhteyteen. (Eduskunnan kanslia 2010c.)

Riskienhallintatoiminnan käynnistämistä eduskunnan kansliassa käsitteleville kehittämis- ja tutkimustöille voidaan siis todeta olevan selkeä tarve niin ulkoisista kuin sisäisistäkin lähtökohdista.

3.2 Kehittämistyön tavoitteet ja tutkimuskysymykset

Tämän tutkimuksellisen kehittämistyön tavoitteena on perustella riskienhallintatoiminnan käynnistämisen tarve eduskunnan kansliassa. Pää tavoitetta tukevia osatavoitteita ovat

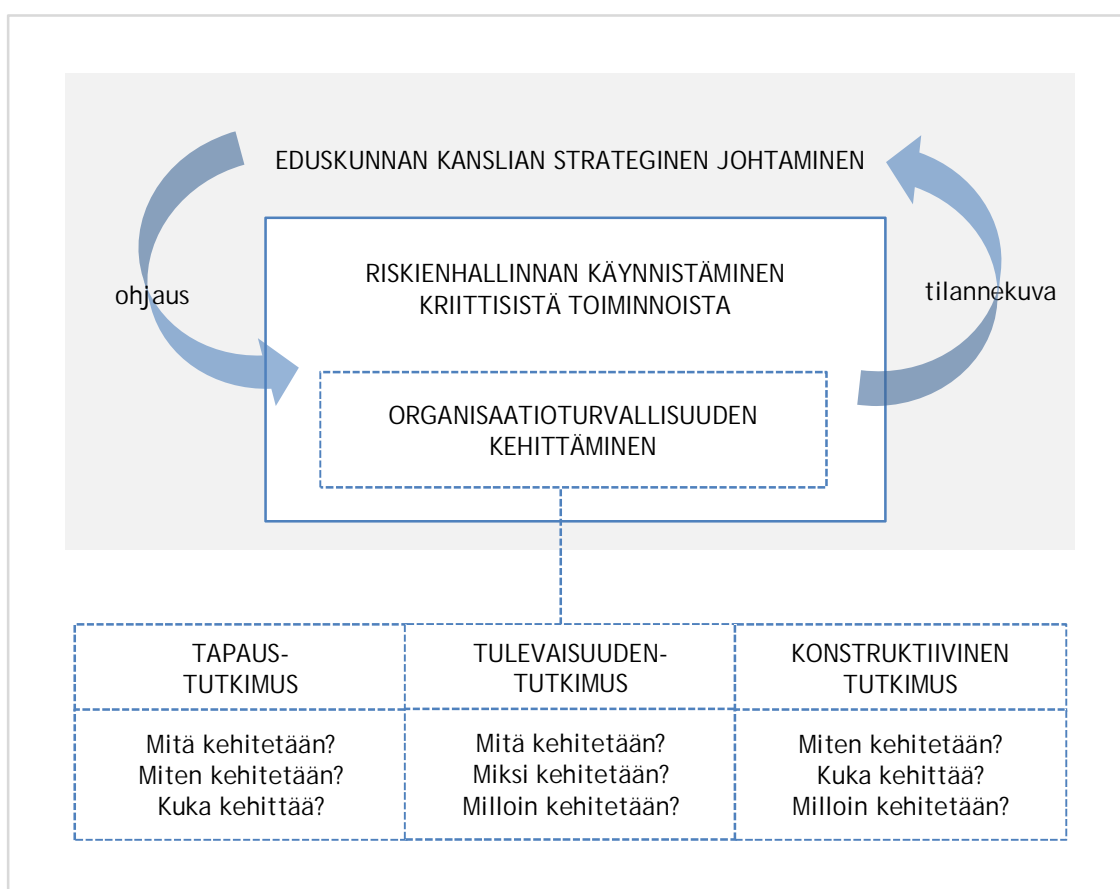
- eduskunnan ylimmän virkamies- ja poliittisen johdon motivoiminen sitoutumaan pitkäjänteiseen ja systematisoituun riskienhallintaan
- riskienhallinnan tarpeellisuutta ja toteuttamista koskevan teoreettisen ja vertailuaineistoon perustuvan tiedon kokoaminen turvallisuusyksikön ja riskienhallinnan asiantuntijan käyttöön
- esittää ehdotus siitä, miten riskienhallinta olisi mahdollista käynnistää ja toteuttaa eduskunnan kansliassa.

Eduskunnan ylimmän johdon motivointi kokonaisvaltaiseen riskienhallintaan sitoutumiseksi on tärkeää, jotta toiminnalle saadaan heti alusta riittävä tuki, oikeat resurssit sekä jatkuvuutta. Tämä haastava tavoite toimii kehittämistyön taustalla punaisena lankana. Riskienhallintaa käsittelevää teoreettista ja käytännön tietoa tarvitaan, koska eduskunnan kanslian henkilöstöllä ei tällä hetkellä ole riskienhallinnan osaamista. Ehdotukset eduskunnan kanslian riskienhallinnan käynnistämisestä ja toteuttamisesta on tärkeää organisaation kehittämisen lisäksi oman ammatillisen kehittymisen kannalta.

Kehittämistyön tavoitteenasetteluun ovat osaltaan vaikuttaneet turvallisuusjohtajan kanssa ja turvallisuuden parissa työskentelevien henkilöiden kanssa käydyt keskustelut, eduskunnan kanslian keskijohdon haastattelut ja edellä mainituista esille nousseet organisaatiotason tarpeet. Lisäksi tutkijan opintojen eteneminen ja ammatillisen osaamisen kehittyminen selkeytti tehtävän sisällön painotuksia.

Kuvio seitsemän mallintaa tämän kehittämistyön teoreettista viitekehystä ja avaa kehittämistyön tavoitteiden ja valittujen tutkimusmenetelmien yhteyttä. Kehittämistyön ydin on eduskunnan kanslian turvallisuustoiminnan kehittäminen ja riskienhallinnan soveltamismahdollisuuksien kartoittaminen. Turvallisuuden lisäksi tutkimuksessa käsitellään riskienhallinnan yhteyttä strategiseen johtamiseen.

Organisaatioturvallisuuden kehittämistä koskeviin kysymyksiin haetaan vastauksia tapaustutkimuksen, tulevaisuudentutkimuksen skenaariotyöskentelyn ja konstruktivisen tutkimuksen avulla. Valitut tutkimustyytit tuottavat vastauksia eri kysymyksiin täydentäen ja tukien toinen toisiaan.



Kuvio 7: Kehittämistyön teoreettinen viitekehys ja tutkimustyytit

Kehittämistyön tavoitteet ovat haastavia, mutta niihin liittyvät tiedonintressit voidaan tiivistää seuraaviin konkreettisiin kysymyksiin

- miten eduskunnan kanslian turvallisuustoiminta on tällä hetkellä toteutettu?
- minkälaiset ovat eduskunnan kanslian turvallisuusympäristön haasteet tulevaisuudessa?
- miten tulevaisuuden turvallisuushaasteisiin voidaan vastata?

- riittääkö turvallisuusyksikön nykyinen suorituskyky vastaamaan tulevaisuuden turvallisuushaasteisiin?
- sovelletaanko eduskunnan kansliassa tällä hetkellä riskienhallintaa, onko riskienhallintaa suunniteltu sovellettavan tulevaisuudessa?
- miten riskienhallintaa voidaan toteuttaa eduskunnan kansliassa rakenteellisesti ja sisällöllisesti niin, että sen avulla kehitetään turvallisuutta rasittamatta liikaa organisaatiota?

3.3 Aiheen rajaus

Valittu tutkimusaihe on laaja, mutta turvallisuusyksiköstä saamani toimeksiannon mukainen. Opintojeni edetessä tuli yhä selvemmäksi, että vaikka tavoite sisältää sinänsä vaikeasti saavutettavan asennemuutosvaatimuksen ja eräänlaisen organisaatioturvallisuuden ja riskienhallinta-alan läpileikkauksen, on laajan pohjatyön tekeminen tarpeellista, jotta yksittäisten osalueiden kehittäminen on kestäväällä pohjalla.

Tutkimusaihetta on rajattu näkökulmaa, organisaatorakennetta ja kehittämistyön lopputulosta koskevin valinnoin seuraavasti

- riskienhallintaa tarkastellaan valtionhallinnon ja siihenkin nähden erityispiirteitä omaavan eduskunnan näkökulmasta yksityisen sektorin tutkimustietoa soveltaen
- kehittämistyö koskee (ei-poliittisen) eduskunnan kansliaa
- kehittämistyö koskee eduskunnan kanslian strategisen ja taktisen tason toimintaa; yksityiskohtainen operatiivinen suunnittelu ja toteutus rajataan tehtävän ulkopuolelle
- riskienhallintaa käsitellään organisaatioturvallisuuden näkökulmasta ja riskilajeista taloudelliset riskit jätetään pääosin tarkastelun ulkopuolelle.

4 Tutkimusmenetelmät

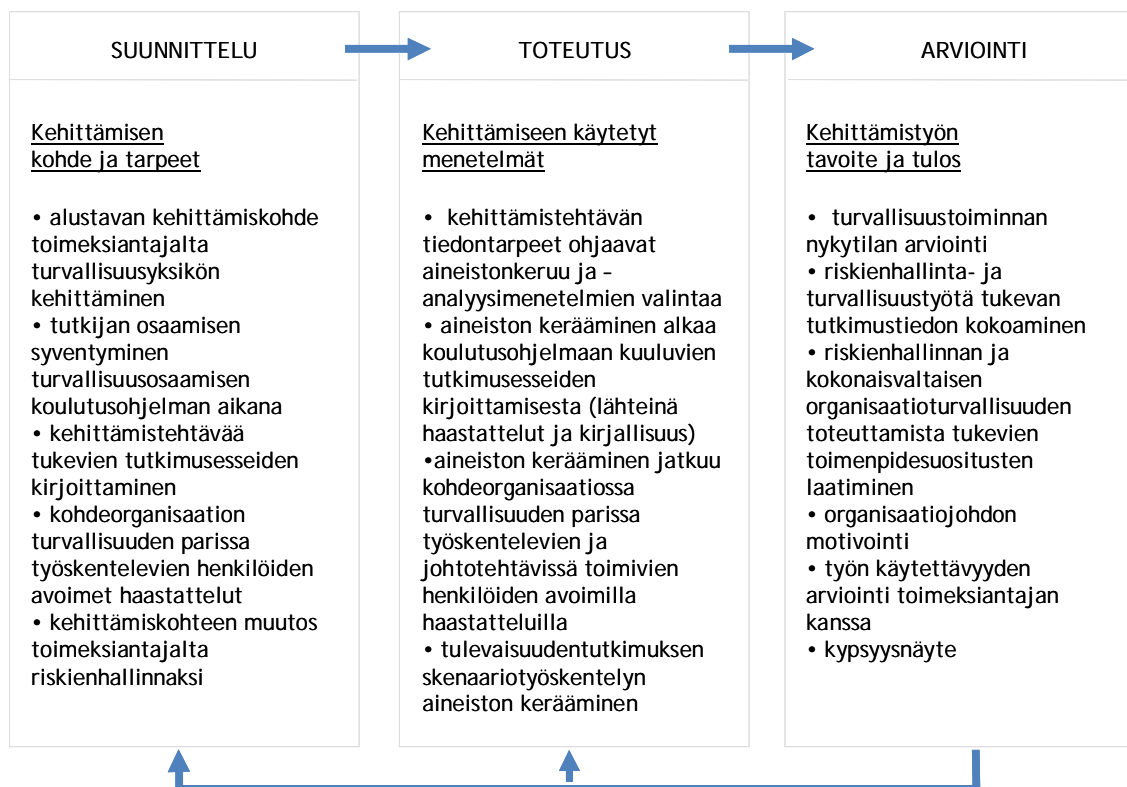
Kehittäminen ja tutkimuksellisuus eivät sulje toisiaan pois, sillä myös kehittämistyössä korostuu tutkimuksellisuus. Tutkimuksellinen kehittämistyö sijoittuukin tieteellisen tutkimuksen ja arkiajatteluun perustuvan kehittämisen väliin. Kehittämistyössä ilmiöiden kuvailun ja selittämisen lisäksi niille etsitään parempia vaihtoehtoja ja asioita viedään eteenpäin myös käytännön tasolla. Tutkimukselliseen kehittämistyöhön kuuluukin uusien ideoiden, käytäntöjen, tuotteiden ja palvelujen tuottaminen ja toteuttaminen sekä käytännön ongelmien ratkaisu. (Ojasalo ym. 2010, 17–19.)

Kehittämistyöhön kulloinkin parhaiten sopiva lähestymistapa riippuu kehittämistyön luonteesta ja tavoitteista. Kehittämistyössä voi myös olla piirteitä useammasta lähestymistavasta. (Ojasalo ym. 2010, 37.) Tämä opinnäytetyö on luonteeltaan tutkimuksellinen kehittämistyö, jossa sovelletaan tapaustutkimusta, tulevaisuudentutkimusta ja konstruktivistista tutkimusta.

Kehittämistyön aineisto on kerätty avoimin haastatteluin, kyselyin, dokumenttianalyysin avulla ja havainnoinnilla. Tutkimusaineiston tulkinta on teoriasidonnaista ja käytetyt analyysimenetelmät pääasiassa laadullisia, kuten sisällön erittely ja dokumenttianalyysi. Määrällisiä analyysimenetelmiä käytetään eurooppalaisen vertailuaineiston ja organisaatioturvallisuuden eri osa-alueiden merkitystä kartoittaneen virkamieskyselyn tulosten analyysissä. Kehittämistyössä yhdistellään luovasti organisaatioturvallisuuden, riskienhallinnan ja strategisen johtamisen teorioita ja kohdeorganisaatiosta kerättyä empiiristä aineistoa.

4.1 Kehittämistyö prosessina

Kehittäminen on aikaa vievää työtä, joka usein etenee selkeiden, toisiaan seuraavien vaiheiden kautta. Kehittämistyötä voidaan tarkastella myös muutostyön prosessina, joka jakautuu suunnittelu-, toteutus- ja arviointivaiheisiin. (Ojasalo ym. 2010, 23.) Tämä opinnäytetyöprosessi on ennen muuta kehittämisprosessi. Muutosprosessikin se on siinä mielessä, että tarkoitus on pohjustaa riskienhallinnan käyttöönottoa eduskunnan kansliassa ja siitä toivottavasti seuraavaa organisaatiotason muutosta.



Kuvio 8: Kehittämistyön prosessi käytännössä Ojasaloa ym. mukailten (2010, 23)

Tämän kehittämistyön vaiheet on konkretisoitu Ojasaloa mukailten kuvioon kahdeksan. Ojasalon ym. mukaan kehittämisprosessin lähtökohta on kehittämiskohteen tunnistaminen ja siihen liittyvien tekijöiden ymmärtäminen. Syvällisen ymmärryksen saavuttaminen voi viedä aikaa, ja lopullinen kehittäminen määritellään ja rajataan usein prosessin jo oltua käynnissä jonkin aikaa. (Ojasalo ym. 2010, 24–25.) Tämän kehittämistyön osalta kehittämiskohde oli tiedossa jo syksyllä 2010, opintojen ollessa vasta alussa. Aihetta muutettiin vuoden vaihteessa 2010–2011, jolloin toimeksiantajan toive oli, että työ koskisi riskienhallintaa. Tutkijan osaamisen ja näkemysten kehittymisen sekä kohdeorganisaatiossa tapahtuneiden riskienhallintaa koskevien tahtotila- ja rakennemuutosten vuoksi oli mahdollista yhdistää alkuperäinen toimeksianto turvallisuusyksikön kehittämisestä uuteen riskienhallintaa käsittelevään toimeksiantoon.

Opinnäytetyöprosessi itsessäänkin sisältää useamman osaprosessin, kuten esimerkiksi kirjoittaminen, aineistonkeruu ja tutkimusaiheen valinta sekä täsmentäminen. Tämän opinnäytetyön osalta kirjoittaminen on osaprosessi, joka alkoi tutkijan turvallisuusosaamisen koulutusohjelman oppimistehtävien myötä syksyn 2010 ja kevään 2011 aikana. Oppimistehtävien aiheet ja tavoitteet valittiinkin tietoisesti tulevaa opinnäytetyötä silmällä pitäen ja nimenomaisella tarkoituksella hyödyntää tekstejä myöhemmin. Tämä oli tärkeää yhtäältä tutkijan varhaisen erikoistumisen kannalta ja toisaalta opinnäytetyön kirjoitusprosessin rasittavuuden

hallinnan kannalta. Kuten Hirsijärvi, Remes ja Sajavaara toteavat usein tapahtuvan, myös tässä työssä kirjoitusprosessin eri vaiheet kiertyivät toisiinsa ja aikaisemmin kirjoitettu materiaali sulautettiin lopulliseen tekstiin (Hirsijärvi, Remes & Sajavaara 2010, 33).

4.1.1 Tapaustutkimus

Tapaustutkimus vastaa kysymyksiin "miten?" ja "miksi?" ja siinä huomioidaan tapaukseen liittyvät paikalliset, ajalliset ja sosiaaliset tilanteet ja yhteydet. Tapaustutkimuksen kohde voi olla yksilö, ihmisryhmä, organisaatio, tapahtuma, toiminto, prosessi tai maantieteellinen alue tai jopa yhdistelmä useampia näistä. Keskeisintä tapaustutkimuksessa on se, että tutkimuskohdetta käsitellään ja se ymmärretään omana ainutlaatuisena kokonaisuutenaan. Kehittämisen kohteen kokonaisvaltainen ymmärtäminen onkin mahdollista erityisesti tapaustutkimusta käytettäessä, sillä se ei pyri ilmiön liialliseen yksinkertaistamiseen tai tilastolliseen yleistämiseen. (Ojasalo ym. 2010, 52–53.)

Tapaustutkimusta on hyvä käyttää silloin, kun tarkoitus on ymmärtää syvällisesti jonkin organisaation tilannetta ja kun tehtävänä on tuottaa tutkimuksen avulla kehittämisehdotuksia tai organisaatiossa ilmenneen ongelman ratkaiseminen. Tapaustutkimus ei vie muutosta eteenpäin käytännössä toimintatutkimuksen tavoin, vaan sen tarkoitus on pikemminkin tuottaa ratkaisuehdotus havaittuun ongelmaan. (Ojasalo ym. 2010, 37–38.)

Tapaustutkimuksen ominaispiirteet näkyvät tässä kehittämistyössä selvästi. Tutkimuksen kohteena on poikkeuksellinen organisaatio ja siinä suoritettavat turvallisuuteen ja riskienhallintaan liittyvät toiminnot. Tavoitteena on lisäksi huomioida aikaan ja sosiaalisiin ulottuvuuksiin liittyvät erityispiirteet, sillä kehittämistehtävän onnistumisen yksi tärkeimmistä mittareista on ehdotettujen ratkaisujen ajankohtaisuus, tulevaisuuden kehityssuuntien relevanttius ja erityisesti kohdeorganisaation henkilöstön näkökulmien huomioiminen kehittämistyössä.

Kehittämistehtävä toteutetaan yksityisestä sektorista saatavilla olevaa tietoa ja kokemusta soveltaen eduskunnan kanslian erityiset tarpeet huomioiden. Kohdeorganisaation ymmärtäminen on tärkeää kehittämistehtävän onnistumisen kannalta, olematta kuitenkaan keskeinen tutkimuskysymys. Tapaustutkimukselle tyypillisesti tässäkin kehittämistehtävässä edetään yhteistyössä eduskunnan kanslian henkilöstön kanssa. Tavoitteena on pohjustaa riskienhallinnan toiminnan aloittamista eduskunnan kansliassa ilman varsinaisten ehdotusten toteuttavaa vaihetta.

4.1.2 Tulevaisuudentutkimus

Tulevaisuudentutkimus on tieteellinen tutkimusala, jolla on sille ominaiset piirteensä ja pätevyysalueensa. Varsinaiseksi tieteenalaksi sitä ei vielä kuitenkaan kutsuta. Tulevaisuudentutkimus erottuu muista tutkimusaloista muun muassa tulevaisuussuuntautuneen tiedonintressin, tutkimusongelmien asettelutavan sekä tutkimusmetodologiansa osalta. Tulevaisuudentutkimus on monitieteellistä, systemaattista ja erilaisin metodein suoritettavaa vaihtoehtoisten tulevaisuusnäkökymien hahmottelua sekä niiden toteutumistodennäköisyyksien ja vaikutusten arviointia. (Vapaavuori 1993, 21.)

Tulevaisuuden tutkijat ovat yhtä mieltä siitä, että tulevaisuutta ei sellaisenaan ole olemassa – on vain lukuisia vaihtoehtoisia kehityssuuntia. Näiden kehityssuuntien toteutuminen ja vaikutukset riippuvat valinnoista, jotka tehdään nykyhetkessä. Vapaavuoren mukaan tulevaisuudentutkimuksen merkitys onkin tulevaisuuden mahdollisuuksien ymmärtämisessä ja aukaisemisessa. Indeterminismi tulevaisuuden tutkimuksessa tarkoittaa, että tulevaisuuden vaihtoehdot eivät vielä ole määräytyneet koettavaksi ja samalla sitä, että nämä vaihtoehdot ovat nykyhetken valintojemme kohteena. (Vapaavuori 1993, 7; Mannermaa 2004.)

Monitieteellinen ja tieteiden välinen tulevaisuudentutkimus pyrkii tiedonalana kuvaamaan, selittämään ja ymmärtämään yhteiskuntaa koskevia laajoja muutos- ja kehitysprosesseja. Tulevaisuudentutkimukseen liittyvä ennakoitintyö tarjoaa yhteiskunnalle ja siinä toimiville yksityisille ja julkisille organisaatioille perustan pitkän aikavälin päätöksenteolle. Tulevaisuudentutkimuksessa tietoa tuotetaan tyypillisesti juuri päätöksenteon tueksi pyrkimyksenä selvittää organisaation tulevaisuuden kannalta mahdolliset, toivottavat, vältettävät tai oletettavat kehityssuunnat. (Ojasalo ym. 2010, 39, 80–82.)

Ennakointiprosessi koostuu tulevaisuutta koskevan tiedon tuottamisesta, hankinnasta, käsitteilystä, muokkauksesta, analysoinnista ja raportoinnista. Ennakointi on luontevaa yhdistää muihin tutkimuksellisiin lähestymistapoihin ja se on tärkeä osa kehittämistyötä. Ennakoinnin avulla voidaan tutkia mahdollisia tulevaisuuksia, todennäköisiä tulevaisuuksia, tulevaisuuskuvia ja mikä parasta – tehdä tulevaisuutta. On siis muistettava, ettei tulevaisuutta ole ennalta määritelty, ennustettu tai etukäteen päätetty. (Ojasalo ym. 2010, 39, 81.)

Tulevaisuuden ennakointi soveltuu hyvin kehittämistöihin ja käytössä on useita erilaisia aineistonkeruumenetelmiä. Tyypillisiä menetelmiä ovat esimerkiksi vaihtoehtoisten tulevaisuuspolkujen etsintä (skenaariotyöskentely), monivaiheinen tarkentuva asiantuntijakysely (myös Delfoi tai Delphi), tulevaisuusverstas ja miellekartta. Kuhunkin kehittämistyöhön parhaiten soveltuvan menetelmän valinnassa on otettava huomioon kohdeorganisaation lisäksi

muun muassa käytössä olevat resurssit ja kehittämiskohteen laajuus. (Ojasalo ym. 2010, 45, 83, 131.)

Tässä opinnäytetyössä sovelletaan tulevaisuudentutkimuksen skenaariotyöskentelyä. Organisaation turvallisuus- ja riskienhallintatoiminta tähtäävät toimintaympäristön muutosten ennakointiin ja niiden vaikutuksen arviointiin. Tulevaisuuden tutkimuksen metodeista erityisesti skenaariotyöskentely tukee erinomaisesti tätä työtä.

4.1.3 Konstruktiivinen tutkimus

Konstruktiivinen tutkimus on lähestymistapa, jolla pyritään muuttamaan organisaation käytänteitä ja toimintaa puolueettoman ja teoreettisen tietämykseen perustuvien ratkaisujen avulla. Konstruktiiviselle tutkimukselle on luonteenomaista tiivis vuoropuhelu käytännön ja teorian välillä. Se tuottaa yleensä jonkin konkreettisen tuotteen, kuten ohjeen, käsikirjan tai mallin. Konstruktiivisen tutkimuksen arvioinnin kannalta on tärkeää, että tuotettu ratkaisu osoittautuu toimivaksi, vaikkakin toimivuuden testaaminen ja tieteellisen lisäarvon osoittaminen vaativat usein lisätyötä. (Ojasalo ym. 2010, 37–38, 65–66.)

Tutkimuksen toteuttajien ja työn tuloksia hyödyntävien välinen kommunikointi on tärkeää konstruktiivisessa tutkimuksessa. Tutkija-kehittäjä on konstruktiivisissa tutkimuksissa aina myös kohdeympäristöönsä voimakkaasti vaikuttava muutosagentti. Lisäksi hän voi toimia oppimisprosessin tukihenkilönä ja oppimisen edistäjänä. (Ojasalo ym. 2010, 66–68.)

Konstruktiivista tutkimusta tässä kehittämistyössä edustavat riskienhallinnan käynnistämistä koskevat ehdotukset. Tutkimustyypille tunnusomainen lopputuote jää tosin toimintasuositusten ja ideoinnin tasolle, yksityiskohtiin meneviä oppaita tai ohjausasiakirjoja ei tuoteta. Ne olisivat uuden kehittämistyön oiva aihe. Myös tässä kehittämistyössä nojataan teorian ja käytännön vahvaan vuoropuheluun. Muutosehdotukset perustellaan turvallisuus- ja riskienhallintatoiminnasta kerätyillä tutkimustiedolla ja käytänteillä.

Tutkijan ja kehitettävän organisaation välinen suhde on tiivis. Eduskunnan kanslian henkilöstön yhteistyö ja haastattelut ovat korvaamattomia yhtäältä kehitettävän kohteen tuntemuksen osalta ja toisaalta kohdeorganisaatiota aidosti palvelevan lopputuloksen kannalta. Tutkijan rooli muutosagenttina on tietoisesti pidetty hienovaraisena. On kuitenkin huomioitava, että tämä kehittämistyö sisältää vaatimuksen asennemuutoksesta. Asenteiden muuttaminen on hidasta ja vaatii tietopohjan laajentamista sekä ajatusten ja mielipiteiden vapaata vaihtoa. Asenteellisen muutosprosessin voidaan katsoa käynnistyneen osittain eduskunnan kansliassa jo syksyllä 2010 tutkijan suorittaessa avoimia haastatteluja kanslian henkilöstölle eri turvallisuuteen ja riskienhallintaan kuuluvien kurssitöiden yhteydessä.

4.2 Kehittämistyössä käytetyt aineistonkeruumenetelmät

Ojasalon ym. mukaan tutkimuksellisessa kehittämistyössä perinteinen valinta laadullisten ja määrällisten aineistonkeruumenetelmien välillä ei ole tarkoituksenmukainen. Keskeistä on pikemminkin menetelmien monipuolisuus; eri menetelmät täydentävät toisiaan uusin näkökulmin ja ideoin ja antavat kehittämistyössä tehtävään päätöksentekoon varmuutta. Edellä esitellyille ja tähän kehittämistyöhön valituille lähestymistavoille on ominaista useiden erilaisten tiedonhankintamenetelmien luova, mutta kuitenkin tarkoituksenmukainen yhdisteleminen. Esimerkiksi haastattelu, kysely ja havainnointi ovat tyypillisiä menetelmiä tapaustutkimuksessa ja konstruktiivisessa tutkimuksessa. (Ojasalo ym. 2010, 38, 40, 68.)

Tässäkin kehittämistyössä on käytetty useampaa erilaista aineistonkeruumenetelmää, jotka esitellään lyhyesti seuraavissa osaluvuissa. Ne ovat pääasiassa laadullisia, mutta laadullinen tutkimus onkin omiaan kuvaamaan ja ymmärtämään ilmiötä tai tapahtumaa ja antamaan sille teoreettisesti mielekkään tulkinnan. Määrällistä menetelmää käytetään ainoastaan virkamiesjohdolle tehdyn kyselyn ja eurooppalaisen vertailuaineiston analyysissä ja niissäkin laadullisen analyysin pohjana. Aineistonkeruuta on sen kaikissa vaiheissa ohjannut kehittämistyöhön liittyvät tiedonintressit.

Laadullisia aineistonkeruumenetelmiä käytettäessä on erityisen tärkeää, että lähteinä toimivat henkilöt tietävät tutkittavasta ilmiöstä mahdollisimman paljon. Näin ollen myös haastattelujen harkittu ja tarkoituksenmukainen valinta korostuu. (Tuomi & Sarajärvi 2002, 87–89.) Ojasalo ym. muistuttavat lisäksi, että kehittämistyössä yhteistyö kohteen kanssa on tärkeää. Tutkijan on tunnettava perusteellisesti tuotoksensa tulevien käyttäjien tarpeet ja käytännössä heidät olisi tärkeä ottaa mukaan kehittämisprosessiin jo sen alkuvaiheessa. (2010, 68.)

4.2.1 Haastattelut ja kyselyt

Eri haastattelutyyppejä edustavat muun muassa strukturoitu haastattelu, puolistrukturoitu haastattelu, teemahaastattelu ja avoin haastattelu. Nimensä mukaisesti teemahaastattelu keskittyy ennalta huolellisesti suunniteltuun teemaan. Kysymysten järjestys, painotus ja sanamuodot voivat sen sijaan vaihdella haastattelusta toiseen. Etukäteen tehdystä suunnittelusta huolimatta tulevien haastattelujen sisältöä on mahdollista tarpeen mukaan muokata jo toteutuneiden haastattelujen perusteella. (Ojasalo ym. 2010, 41.)

Avoin haastattelu on haastattelutyypeistä joustavin muistuttaessaan enemmän keskustelua kuin haastattelua. Avoin haastattelu toimii hyvin esimerkiksi silloin kun tarkoitus on syvästi selvittää ihmisten todellisia ajatuksia tai heidän tiettyä käytöstään. Nopeasti ajateltuna helpolta kuulostava avoin haastattelu on itse asiassa suhteellisen vaativaa, sillä sen menestyk-

sekäs toteuttamiseen edellyttää ajan lisäksi haastattelijan, joka pystyy viemään keskustelua eteenpäin, maltaa kuunnella ja – osaa tulkita kuulemaansa. (Ojasalo ym. 2010, 42.)

Avointa haastattelu on tämän kehittämistyön yksi merkittävimmistä aineistonkeruumenetelmistä. Avoimet haastattelut alkoivat syksyllä 2010 turvallisuusosaamisen koulutusohjelmaan kuuluvien kurssien oppimistehtävien myötä. Oppimistehtävän teemat valittiin niin, että niiden tuloksena syntyneitä tutkielmaesheitä olisi mahdollisuus hyödyntää opinnäytetyössä. Avoimen haastattelun etuja tämän kehittämistyön osalta on useita

- vapautunut keskusteluilmapiiri mahdollistaa virallisen tiedon lisäksi epävirallisen tiedon jakamisen
- avoin keskustelurunko antaa mahdollisuuden keskustelun syvenemiselle ja uusien keskustelunaiheiden ja ideoiden syntymiselle
- luonteva keskustelutilaisuus on omiaan luomaan haastateltavan ja haastattelijan välille henkilökohtaisen suhteen, joka yhtäältä parantaa keskinäistä luottamusta ja toisaalta auttaa haastattelijaa saadun tiedon arvioinnissa
- helposti toteutettava avoin haastattelu mahdollistaa laajan aineiston keräämisen, joka puolestaan lisää tutkijan ymmärrystä tutkittavan aiheen lisäksi myös organisatiokulttuurista ja valtarakenteista.

Myös tässä kehittämistyössä korostuu eduskunnan kanslian henkilöstön osallistaminen kehittämisprosessiin, jotta sen lopputulos palvelisi mahdollisimman hyvin organisaation – käytännössä siis organisaatiossa työskentelevien ihmisten – tarpeita. Haastattelujen kannalta suuri haaste oli se, ettei eduskunnan kanslian henkilöstöllä ole riskienhallinnan osaamista. Tämä seikka otettiin kuitenkin huomioon avoimia haastatteluja valmisteltaessa muun muassa

- sisällyttämällä avoimiin haastatteluihin haastateltavan riskienhallintaan liittyviä tietoja, taitoja ja asenteita koskevia kysymyksiä
- välttämällä riskienhallinnan ammattitermistön liiallista käyttöä
- painottamalla avoimissa haastatteluissa haastateltavan vastualueen asioita
- johtamalla keskustelua teorian sijaan käytännön ilmiöihin sitoen
- välttämällä aktiivisesti konsultin, sanelijan tai opettajan roolia.

Avoimien haastattelujen alussa tuotiin aina selvästi esiin keskustelun aiheen kokonaiskuva, haastattelujen tavoitteet ja kehittämistyön sisältö. Haastattelurunko myötäili koulutusohjelman kurssikohtaisia teemoja, kuten esimerkiksi strateginen johtaminen, vastuullinen johtajuus ja työyhteisön kehittäminen, turvallisuusjohtaminen riskienhallintaprosessissa sekä poikkeustilanteiden hallinta ja kriisiviestintä. Haastattelurunkoon vaikutti kunkin haastateltavan asema, toimenkuva sekä turvallisuuden ja riskienhallinnan osaaminen. Haastattelun ydinkohdat kirjattiin tilaisuuden jälkeen sähköiseen muotoon keskustelun aikana tehtyjen muistiin-

panojen pohjalta. Avoimista haastatteluista saatua tietoa käytettiin opinnäytetyön lisäksi myös kurssitöissä ja molemmissa vastauksia käsiteltiin anonyymisti.

Kysely sopii tilanteisiin, joissa tutkittava aihealue tunnetaan hyvin, mutta tulkintojen ja johdopäätösten paikkansapitävyys halutaan varmistaa. Kysely toteutetaan siten, että sama asia kysytään samalla tavalla isolta joukolta kysymysten ollessa täysin yksiselitteisiä ja helposti vastattavia. Kehittämistyötä ajatellen kysely sopii esimerkiksi lähtötilanteen selvittämiseen tai työn tulosten arviointiin. (Ojasalo ym. 2010, 41.) Tässä kehittämistyössä kyselyä käytetään eduskunnan kanslian turvallisuusympäristön muutoksia käsittelevässä luvussa eurooppalaisen vertailuaineiston keräämiseen ja virkamiesjohdon käsitysten kartoittamiseen organisaatioturvallisuuden eri osa-alueiden tärkeydestä.

Eurooppalainen vertailuaineisto kerättiin eduskunnan sisäisen tietopalvelun välityksellä The European Centre for Parliamentary Research and Documentation (ECPRD) - yhteisön kautta (Liite 3). Määrämuotoinen, riskienhallinnan toteuttamisen perusteita koskeva kysely (Liite 4) lähetettiin kaikkiin eurooppalaisiin parlamentteihin. Ennako-olettamuksena oli, ettei riskienhallintaa sovelleta sen kokonaisvaltaisessa merkityksessä vielä kovin monessa parlamentissa. Toisaalta tietyissä maissa parlamentin turvallisuustoiminta ja riskienhallinta voivat olla myös varsin pitkälle vietyä. Kyselyn tuloksia käsitellään tarkemmin osaluvussa 5.3.

Virkamiesjohdon näkemykset organisaatioturvallisuuden eri osa-alueiden merkityksestä ovat tärkeitä kehittämistyön kannalta yhtäältä täydentävänä ja toisaalta vertailuaineistona. Virkamiesjohdolle suunnatussa kyselyssä pyydettiin määrittelemään oman yksikön kannalta kolme tärkeintä organisaatioturvallisuuden osa-aluetta ja koko eduskunnan kanslian kannalta kolme eniten kehittämistä kaipaavaa organisaatioturvallisuuden osa-aluetta (Liite 1). Kyselyn tuloksia käsitellään tarkemmin osaluvussa 5.1.2.

4.2.2 Havainnointi ja dokumenttianalyysi

Ojasalo ym. suosittelevat havainnointia kaikenlaiseen kehittämistyöhön. Kehitettävää ilmiötä koskeviin haastatteluihin ja kyselyihin verrattuna havainnoinnin avulla on helpompi saada hyödyllistä tietoa todellisista tapahtumista tarkkaillen. Havainnoitsijan valinnaksi jää, seuraako hän tilanteita ulkopuolisena vai osallistuuko itse toimintaan tehden samalla havaintoja. (2010, 42.)

Havainnointia sisältyy tämän kehittämistyön kaikkiin aineistonkeruun menetelmiin ja vaiheisiin. Osa aineiston tulkintaan vaikuttavista havainnoista ovat peräisin jo syksyltä 2009, aikaan ennen tutkijan turvallisuusosaamisen opintojen alkua. Havainnointi on tapahtunut sekä ulkopuolisen, että osallistujan asemasta – ulkopuolisena turvallisuusyksikköön nähden ja osallistu-

jana eduskunnan kanslian näkökulmasta. Havainnointi mahdollistaa aineiston lähteiden ja saadun tiedon arvioinnin sekä organisaation erityispiirteiden esilletulon.

Eduskunnan kansliaan liittyvää havainnointia on tapahtunut myös itse organisaation ulkopuolella. Oppilaitoksessa, mediassa ja muissa yhteyksissä kolmansien osapuolien kanssa käydyt keskustelut heijastavat eduskuntaan yleisesti, mutta myös sen turvallisuuteen liittyviä asenteita, tietoa ja odotuksia. Tämän kaltaista spontaania havainnointia on haastavaa raportoida. Kaikkea havaintoja on kuitenkin käytetty hyväksi erityisesti riskienhallinnan toteuttamishetkiä käsittelevässä luvussa, jossa kohdeorganisaatiota pyritään käsittelemään mahdollisimman kokonaisvaltaisesti ja realistisesti.

Dokumenttianalyysin kohteita voivat olla esimerkiksi muistiot, projektiraportit, pöytäkirjat, tiedotteet, käsikirjat, www-sivut, vuosikertomukset, budjetit, tilastot, selvitykset ja rekisterit. Sitä käytetään yleensä muihin tiedonkeruumenetelmiin yhdistettynä tuomaan lisänäkökulmaa kehitettävään kohteeseen. Dokumenttianalyysiin liittyvä haaste on se, että joidenkin kehittämistyön kannalta hyödyllisten dokumenttien olemassa olo ei aina tule tutkijan tietoon tai sitten niitä ei saada käyttöön esimerkiksi tietoturvaluokituksiin liittyvistä syistä. Tutkijan on muistettava kriittisyys; kunkin dokumentin kohdalla on syytä pohtia, mihin tarkoitukseen ne on laadittu ja kenen laatimia ne ovat. (Ojasalo ym. 2010, 43.)

Tässä kehittämistyössä dokumenttianalyysiä on käytetty haastatteluin, kyselyin saadun tiedon ja kerätyn tutkimustiedon täydentämiseksi. Opinnäytetyön julkisuuden takia turvallisuus ja riskienhallinta ovat aiheina haastavia ja niin myös tämän kehittämistyön osalta osa eduskunnan kanslian turvallisuuden liittyvistä sisäisistä dokumenteista jäi tutkimuksen ulkopuolelle. Dokumenttianalyysi kohdistetaan ensisijaisesti eduskunnan kanslian sisäisiin asiakirjoihin – tehtyihin päätöksiin ja ohjeisiin sekä organisaatiossa aikaisemmin turvallisuuden ja riskienhallinnan parissa tehtyyn työhön. Lähdeaineisto täydentämään valikoituivat muun muassa seuraavat dokumentit

- eduskunnan kanslian strategialuonnoksia syksyltä 2010 ja keväältä 2011
- eduskunnan kanslian toiminta- ja taloussuunnitelmat ja niihin liittyvä muut asiakirjat
- eduskunnan kanslian toimintakertomukset
- henkilöstötilastot
- valtioneuvoston ja valtionvarainministeriön päätökset, suositukset ja pöytäkirjat
- ECPRD:n kautta lähetettyyn kyselyyn saadut kirjalliset vastaukset.

Kehittämistyössä käytetyt dokumentit eivät itsessään olleet syvällisen analyysin kohteena. Niitä käytettiin lähteinä kehittämistyön eri vaiheissa ja niiden sisältämä tieto prosessoitiin yhdessä muista lähteistä saatujen tietojen rinnalla kulloinkin käsitellyssä olevan aihealueen

yhteydessä. Dokumenttianalyysin asiakirjoihin yksityiskohtaisesti pureutuva puoli jäi näin ollen tässä kehittämistyössä toteutumatta, pois lukien lähdekritiikki.

4.2.3 Parhaat käytänteet

Kehittämistyötä voidaan tehdä vertaamalla omaa kehittämiskohdetta johonkin toiseen vastaavaan, usein niin sanottuun parhaaseen käytäntöön (benchmarking). Vertauskohteita ei kuitenkaan ole tarkoitus ottaa käyttöön sellaisenaan, vaan niitä tulee soveltaa omaan organisaation tarpeiden mukaan. (Ojasalo ym. 2010, 43.)

The European Centre for Parliamentary Research and Documentation (ECPRD) - yhteisön kautta saatujen vastausten perusteella voidaan tehdä karkea arvio riskienhallinnan kokonaisvaltaisen toteuttamisen yleisyydestä eurooppalaisissa parlamenteissa. Kyselyn tavoitteena on löytää vastanneiden joukosta parlamentteja, joissa riskienhallinta on pidemmälle vietyä ja joiden toiminnasta olisi mahdollista ottaa mallia. Konkreettisten parhaiden käytänteiden kerääminen ja niiden käytännön hyödyntäminen olisi kuitenkin erillisen tutkimuksen aihe.

Kuten Ojasalokin toteaa, on parhaiden käytänteiden hyödyntämisessä oltava tarkkana. Riskienhallinnan ja turvallisuustoiminnan suunnittelu ja toteuttaminen tulisi aina olla organisaatiokohtaista. Vaikka eri maiden parlamenttien toiminta-ajatus saattaa olla samankaltainen, ovat niiden toimintaympäristö, turvallisuusympäristö ja sisäinen dynamiikka toisistaan poikkeavia. Riskienhallinnan ja turvallisuuden kehittämistä koskeva ajattelutyö, suunnitteluvaihe ja päätöksenteko tulisi tehdä organisaatiossa itsessään, muuten tehtyjen päätösten oikeellisuus ja käynnistettävien prosessien toimivuus voi jäädä vähäiseksi. Riskienhallinnan ja turvallisuuden kestävä toteuttaminen riippuvat henkilöstön osallistumisesta ja sitoutumisesta. Näin ollen valmiin mallin istuttaminen ilman organisaatiokohtaista soveltamista tuottaa todennäköisesti tavoitteisiin nähden päinvastaisen tuloksen.

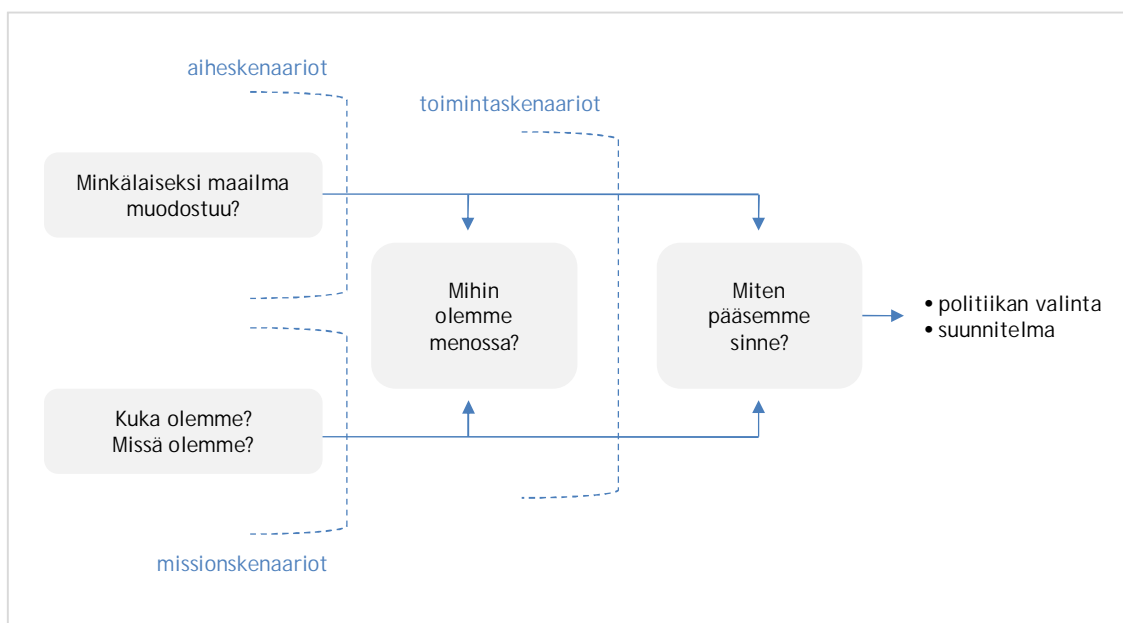
4.2.4 Skenaariotyöskentely

Ojasalo määrittelee skenaariot ajallisesti toisiaan seuraaviksi ja perusteltavissa olevien tulevaisuuskuvien sarjaksi, joiden tarkoitus on toivottavan tulevaisuuden saavuttaminen. Skenaarioiden avulla voidaan lisäksi hahmotella erilaisten päätösten ja valintojen seuraamuksia tapahtumien kehityksen suhteen. (Ojasalo ym. 2010, 132.)

Vapavuoren mukaan skenaario on oletuksiin perustuva tulevaisuudenkuva, joka luonnostelee kokonaisvaltaisesti ja moniulotteisesti organisaation tulevaisuuden toimintaympäristön sekä kuvaa kehityspolun nykyisestä tulevaisuuteen. Skenaariot auttavat kuvittelemaan, mikä on

mahdollista ja toisaalta analysoimaan, mikä on todennäköistä. Lisäksi skenaariot toimivat perustana valittaessa haluttavaa ja toteutettavaa tulevaisuutta. (Vapaavuori 1993, 215–216.)

Skenaariotyöskentely sopii hyvin organisaation strategisen suunnittelun tueksi, sillä sen avulla organisaatio voi saada tietoa mahdollisista maailmoista ja toimintaympäristöstä (aiheskenaariot), organisaation reaalista tilasta (mission-skenaariot) ja siitä, mihin suuntaan organisaatio voi kehittyä ja miten (toimintaskenaariot). Aiheskenaarioiden teemat ovat tyypillisesti yhteisiä organisaation useammalle yksikölle ja skenaariot voivat toimia yksikötason päätöksenteon tukena tai taustatietoina yksikötason skenaarioille (Meristö 1991, 31–32, 37). Eri skenaariotyöskentelyjen sijoittumista organisaation strategisen suunnittelun prosessiin on kuvattu Meristöä (1991, 38) mukaillen kuviossa yhdeksän.



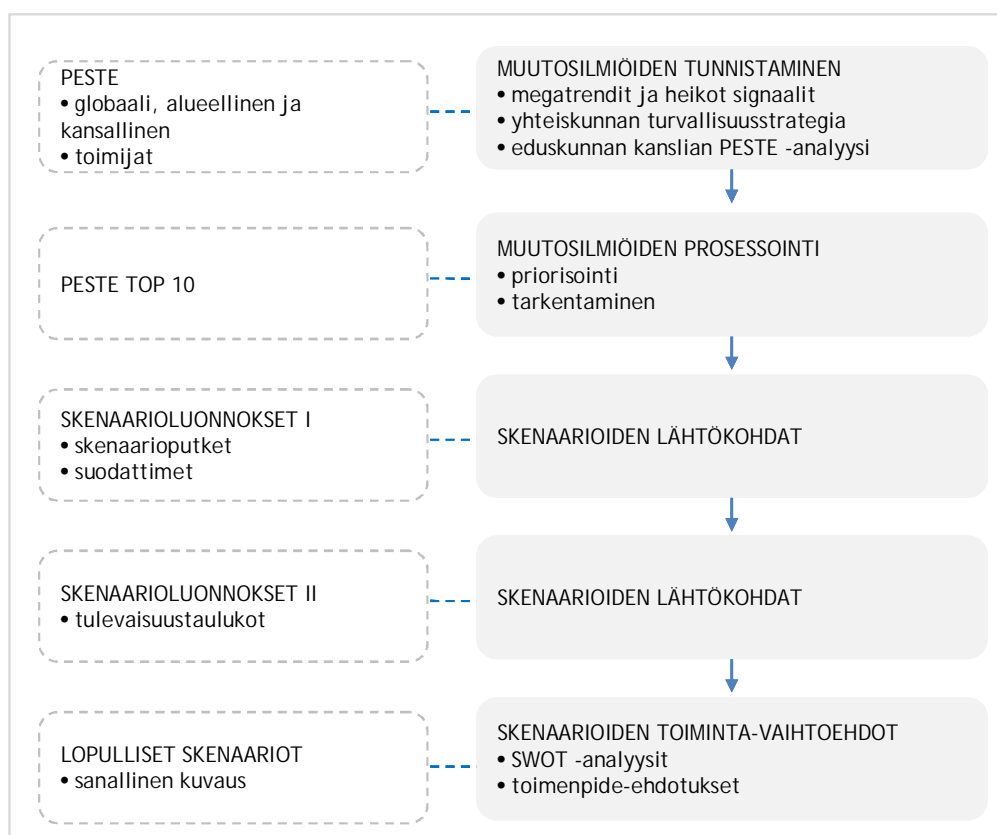
Kuvio 9: Skenaariotyöskentely ja strateginen suunnitteluprosessi (Meristö 2011, 38)

Skenaariot eivät ole ennusteita, vaan kuvauksia mahdollisista ja vaihtoehtoisista kehityssuunnista. Ennusteen ja skenaarion eroja voidaan havainnollistaa taulukon neljä mukaisin vertauksin (Ojasalo ym. 2010, 132; Schoemaker 1983, Meristö 1991, 42 mukaan; Schwartz 1991).

ENNUSTE	SKENAARIO
<ul style="list-style-type: none"> • tilastollinen yhteenveto asiantuntijoilta kerätyistä mielipiteistä • ei nimeä epävarmuuden syitä ja lähteitä 	<ul style="list-style-type: none"> • sanallinen kuvaus mahdollisista tulevaisuuden kehityskuluista • kiinnittää huomiota avainmuuttujiin ja -suhteisiin
<ul style="list-style-type: none"> • tehokas, mutta informatiivisesti ohuempi asiantuntemuksen yhteenveto • käytettävissä suoraan päätöksentekoprosessiin 	<ul style="list-style-type: none"> • paljon informaatiota sisältävä, mutta toisaalta tehoton yhteenveto • vaatii lisäharkintaa ja tulkintaa
<ul style="list-style-type: none"> • ennusteen tarkkuus voidaan mitata pitkällä aikavälillä 	<ul style="list-style-type: none"> • vaikeasti mitattava, toimii ennen muuta ajattelun työkaluna
<ul style="list-style-type: none"> • perustuu olettamukseen, jonka mukaan tulevaisuuden ennustaminen on hyödyllistä ja mahdollista 	<ul style="list-style-type: none"> • perustuu olettamukseen, jonka mukaan tulevaisuutta ei voida ennustaa tai niin on vaarallista tehdä

Taulukko 4: Ennusteen ja skenaarion ero Schoemakeria mukaillen (Meristö 1991, 42)

Tässä opinnäytetyössä tulevaisuudentutkimusta toteutetaan eduskunnan kanslian turvallisuusympäristöä käsittelevissä aiheskenaarioissa. Aiheskenaariotyöskentelyä lähestytään eksploraatiivisesti, jolloin nykyhetkessä esiintyvien eduskunnan kanslian turvallisuusympäristön ilmiöiden tarkastelun ja yhdistelyn avulla pyritään rakentamaan mahdollisia tulevaisuuksia ajassa eteenpäin (Meristö 1991, 42).



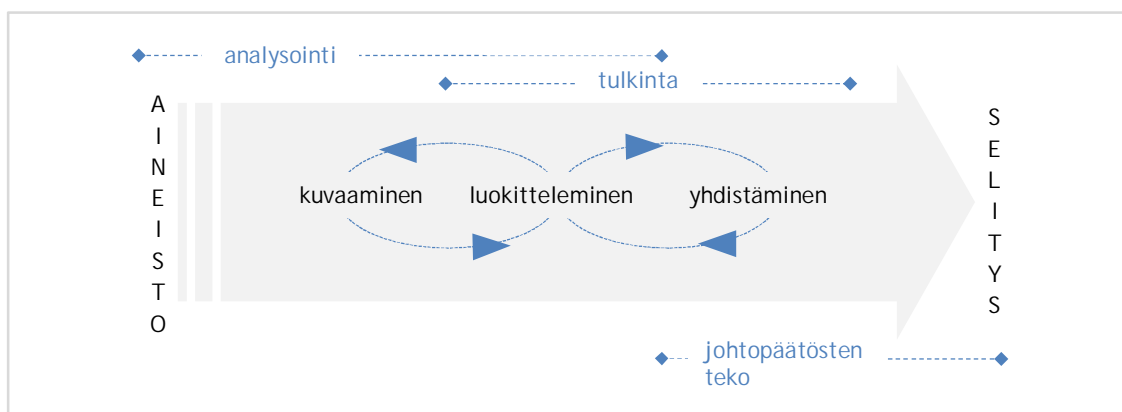
Kuvio 10: Skenaariotyöskentelyn vaiheet Meristöä ja Tammea mukaillen (2003, 12)

Skenaariotyöskentelyn vaiheet on hahmoteltu Meristöä ja Tammea mukaillen kuviossa 10. Tausta-aineiston kerääminen ja käsittely muodostavat lähtökohdat eri skenaarioille, joita tarkennetaan tulevaisuustaulukoinnin keinoin. Lopulliset skenaariot esitetään sanallisessa muodossa. (Meristö & Tammi 2003, 12.) Skenaarioita käsitellään yksityiskohtaisemmin osaluvussa 5.2.

4.3 Aineiston analysointi

Tutkimusaineiston analyysimenetelmät voidaan jaotella määrällisiin ja laadullisiin analyysitekniikoihin. Laadullisia menetelmiä ovat teemoittelu, tyypittely, sisällönerittely, diskursiivinen analyysi ja keskusteluanalyysi (Eskola & Suoranta 2000, 160). Karkeasti yleistettynä voidaan sanoa, että määrällinen analyysi pyrkii selittämään tutkittavaa ilmiötä ja laadullinen analyysi puolestaan pyrkii kohteen ymmärtämiseen (Hirsjärvi 2010, 224).

Hirsjärvi ym. mukaan aineiston analyysi, tulkinta ja johtopäätösten teko ovat tutkimuksen ydin. Erityisesti laadullisessa tutkimuksessa analyysiä suoritetaan pitkän tutkimusprosessin etenemistä kun taas analyysin aloittaminen vasta aineistonkeruuvaiheen jälkeen soveltuu paremmin määrällisiin tutkimuksiin. (2010, 223.) Hirsjärven ym. korostamat tutkimuksen ydinasiat ja aineiston analyysin vaihteisuus ja syklisyys on yhdistetty kuviossa 11.



Kuvio 11: Aineiston analysointiprosessi Ojasalo ym. mukaillen (2010, 223–224)

Analyysimenetelmät voidaan luokitella myös aineistolähtöisiksi, teorialähtöisiksi tai teoriasidonnaisiksi riippuen siitä, millainen suhde niillä on tutkimuksen tai kehittämistyön teoriaan. Nimensä mukaisesti teoriasidonnaisessa analyysissä on tiettyjä teoreettisia kytkentöjä, jotka eivät kuitenkaan suoraan pohjaudu teoriaan. Teoria toimii apuna analyysin etenemisessä ja aikaisemman tiedon vaikutus on tunnistettavissa analyysissä. Sen merkitys on kuitenkin ennen muuta uusia ajatuksia synnyttävä. Teoriasidonnaisessa analyysissä vaihtelevat aineistolähtöisyys ja valmiit mallit, joita tutkija sitten yhdistelee. (Tuomi & Sarajärvi 2002, 97–99.)

Tässä kehittämistyössä käytetyt aineistonkeruumenetelmät ovat avoin haastattelu, kysely, havainnointi, dokumenttianalyysi, parhaat käytänteet ja skenaariotyöskentely. Määrällisiä analyysimenetelmiä sovelletaan kansainväliseen vertailuaineistoon ja organisaatioturvallisuutta koskevaan virkamieskyselyyn. Niiden osalta avointen vastausten sisällön erittely on kuitenkin suuremmissa roolissa ja myös kehittämistyön tavoitteiden kannalta tarkoituksenmukaisempaa. Aineiston analysointi on teorialähtöistä; aineiston sisällön erittely suoritettiin organisaatioturvallisuuden, strategisen johtamisen ja riskienhallinnan teoriaan sitoen.

Avoimien haastattelujen aineisto analysointiin sisällönerittelyllä, jonka avulla pyrittiin selvittämään haastateltavien

- asenteita riskienhallintaa kohtaan
- turvallisuuteen ja riskienhallintaan liittyvää tieto-, ja taitotasoa
- suhtautumista riskienhallintatoiminnan käynnistämiseen eduskunnan kansliassa
- näkemyksiä ja ideoita eduskunnan turvallisuustoiminnan kehittämiseksi.

Tutkimusstrategisilla valinnoilla mahdollistetaan haluttuun lopputulokseen pääseminen. Kehittämistyössä onnistumisen kannalta on tärkeää, että kehittämistyön kohteet, tarpeet ja -keinot valitaan tarkoituksenmukaisesti. Nämä valinnat ovat lisäksi toisistaan riippuvaisia ja toisiaan tukevia, eikä kokonaisuus ole johdonmukainen, mikäli yksi osa-alueista on epäjohdonmukainen toisiin verrattuna. Eduskunnan kanslian riskienhallintatoiminnan kehittämisen kannalta tämä tarkoittaa muun muassa sitä, että

- vältetään sellaisten turvallisuuden ja riskienhallinnan osa-alueiden painottamista, jotka eivät ole eduskunnan kanslian toiminnan kannalta oleellisimpia ja joihin keskittyminen aiheuttaisi riskienhallintatoiminnan käynnistämisen osalta tarpeetonta tietotaitoon ja resursseihin liittyvää painetta
- pyritään esittämään sellaisia toimenpide-ehdotuksia, joihin eduskunnan kanslian henkilöstön on mahdollista ja realistista sitoutua
- vältetään liiallista yleistämistä ja valmiiden mallien kritiikitöntä soveltamista; eduskunnan kanslian erityispiirteet ohjaavat kehittämistyötä sen kaikissa vaiheissa.

Tutkimusstrategisia valintoja on hyvä tarkastella suhteutettuna varsinaiseen kehittämistyöhön (Taulukko 5) jo työn alkuvaiheessa, jotta tehtyjen valintojen tarkoituksenmukaisuutta voidaan paremmin arvioida. Tutkimusstrategisten valintojen kokonaisuus on tärkeää hahmottaa, jotta tutkimuksen perusteen luovia tutkimusstrategisia valintoja ei olisi työn jo edettyä pidemmälle tarvetta radikaalisti muuttaa.

Tutkimusstrategiset valinnat	Kehittämiskohteet: erittely-määrittely	Kehittämistarpeet: kartoitus-perustelu	Kehittämiskeinot: arviointi-valinta
tapaustutkimus	x	x	x
tulevaisuudentutkimus		x	x
konstrukt. tutkimus			x
skenaariotyöskentely	x	x	
haastattelu	x	x	x
kysely			x
havainnointi	x		x
dokumenttianalyysi	x	x	
parhaat käytänteet			x
aineiston analyysi		x	x
käsitteiden määrittely	x		x

Taulukko 5: Tutkimusstrategiset valinnat ja kehittämistyön sisältövaatimukset

5 Tutkimuksen tulokset

Tämän kehittämistyön tavoitteena on siis edesauttaa ja vauhdittaa riskienhallintatoiminnan käynnistämistä eduskunnan kansliassa. Osatavoitteita puolestaan ovat

- eduskunnan ylimmän virkamies- ja poliittisen johdon motivoiminen sitoutumaan pitkäjänteiseen ja systematisoituun riskienhallintaan
- riskienhallinnan tarpeellisuutta ja toteuttamista koskevan teoreettisen ja vertailuaineiston perustuvan tiedon kokoaminen turvallisuusyksikön käyttöön
- perustellun ehdotuksen tuottaminen siitä, miten riskienhallinta olisi mahdollista käynnistää ja toteuttaa eduskunnan kansliassa.

Kehittämistyön tavoitteiden toteutumista tukevia kysymyksiä ovat

- miten eduskunnan kanslian turvallisuustoiminta on tällä hetkellä toteutettu?
- minkälaiset ovat eduskunnan kanslian turvallisuusympäristön haasteet tulevaisuudessa?
- riittääkö turvallisuusyksikön suorituskyky vastaamaan tulevaisuuden turvallisuushaasteisiin?
- miten tulevaisuuden turvallisuushaasteisiin voidaan vastata?
- sovelletaanko eduskunnan kansliassa riskienhallintaa, onko riskienhallintaa suunniteltu sovellettavan tulevaisuudessa?
- miten riskienhallintaa voidaan toteuttaa eduskunnan kansliassa rakenteellisesti ja sisällöllisesti niin, että sen avulla turvallisuutta voidaan kehittää rasittamatta organisaatiota?

Tässä luvussa käsitellään tutkimuksen tuloksia. Riskienhallintatoiminnan käynnistämistä eduskunnan kansliassa käsitellään luvussa seitsemän.

5.1 Eduskunnan kanslian riskienhallinnan nykytila

Eduskunnan kansliassa ei tällä hetkellä sovelleta koko organisaatiotason riskienhallintaa vaan riskienhallinnallisia toimenpiteitä tekevät eduskunnan kanslian turvallisuusyksikkö, sisäinen tarkastus ja erityisesti teknisestä tietoturvallisuudesta vastaava henkilöstö. Eduskunnan riskienhallinnasta ei ole laadittu strategiaa tai politiikkaa. Riskienhallinnan vastuisiin ja sisältöön ottavat kuitenkin kantaa eduskunnan kanslian ohjesäännön sisäistä tarkastusta käsittelevä osio, vuosittain laadittavat Toiminta- ja taloussuunnitelmat (TTS) sekä muun muassa turvallisuusyksikön toimintaa käsittelevä Schroderuksen (2008) lopputyö.

Eduskunnan turvallisuusyksikön toiminta käynnistyi Schroderuksen läpi viemän toimintatutkimuksen myötä vuonna 2005. Vuonna 2008 valmistuneen, turvallisuusasioita käsitelleen työ-

ryhmän loppuraportin mukaan eduskunnan kanslian riskienhallintapäällikön tehtävät kuuluvat turvallisuusjohtajalle. Eduskunnan kanslian ohjesäännössä ei riskienhallintaa mainita lainkaan, vaikkakin esimerkiksi esimiestehtävässä toimivien osalta korostetaan toiminnan kehittämistä ja ajan hermoilla pysymisen tavoitetta (Eduskunnan kanslian ohjesääntö, 19 §).

Syksyn 2010 ja kevään 2011 aikana toteutettuihin avoimiin haastatteluihin osallistui henkilöstöä keskuskansliaa lukuun ottamatta kaikista eduskunnan kanslian yksiköistä sekä sisäinen tarkastus. Haastatteluissa käytiin läpi haastateltavien mielikuvia ja tietämystä riskienhallinnasta, eduskunnan kanslian näkökulmaa riskienhallintaan, yksikötason tarpeita tai kehittämisehdotuksia riskienhallintatoiminnalle sekä tulevan opinnäytetyön tavoitteita.

Yleisenä havaintona voidaan todeta, että vaikka haastateltavien käsitykset riskienhallinnan mahdollisuuksista ovatkin vaihtelevia, on suhtautuminen riskienhallinnan kehittämiseen keskimääriin positiivista. Muutamassa yksikössä on jopa jonkin aikaa kaivattu riskienhallinnan ohjausta ja toimenpiteitä muun muassa toiminnan jatkuvuussuunnitteluun liittyen. Riskienhallinnan puutetta pidettiin ylimmän virkamiesjohdon sekä tiedostamattomana että tietoisena päätöksenä ja jopa laiminlyöntinä.

Johdon näkemyksiä riskienhallinnasta on kartoitettu aikaisemminkin. Sisäinen tarkastus toteutti vuonna 2008 eduskunnan kanslian yksiköiden johdolle suunnatun haastattelun, jonka tuloksien pohjalta laadittiin katsaus kanslian ”inhimillisiin, toiminnallisiin, taloudellisiin ja vahinkoriskeihin”. Johtajat nostivat jo tuolloin esiin organisaatioturvallisuuteen liittyviä asioita, joista he kantoivat huolta

- lainsäädäntötyöhön liittyvien asiakirjojen laadintaan, jakeluun ja arkistointiin liittyvä tietoliikenneyhteyksien varmuus ja häiriöttömyys
- henkilöstön riittävyys, organisaation haavoittuvuus poissaolojen suhteen
- hiljaisen tiedon katoaminen
- johtamisen, esimiestyön ja valvonnan kehittäminen
- salityöskentelyyn liittyvä vierailijoiden tarkastus, häiriköinnin estäminen
- eduskuntarakennuksessa työskenteleviin kohdistuvat uhkat ja vaarat
- matkustamiseen liittyvät vaarat ja uhkat, vahinkoriskit ja rikosturvallisuus
- ATK-järjestelmän infrastruktuurin ikä ja toimintavarmuus
- tietomurto, tietovuoto tai tietojärjestelmiin tunkeutuminen
- turvaluokitellun aineiston käsittely
- erityistilanteiden ja poikkeus- ja kriisiolojen hallinta, kriisiviestintä
- yleinen tilannekuva eduskunnan kansliaan kohdistuvista riskeistä, terrorismi. (Eduskunnan kanslia 2008c.)

Hallinnon kehittämiseen liittyen ehdotettiin myös, että riskienhallinta otettaisiin osaksi yksiköiden hallinnollista työtä esimerkiksi hankinnoissa tai ulkopuolisten hankkeiden ja sopimusten osalta. Lisäksi korostettiin ulkopuolisten konsulttien käytön vaaroja viitaten aikaisemmin toteutettuihin tai käynnissä olevien organisaatiomuutosten osalta. (Eduskunnan kanslia 2008c.) Edellä mainitut sisäisen tarkastuksen kyselyn poiminnat antavat ymmärtää, että eduskunnan kanslian keskijohto olisi valmis osallistumaan käytännön riskienhallintatyöhön oman yksikkönsä osalta ja myös osana koko organisaation riskienhallintaa. Tämä edellyttäisi kuitenkin sitä, että riskienhallintatoimet suunnitellaan sujuvaksi, eduskunnan kanslian organisaatioon ja arkeen hyvin istuva.

5.1.1 Eduskunnan kanslian strategia ja arvot

Eduskunnan strategiatyössä alkoi uusi vaihe vuonna 2007, kun kansliatoimikunta käynnisti syksyllä 2007 eduskunnan kanslian toiminnan kehittämishankkeen (HALKE 2010). Hankkeen tavoitteita olivat muun muassa johtamisen sekä esimies- ja päätöksentekovastuiden selkeyttäminen, läpinäkyvyyden lisääminen, toiminnan tehostaminen, laadun kehittäminen, palveluprosessien kustannustehokkuuden lisääminen, suunnittelu- ja raportointijärjestelmien kehittäminen sekä henkilöstösuunnittelun ja osaamisen kehittäminen. (Eduskunnan kanslia 2008b, 28–29.) Halke-2010:n jalkautus ei haastateltujen mukaan kuitenkaan onnistunut. Syinä tähän olivat muun muassa ehdotettujen ratkaisumallien sopimattomuus eduskunnan kanslian toimintaan sekä tiukka toteutusaikataulu; muutokset tuntuivat osasta virkamieskuntaa pakotetuilta, yllättäviltä ja heikosti perustelluilta.

Eduskunnan kanslian strategiaa ja sen toteutusta käsittelevät eduskunnan kanslian strategia sekä eduskunnan kanslian Toiminta- ja Taloussuunnitelma (myöhemmin TTS). TTS perustuu eduskunnan kanslian strategisiin tavoitteisiin ja linjauksiin ja määrittelee käytännön toimet sekä vastuunjaon tahtotilan saavuttamiseksi aina vuosi kerrallaan. Eduskunnan kanslian osastot ja yksiköt suunnittelevat oman toimintansa niin, että ne tukevat koko kanslian strategisten tavoitteiden saavuttamista (Eduskunnan kanslia 2008a, luku 4).

TTS viittaa strategian lisäksi eduskunnan tilisäännön (21.11.2006/1064) neljänteen pykälään ja sen laadintaa koordinoi eduskunnan kanslian tilitoimisto. (Eduskunnan kanslia 2008a, luku 1., luku 3). Päivitetty strategia koskee vuosia 2011–2014 ja sen pohjalta laadittava TTS 2012 on neljäs laatuaan.

Strateginen uudistustyö eduskunnan kansliassa on ollut käynnissä reilun vuoden ajan. Uudistusprosessin aikana esitetyt luonnokset olivat lausuntokierroksella kanslian yksiköissä. Yksiköiltä saatu palaute aiheutti luonnokseen muutoksia. Kanslian uusi strategia vuosille 2012–2015 on nyt hyväksytty kanslian johtoryhmässä. Strategiaan kirjattu eduskunnan kanslian visio

on "tuottaa edustuksellisen kansanvallan tarvitsemat palvelut laadukkaasti, tehokkaasti ja taloudellisesti." Eduskunnan kanslian strategiset päämäärät näin ollen ovat

- eduskunnan valtiosääntöisen toiminnan ylläpitäminen ja kehittäminen
- infrastruktuurin kehittäminen
- johtamisen sekä suunnittelu- ja raportointijärjestelmän kehittäminen
- eduskunnan kanslia on oppiva, osallistuva ja hyvinvoiva työyhteisö. (Eduskunnan kanslia 2011a.)

Valtionhallinnon arvoperustan muodostavat toiminnan tuloksellisuus, luottamus, tasa-arvo, puolueettomuus, riippumattomuus, vastuullisuus, palveluperiaate, avoimuus sekä laatu ja vahva asiantuntemus. Valtion henkilöstöpolitiikan mukaan tuloksellisuudelle ja palvelukyvyille luodaan edellytykset muun muassa hyvällä työnantaja- ja henkilöstöpolitiikalla sekä hyvällä johtamisella. (Valtioneuvosto 2001, 3–4.)

Eduskunnan kanslian arvoiksi oli ennen uudistusta kirjattu demokratian tukeminen, luotettava ja palveluhenkinen hallinto sekä oikeudenmukainen johtaminen. Syksyllä 2011 vahvistetut kanslian arvot ovat hyvä palvelu, avoimuus ja vuorovaikutteisuus sekä oikeudenmukaisuus. Keskusteluun kuului prosessin aikana myös arvot ammattitaito ja tehokkuus, mutta ne jäivät lopulta pois. Uudet arvot peilaavat kohtuullisen hyvin valtioneuvoston periaatepäätökseen vuonna 2001 kirjaamaa valtionhallinnon arvoperustaa (Taulukko 5).

Vuorovaikutteisuus ja oikeudenmukaisuus eivät suoranaisesti sisälly valtioneuvoston kirjaamiin valtionhallinnon arvoihin, mutta oikeudenmukaisuuden tavoitteen voidaan osaltaan katsoa sisältyvän valtionhallinnon arvoihin luottamus, tasa-arvo, puolueettomuus, riippumattomuus ja vastuullisuus.

Eduskunnan kanslian vahvistettuja arvoja on hyvä tarkastella myös riskienhallinnan näkökulmasta. Syyskuussa 2011 julkaistussa työtyytyväisyyskyselyssä nousi esiin henkilöstön kokemaa ristiriitaa sovittujen arvojen ja käytännön toiminnan välillä. Lisäksi arvo- ja strategiakeskustelussa esiintyvä palvelupainotteisuus on herättänyt paljon keskustelua eduskunnan kanslian henkilöstön keskuudessa. Arvotyön ja strategian laatimisprosessin laatu näkyy suoraan henkilöstön sitoutumisessa niiden käytännön toteutukseen. Arvojen vaikutukset näkyvät kuitenkin vasta pidemmällä aikavälillä ja edellytyksenä on arvojen johdonmukainen jalkauttaminen eduskunnan kanslian arkeen, erityisesti päätöksentekoon ja johtamiseen.

Riskienhallintatyö osallistuu organisaation arvotyöskentelyyn, sillä sen tehtävänä on toiminnan seurannan ja analysoinnin lisäksi esittää parannuskeinoja riskienhallintakeinojen muodossa ja määritellä kehittämistyön vastuut ja aikataulu. Lisäksi on hyvä muistaa, että työntekijöiden henkinen hyvinvointi on osa vahinkoriskejä, eli henkilöturvallisuutta ja työturvallisuutta.

ta. Näin ollen myös työtyytyväisyyskyselyn ja esimerkiksi tasa-arvokyselyn tulosten purkaminen käytännön kehittämistoimiksi olisi mahdollista riskienhallintaprosessin kautta esimerkiksi työryhmätyöskentelyä hyödyntäen ja parhaiden käytänteiden jakamisen myötä eri yksiköiden välillä.

<p>Valtionhallinnon arvot</p> <ul style="list-style-type: none"> • tuloksellisuus • laatu • luottamus • vastuullisuus • tasa-arvo • puolueettomuus • riippumattomuus • avoimuus • palveluperiaate • vahva asiantuntemus
<p>Eduskunnan kanslian arvot</p> <ul style="list-style-type: none"> • hyvä palvelu • avoimuus ja vuorovaikutteisuus • oikeudenmukaisuus
<p>Hyvä ammattitaito</p> <p>”Palvelemme kansanedustajia, työtovereitamme ja yhteistyökumppaneita ammattimaisesti ja hyvin. Tuotamme korkealaatuisia palveluja tehokkaasti ja taloudellisesti. Pidämme huolen siitä, että osaamisemme ja asiantuntemuksemme ovat ajan tasalla. Osaamisen ja johtamisen keittämisellä tuemme ammattimaista työntekoa. Kannamme vastuun työstämme.”</p> <p>Avoimuus ja vuorovaikutteisuus</p> <p>”Toimimme avoimesti ja läpinäkyvästi. Huolehdimme siitä, että työtehtävissä tarvittava tieto on saatavilla ja käytettävissä. Luomme mahdollisuuksia osallistua ja vaikuttaa yhteisten asioiden valmisteluun. Arvostamme ja kunnioitamme toisiamme sekä annamme rakentavaa palautetta työstä. Kannustamme yhteistyöhön ja edistämme vuorovaikutteista työ- ja keskustelukulttuuria.”</p> <p>Oikeudenmukaisuus</p> <p>”Edistämme tasa-arvoa, yhdenvertaisuutta ja tasapuolista kohtelua. Työtämme ohjaavat selkeät ja yhdessä sovitut pelisäännöt. Puutemme epäkohtiin ja korjaamme ne. Toimimme sovittujen tavoitteiden saavuttamiseksi. Vastuunjako on selkeä ja jokainen tietää, mitä häneltä odotetaan. Kaikilla on oikeus kehittyä työssään.”</p>

Taulukko 6: Arvovertailu (Eduskunnan kanslia 2011f, Valtioneuvosto 2001)

Riskienhallinta mahdollistaa organisaation osaamistason seurannan ja arvioinnin. Sen avulla voidaan todentaa myös osaamisen kypsyyden turvallisuuden tai riskienhallinnan osalta. Toimintaympäristön muutosten huomioiminen ja sen vaikutusten arviointi konkretisoi hyvin tulevaisuuden osaamistarpeet. Riskienhallinnan näkökulma tukee eduskunnan kanslian ylimmän ja keskitason johtamista, sillä se antaa työkalut yksikkökohtaisten toimintojen arviointiin uudeltaisesta näkökulmasta ja tuottaa toiminnan painopisteiden oikeanlaista asettamista tukevaa tietoa. Riskienhallinnan tehtävänä on osaltaan auttaa löytämään ongelmien todellinen ydin ja etsiä keinoja niihin vaikuttamiseksi.

Riskienhallinnan soveltamisen kautta on mahdollista myös lisätä vuorovaikutusta eduskunnan kanslian eri yksiköiden ja osastojen välillä. Turvallisuus on kaikkia koskeva tavoite, vaikkakin yksiköiden välillä on eroja organisaatioturvallisuuden eri osa-alueiden painottumisen ja näin ollen myös riskien suhteen. Riskien hallintakeinoja valitessa tulisi lisäksi hyödyntää eduskun-

nan kanslian eri yksiköissä olevaa osaamista esimerkiksi tiedotuksen, tietotekniikan, koulutuksen ja työterveydenhuollon osalta. Samalla eri yksikköjen välinen yhteistyö ja keskinäinen arvostus lisääntyisivät nykyisestään.

Riskienhallinta tukisi hyvin myös oikeudenmukaisuutta siten kuin se on kirjattu auki eduskunnan kanslian arvoihin. Riskienhallinta perustuu yhdessä sovittuihin tavoitteisiin ja pelisääntöihin. Riskienhallintatoiminnan tarkoitus on vaikuttaa organisaation heikkouksiin ja kehittää toimintaa niin, että ainakin ydintoiminnot on turvattu. Riskienhallinnan tarkoitus ei ole syyllistää tai osoitella sormella, vaan tavoitteena on avoin ja rakentava lähestymistapa organisaation ja sen henkilöstön jatkuvaan kehittymiseen. Riskienhallinnan käytännön toteutus vaatii systemaattisuutta, joka osaltaan muodostuu selkeästä vastuualueiden ja tehtävien jaosta. Riskienhallinta ja turvallisuus ovat lisäksi eduskunnan kanslian henkilöstön yhteisiä asioita – kaikki kansliassa työskentelevät toteuttavat osaltaan käytännön riskienhallintatyötä valinnoiltaan ja toiminnallaan.

5.1.2 Turvallisuusjohtamisen painopisteet

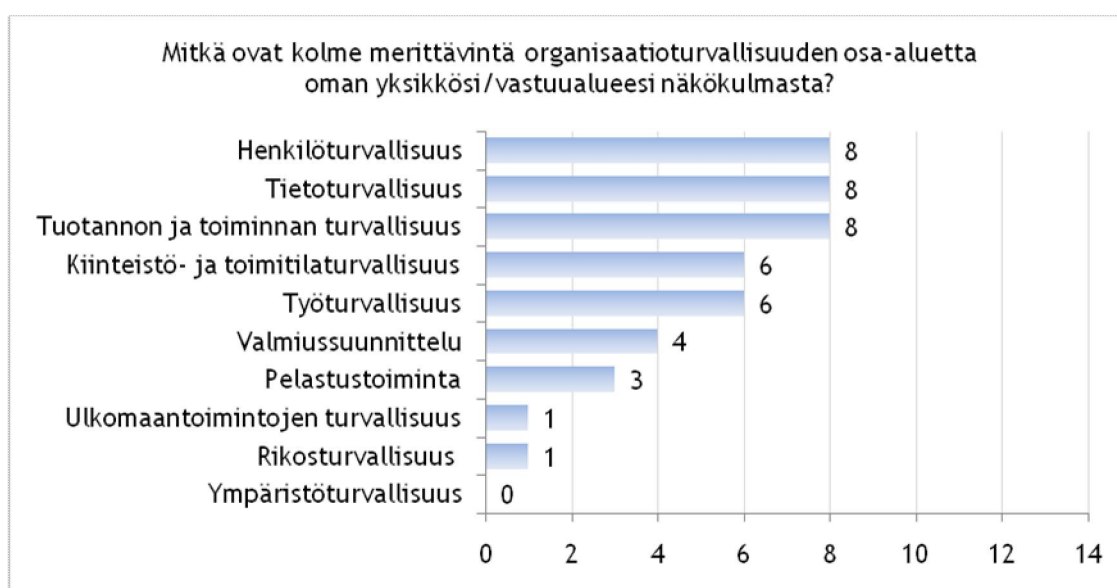
Eduskunnan turvallisuustoiminta keskitettiin omaan yksikköön vuonna 2005. Siihen asti eduskunnan kanslian turvallisuudesta vastasi turvallisuusosasto, joka toimi hallintotoimiston alaisuudessa ja fyysisesti kiinteistötoimiston yhteydessä. Yksikön perustamisen myötä toteutettiin myös henkilöstömuutoksia: turvallisuusjohtajan virka perustettiin ja sisäänkäyntien virastoavustajat ja puhemiehen kuljettajat siirtyivät turvallisuusyksikön alaisuuteen. Lisäksi aloitettiin turvallisuusyksikön henkilöstön koulutus. Vuonna 2008 voimaan astunut laki turvatoimista eduskunnassa mahdollisti turvallisuusasioiden paremman huomioimisen eduskunnan kanslian toiminnan suunnittelussa ja paransi turvallisuusyksikön kehittämisen mahdollisuuksia.

Eduskunnan turvallisuusyksikön keskeisiksi toiminnan painopisteiksi ovat ajan myötä muodostuneet kiinteistö- ja toimitilaturvallisuus, ympäristöturvallisuus (ISO 14001 -standardi vuodesta 2008) sekä henkilöturvallisuus (yhteistoiminnassa viranomaisten kanssa). Eduskunnan tietohallintotoimisto puolestaan huolehtii teknisestä tietoturvallisuudesta. Pelastustoiminnassa noudatetaan lainsäädäntöä ja varautumissuunnitelmat koskevat pääasiassa täysistuntoja.

Loppusyksystä 2011 toteutetussa virkamiesjohdolle suunnatussa kyselyssä (Liite 1) pyrittiin selvittämään yksikkö- ja osastotason näkemyksiä eduskunnan kanslian turvallisuustoiminnan kehittämistarpeista. Eduskunnan kanslian virkamiesjohdolle sähköpostin välityksellä suunnattuun kyselyyn vastasi yhteensä 15 henkilöä (75 %). Johtajia pyydettiin valitsemaan kolme oman yksikkönsä kannalta merkittävintä organisaatioturvallisuuden osa-aluetta ja kolme eduskunnan kanslian tasolla eniten kehittämistä kaipaavaa organisaatioturvallisuuden osa-

aluetta. Organisaatioturvallisuuden jako ja osa-alueiden kuvaus tehtiin Elinkeinoelämän keskusliiton alaisen Yritysturvallisuus EK:n suositusten mukaisesti (Kuvio 6).

Vastausten perusteella eduskunnan kanslian eri yksikköjen toiminnassa kolmeksi merkittävimmäksi organisaatioturvallisuuden osa-alueeksi koetaan henkilöturvallisuus, tietoturvallisuus ja tuotannon ja toiminnan turvallisuus. Seuraavaksi tärkeimmiksi koetaan kiinteistö- ja toimitilaturvallisuus, työturvallisuus ja valmiussuunnittelu. Vähiten tärkeäksi koettiin pelastustoiminta, ulkomaantoimintojen turvallisuus, rikosturvallisuus ja ympäristöturvallisuus (Kuvio 12).

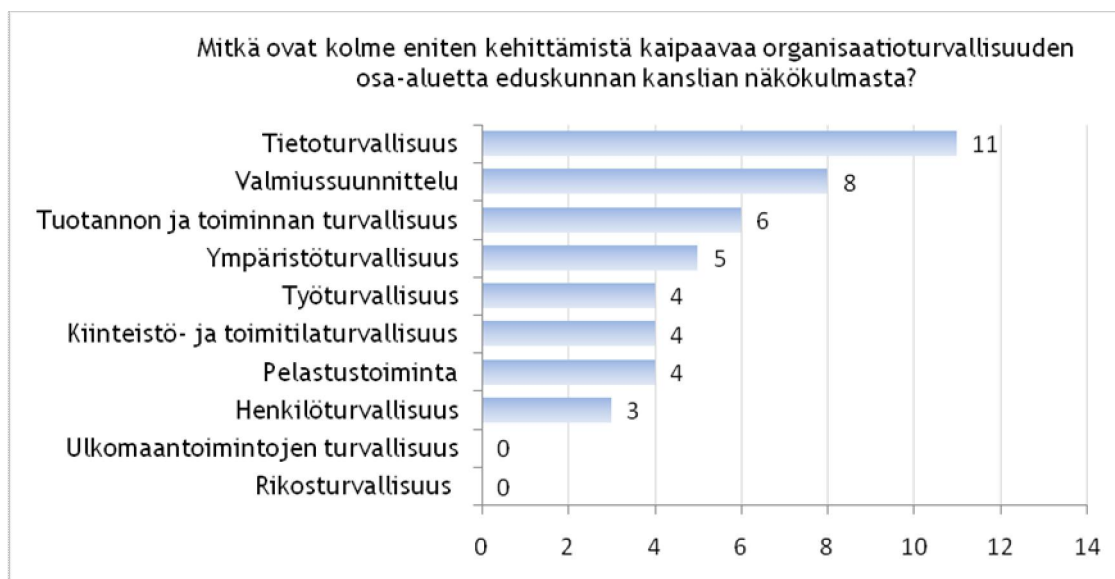


Kuvio 12: Eduskunnan kanslian yksikköjen kannalta tärkeimmät organisaatioturvallisuuden osa-alueet (virkamiesjohdon kysely 2011)

Vastausten painotukset olivat varsin selviä; eniten ääniä saaneet saivat yhtäläisen määrän ääniä (8) ja ero seuraavaan ryhmään oli kahden äänen myötä selvä. Myös vähiten ääniä saaneet osa-alueet erottuvat vähintään kahdella äänellä keskimäärän ääniä saaneista osa-alueista. On huomioitava, että vaikka kysely sisälsi kunkin osa-alueen sisällöllisen kuvauksen, voivat vastaajien eri osa-alueisiin liittämät mielikuvat ja olettamukset vaikuttaa annettuihin ääniin. Kehittämistyön kannalta mielenkiintoista on kuitenkin se, miksi valmiussuunnittelu, sisältäen myös toiminnan jatkuvuussuunnittelun, jää vähälle painotukselle. Selitystä tälle voidaan toisaalta hakea viiden eniten ääntä saaneista osa-alueista - on mahdollista, että näiden osa-alueiden painottumisen koetaan vaikuttavan myös yksikön toiminnan jatkuvuuteen.

Kun näkökulma vaihdettiin koko eduskunnan kanslian tasolle ja tehtävänä oli määritellä eniten kehittämistä vaativat organisaatioturvallisuuden osa-alueet, saatiin kolmeksi tärkeimmäk-

si osa-alueeksi tietoturvallisuus, valmiussuunnittelu sekä tuotannon ja toiminnan turvallisuus. Keskimäärän ääniä saivat ympäristöturvallisuus, työturvallisuus, kiinteistö- ja toimitilaturvallisuus ja pelastustoiminta. Vähiten kehittämistä kaipaaviksi koettiin henkilöturvallisuus, ulkomaantoimintojen turvallisuus ja rikosturvallisuus (Kuvio 13).



Kuvio 13: Eduskunnan kansliassa eniten kehittämistä vaativat organisaatioturvallisuuden osa-alueet (virkamiesjohdon kysely 2011)

Koko eduskunnan kanslian kehittämistä koskevassa kyselyssä tietoturvallisuus nousi selvästi yli muiden osa-alueiden (11 ääntä), seuraavaksi tärkeänä koettuun valmiussuunnitteluun on eroa kolme ääntä. Tuotannon ja toiminnan turvallisuus, ympäristöturvallisuus, kiinteistö- ja toimitilaturvallisuus ja pelastustoiminta muodostavat keskimäärän ääniä saaneiden ryhmän. Vähiten kehittämistarvetta koettiin puolestaan olevan henkilöturvallisuudessa, ulkomaantoimintojen turvallisuudessa ja rikosturvallisuudessa. Viimeisen ryhmän osalta on todennäköistä, että henkilöturvallisuus koetaan tärkeäksi turvallisuuden osa-alueeksi, joka on jo hyvällä tasolla, kun taas ulkomaantoimintojen turvallisuuden tai rikosturvallisuuden kehittämistä ei koeta tarpeelliseksi joko niiden vähäisen merkityksen vuoksi tai siksi, että niiden piiriin kuuluvia osa-alueita koetaan voitavan kehittää muiden, enemmän ääniä saaneiden organisaatioturvallisuuden osa-alueiden yhteydessä.

Puhemiehen vuonna 2003 asettaman turvallisuusasioita käsitelleen työryhmän loppuraportin mukaan riskienhallinta kuuluvat turvallisuusjohtajan toimenkuvaan (Schroderus 2008, 31). Ylimmän johdon vahvistaman riskienhallinnan strategian tai politiikan puuttuessa kokonaan, on riskienhallinnan vastuunjako eduskunnan kansliassa vielä epäselvää ja sen käytännön to-

teutus hajanaista ja vaihtelevaa. Pitkäjänteistä ja systemaattista, koko organisaation toiminnan kattavaa riskienhallintaa ei tähän mennessä ole eduskunnan kansliassa toteutettu. Riskien arviointia on sen sijaan tehty tarpeen mukaan esimerkiksi yksittäisiin hankkeisiin liittyen, kuten esimerkiksi eduskunnan peruskorjaus.

Vuoden 2011 alussa eduskunnan kanslian turvallisuusyksikön yhteyteen liitettiin virka, jonka haltija keskittyy jatkossa riskienhallinnan kehittämiseen. Riskienhallinnan asiantuntijan tehtävän täyttäminen jo olemassa olevasta henkilöstöstä on linjassa kanslian henkilöstöpolitiikan kanssa, mutta viivästyttää riskienhallintatoiminnan käynnistämistä kouluttautumistarpeen vuoksi.

5.1.3 Sisäinen tarkastus

Eduskunnan kanslian sisäinen tarkastus perustettiin kansliatoimikunnan alaisuuteen vuonna 2008 tiliohjesäännön 51 §:n perusteella. Sen toimintaan on sittemmin ehdotettu kehittämistoimenpiteitä yksikön hallinnollisen aseman selkeyttämiseksi ja sen asettamiseksi suoraan kanslian ylimmän johdon alaisuuteen, jotta raportointi ja tarkastuksen kohteena olevan tiedon saanti parantuisi (Eduskunnan kanslia 2010a).

Sisäistä tarkastusta hoidetaan eduskunnan kansliassa yhden virkamiehen voimin. Sisäisen tarkastuksen tehtävänä on tilivirastona toimivan eduskunnan kanslian sisäisen tarkastuksen ja valvonnan suunnittelu ja toteutus. Lisäksi sen tehtäviin kuuluu kontrolleritoiminnon kehittäminen, osallistuminen kanslian strategiseen suunnitteluun ja valiokuntasihteeristön tutkimustoiminnan asiantuntijana toimiminen. (Eduskunta 2011.) Myös riskikartoituksia on tehty sisäisen tarkastuksen toimesta, mutta ne eivät ole koskeneet strategisia tai operatiivisia riskejä organisaatioturvallisuuden kehittämisen näkökulmasta. Riskienhallinnallista näkökulmaa on sisällytetty myös sisäisen tarkastuksen laatimiin toimintaympäristön analyysihin.

Eduskunnan kanslian vuoden 2010 sisäisen tarkastuksen arviointi- ja vahvistuslausuma sisältää riskienhallinnan ja organisaatioturvallisuuden kehittämisen kannalta lupaavia kannanottoja. Lausuma pohjautuu sisäisen tarkastuksen tammikuussa 2011 toteuttamaan eduskunnan kanslian johdolle suunnattuun kyselyyn. Kyselyyn vastanneiden mielestä riskienhallinta kuuluu kanslian vastuulliseen johtamiseen, sillä sen avulla lisätään luottamusta kanslian toimintaan ja talouteen. (Eduskunnan kanslia 2010c.)

Alla olevien avointen vastausten poimintojen perusteella voidaan todeta, että tarve riskienhallinnan ja turvallisuuden kehittämiseksi on tunnustettu myös eduskunnan kanslian johdossa

- huomion kiinnittäminen riskienhallintaan saa johdolta yksimielisen tuen, ja riskienhallinnan tilan arvioinnilla pyritään vahvistamaan avoimuutta, vuorovaikutusta ja hyvää hallintoa eduskunnan kansliassa
- kanslian johdon on kiinnitettävä huomioita riskeihin niin, että toimintayksikön johtavat virkamiehet tuntevat vastuunsa oman yksikkönsä hallinnon ja talouden oikeellisuudesta kanslian tiliohjesäännön edellyttämällä tavalla. (Eduskunnan kanslia 2010c.)

5.1.4 Eduskunnan kanslian nelikenttäanalyysi

Organisaation uusiutuminen vaatii Kamenskyn (2008, 33) mukaan kyseenalaistamisen taitoa, tosiasioiden tunnustamista, tervettä itsetuntoa ja nöyryyttä, luovuutta ja innovatiivisuutta ja herkkyyttä ympäristölle. Uusiutuminen ei kuitenkaan tarvitse tarkoittaa vanhan totaalista hylkäämistä vaan uusiutua voi myös olemassa olevaa kehittämällä. Organisaation kehittäminen vaatii siinä toimivien henkilöiden halua kehittää itseään ja toimintatapojaan. Käytännössä tämä tarkoittaa sitä, että Kamenskyn mainitsemat ominaisuudet vaaditaan organisaation henkilöstöltä ja ennen kaikkea johtotehtävissä toimivilta.

Lähtötilanteen realistinen tunnistaminen ja olemassa olevien toimintamallien, organisaatiorakenteiden ja -kulttuurien kyseenalaistaminen on vaikeaa ilman järjestelmällistä tiedon keruuta ja analysointia. Eduskunnan kanslian kaltaisissa suurissa organisaatioissa tehtävä on vaikeaa siksikin, että yksiköillä on toisistaan poikkeavat vastuualueensa ja henkilöstön toimenkuvat ovat varsin moninaiset. Kokonaisvaltaisen tilannekuvan ja sitä kautta aitojen kehittämistarpeiden tunnistaminen vaatii kokonaisvaltaista, yksikkörajoista riippumatonta johtamista. (Riskienhallintatoiminnan sijoittumista eduskunnan kanslian organisaatioon on hahmoteltu liitteessä seitsemän.)

Tilannekuvaa eduskunnan kanslian tilasta on rakennettu aikaisemmin muun muassa eduskunnan kansliassa laaditun PEST-analyysin (political, economical, social, technological) avulla vuoden 2010 strategia- ja toimintasuunnitelmatyöskentelyn yhteydessä. Myös sisäinen tarkastus on käsitellyt eduskunnan kanslian toimintaympäristön muutoksia. Sisäisiä muutostarpeita voidaan etsiä esimerkiksi eduskunnan kanslian työtyytyväisyyskyselyistä, joista ilmenee henkilöstön mielipiteet, haasteet ja kehittämis ehdotukset työyhteisön ja johtamisen suhteen. Edellä mainitut lähteet on yhdistetty ja niitä on täydennetty havainnoinnin pohjalta kuviossa 12 eduskunnan kanslian nelikenttäanalyysin (SWOT) muodossa.

Suurimmat kehittämistarpeet eduskunnan kanslian suhteen johtuvat juuri organisaation sisäisistä ilmiöistä. Tässä piilee myös mahdollisuus sikäli, että eduskunnan kanslian kehittäminen

on tässä tapauksessa suurelta osin kiinni sen omasta tahdosta ja kyvystä tehdä niin. Eduskunnan kanslian ulkoisiin haasteisiin on sen sijaan vaikeampi, ellei joiltain osin myös mahdotonta, vaikuttaa.

	Hyödyllisiä tavoitteiden saavuttamisen kannalta	Haitallisia tavoitteiden saavuttamisen kannalta
Sisäiset vaikuttimet (organisaatio)	VAHVUUDET (S) <ul style="list-style-type: none"> • työtehtävien haastavuus • mielenkiintoiset työtehtävät • hyvä työilmapiiri yksiköissä • työvoiman pysyvyys • hyvät työsuhte-edut • hyvä palkkataso • henkilöstön laaja-alainen osaaminen • henkilöstön erikoisosaaminen • monipuoliset toimitilat • toimipaikan keskeinen sijainti 	HEIKKOUEDET (W) <ul style="list-style-type: none"> • politisoituminen ja byrokraattisuus • muutosvastaisuus • henkilöstön tyytymättömyys johtamiseen ja palkkaukseen • epäviralliset valtarakenteet • kokonaisvaltaisen johtamisen puute • päätöksenteon epäjohdonmukaisuus • sisäinen tiedon kulku • organisaatiokulttuurin heikkous • sokkeloiset toimitilat
Ulkoiset vaikuttimet (ympäristö)	MAHDOLLISUUDET (O) <ul style="list-style-type: none"> • suurten ikäluokkien eläköitymisen ennakointi • yhteiskunnan monimuotoistuminen ja muutosten nopeutuminen • sähköisen toimintatavan yleistyminen • arvostetun instituution aseman kehittäminen • organisaation sisäinen kehittäminen • julkisuuskuvan parantaminen • henkilöstön kehittämisinnokkuuden arvostaminen ja hyödyntäminen 	UHKAT (T) <ul style="list-style-type: none"> • parlamentarismien arvostuksen ja äänestysaktiivisuuden lasku • kansalaisten loitontuminen poliittisesta keskustelusta • suurten ikäluokkien eläköityminen • työntekijämarkkinoiden kilpailutilanteen kiristyminen • yhteiskunnan monimuotoistuminen ja muutosten nopeutuminen • kansainvälisen yhteisön muutosten vaikutukset • kehityksen tahallinen jarruttaminen

Kuvio 14: Eduskunnan kanslian SWOT-analyysi Eyelinea mukailen (2011)

Henkilöstön mielestä eduskunnan kanslian suurimmat haasteet liittyvät johtamiseen, viestintään ja palkkausjärjestelmään (Eduskunnan kanslia 2011b). Eduskunnan kanslian kaltaisen organisaation kehittäminen ei ole yksinkertainen eikä varsinkaan nopeasti toteutettavissa oleva tehtävä. Organisaation muuttuminen vaatii siinä toimivien yksilöiden muuttumista; oikeanlaista asennetta, rohkeutta ja uuden oppimisen lisäksi mahdollisesti myös vanhan poisoppimista. Ennen muuta se kuitenkin edellyttää kykyä erottaa kehittämistarpeiden ydin seurannaisvaikutuksiin reagoimisen sijaan.

Otala (2002, 104–106) kuvaa yksilön osaamista arvojen, asenteiden, tietojen, taitojen, kontaktien ja kokemusten yhdistelmänä, joita voidaan kehittää läpi elämän (elinikäinen oppimi-

nen). Yksilön osaamisen kehittyminen vaatii tietojen ja taitojen kartuttamisen ohella myös muiden osa-alueiden muuttumista. Toisaalta oppiminen on myös yksilöllistä, siihen vaikuttavat henkilön henkinen ja fyysinen energia sekä erityiset henkilökohtaiset taidot ja lahjakkuus. Yksilön osaamisen osa-alueet on esitelty tarkemmin taulukossa seitsemän.

Arvot ja asenteet	<ul style="list-style-type: none"> • asenteiden merkitys on korostunut ihmisen osaamisen kriteerinä • asenteet vaikuttavat yksilön sopeutumiskykyyn • vaikuttavat myös tiedon haluun, tahtoon oppia uutta • asenteet ovat yksilön toimintaa ja ajattelua ohjaava sisäinen malli • arvoja ja asenteita on vaikea muuttaa
Tiedot ja taidot	<ul style="list-style-type: none"> • ammattitaito, yleiset taidot, sosiaaliset taidot • faktat, menetelmät, mallit • kommunikointikyky, yhteistyökyky ja -halukkuus, empatiakyky • taito yhdistellä asioita ja ihmisiä • motivoitumiskyky ja motivoitaito
Kontaktit ja kokemukset	<ul style="list-style-type: none"> • kokemus auttaa ymmärtämään uutta tietoa ja oppimaan nopeammin • kokemus muodostaa viitekehysten, joka laajenee kokemusten karttumisen myötä - ihmisen oppimiskyky lisääntyy iän myötä • kontaktit ovat oleellinen osa pätevyyttä • kontaktien kautta tulevat heikot signaalit muutoksista ja tulevista asioista • kontaktit auttavat muutosten merkityksen oivaltamisessa ja niistä selviytymisessä • kontakteihin lasketaan ihmissuhdeverkostojen lisäksi kirjalliset ja sähköiset tiedonlähteet

Taulukko 7: Yksilön osaamisen osa-alueet Otalaa mukailen (2002, 104–106)

Uuden asiakokonaisuuden hyväksyminen ja sisäistäminen on siis pitkäjänteisen työstämisen tulos. Riskienhallintatoiminnan käynnistämisen alkuvaiheessa painottuvat erityisesti tieto, asenteet ja kokemukset. Tieto ja kokemukset auttavat riskienhallinnan merkityksen ymmärtämisessä ja tunneperäisessä motivoitumisessa, asenteet ratkaisevat sen, mihin toimiin ryhdytään ja minkälaisia valintoja riskienhallinnan tavoitteiden suhteen tehdään. Riskienhallinnan asiantuntijan tehtävässä toimivan yksi tärkeimmistä tehtävistä onkin organisaation sisäinen markkinointi; koulutuksessa ja tiedotuksessa täytyy yksikkö- ja osastorojen lisäksi huomioida eri henkilöstöryhmien tarpeet. Riskienhallinnan ja turvallisuuden kehittäminen eduskunnan kansliassa koskettaa näin ollen kaikkia edellä mainittuja osaamisen osa-alueita (Taulukko 8).

Arvot ja asenteet	<ul style="list-style-type: none"> • muutosvastarinnan syiden ymmärtäminen ja sen työstäminen • riskienhallinnan ja turvallisuuden arvon ymmärtäminen • organisaation kehittämiseen sitoutuminen • tunnetason ja arvopohjainen motivoituminen • valintojen ja päätösten kypsyyden ja kestävyys • kehittämistyöhön vaadittava pitkäjänteisyys ja sinnikkyys
Tiedot ja taidot	<ul style="list-style-type: none"> • riskienhallinnan tietoperustan laajentaminen • organisaatioturvallisuuden ammattitaidon laajentaminen • tiedon jakaminen, viestinnän muoto, tyyli ja kanavat • johdon ja henkilöstön sitoutuminen • tehtävien ja vastuualueiden määrittely ja kohdentaminen • tosiasioiden avulla motivoituminen • organisaation kannalta tarkoituksenmukaiset valinnat ja niiden kestävät perustelut
Kontaktit ja kokemukset	<ul style="list-style-type: none"> • organisaatiotason muutostarpeen tunnustaminen • tulevaisuuden toimintaympäristön muutosten ymmärtäminen • organisaatiolle parhaiten sopivan toimintamallin rakentaminen • vertailukohteiden avulla motivoituminen • turvallisuuden ja riskienhallinnan tarpeellisuuden tunnustus

Taulukko 8: Osaamisen osa-alueet ja riskienhallinnan kehittäminen

5.1.5 Eduskunnan kanslian ydintoimintoihin liittyvät riskit

Eduskunnan kanslian kannalta kriittisimpiä organisaatioturvallisuuden osa-alueita pohdittaessa on osaltaan palattava kanslian ydintehtävään ”luoda eduskunnalle edellytykset hoitaa sille valtioneelimenä kuuluvat tehtävät” (Eduskunnan työjärjestys 2000). Nämä tehtävät ovat käytännössä lakien säätäminen, valtion talousarviosta päättäminen, kansainvälisten sopimusten käsittely, maan hallituksen toimien valvominen ja pääministerin valitseminen (Eduskunta 2011).

Eduskunnan kanslian yksiköistä ydintehtävää suorittavat keskuskanslia ja valiokuntasihteeristö. Näiden kahden yksikön suoritus- ja toimintakyky on näin ollen taattava kaikissa olosuhteissa. Ydintoimintaa suorittavien yksikköjen osalta riskienarviointi ja riskienhallintakeinojen soveltaminen on edellytys toiminnan jatkuvuuden takaamiseksi. Ydintoimintoja suorittavien yksikköjen toiminnassa vaikuttavat riskit ovat organisaatioturvallisuuden osa-alueina kuvattuina erityisesti

- henkilöturvallisuus
- työturvallisuus
- tietoturvallisuus
- tuotannon ja toiminnan turvallisuus
- valmiussuunnittelu
- pelastustoimi.

Eduskunnan kanslian ydintoimintoja suorittavat yksiköt ovat puolestaan riippuvaisia niitä tukevien yksikköjen toiminnasta. Keskuskanslian ja valiokuntasihteeristön toimintaa tukevat yksiköt ovat hallinto-osasto, tieto- ja viestintäyksikkö, kansainvälisten asian yksikkö sekä turvallisuusyksikkö, ja ne palvelevat osaltaan myös kansanedustajia. Näissä yksiköissä oleva ammattitaito ja erityisosaaminen on monipuolista (mm. tietotekniikka, viestintä, kielitaito, henkilöstöhallinto, koulutustaito, terveydenhoito, kiinteistöosaaminen).

Yksikköjen erikoistuminen merkitsee riskienhallinnan ja organisaatioturvallisuuden kehittämisen näkökulmasta sitä, että toiminnassa tulee soveltaa yksikkökohtaista lähestymistapaa. Aiheellista olisi pohtia myös sitä, miten yksikkökohtaista erikoisosaamista voitaisiin hyödyntää koko organisaation riskienhallinnan ja organisaatioturvallisuuden eduksi. Tukitoimintoja suorittavien yksikköjen osalta korostuvat organisaatioturvallisuuden osa-alueina kuvattuina erityisesti

- työturvallisuus (erityisesti työhyvinvointi)
- pelastustoimi
- valmiussuunnittelu (toiminnan jatkuvuussuunnittelu).

Yhteiskunnan turvallisuusstrategian näkökulmasta katsottuna eduskunnan kanslian turvallisuustoiminnassa tulisi panostaa erityisesti valmiussuunnitteluun, tietoturvallisuuteen, henkilöturvallisuuteen, pelastustoimintaan ja rikosturvallisuuteen. Eduskunnan kanslian PESTE-analyysistä heijastuvien organisaatioturvallisuuteen liittyvien ilmiöiden perusteella eduskunnan kanslian kriittisimmät organisaatioturvallisuuden osa-alueet ovat pelastustoiminta, valmiussuunnittelu, tietoturvallisuus, henkilöturvallisuus, tuotannon ja toiminnan turvallisuus.

Organisaatioturvallisuuden eri osa-alueiden painottuminen vaihtelee lähteaineistosta riippuen (Taulukko 9). Virkamiesjohdon kyselylle (Liite 1) on kuitenkin syytä antaa erityinen painoarvo, sillä turvallisuustoiminnan ja riskienhallinnan suunnittelu ja toteutus tulee aina tehdä organisaation omilla ehdoilla ja sen tarpeita vastaten. Virkamiesjohtajien näkemykset omien yksikköjensä toiminnasta – yhtäältä itsenäisenä ja toisaalta osana eduskunnan kanslian kokonaisuutta – luovat realistisen lähtökohdan riskienhallintatoiminnan käynnistämiseksi.

Organisaatioturvallisuuden osa-alueet	PESTE-analyysi	Virkamiesjohdon kysely	Yhteiskunnan turvallisuusstrategia
Henkilöturvallisuus	x	x	x
Kiinteistö- ja toimitilaturvallisuus			
Pelastustoiminta	x		x
Rikosturvallisuus			x
Tietoturvallisuus	x	x	x
Tuotannon ja toiminnan turvallisuus	x	x	
Työturvallisuus		x	
Ulkomaantoimintojen turvallisuus			
Valmiussuunnittelu	x	x	x
Ympäristöturvallisuus			

Taulukko 9: Organisaatioturvallisuuden painopisteet eduskunnan kansliassa

Eri lähteiden yhteisvaikutuksena tärkeimmiksi organisaatioturvallisuuden osa-alueiksi eduskunnan kanslian osalta nousevat henkilöturvallisuus, tietoturvallisuus ja valmiussuunnittelu. Valmiussuunnittelu korostuu erityisesti sen alle kuuluvan toiminnan jatkuvuussuunnittelun osalta. Virkamiesjohto antoi paljon ääniä tuotannon ja toiminnan turvallisuudelle (osaluku 5.1.2). Tähän osa-alueeseen kuuluvat häiriötön toiminta, nopea häiriötilanteesta toipuminen ja organisaation jokapäiväisten toimintojen sujuvuuden varmistaminen heijastavatkin valmiussuunnittelua juuri toiminnan jatkuvuuden näkökulmasta.

Jatkuvuussuunnittelun painoarvoa tuotannon ja toiminnan turvallisuudelle annettujen äänien takana on kuitenkin vaikea todentaa avovastausten vähyden vuoksi. Tämän organisaatioturvallisuuden osa-alueen kuvausta tarkastellessa on kuitenkin selvää, että eduskunnan kanslian kaltaisen organisaation kohdalla tuotteiden ja palveluiden turvallisuus ei liene oleellinen osatekijä. Tässä kehittämistyössä virkamiesjohdon tuotannon ja toiminnan turvallisuudelle antamat äänet tulkitaan näin ollen pääasiassa toiminnan jatkuvuuteen liittyviksi. Kolmanneksi tärkeimmäksi turvallisuuden osa-alueeksi henkilö- ja tietoturvallisuuden rinnalle nousee valmiussuunnittelu.

Riskienhallinta lähtee liikkeelle riskien identifioinnista. Taulukkoon kymmenen on kerätty esimerkkejä organisaatioturvallisuuden eri osa-alueisiin jaoteltuna eduskunnan kansliaa koskevia uhkia ja riskejä tutkimusaineiston pohjalta. Päätös organisaatioturvallisuuden osa-alueiden kehittämisen painopisteistä tehdään kuitenkin eduskunnan kansliassa.

Organisaatioturvallisuuden osa-alueet	Esimerkkejä organisaatioturvallisuuden eri osa-alueisiin liittyvistä uhkista/riskeistä eduskunnan kansliassa
Henkilöturvallisuus	<ul style="list-style-type: none"> • oman henkilöstön jäsenen hyökkäys toista kohtaan • panttivankitilanne • avainhenkilöiden kiristys • usean avainhenkilön samanaikainen kykenemättömyys hoitaa tehtävänsä (esim. sairaus tai jokin edellä mainittu)
Kiinteistö- ja toimitilaturvallisuus	<ul style="list-style-type: none"> • Pikkuparlamentin tai eduskuntarakennuksen lähiympäristön vakava järjestyshäiriö (yleisöllä esteetön kulku) • kulkuoikeuksiin liittyvät väärinkäytökset etuoikeutettujen sidosryhmien toimesta
Pelastustoiminta	<ul style="list-style-type: none"> • ilmastointikanavien kautta tapahtuva tahallinen saastuttaminen • tilannekuva rakennuksessa olevan henkilöstön ja sidosryhmien edustajien olipaikasta pelastustoimia vaativassa tilanteessa • pelastuslaitoksen resurssien riittävyys; onko apua saatavilla, jos priorisoitavia kohteita on samanaikaisesti useita?
Rikosturvallisuus	<ul style="list-style-type: none"> • henkilöstöön kohdistuva väkivalta eduskuntarakennusten alueella poikkeuksellisin työaikoina • henkilöstön tekemät vakavat rikokset - maineenhallinta?
Tietoturvallisuus	<ul style="list-style-type: none"> • eduskunnan tiloissa tapahtuva laiton tiedonvaihto • sosiaalinen hakkerointi • kolmansien osapuolien tekemä eduskunnan kanslian henkilöstön värväys (myös kohteen sitä tiedostamatta?) • henkilö- ja rikosturvallisuuden heijastevaikutukset tietoturvasuuteen
Tuotannon ja toiminnan turvallisuus	<ul style="list-style-type: none"> • pitkäkestoinen häiriö sähköjakelussa • pitkäkestoinen häiriö tietoliikenteessä • yhteistoimintaedellytysten heikkeneminen (esim. muista valtionhallinnon toimijoista poikkeavat turvaluokittelut ja/tai tietoturvallisuuden eri osa-alueiden ylikorostuminen) • ulkoistettujen peruspalveluiden turvallisuus ja riskienhallinta
Työturvallisuus	<ul style="list-style-type: none"> • johtamisen arvioinnin ja seurannan puutteesta johtuva työssä pahoinvointi ja sen vaikutukset henkilöstön lojaalisuuteen, eduskunnan kanslian maineeseen työnantajana ja toiminnan tehokkuuteen) • työntekijöiden heikenneen lojaalisuuden vaikutukset organisaatiturvallisuuden osa-alueisiin? • työtyytyväisyys- ja hyvinvointi- sekä muiden kyselyjen jääminen irrallisiksi, ilman konkreettisia kehittämistoimenpiteitä
Ulkomaantoimintojen turvallisuus	<ul style="list-style-type: none"> • henkilöstön joutuminen paikallisen selkkauksen välikädeksi (mitä eri tilanteita, kuka viestii, miten viestii?) • kidnappaukset ulkomailla (yhteistoiminta kansallisten ja kansainvälisten sidosryhmien kanssa)
Valmiussuunnittelu	<ul style="list-style-type: none"> • keskuskanslian virkamiesten joukkopaon (esim. epidemiat) vaikutus täysistuntotyöskentelyyn (varamiehet, aikataulut, priorisointi) • valiokuntasihteeristön virkamiesten joukkopaon vaikutus täysistuntotyöskentelyyn • eri yksikköjen, osastojen ja toimistojen toiminnan lamaantumisen vaikutukset koko eduskunnan toimintaan (kriittinen aikajänne, varamiehet, varajärjestelmät, tehtävien priorisointi, resurssien kohdentaminen) • perusinfrastruktuurin turvaaminen (vaihtoehtoinen energiantuotanto, tietoliikenteen varajärjestelmät, manuaaliset varajärjestelmät, LVI-tekniikan häiriöttömyys)

Ympäristöturvallisuus	<ul style="list-style-type: none"> • eduskunnan toiminnasta mahdollisesti aiheutuvat ympäristöhaitat (peruskorjaus, matkustus?)
-----------------------	--

Taulukko 10: Esimerkkejä eduskunnan kanslian riskientunnistamistyön pohjaksi

Myös yksittäisten riskien tunnistaminen, arviointi, mahdollinen luokitus ja sopivien hallintakeinojen valitseminen on tehtävä kohdeorganisaation itsensä toimesta. Se on juuri sitä käytännön riskienhallintatyötä, joka lisää erityisesti organisaation johdon osalta riskienhallintaan ja turvallisuuteen liittyvää tietoisuutta ja osaamista.

5.2 Eduskunnan kanslian mahdolliset tulevaisuuden turvallisuusympäristöt

Tulevaisuutta ei voi ennustaa, mutta tulevaisuuden vaihtoehtoisia kehityssuuntia voidaan yrittää hahmotella. Vaihtoehtoisten tulevaisuuspolkujen hahmottelu edellyttää nykyisyydessä vaikuttavien ilmiöiden hyvää tuntemusta ja kykyä ajatella luovasti – on uskallettava käydä läpi myös nykyisyyteen suhteutettuna absurdilta tai mahdottomalta tuntuvat tulevaisuuden kehityksen vaihtoehdot.

Paras tapa vaikuttaa tulevaisuuteen on vaikuttaa nykyisyydessä tapahtuvaan toimintaan. Tulevaisuuden skenaariotyöskentelyn tarkoitus ei ole lietsoa pelkoa saati epätoivoa, vaan tarkoitus on motivoida toimimaan nykyisyydessä siten, ettei organisaation oma toiminta ainakaan edesauta skenaariotyöskentelyssä esille nousseiden ja epäsuotuisiksi määriteltyjen kehityssuuntien toteutumista tulevaisuudessa.

Tulevaisuudentutkimukseen liittyy kysymys tiedon luotettavuudesta ja tiedon yksittäisten tulevaisuutta koskevien väittämien merkityksestä. Tulevaisuudentutkimusta ja siinä esitettyjen väittämien arviointia auttaa osaltaan tiedon luokittelu ja eri luokkien merkityksen ymmärtäminen (Taulukko 11).

Varma tieto	<ul style="list-style-type: none"> • vain yksi vaihtoehto
Todennäköinen tieto	<ul style="list-style-type: none"> • yksi vaihtoehto ylitse muiden
Epävarma tieto	<ul style="list-style-type: none"> • aidosti useita erilaisia samanarvoisia vaihtoehtoja
Heikko signaali	<ul style="list-style-type: none"> • ei tunnisteta muuttujaa eikä vaihtoehtoja, toteutuessaan suuri vaikutus
Megatrendi	<ul style="list-style-type: none"> • muuttuja ja vaihtoehdot tunnistettu todennäköinen toteutuminen ja suuri vaikutus
Musta joutsen	<ul style="list-style-type: none"> • vaihtoehto, jonka piti olla mahdoton
Tabu	<ul style="list-style-type: none"> • tietoisesti tai tiedostamatta vaiettu muuttuja tai jokin sen vaihtoehdon arvo

Taulukko 11: Tulevaisuustiedon tyypittely Meristöä ja Kivelää mukailten (2011)

Heikolla signaalilla tarkoitetaan tulevaisuuden ilmiötä, jolla on pieni toteutumistodennäköisyys, mutta toteutuessaan suuri merkitys. Heikon signaalin hyödyntämisestä tekee hankalaksi havaitsemisen lisäksi sen lyhyt elinkaari; kehityttyään vahvaksi signaaliksi on sen arvo heikkona signaalina samalla mitätöitynyt. Heikkojen signaalien suhteen on hyvä muistaa niiden suhteellisuus – yhtäällä määritelty heikko signaali saattaa toisaalla olla jo trendi. (Mannermaa 2004, 44, 121.)

Megatrendillä tarkoitetaan ilmiötä tai ilmiökokonaisuutta, jolla nähdään olevan tunnistettava suunta ja jonka uskotaan jatkuvan samansuuntaisesti myös tulevaisuudessa. Megatrendien avulla voidaan jäsentää kehitysilmioita ja ymmärtää olennaisia toimintaympäristön tapahtumia. Mannermaa kuvaa megatrendejä havainnollisesti suureksi joeksi, joka virtaa kohti merta – joessa on parempi soutaa myötävirtaan. (Mannermaa 2004, 73–74.)

Eduskunnan kanslian turvallisuustoiminnan ja riskienhallinnan kehittäminen vaativat niiden osalta tehtävää strategista suunnittelua ja strategisen tason päätöksiä. Kumpaakaan niistä ei myöskään voida kestävästi ja uskottavasti suunnitella ilman, että huomioidaan eduskunnan kanslian toimintaympäristö ja turvallisuusympäristö tulevaisuuden kehitysnäkymät mukaan lukien.

Tässä luvussa pyritään kuvaamaan eduskunnan kanslian turvallisuusympäristössä tapahtuvia muutoksia ja vaihtoehtoisia kehityskulkuja tulevaisuudentutkimukseen liittyvän aiheskenaariotyöskentelyn avulla. Skenaariotyöskentelyssä huomioidaan äkillisten muutosten lisäksi pitkäaikaiset demograafiset ja muut yhteiskunnalliset muutosten mahdollisuudet, jolloin työskentelyn aikajänteen voidaan sanoa ulottuvan vähintään 2020–2030 luvuille asti.

Eduskunnan kanslian tulevaisuuden turvallisuusympäristön tarkastelun tarkoitus on mahdollistaa systemaattiseen analyysiin pohjautuvat perustelut opinnäytetyössä esitetyille eduskunnan kanslian turvallisuustoiminnan ja riskienhallinnan kehittämisehdotuksille.

5.2.1 Valtionhallinnon turvallisuusympäristöä kuvaava tulevaisuustieto

Tässä luvussa käsiteltävä tulevaisuustieto on kerätty valtionhallinnon turvallisuusympäristön näkökulmasta. Aineisto koostuu pääasiassa ministeriöiden ja valtioneuvoston kanslian tulevaisuusksatsauksista, niiden strategioista ja muista julkaisuista sekä tulevaisuudentutkijoiden julkaisemista tutkimusartikkeleista tai kirjallisuudesta. Huomioon on otettu myös vuoden 2010 lopulla päivitetty yhteiskunnan turvallisuusstrategia (YTS).

YTS on valtioneuvoston ensisijaisesti ministeriöille laatima ohjausasiakirja. Strategiassa painottuvat yhteiskunnan varautuminen sekä kriisijohtaminen niin normaali- kuin poikkeusoloisakin. Strategiassa esitellyt uhkamallit kattavat

- voimanhuollon
- tietoliikenteen ja tietojärjestelmät (kyberuhkat)
- yhdyskuntatekniikan, kuljetuslogistiikan ja elintarvikehuollon
- rahoitus- ja maksujärjestelmän ja julkisen talouden rahoituksen saatavuuden
- väestön terveyden ja hyvinvoinnin
- suuronnettomuudet, luonnon ääri-ilmiöt ja ympäristöuhkat
- terrorismin ja muun yhteiskuntajärjestystä vaarantavan rikollisuuden
- rajaturvallisuuden
- poliittisen, taloudellisen ja sotilaallisen painostuksen
- sotilaallisen voiman käytön. (YTS 2010, 15–16.)

Yhteiskunnan turvallisuusstrategiassa esitetyt uhkamallit on tarkoitettu yhteismitallisiksi varautumisen lähtökohdaksi ja tausta-aineistoksi. Eri uhkamallit voivat itsenäisen esiintymisen lisäksi ilmaantua samanaikaisina tai toistensa jatkumoina. Uhkien toteutumisen todennäköisyyttä on vaikea luotettavasti ennustaa. (YTS 2010, 16.)

Toimintaympäristön muuttujia käsiteltäessä yleisesti käytettyä PESTE-mallia ei tässä yhteydessä käytetä kerätyn tulevaisuustiedon jäsentelyyn siksi, että tulevaisuusväittämät olisivat sopineet jaoteltavaksi useampaan kohtaan luokissa poliittinen, taloudellinen, sosiaalinen, teknologinen ja ympäristönsuojelullinen. Saman tulevaisuutta koskevan väittämän esiintyminen useassa luokassa saattaisi puolestaan antaa vääristyneen kuvan väittämien todellisesta merkityksestä tai niiden toteutumisen todennäköisyydestä.

PESTE -jaottelun sijaan kerätty tulevaisuustieto on käsittelyn helpottamiseksi jäsennelty taulukon 12 seuraavan jaon mukaan

- globaali keskinäisriippuvuus
- Suomen väestö ja arvot
- poliittinen päätöksenteko
- luonnonvarat ja yhteiskunnan huoltovarmuus.

GLOBAALI KESKINÄISRIIPPUVUUS

- Laaja-alainen globaali epävarmuus lisääntyy: maailmantalouden haavoittuvuus, kulttuurien konfliktit, ympäristö- ja kehitysongelmat, terrorismi (Mannermaa 2004).
- Nykyinen kansainvälinen järjestelmä ei kestä tulevaisuuden kriisejä. Globaalit rakenteet ja käytännöt on uusittava moninapaistumisen ja epävirallisten ja ei-valtiollisten toimijoiden merkityksen lisääntyessä. Globaalihallinnan tulevaisuuden haasteet ovat energia, ruoka, veteen kohdistuva resurssikiipailu, siirtolaisuus, arktinen alue ja biotekniikka. (EUISS 2010, 22–30, 52–56: Valtioneuvoston kanslia 2007, 25.)
- Globalisaatio lisää vaurautta, mutta vauraus jakautuu epätasaisesti maiden välillä ja johtaa yhteiskuntien sisällä syveneviin hyvinvointikiiluihin ja syrjäytymiseen (Ulkoasiainministeriö 2006). Kansainvälisen talouden levottomuus kasvaa (Valtioneuvoston kanslia 2010). Resurssit niukkenevat ja on pakko keskittyä olennaiseen (Tekes 2009).
- Uhkaympäristö muuttuu yllätyksellisemmäksi ja vakavammaksi, ulkoinen ja sisäinen turvallisuus kytkeytyvät tiiviimmin yhteen. (Puolustusministeriö 2011a, 3; ESDA 2010; Valtioneuvoston kanslia 2007, 72–73).
- Turvallisuusongelmien vaikutukset välittyvät entistä nopeammin ja laajemmalle alueelle. Alueellisten konfliktien vaikutukset heijastuvat laajasti, ja niihin kytkeytyy muita uusia rajat ylittäviä turvallisuusuhkia. (Puolustusministeriö 2006.) Kansainvälisiin kriisinhallintaoperaatioihin osallistuminen saattaa lisätä terrori-iskujen uhkaa Suomessa (Puolustusministeriö 2011a, 4; Sisäasiainministeriö 2010, 6).
- Suureen tuho vaikutukseen pyrkivän kansainvälisen terrorismin globaali uhka lisääntyy (Puolustusministeriö 2006). Inhimillinen turvattomuus ja valtioihin kohdistuvat uhat lisääntyvät (Ulkoasiainministeriö 2006; Puolustusministeriö 2011a, 4).
- Epäsymmetrinen sodankäynti yleistyy ja niihin kytkeytyy muita uusia rajat ylittäviä turvallisuusuhkia (Puolustusministeriö 2006).
- Tuleva talouskehitys ja julkisen talouden kestävyysvajeeseen vastaaminen: edellyttävät valtioneuvoston toiminnan entistä keskitetympää strategista ohjausta ja tätä tukevia päätöksentekofoorumeita, prosesseja ja hyvää tietopohjaa (Valtioneuvoston kanslia 2010).

SUOMEN VÄESTÖ JA ARVOT

- Työikäinen väestö alkaa supistua Suomessa (Valtioneuvoston kanslia 2010; Puolustusministeriö 2006). Työelämään siirtyvät ”pienet ikäluokat” suhtautuvat vapaa-aikaansa ja harrastuksiinsa suuria ikäluokkia intohimoisemmin, mikä saattaa johtaa työelämän kulttuurin muutokseen, jossa työntekijöiden sitoutuminen työhön ja lojaliteetti työnantajaa kohtaan ovat astetta aiempaa ohuempia (EVA 2010, 38).
- Sosiaaliseen kestävyysongelmat (Valtioneuvoston kanslia 2009). Alueet ja kansalaiset eriarvoistuvat (Heinonen 2008; Tulevaisuuden tutkimuskeskus 2011; OECD 2003). Pieni eliitti kuroo komean kaulan muihin väestöryhmiin, tuntuva osa syrjäytyy, keskiluokka sinnittelee. (Mannermaa 2004.)
- Väestö keskittyy suuriin keskuksiin tai niiden ympäriskuntiin (Mannermaa 2004). Keskityminen on erityisen voimakasta pääkaupunkiseudulla (Puolustusministeriö 2011b, 5). Woody Allen -yhteiskunta: tulevaisuudessa yhteiskunta on aina auki 24 tuntia vuorokaudessa, seitsemän päivää viikossa (Mannermaa 2004).
- Yhteiskunnan arvostukset kehittyvät edelleen yksilöllisyyttä korostavaan suuntaan. Yleinen välinpitämättömyys kasvaa. (Heinonen 2008.) Kansallisvaltiot ovat menettämässä ar-

vomonopoliaan virtuaalisille yhteisöille. (Heinonen 2008.) Tietoyhteiskuntakehitys syrjäyttää osan kansalaisista (Kaivo-oja 2011)

- Kansakunnat polarisoituvat etnisen alkuperän, kielen tai uskonnon perusteella (Puolustusministeriö 2007). Etnisiin vähemmistöryhmiin tai niiden uskontoon kohdistuvat negatiiviset asenteet tai selkeän maahanmuuttopolitiikan puuttuminen saattavat pitää terrorismin uhkaa korkeana. Toisen tai kolmannen maahanmuuttajasukupolven lukumäärä Suomessa kasvaa ja heidän kokema irrallisuus yhteiskunnasta voi johtaa väkivaltaiseen toimintaan radikalisoitumisen seurauksena. (Sisäasiainministeriö 2010, 5–6.)
- Järjestäytyneen rikollisuuden määrä kasvaa. Se tiivistää verkostojaan ja keskinäistä yhteistyötään. (Puolustusministeriö 2011a, 3; KRP 2009).
- Kansallisvaltiot voivat pian huomata olevansa yhä useammin vastakkain omien kansalaistensa kanssa hillitsemässä milloin mitään paikallista, kansallista tai kansainvälistä mellakkaa (Heinonen 2008; Valtioneuvoston kanslia 2007, 70). Luottamus ja arvostus politiikkaa ja instituutioita kohtaan heikentyy. Kansalaiset irtaantuvat "virallisesta Suomesta" vetäytyen yksityiselämänsä piiriin. (Valtioneuvoston kanslia 2007, 69).
- Suurten ikäluokkien korvautuminen nuorilla työelämässä saattaa johtaa työmarkkinoiden siirrosta "työntekijöiden markkinoiksi" (EVA 2010, 36).
- Tieto- osaamis- ja merkitysintensiivisessä yhteiskunnassa syrjäytymisen riski on yhä suurempi: osallisuuden, luottamuksen ja koko yhteiskunnan voimavarojen hyödyntämisen ongelmat (Tulevaisuuden tutkimuskeskus 2011).
- Suomi on polarisoitumassa ja eriarvoistumassa ja tämä aiheuttaa syrjäytymistä ja rikollisuutta (Tulevaisuuden tutkimuskeskus 2011). Ääri-ilmiöiden sekä väkivaltaisen henkeen ja omaisuuteen kohdistuvan rikollisuuden todennäköisyys kasvaa (Heinonen 2008).
- Rakenteelliset erot: taloudelliset erot kasvavat olennaisesti. Pieni eliitti kuroo komean kaulan muihin väestöryhmiin, tuntuva osa syrjäytyy, keskiluokka sinnittelee (Mannermaa 2004).
- Monikulttuuriset yhteiskunnat ovat kulttuurin näkökulmasta rikkaita, mutta näyttäisivät haavoittuvaisemmilta muun muassa kanssakäymiseen ja kommunikointiin sisältyvien potentiaalisten väärinymmärrysten ja virhetulkintojen takia. (Heinonen 2008.)
- Eri konfliktialueiden terrorismiin kytköksissä olevin henkilöiden määrän kasvu Suomessa saattaa nostaa terroriuhan tasoa (Sisäasiainministeriö 2010, 6).
- Suomesta osallistutaan ulkomailla toimivien terroristiverkostojen tukemiseen (Sisäasiainministeriö 2010, 6; SUPO 2009).
- Terroristien kohteena olevien valtioiden Suomessa oleviin lähetystöihin ja muihin intresseihin kohdistuva uhka kasvaa (Sisäasiainministeriö 2010, 7).

POLIITTINEN PÄÄTÖKSENTEKO

- Valtion merkitys heikkenee, kun rajat ylittävä kansalaisvaikuttaminen lisääntyy globalisaation sosiaalisten vaikutusten, ilmastonmuutoksen, asevalvonnan ja yksilön turvallisuuden suhteen (Valtioneuvoston kanslia 2007, 25).
- Kehittyneet hyvinvointivaltiot ovat aikaisempaa alttiimpia sisäiselle epävakaudelle. Poliittisten ääriliikkeiden vaikutuksen kasvu voi lisätä väkivaltaisia protesteja ja kotoperäistä terrorismia. (Puolustusministeriö 2006.)

- Avoimuuden vaatimukset korostuvat entisestään ja kansalaisten mahdollisuudet vaikuttaa päätöksiin jo niiden valmisteluvaiheessa tulevat lisääntymään (Valtioneuvoston kanslia 2010). Yksilöiden merkitys kasvaa. Yksittäiset ihmiset voivat saada aikaan globaaleja vaikutuksia muun muassa median ja uuden teknologian avustuksella. (Heinonen 2008.)
- Teknologian kehitys lisää ei-valtiollisten toimijoiden vaikuttamismahdollisuuksia (Puolustusministeriö 2011a, 4). Teknologian kehitys ja uusien teknologioiden käyttöönotto nopeutuvat. Samalla turvallisuusriskit kasvavat (Puolustusministeriö 2006). Yksittäisillä henkilöillä tai ryhmittymillä voi olla tekniset mahdollisuudet aiheuttaa sellaista laajamittaista vahinkoa, johon aiemmin pystyivät vain valtiolliset toimijat (Puolustusministeriö 2011a, 4; OECD 2003).
- Turvallisuusympäristön strategisen tason seurannan, arvioinnin ja ennakoivien päätösten merkitys kasvaa tulevaisuudessa (Puolustusministeriö 2006). Ennakoinnin ja ennalta ehkäisyksen merkitys kasvaa monimutkaistuvassa ja nopeutuvassa maailmassa. (Heinonen 2008.)
- Kansakunnat joutuvat voimakkaasti erikoistumaan tietyille suppeille osaamisalueille. Tiedustelu yhteistyö syvenyy. (Puolustusministeriö 2007.) Suomi on jatkuvan tiedustelun kohteena, eikä perinteiset vakoilun keinot ole menettäneet merkitystään (Puolustusministeriö 2011a, 3). EU-maana Suomi säilyy jatkossakin merkittävänä kohteena useammille tiedustelupalveluille (SUP0 2009).
- Yhteistoiminnan lisääntyminen ja syveneminen NATO:n kanssa voi johtaa Suomen Venäjä-suhteiden kannalta ristiriitaisiin tilanteisiin (esimerkiksi meriliikenteen valvonnan suhteen) (Puolustusministeriö 2007).
- Euroopan Unionin sisäiset haasteet ja hajoamisen uhka (Ulkoasiainministeriö 2011).
- Poliittisten ääri liikkeiden vaikutuksen kasvu voi lisätä väkivaltaisia protesteja ja kotopäisiä terrorismia. (Puolustusministeriö 2006).
- Informaatioteknologian sovellutusten leviäminen mahdollistaa poliittisten aatteiden ja käytäntöjen tarkoitushakuisen ja nopean leviämisen (Puolustusministeriö 2006).
- Demokratia kriisiytyy (Valtioneuvoston kanslia 2007, 69; Tulevaisuusvaliokunta 2007; Mannermaa 2006)
- Poliittiseen päätöksentekoon liittyvä korruptio lisääntyy virka- ja lahjusrikosten muodossa (KRP 2011).

LUONNONVARAT JA YHTEISKUNNAN HUOLTOVARMUUS

- EU:n riippuvuus tuontienergiasta nousee nykyisestä 50 %:sta 70 %:in vuoteen 2030 mennessä. Öljyn tuonnin osalta riippuvuus tulee olemaan jopa 90 % ja kaasun osalta 80 % vuonna 2025. Epätasapaino muidenkin luonnonvarojen kysynnän ja tarjonnan välillä kärjistyy. (Valtioneuvoston kanslia 2007, 45–45; Puolustusministeriö 2006.)
- Puhtaan juomaveden puute on ongelma yli puolelle maailman väestöstä vuonna 2030. Veden merkitys maailmanpolitiikassa ja konfliktien aiheuttajana kasvaa. (Puolustusministeriö 2006.)
- Yhteiskunta kehittyy ympäristöksi, jossa yhä useammat palvelut ovat tietoteknisesti ohjattuja tai kokonaan sähköisiä, yhteiskunnan haavoittuvuus lisääntyy (Puolustusministeriö 2011a, 3). Symmetrinen ja asymmetrinen informaatio- ja tietoverkkosodankäynti yleistyy saaden uusia muotoja, kohteita ja vaikutuskanavia. Kynnys keinovalikoiman käyttöön laskee ja toimijoina ovat valtiollisten lisäksi ei-valtiolliset toimijat, kuten rikolliset tai po-

liittisesti motivoituneet ryhmittymät tai yksilöt. (Puolustusministeriö 2011a, 3.)

- Informaatio- ja tietoverkkosodankäynnin kohteina voivat päättäjien, kansalaisten ja tiedotusvälineiden lisäksi olla energianlähteet, tietoverkot tai maanpuolustuksen keskeiset elementit. (Puolustusministeriö 2011a, 4). Infrastruktuurin toimintakatkokset yleistyivät (Heinonen 2008). Voimanhuollon vakavat häiriöt valtakunnallisessa kanta- ja jakeluverkossa vaikuttavat yhteiskunnan toimivuuteen (YTS 2010, 67).
- Yhteiskunnan kriisikestävyys, osaaminen, huoltovarmuus ja infrastruktuurin kehittäminen vaatii kansallista verkottumista ja yhteistyötä (Puolustusministeriö 2011b, 3; Sisäasiainministeriö 2010, 2). Haasteet kasvavat ja resurssit pienenevät (ESDA 2010).
- Ääriliikkeet sekä erilaiset kansalliset ja kansainväliset keinoja kaihtamattomat järjestöt nostavat suosiotaan. Anarkistinen toiminta ei ole pelkästään viranomaisten toimintaa vastustavaa, vaan yhteiskunnan rakenteisiin ja infrastruktuuriin kohdistuvaa vandalismia ja myös järjestäytyntä rikollisuutta. (Heinonen 2008.)
- Kemiallisten, biologisten ja säteilevien aineiden käyttömahdollisuus terroriteoissa on tulevaisuudessa vakava uhka (Puolustusministeriö 2011a, 4).
- Barentsin meren energiavarojen omistuksesta ja hyödyntämisestä sekä Itämeren laivaliikenteen kysymykset tuottavat erimielisyyksiä asianomaisten valtioiden välille (Puolustusministeriö 2007).

Taulukko 12: Valtionhallinnon turvallisuusympäristöön vaikuttava tulevaisuustieto

Edellä esiteltyyn taulukkoon 12 kerätystä tulevaisuustiedosta voidaan muotoilla seuraavat valtionhallinnon turvallisuusympäristöön vaikuttavat megatrendit, joiden toteutuminen on todennäköistä ja vaikutus suuri

1. taloudelliset resurssit niukkenevat
2. toiminnan tehokkuusvaatimukset lisääntyvät
3. työikäisten määrä vähenee, kilpailu työntekijöistä kovenee
4. yhteiskunta eriarvoistuu
5. yksilön vaikutusmahdollisuudet lisääntyvät
6. valtion merkitys heikkenee
7. kansallisvaltion sisäiset uhkat lisääntyvät
8. yhteiskunnan haavoittuvuus lisääntyy
9. kansainväliset turvallisuusuhkat vaikuttavat myös Suomessa
10. globaali resurssien väheneminen johtaa voimistuviin riippuvuussuhteisiin.

Taulukkoon 12 kerätystä tulevaisuustiedosta voidaan lisäksi johtaa seuraavat, valtionhallinnon turvallisuusympäristöön mahdollisesti vaikuttavat heikot signaalit, joiden toteutuminen on epätodennäköistä, mutta vaikutus toteutuessaan suuri

1. kriisinhallintaoperaatiot heijastuvat turvallisuusuhkina Suomessa
2. ääriliikkeet yleistyvät ja ilmaisevat itseään avoimen väkivaltaisesti
3. väkivalta suunnataan instituutioita ja yhteiskunnan rakenteita vastaan

4. suomesta kehittyä luokkayhteiskunta
5. yhteiskunnan alakulttuurien omavaltainen välienselvittely lisääntyy
6. valtionhallinto modernisoituu harppauksella
7. demokratian muoto muuttuu
8. lähialuepolitiikka kärjistyy
9. väkivallanteot siirtyvät työyhteisöihin
10. työntekijöiden lojaalisuus työnantajaa kohtaan heikkenee

5.2.2 Eduskunnan kanslian toimintaympäristön PESTE-analyysi

Valtionhallinnon turvallisuusympäristön lisäksi on syytä paneutua eduskunnan kanslian toimintaympäristöön. Organisaation toimintaympäristön analyysin tarkoitus skenaariotyöskentelyprosessissa on kartoittaa organisaation nykytilaa; vahvuudet, heikkoudet, mahdollisuudet, uhkat, käytettävissä olevat resurssit ja mahdolliset kehityskulkuun vaikuttavat ulkoiset tekijät (NexusSkenarix 2011). PESTE-analyysi auttaa toimintaympäristön kokonaisvaltaisessa tarkastelussa, sillä sen avulla tarkastellaan organisaatiota eri sektoreiden näkökulmasta, toimintaympäristön eri ulottuvuuksista sekä organisaation toimintaan vaikuttavat osapuolet huomioon ottaen.

Eduskunnan kansliaa koskevan PESTE -analyysin pohja-aineistona käytetään eduskunnan kanslian vuoden 2010 strategiatyön aikana laadittua toimintaympäristön analyysia (PEST), jota on täydennetty ympäristövaikutusten osalta (E). Lisäksi analyysiin on sisällytetty eduskunnan strategiatyöskentelyn aikana esille nousseet toimintaympäristön muutoksiin liittyvät ja eduskunnan kanslian toimintaan vaikuttavat haasteet, joita ovat

- eduskunnan arvostuksen vahvistaminen instituutiona
- valtionhallinnon keulakuvana toimiminen (tuottavuusajattelun soveltamisessa)
- kilpailukyvyyn säilyttäminen työpaikkana
- tiivis ja aito yhteistyö muun valtionhallinnon kanssa (tiedonvälitys ja -hallinta) sekä
- eduskunnan uudenaikaistaminen (organisaation joustavuus, muutosvalmius ja sähköisten toimintamallien kehittäminen). (Eduskunnan kanslian hallintotoimisto 2010.)

PESTE-analyysin (Kuvio 15) loppuun liitetyt kentät kuvaavat sidosryhmien erilaista asemaa, vaikutusta, motiiveja, intressejä ja toimintatapaa suhteessa eduskunnan kansliaan. Kuvausten avulla hahmotellaan eri toimijoiden merkitystä ja roolia erityisesti eduskunnan kanslian sisäisestä näkökulmasta. On huomioitava, että saman harjoituksen sitominen esimerkiksi organisaatiturvallisuuden näkökulmaan tuottaisi erilaisen tuloksen. Siinä tapauksessa myös kansalaiset voisivat saada käsikirjoittajan aseman – onhan yksittäisten ihmisten vaikutusvalta edelleen kasvussa ja kynnys suoraan toimintaan samaan aikaan silminnähden laskussa.

P (poliittinen)	E (taloudellinen)	S (sosiaalinen)	T (teknologinen)	E (ympäristö)
<p>EU ja maailma</p> <ul style="list-style-type: none"> • globaalien rakenteiden muutokset • yhteiskuntien (yhteisöjen) monimuotoistuminen ja muutosten nopeutuminen • tehokkuus- ja tuottavuusajattelun korostuminen • tiedonvirtojen kasvu, informaatiotulva • luonnonilmiöiden kärjistyminen ja yleistymisen • kestävä kehitystä tukevien toimintamallien yleistymisen • luonnonvarojen niukkeneminen • keskinäisriippuvuuden ja seurannaisvaikutusten lisääntyminen 				
<p>Suomi ja lähialueet</p> <ul style="list-style-type: none"> • mahdolliset puoluerakenteiden ja -toiminnan muutokset • suurten ikäluokkien eläköityminen • yhteiskunnan monimuotoistuminen ja muutosten nopeutuminen • tehokkuus- ja tuottavuusajattelun korostuminen • tiedonvirtojen kasvu, informaatiotulva • viestintätekniikan jatkuva kehittyminen • sähköisen toimintaympäristön yleistymisen • parlamentarismin arvostuksen ja äänestysaktiivisuuden muutokset, loitontuminen poliittisesta keskustelusta • luonnonilmiöiden kärjistyminen ja yleistymisen • kestävä kehitystä tukevien toimintamallien vaatimuksen yleistymisen 				
<p>Eduskunnan kanslia</p> <ul style="list-style-type: none"> • parlamentarismin arvostuksen lasku, maineriskit • mahdolliset puoluerakenteiden ja -toiminnan muutokset • henkilöstön eläköityminen, kilpailu työvoimasta • yhteiskunnan monimuotoistuminen ja muutosten nopeutuminen • sähköisen toimintaympäristön yleistymisen • tehokkuus- ja tuottavuusajattelun korostuminen • kestävä kehitystä tukevien toimintamallien vaatimuksen yleistymisen 				
Käsikirjoittajat	valtionneuvosto, eduskuntaryhmät, puhemies, kansliatoimikunta, johtoryhmä			
Kuiskaajat	poliittiset puolueet, valtionneuvoston kanslia, valtionkonttori, yksityinen tutkija- ja tiedeyhteisö, media			
Ohjaajat	presidentti, puhemies, kansliatoimikunta, eduskuntaryhmät, virkamiesjohto			
Rahoittajat	kansalaiset, eduskunnan kanslia, valtiovarainministeriö			
Näyttelijät	puhemies, eduskuntaryhmät, toimikunnat, johtoryhmä, henkilöstö, media			
Katsojat	kansalaiset, henkilöstö, media			

Kuvio 15: Eduskunnan kanslian PESTE-analyysi

Eduskunnan kanslian PESTE-analyysissä on nähtävissä heijasteita organisaatioturvallisuuden eri osa-alueista. Analyysissä kuvatuista ilmiöistä turvallisuuteen eniten vaikuttavia ovat

- luonnonilmiöiden kärjistyminen ja yleistymisen
- luonnonvarojen niukkeneminen

- keskinäisriippuvuuden ja seurannaisvaikutusten lisääntyminen
- sähköisen toimintaympäristön yleistymisen
- parlamentarismin arvostuksen ja äänestysaktiivisuuden muutokset, loitontuminen poliittisesta keskustelusta
- parlamentarismin arvostuksen lasku
- mahdolliset puoluerakenteiden ja -toiminnan muutokset
- henkilöstön eläköityminen, kilpailu työvoimasta
- kestävän kehitystä tukevien toimintamallien vaatimuksen yleistymisen.

Vaikka organisaatioihin yleensä viitataan ikään kuin itsenäisinä subjekteina, on tärkeää muistaa, että niiden toiminta on itse asiassa organisaatioissa vaikuttavien ihmisten toimintaa. Eduskunnan kanslia on tässä suhteessa poikkeuksellisen monimuotoinen organisaatio – henkilöstön eri ryhmien lisäksi siihen vaikuttavat muun muassa kansanedustajat, media ja kansalaiset. Voimakkaimmin organisaatioon vaikuttavat käsikirjoittajat, ohjaajat ja rahoittajat. Kuis-kaajat, näyttelijät ja katsojat ovat passiivisemmassa, mutteivät suinkaan merkityksettömässä roolissa. Eduskunnan kanslian toimintaan vaikuttaminen edellyttää kaikkiin edellä mainittuihin tahoihin vaikuttamista sekä niiden erilaisten ja mahdollisesti keskenään ristiriitaistenkin tarpeiden ymmärtämistä.

5.2.3 Eduskunnan kanslian turvallisuusympäristön ennakointiteemat

Tausta-aineisto työstetään skenaarioiksi tulevaisuustaulukoiden ja aineiston teemoittelun avulla. Valtionhallinnon turvallisuusympäristöä kuvaava tulevaisuustieto on ryhmitelty yhteiskunta- ja teknologiateemoihin taulukossa 13. Osa väittämistä sopii molempiin teemoihin. Skenaariotyöskentelyssä käytetään yleensä myös markkinat -teemaa, joka on tässä kehittämistyössä jätetty pois, koska yhteiskunta- ja teknologiateemat mahdollistavat eduskunnan turvallisuusympäristön muutoksien hahmottamisen tämän kehittämistyön kannalta riittävällä syvyydellä.

Teemat	
Teknologia	<ul style="list-style-type: none"> • taloudelliset resurssit niukkenevat • toiminnan tehokkuusvaatimukset lisääntyvät • työikäisten määrä vähenee, kilpailu työntekijöistä kovenee • yksilön vaikutusmahdollisuudet lisääntyvät • valtion merkitys heikkenee • yhteiskunnan haavoittuvuus lisääntyy • kansainväliset turvallisuushkat vaikuttavat myös Suomessa • globaali resurssien väheneminen johtaa voimistuviin riippuvuussuhteisiin • valtionhallinto modernisoituu harppauksella • demokratian muoto muuttuu • työntekijöiden lojaalisuus työnantajaa kohtaan heikkenee

Yhteiskunta	<ul style="list-style-type: none"> • taloudelliset resurssit niukkenevat • työkäisten määrä vähenee, kilpailu työntekijöistä kovenee • yhteiskunta eriarvoistuu • yksilön vaikutusmahdollisuudet lisääntyvät • valtion merkitys heikkenee • kansallisvaltion sisäiset uhkat lisääntyvät • yhteiskunnan haavoittuvuus lisääntyy • kansainväliset turvallisuusuhkat vaikuttavat myös Suomessa • globaali resurssien väheneminen johtaa voimistuviin riippuvuussuhteisiin • kriisinhallintaoperaatiot heijastuvat turvallisuusuhkina Suomessa • ääriliikkeet yleistyvät ja ilmaisevat itseään avoimen väkivaltaisesti • väkivalta suunnataan instituutioita ja yhteiskunnan rakenteita vastaan • suomesta kehittyi luokkayhteiskunta • yhteiskunnan alakulttuurien omavaltainen välienselvittely lisääntyy • demokratian muoto muuttuu • lähialuepolitiikka kärjistyy • väkivallanteot siirtyvät työyhteisöihin • työntekijöiden lojaalisuus työnantajaa kohtaan heikkenee
-------------	---

Taulukko 13: Eduskunnan kanslian turvallisuusympäristön suodattimet ja ajurit

Konkretian vuoksi yllä oleva aineisto on ryhmitelty ja havainnollistettu myös eduskunnan kanslian organisaatioturvallisuuden näkökulmasta liitteessä 2.

Valtionhallinnon turvallisuusympäristöön vaikuttava tulevaisuustieto (megatrendit) ja eduskunnan kanslian PESTE-analyysin tulokset on yhdistetty skenaariotyöskentelyn ennakoititeemoiksi taulukossa 14. Ennakoititeemat toimivat skenaariotyöskentelyn pohjana ja niitä käsitellään yksityiskohtaisemmin myöhemmin tässä luvussa (Meristö & Tammi 2003, 15).

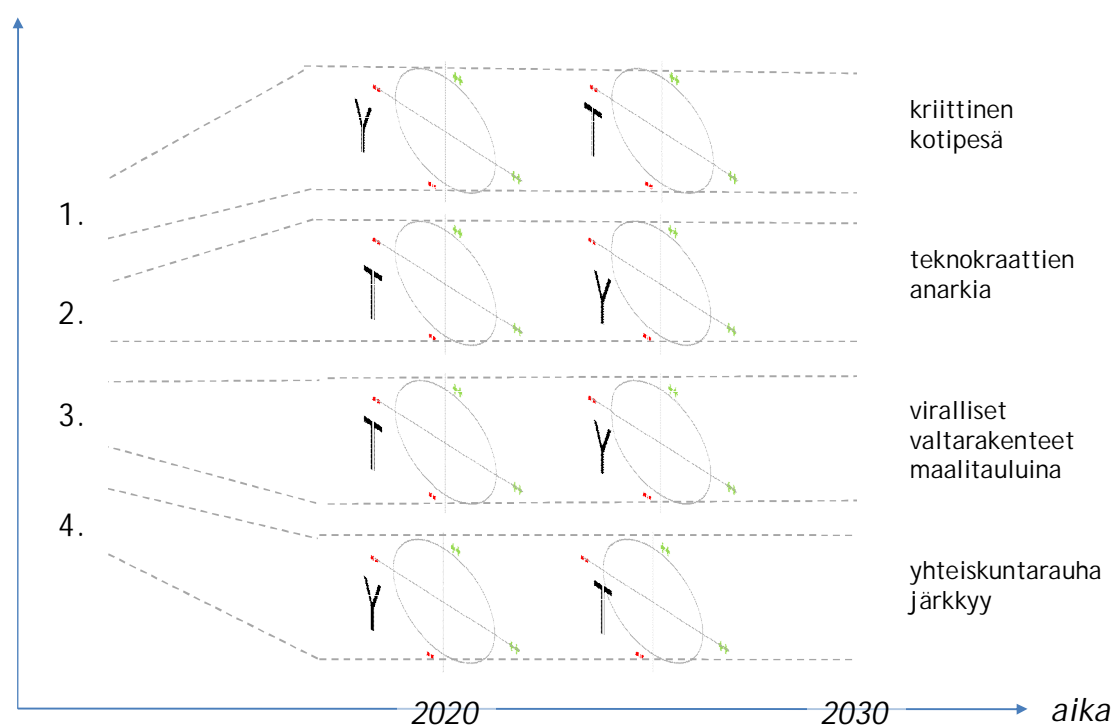
Tunnistetut ennakoititeemat			
1.	taloudelliset resurssit niukkenevat	11.	luonnonilmiöt kärjistyvät ja yleistyvät
2.	toiminnan tehokkuusvaatimukset lisääntyvät	12.	luonnonvarat niukkenevat
3.	työkäisten määrä vähenee	13.	keskinäisriippuvuus ja seurannaisvaikutukset lisääntyvät
4.	yhteiskunta eriarvoistuu	14.	sähköinen toimintaympäristö yleistyy
5.	yksilön vaikutusmahdollisuudet lisääntyvät	15.	äänestysaktiivisuus laskee, kansalaiset loitontuvat politiikasta
6.	valtion merkitys heikkenee	16.	parlamentarismin arvostus laskee
7.	kansallisvaltion sisäiset uhkat lisääntyvät	17.	puoluerakenteet ja -toiminta muuttuvat
8.	yhteiskunnan haavoittuvuus lisääntyy	18.	henkilöstö eläköityy, työvoimasta täytyy kilpailla
9.	kansainväliset turvallisuusuhkat vaikuttavat myös Suomessa	19.	kestävää kehitystä tukevien toimintamallien vaatimukset yleistyvät
10.	globaali resurssien väheneminen johtaa voimistuviin riippuvuussuhteisiin	20.	tehokkuus- ja tuottavuusajattelu korostuu

Taulukko 14: Tunnistetut ennakoititeemat skenaariotyöskentelyn taustalla

Ennakointiteemat on priorisoitava. Eduskunnan kanslian organisaatioturvallisuuden kehittämisen näkökulmasta katsottuna kriittisimmät ennakoititeemat liittyvät ensisijaisesti toiminnan jatkuvuuden turvaamiseen sekä eduskunnan ydintoimintojen suojaamiseen. Näiden kriteereiden pohjalta voidaan muodostaa neljä skenaariota.

Seuraavissa alaluvuissa esitellään eduskunnan kanslian organisaatioturvallisuuden kehittämisen pohjaksi rakennetut neljä skenaariota. Kustakin skenaariosta käsitellään niiden taustalla olevat oletukset skenaarioissa kuvatun kehityskulun aikaansaavista tapahtumista ja niiden vaikutuksista. Skenaariokohtaiset suodattimet on esitelty ristikkomuodossa, joihin on lisätty oletettu läpäisykohta, eli toteutumisaste. (Meristö & Tammi 2003, 26.)

Ensimmäiset skenaarioluonnokset esitellään kuviossa 16 niin kutsuttujen skenaarioputkien muodossa. Skenaarioputket osoittavat myös, mistä lähtöoletuksesta käsin kukin skenaario on muodostettu (Y=yhteiskunta, T=teknologia).



Kuvio 16: Skenaarioputket Meristöä & Tammea mukailien (2003)

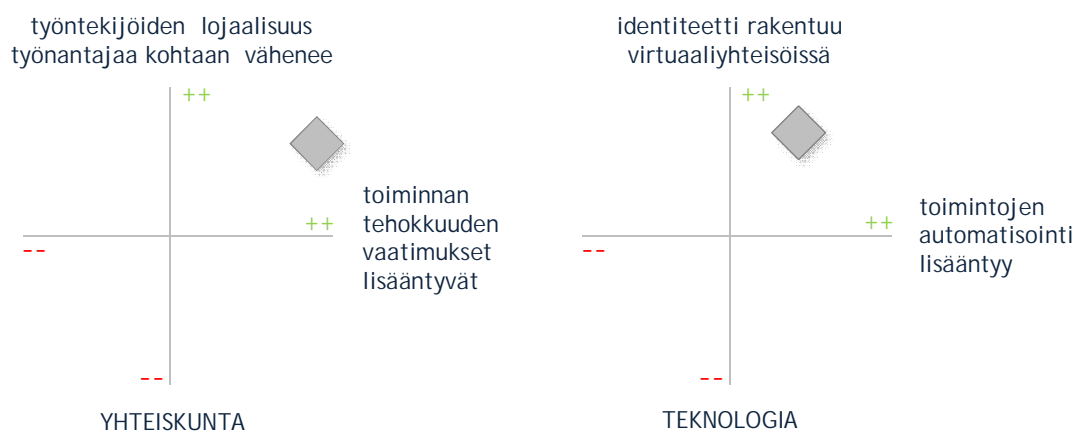
5.2.4 Skenaario 1: Kriittinen kotipesä

Skenaario yksi käynnistyy yhteiskunnassa tapahtuvien arvomuutosten pohjalta. Olettamuksena on, että ihmiset panostavat yhä enemmän vapaa-aikaan ja työnteon itseisarvo vähenee. Samaan aikaan resurssien niukkenemisen myötä työelämän suoritusten ja toimintojen tehokkuu-

delle asetetut vaatimukset kasvavat. Yksilön identiteetti rakentuu yhä voimakkaammin muiden kuin työhön liittyvien (virtuaali-)yhteisöjen kautta (harrastukset, järjestöt, asiantuntijaverkostot, sosiaalinen media ym.). Virtuaalisen ympäristön yleistymisen myötä teknologiaa kehitetään ja sitä hyödynnetään sekä yksityis- että työelämässä ja toimintaympäristö yleensäkin teknistyy.

Skenaarion yksi toteutuessa työnantajan tahto ei enää tavoita ja sitouta henkilökuntaa. Laiminlyönnit työyhteisössä voivat lisääntyä joko tiedostamatta tai tahallisesti. Identiteetin nojautuminen virtuaalisiin ympäristöihin voi tarkoittaa myös sen nopeaa murenemista ja vaikuttaen yksilöiden tasapainoisuuteen ja paineensietokykyyn. Teknologian mahdollistama nopea tiedonjakaminen ja toisaalta virtuaaliyhteisöjen sisäinen koheesio voi edesauttaa harkitsemattomia reaktioita vastoinkäymisiä kohdattaessa. Organisaatioturvallisuuden näkökulmasta skenaarion yksi toteutumisen kärjistetyimpiä ilmenemismuotoja voivat olla esimerkiksi

- työntekijöiden sitoutuminen työnantajaan heikkenee ja työssä koettu suorituspainee kasvaa aiheuttaen turhautumisen väkivaltaiseen purkamiseen työyhteisössä
- virtuaaliyhteisöt tukevat jäseniään kriittittömästi ja puolueellisesti, yksilön on mahdollista toimia nopeasti ja osittain huomaamatta turhautumisenkohdettaan vastaan
- vahingollisen toiminnan alullepanijaa on vaikea yksiselitteisesti osoittaa, mikä madaltaa edelleen toimintaan ryhtymisen kynnystä
- vahingonteot painottuvat verkkoympäristöön, tietoliikenteen häirintään, tietoverkkojen kaatamiseen ja vakoiluun.



Kuvio 17: Skenaario 1 – Kriittinen kotipesä

Skenaariossa yksi myös eduskunnan kanslian toimintaan vaikuttavissa sidosryhmissä tapahtuu muutoksia. Henkilöstön rooli korostuu. Työnantajan arvovalta saattaa heiketä ja auktoriteetiksi pyrkivältä vaaditaan yhä vahvempaa sisällöllistä osaamista. Työntekijöiden ensisijaiset kiinnostuksen ja sitoutumisen kohteet alkavat enenevässä määrin siirtyä työelämän ulkopuo-

lelle. Työyhteisön sisäiset jännitteet kasvavat yhtäältä tehokkuusvaatimusten myötä ja toisaalta sähköisen toimintatavan yleistymisen aiheuttamien henkilöstöpoliittisten muutosten takia. Lisäksi työyhteisössä koetut haasteet leviävät herkästi julkiseen keskusteluun sosiaalisen median yleisyyden ja työntekijöiden turhautumisen seurauksena. Eduskunnan kanslian viestinnän aktiivisuus ja johdonmukaisuus sosiaalisilla viestintäfoorumeilla korostuu.

Eduskunnan kanslian turvallisuustoiminnan vahvuudet skenaarion yksi suhteen ovat tekninen tietoturvallisuus, monipuolinen ja tehokas työterveydenhoito, työsuojelutoiminta ja henkilöstöryhmien sisäinen koheesio. Heikkouksia puolestaan ovat vahvan ja yhtenäisen organisaatiokulttuurin puute, henkilöstön huono turvallisuustietoisuus, turvallisuustoiminnan painottuminen teknisiin osa-alueisiin, passiivinen maineenhallinta ja toiminnan jatkuvuuden varmistaminen. Skenaariossa yksi painottuvat erityisesti taloudelliset, operatiiviset ja vahinkoriskit.

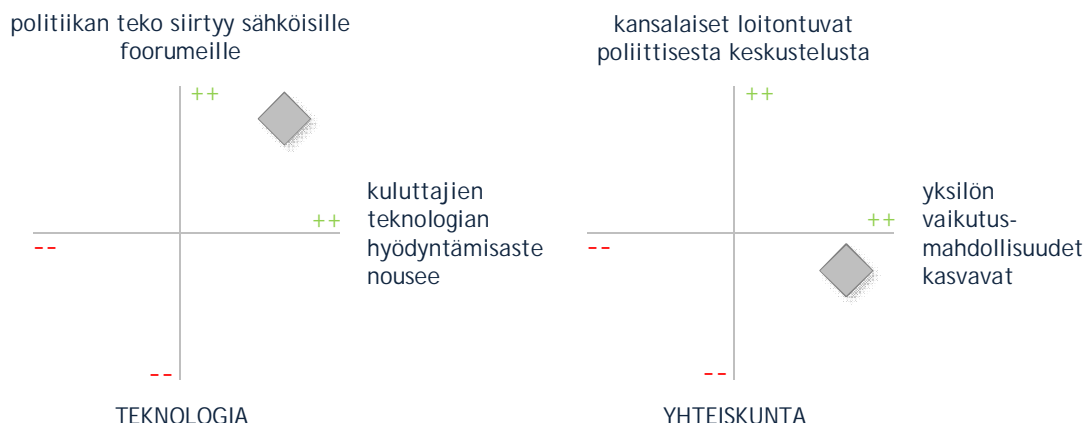
5.2.5 Skenaario 2: Teknokraattien anarkia

Skenaario kaksi perustuu viestintäteknologian mahdollistamalle aktiiviselle politiikan teolle. Olettamuksena on, että yhteiskunnallisiin asioihin vaikuttamisen mahdollisuudet yksilötasolla kasvavat uusien palvelu- ja asiointimuotojen sekä tietoliikenteen kehityksen myötä. Yksilön halukkuus hyödyntää näitä mahdollisuuksia pysyy ennallaan tai kasvaa ja toisaalta kynnys asioiden eteenpäin viemiseksi käytännön tasolla madaltuu. Kansalaiset kokevat virallisen politiikan etäiseksi, siinä käsiteltävät asiat painottuvat liian suurin viiteryhmiin ja avautuvat vaikeasti yleisölle. Kansalaisille tärkeistä asioista keskustelu siirtyy entistä voimakkaammin virtuaaliyhteisöihin ja sähköisille foorumeille. Teknologian kehittämiseen panostetaan, sillä kansalaisten suunnasta tuleva kysyntä kasvaa teknologian hyödyntämistään kasvun myötä. Toisaalta informaatioteknologian innovaatiot voimistavat osaltaan virtuaaliyhteisöjä.

Skenaarion kaksi toteutumisen seurauksena kansalaiset eivät enää tyydy etäiseen politiikkaan tai sisäpiirin dominanssiin, vaan aktivoituvat yhä voimakkaammin ajamaan tärkeiksi kokemiin asioita. Kärsimättömyys ja suvaitsemattomuus asioita ja ihmisiä kohtaan lisääntyvät. Poliittinen keskustelu on vilkasta, mutta siirtyy samalla sähköisille areenoille. Valtionhallinnon merkitys yhteiskunnan toimivuuden kannalta ei sinänsä muutu, mutta sen asema ja uskottavuus kansalaisten silmissä heikkenee. Auktoriteettien on ansaittava uusien sukupolvien kunnioitus ja sitä on ylläpidettävä johdonmukaisella ja asiantuntevalla toiminnalla. Organisaatioturvallisuuden näkökulmasta skenaarion kaksi toteutumisen kärjistetyimpiä ilmenemismuotoja voivat olla esimerkiksi

- viralliselle valtionhallinnolle rinnakkaisen virtuaalisesti toimivan järjestelmän syntyminen ja näiden kahden järjestelmän välinen valtataistelu
- poliittisten erimielisyyksien ratkaisemisen painottuminen keskustelun sijaan suoraan toimintaan

- yhteiskunnan sisäiset jännitteet kasvavat lisäten myös turvallisuusuhkia.



Kuvio 18: Skenaario 2 – Teknokraattien anarkia

Skenaarion kaksi vaikutukset eduskunnan kanslian sidosryhmädynamiikkaan liittyvät kansalaisten vaikutusvallan kasvamiseen ja virtuaalimaailmaa suvereenisti hyödyntävän politiikan teon epäsuoraan vaikutukseen kanslian toimintaprosesseihin. Teknologian ja tietotekniikan hyödyntämisen laajentuminen ja syventyminen voivat lyhyelläkin aikavälillä asettaa byrokraatiaan tottuneen ja tavanomaisiin työskentelytapoihin pinttyneen organisaation kovan muutospaineen alle. Myös pelastustoimen, poliisin ja muiden turvallisuusviranomaisten merkitys kasvaa ja yhteistyö lisääntyy. Skenaarion kaksi kehittyminen tarkoittaa muutospainetta koko yhteiskunnan tasolla ja kaikkein pisimmilleen vietyinä se voi tarkoittaa myös nykymuotoisen demokratian kriisiä.

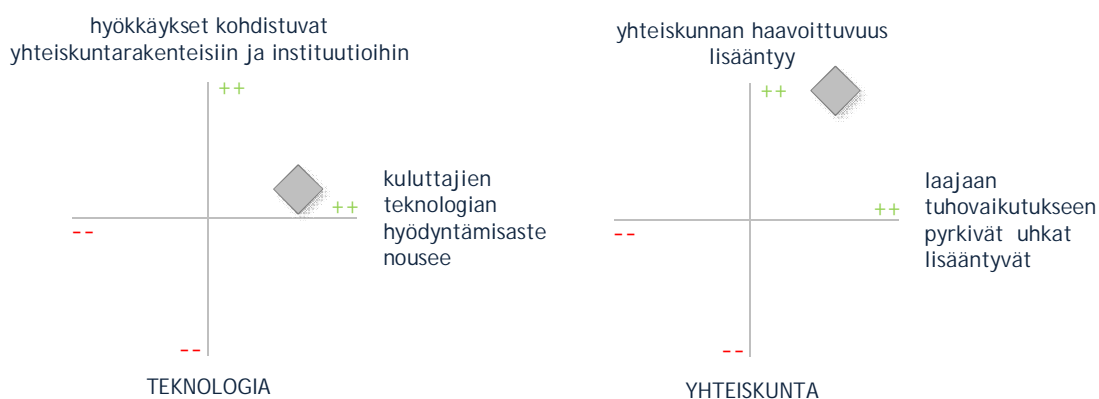
Eduskunnan kanslian turvallisuustoiminnan vahvuudet skenaarion kaksi suhteen ovat tekninen tietoturvallisuus, kiinteistö- ja toimitilaturvallisuus ja viranomaisyhteistyö. Heikkouksia puolestaan ovat turvallisuuskulttuurin puute, kriisiviestintä, passiivinen maineenhallinta, toiminnan jatkuvuuden varmistaminen. Skenaariossa kaksi painottuvat erityisesti strategiset, operatiiviset ja vahinkoriskit.

5.2.6 Skenaario 3: Viralliset valtarakenteet maalitauluina

Skenaario kolme käynnistyy teknologian hyödyntämistason kasvusta. Vaikutusväylät painottuvat tietoliikenteen, virtuaaliyhteisöjen ja korkean teknologian hyödyntämiseen. Kohteina on edellä mainittuja omassa toiminnassaan soveltava virallinen valtakoneisto, josta kansalaiset kokevat vieraantuvansa ja jota kohtaan näin ollen hyökätään turhautumisen seurauksena tahallisen vahingonteon vuoksi tai esimerkiksi poliittisten tavoitteiden ajamina. Uudet sukupolvet omaksuvat nopeasti uudet teknologiat ja kehittävät niitä aktiivisesti edelleen.

Ihmisten välisen kommunikaatiorytmin ja asioiden hoitamisen vauhdin kiihtyessä edelleen karsimättömyys lisääntyy. Lisääntyvä teknologian käyttöaste kautta yhteiskunnan eri toimintojen lisää samalla keskinäisriippuvuutta. Turvallisuuden näkökulmasta suureen tuho vaikutukseen joko pyritään tietoisesti tai sellainen seuraa yhä useammin laajan verkottumisen myötä. Organisaatioturvallisuuden näkökulmasta skenaarion kolme toteutumisen kärjistetyimpiä ilmenismuotoja voivat olla esimerkiksi

- hyökkäykset yhteiskunnan valta- ja perusrakenteita vastaan tai niillä uhkailu
- hyökkäykset painottuvat tietoliikenteeseen – tietomurrot lisääntyvät, tietoa käytetään kauppatavarana tai kiristyskeinona
- laittoman tiedustelutoiminnan merkitys korostuu
- yhteiskunnan huoltovarmuus vaarantuu
- yhteiskunnan johtohenkilöiden ja heidän läheisiensä henkilöturvallisuus heikkenee.



Kuvio 19: Skenaario 3 – Viralliset valtarakenteet maalitauluina

Kun kansalaisten turhautuminen kanavoituu julkisten kohteiden kautta, korostuu eduskunnan kanslian turvallisuusyksikön ja riskienhallinnan asiantuntijan kyky verkostoitua yhteiskunnan muiden turvallisuustoimijoiden (viranomaiset ja yksityiset palveluntarjoajat) kanssa sekä tilannetietoisuus. Toiminnan jatkuvuussuunnitelmien kypsyyt ja niiden mukaisen toiminnan harjoittelu on tärkeää. Eduskunnan kanslian yksiköistä tietohallintotoimiston asiantuntemusta tulisi viimeistään tässä vaiheessa hyödyntää turvallisuusyksikön toiminnan tehostamiseen ja riskienhallintaan. Erityisen tärkeässä asemassa on myös tässä skenaariossa eduskunnan kanslian viestintäyksikkö, sillä eduskunnan kansliaan maine ja kansalaisten eduskuntaan instituutioon liittämät mielikuvat vaikuttavat suoraan kansliaan kohdistuviin riskeihin.

Eduskunnan kanslian turvallisuustoiminnan vahvuudet skenaarion kolme suhteen ovat tekninen tietoturvallisuus, kiinteistö- ja toimitilaturvallisuus ja viranomaisyhteistyö. Heikkouksia puo-

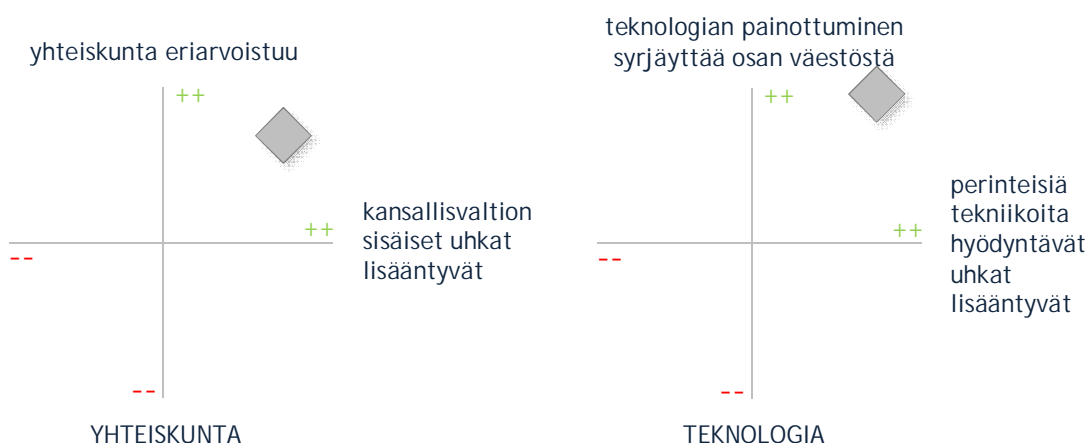
lestaan ovat henkilöstön huono turvallisuustietoisuus (erityisesti liittyen tietoturvaluuteen), turvallisuuskulttuurin puute, passiivinen maineenhallinta ja toiminnan jatkuvuuden varmistaminen. Skenaariossa kaksi painottuvat erityisesti strategiset ja operatiiviset riskit.

5.2.7 Skenaario 4: Yhteiskuntarauha järkkyy

Skenaario neljä kehittyi yhteiskunnassa lisääntyvän eriarvoistumisen pohjalta. Olettamuksena on, että yhteiskunta eriarvoistuu taloudellisista, arvomaailman kovenemisesta ja toimintaympäristön teknistymisestä johtuvista syistä. Kansa jakautuu teknologiaa sujuvasti ja suvereenisti hyödyntäviin ja toisaalta nopean teknisen kehittymisen ulkopuolelle jääneisiin tai siitä tietoisesti irtautuviin ihmisiin. Vuoropuhelu näiden ryhmien välillä on vähäistä ja niihin kuuluvien ihmisten ajatusmaailmat ja asenteet poikkeavat selvästi toisistaan.

Skenaarion neljä toteutumisen seurauksena valtion sisäinen turvallisuusympäristö muuttuu huonompaan suuntaan ja turhautuminen kanavoidaan kanssaihmiin. Teknistyneen toimintaympäristön yleistymisestä huolimatta tavanomaista tekniikkaa ja matalaa teknologiaa hyödyntävät vahingonteot lisääntyvät. Organisaatioturvallisuuden näkökulmasta skenaarion neljä toteutumisen kärjistetyimpiä ilmenemismuotoja voivat olla esimerkiksi

- kansalaisten vakava eriarvoistuminen ja yhteiskunnan jakautuminen kahtia
- laajaa fyysistä tuhoa aiheuttavien iskujen lisääntyminen
- henki- ja väkivaltarikosten lisääntyminen
- laittoman tiedustelutoiminnan ja tahallisten tietovuotojen lisääntyminen.



Kuvio 20: Skenaario 4 – Yhteiskuntarauha järkkyy

Eduskunnan kanslian sidosryhmien näkökulmasta skenaario neljä on varsin haastava. Suuri yleisö jakautuu osiin ja sillä voi olla suoria vaikutuksia poliittiseen päätöksentekoprosessiin ja sitä myöten myös eduskunnan kansliaan. Henkilöstön ja avainhenkilöiden turvallisuuteen tu-

lee kiinnittää erityistä huomiota. Turvallisuusuhat voivat syntyä anonyymeistä hakkereista tai pesäpallomailalla maailmaa parantavista yksilöistä. Turvallisuusuhkien tunnistaminen vaikeutuu, väkivallantekojen takana ei välttämättä olekaan psyykkiset sairaudet, taloudellinen ahdinko tai päihteiden käyttö. Turvallisuusympäristöön liittyvä tilannetietoisuus on tärkeää, ja kokonaisvaltainen tilannekuva vaatii yhteiskunnan kaikkien kerrosten seuraamista. Eduskunnan kanslian viestinnän tulee puhutella koko kansaa sen jakautuneisuudesta huolimatta. Ristiriita yhtäältä alati syvenevän sähköisen ja korkeaa teknologiaa hyödyntävän toimintatavan ja toisaalta tavanomaisempaa viestintää kaipaavan yleisön palvelemisen välillä on ilmeinen. Sama ristiriita koskee viestintäyksikön lisäksi myös turvallisuusyksikköä sen toiminnan painopisteiden määrittelyn ja turvallisuustoiminnan toteutuksen osalta.

Eduskunnan kanslian turvallisuustoiminnan vahvuudet skenaarion neljä suhteen ovat kiinteistö- ja toimitilaturvallisuus sekä viranomaisyhteistyö. Heikkouksia puolestaan ovat turvallisuuskulttuurin puute, henkilöstön huono turvallisuustietoisuus ja toiminnan jatkuvuuden turvaaminen. Skenaariossa kaksi painottuvat erityisesti operatiiviset ja vahinkoriskit.

5.3 Riskienhallinnasta muissa eurooppalaisissa parlamenteissa

Riskienhallinnan yleisyyttä ja tasoa muissa EU-maiden parlamenteissa kartoitettiin The European Centre for Parliamentary Research and Documentation -yhteisön (Liite 3) kautta kaikkiin 27:ään EU-jäsenmaahan lähetetyllä englanninkielisellä kyselyllä (Liite 4). Kysely tehtiin eduskunnan turvallisuusjohtajan pyynnöstä ja eduskunnan kanslian tietopalvelun hallinnoimana. Kyselyn vastausprosentiksi muodostui 59. Vastausten laajuus ja sisältö vaihtelivat.

5.3.1 Määrällinen analyysi

Vastauksia kyselyyn saatiin yhteensä 16 jäsenmaasta, joista 12 soveltaa ja neljä maata ei sovelta riskienhallintaa. Ruotsi ja Tanska puolestaan ilmoittivat, että jättivät tietoisesti vastaamatta kyselyyn. Kyselyyn täysin vastaamatta jätti 10 maata: Alankomaat, Bulgaria, Espanja, Irlanti, Itävalta, Luxemburg, Malta, Slovenia ja Sveitsi. (Taulukko 15)

EU-MAITA, JOISSA RISKIENHALLINTAA SOVELLETAAN (12)	EU-MAITA, JOISSA RISKIENHALLINTAA EI SOVELLETA (4)
<ul style="list-style-type: none"> • Belgia • Iso-Britannia (ylä- ja alahuone) • Italia • Kreikka • Portugali • Puola (ylä- ja alahuone) • Ranska • Romania • Slovakia • Tšekki • Unkari • Viro 	<ul style="list-style-type: none"> • Kypros • Latvia • Liettua • Saksa (eduskunta ja liittoneuvosto)
EU-MAAT, JOTKA JÄTTIVÄT VASTAAMATTA KYSELYYN (11)	
<ul style="list-style-type: none"> • Alankomaat • Bulgaria • Espanja • Irlanti • Itävalta • Luxemburg • Malta • Ruotsi (ilmoitti jättävänsä tietoisesti vastaamatta) • Slovenia • Sveitsi • Tanska (ilmoitti jättävänsä tietoisesti vastaamatta) 	

Taulukko 15: Riskienhallinnan yleisyys eurooppalaisissa parlamenteissa

Riskienhallintaa soveltavien parlamenttien joukko on varsin mielenkiintoinen. Riskienhallintaa soveltavien jäsenmaiden joukossa on hyvä edustus suurien maiden parlamentteja tai parlamentteja, joiden voidaan olettaa toimivan suomalaisittain verrattuna haastavammassa turvallisuusympäristössä. Lisäksi riskienhallintaa ovat ilmoittaneet soveltavansa myös pienempien maiden tai verrattain rauhallisessa toimintaympäristössä toimivat parlamentit. Niiden parlamenttien joukossa, jotka eivät omien sanojensa mukaan sovelle riskienhallintaa, mielenkiintoinen on Saksa. Kyseessä on kuitenkin pinta-alaltaan ja väestömäärältään suuri valtio, jonka sisällä on merkittäviä vähemmistöjä ja joka osallistuu aktiivisesti kansainvälisiin rauhanturvaoperaatioihin, ja jonka parlamentin ja liittoneuvoston turvallisuusympäristö on edellä mainituista syistä vähintäänkin haastava.

Annettujen vastausten takana voivat vaikuttaa kieliongelmat tai laskelmointi. Tanskan ja Ruotsin parlamenttien ilmoitukset jättää vastaamatta esitettyihin kysymyksiin herättävät ajatuksen siitä, että näin menettelemällä he itse asiassa osoittivat soveltavansa riskienhallintaa,

joka tässä tapauksessa estää heitä jakamasta kysyttyä tietoa oman organisaationsa ulkopuolelle. Vastaushalukkuuteen ja vastausten sisältöön on varmasti vaikuttanut myös se, että ECPRD:n toimintaperiaatteiden mukaan kaikkien sen kautta lähetettyjen kyselyiden vastaukset on hyvä julkaista jälkikäteen kaikkien yhteisöä käyttävien, myös kyselyyn vastaamattomien, saataville. Toisaalta riskienhallintaa koskeneeseen kyselyyn olisi ollut mahdollista vastata laveasti yksityiskohtaisia toimintatapoja paljastamatta.

Myös vastaamatta jättämisen taustalla voivat vaikuttaa useat syyt, kuten esimerkiksi kieliongelmat, kyselyn ajoittuminen lomakaudelle, kohdeorganisaatioiden sisäinen epäselvyys siitä, kenen kyselyyn tulisi vastata, unohtus tai kyselyn jakelun häiriöt. Turvallisuusympäristön haastavuuden näkökulmasta ainakin Espanjan ja Irlannin vastaukset olisivat olleet mielenkiintoisia edellyttäen, että niiden parlamenteissa sovelletaan riskienhallintaa.

5.3.2 Laadullinen analyysi

Kyselyn tavoitteena oli selvittää riskienhallintatoiminnan yleisyys muiden EU-jäsenmaiden parlamenteissa. Kyselyn ydinkysymys siitä, sovelletaanko parlamenteissa riskienhallintaa vai ei, on sikäli haasteellinen, että vaikka kyselyyn liitettiin riskienhallinnan määritelmä, voidaan sen käsitteen alle katsoa kuuluvan varsin laaja ja vaihteleva skaala toimintoja. Ydinkysymystä täydennettiin näin ollen riskienhallinnan toteutukseen liittyvillä lisäkysymyksillä, jotta saatuja vastauksia voitaisiin paremmin arvioida.

Toisaalta eduskunnan kanslian kehittämistyön kannalta on oleellista myös selvittää, ovatko riskienhallintaa koskevat ratkaisut erityisesti niissä tapauksissa, jossa sitä ei sovelleta, tietoisien harkinnan tuloksia. Kiinnostavaa on myös se, onko näissä parlamenteissa suunnitteilla riskienhallintatoiminnan käynnistäminen tulevaisuudessa.

Tutkimusyhteisön kautta lähetetyn kyselyn vastaajaan kussakin parlamentissa ei voitu vaikuttaa, vaikka kyselyt pyritäänkin aina ohjaamaan organisaatiossa eteenpäin asiasta parhaiten tietävälle henkilölle. Saatujen vastausten syvyys ja kyselyyn vastanneiden henkilöiden toimenkuva vaihtelikin selvästi. Toisaalta edellä mainittujen välillä oli luonnollinen korrelaatio, sillä riskienhallintaa tuntevan on huomattavasti helpompi vastata kysymyksiin, ja toisaalta tehdä myös päätös olla vastaamatta niihin.

Aineistoa luokiteltaessa raja riskienhallintaa soveltavien ja sitä soveltamattomien parlamenttien välille vedettiin sen perusteella, ilmoittivatko he pyrkivänsä tunnistamaan ja arvioimaan säännöllisesti organisaatioonsa ja sen toimintaan liittyviä uhkia ja riskejä ja pyrkivänsä pienentämään niitä. Riskienhallintatyökaluistaan, raportointiprosessistaan, riskienhallintaan liittyvästä vastuunjaostaan tai standardien käytöstään kertoneiden parlamenttien osalta saatuja

vastauksia on helpompi arvioida. Taulukkoon 16 on laadittu tiivis yhteenveto kunkin parlamentin vastauksesta. Alkuperäiset vastaukset on luovutettu eduskunnan kanslian turvallisuusyksikön käyttöön.

EU:N JÄSENMAA	KUVAUS RISKIENHALLINNAN TOTEUTUKSESTA KÄYTÄNNÖSSÄ
Belgia	<ul style="list-style-type: none"> • painotus toimitilaturvallisuudessa • perustettu erillinen turvallisuuskomitea • toiminta perustuu turvallisuudesta laadittuun toimintapolitiikkaan, joka on osa parlamentin strategiaa • riskianalyysit ja -arviot otetaan huomioon strategisia päätöksiä tehtäessä ja mahdollisuuksien mukaan niitä tehdään myös strategisista päätöksistä itsestään
Iso-Britannia (ylä- ja alahuone)	<ul style="list-style-type: none"> • riskienhallinnan politiikka ja ohjeistus (Risk Management Handbook 2011) • suuri määrä henkilöstöä erikoistuneena ainoastaan riskienhallintaan • käytännön riskienhallintatyö tehdään yksikkötasolla, raportointi on säännöllistä (vaihteluväli päivittäin – neljännesvuosittain riippuen riskistä) • sisäinen tarkastus valvoo riskienhallinnan raportointia ja integroi yksiköjen tiedot koko organisaation riskienhallintaraporttiin • kaikilla riskiryhmillä on oma vastuhenkilö johtokunnassa, joka vastaa oman alueensa riskienhallinnan kehittämisestä • riskejä kartoitetaan ja arvioidaan suhteessa toiminnan jatkuvuuteen, ympäristöuhkiin, pelastustoimintaan, tietojärjestelmiin, henkilöturvallisuuteen, talouteen, projekteihin, maineeseen ja tiedostoihin • riskienhallintaa toteutetaan BS 25999 -standardin mukaan (Business Continuity and Resilience)
Italia	<ul style="list-style-type: none"> • riskienhallinta painottuu toiminnan jatkuvuussuunnitteluun (tietoyhteydet ja tietoturvallisuus erityisesti), henkilöturvallisuuteen (henkilöstö ja vierailijat) ja poikkeustilanteiden johtamiseen • tietoturvallisuuteen liittyvä riskienhallinta on toteutettu kansainvälisten standardien mukaisesti • turvallisuusyksikkö ja tietohallintoyksikkö ovat voimakkaasti mukana riskienhallintatoiminnassa (myös erillinen lainvalvontayksikkö ja Carabinieriin edustus) • riskienhallintaa sovelletaan myös korkeantason päätöksenteossa erityisesti liittyen henkilöturvallisuuteen, toimitilaturvallisuuteen ja tietoturvallisuuteen
Kreikka	<ul style="list-style-type: none"> • ei riskienhallintaa sen kokonaisvaltaisessa merkityksessä • pelastustoimintaan, henkilöturvallisuuteen, toimitilaturvallisuuteen, tietoturvallisuuteen liittyvät riskit arvioidaan kahden vuoden välein • poikkeustilanteita varten on laadittu erilliset ohjeet

Portugali	<ul style="list-style-type: none"> • koko parlamenttia koskevaa riskinhallintaa ei ole, mutta riskiarvioita laaditaan turvallisuuskysymyksiin liittyen • turvallisuustoiminta painottuu toimitilojen, omaisuuden ja henkilöiden turvallisuuteen • tietoturvallisuuden osalta on laadittu riskienhallintapolitiikka, joka on tällä hetkellä hyväksyttävänä: tavoitteena on perustaa ISO 27001:2005 -standardin mukainen tietoturvallisuuden hallintajärjestelmä (ISMS) • riskienhallintatyöhön osallistuvat pääsihteeri, tietoturvallisuus-päällikkö sekä tietoturvallisuuteen liittyvistä resursseista vastaavat henkilöt • riskienhallintaa ei hyödynnetä strategisessa päätöksenteossa
Puola (ylä- ja alahuone)	<ul style="list-style-type: none"> • riskienhallintaa toteutetaan muuhun toimintaan integroituna ilman virallisia politiikkoja tai ohjeita • riskienhallinta perustuu toiminnan jatkuvaan kehittämiseen • eniten painotetaan toimitilaturvallisuutta, työturvallisuutta, taloutta, sisäistä tarkastusta ja toiminnan jatkuvuutta • kunkin osaston/yksikön päällikkö huolehtii oman vastuualueensa riskienhallinnasta, tuloksia painotetaan yli menetelmien • sisäisen tarkastuksen osalta käytössä ovat standardit COSO INTOSAI ja SEC 1341 liite 1 • yksikötason operatiiviseen suunnitteluun liitetään riskiarviot • vuonna 2010 käytiin keskustelua riskienhallinnan soveltamisesta strategisella tasolla
Ranska	<ul style="list-style-type: none"> • ei riskienhallintapolitiikkaa • turvallisuuskysymyksiin liittyen sovelletaan käytännönläheistä toimintapolitiikkaa, joka perustuu institutionaalisten riskien ja uhkien sekä turvallisuustoimien heikkouksien arviointiin • havaitut epäkohdat korjataan niiden merkittävyyden, käytettävissä olevien hallintakeinojen ja viranomaisten asettamien prioriteettien pohjalta • yksikötason johtajista ja puhemiehen kabinetin edustajasta koostuva turvallisuusasioista vastaava ryhmä kokoontuu säännöllisesti arvioimaan turvallisuuden toimintapolitiikkaa
Romania	<ul style="list-style-type: none"> • riskienhallintaa toteutetaan kansallisen lainsäädännön pohjalta • riskienhallinnalla pyritään vaikuttamaan toimitilaturvallisuuteen, pelastustoimeen ja tuotannon ja toiminnan turvallisuuteen • riskienhallinnasta vastaa sisäisten asioiden direktoraatti • direktoraatti on tarvittaessa yhteydessä parlamentin eri yksiköihin/osastoihin ja ylläpitää viranomaisyhteistyötä • riskienhallintaprosessin tuottamaa tietoa hyödynnetään strategisen johtamisen tukena ja riskiarvioita tehdään myös strategisista päätöksistä itsestään
Slovakia	<ul style="list-style-type: none"> • ei riskienhallintaa kyselyssä tarkoitetussa merkityksessä • riskejä arvioidaan kuitenkin perustuen kansalliseen yhteiskunnan turvallisuutta säätelevään lainsäädäntöön • parlamentin kansliaan on perustettu kanslian yksiköiden johtajista koostuva kriisiryhmä, joka johtaa toimintaa kriisi- ja poikkeustilanteissa (onnettomuudet, luonnonkatastrofit, terrorismi) • erillistä riskienhallintapolitiikka ei ole, mutta kriisitilanteita varten on laadittu toimintaohjeisto, joka perustuu kansalliseen lainsäädännön asettamiin vaatimuksiin • toimintaa kehitetään ja harjoitellaan vuosittain

Tšekki	<ul style="list-style-type: none"> • ei riskienhallintaa kyselyssä tarkoitettussa merkityksessä • riskejä arvioidaan kuitenkin perustuen kansalliseen poikkeusolojen toimintaa säätelevään lainsäädäntöön • riskienhallintaa hoitaa kansliapäällikkö ja yksiköiden johtajat • riskienhallinnalliset toimet on keskitetty pelastustoimintaan, toiminnan jatkuvuussuunnitteluun, tuotannon ja toiminnan turvallisuuden, tietoturvallisuuden ja terrorismin uhkaa silmällä pitäen • riskienhallintapolitiikkaa ei ole, mutta kriisitilanteiden varalle on laadittu erillinen ohjeistus
Unkari	<ul style="list-style-type: none"> • ei riskienhallintaa kyselyssä tarkoitettussa merkityksessä • tietohallintotoimisto vastaa tietoturvallisuuteen liittyvästä riskienhallintamenettelystä
Viro	<ul style="list-style-type: none"> • ei riskienhallintaa kyselyssä tarkoitettussa merkityksessä • turvallisuuden, tietohallintoon ja työturvallisuuden liittyvät riskit arvioidaan säännöllisesti • poikkeustilanteita varten on laadittu erilliset ohjeet

Taulukko 16: Riskienhallinnan käytännön toteutus eurooppalaisissa parlamenteissa

Kokonaisvaltaisin ja järjestelmällisin riskienhallintatoiminta on Iso-Britannian parlamentissa, jossa toiminta perustuu standardeihin ja organisaation itsensä laatimiin strategiin asiakirjoihin ja jossa riskienhallintatoimintaan on osoitettu paljon henkilöstöresursseja. Riskienhallintaan on panostettu myös Belgiassa, Italiassa ja Romaniassa, joissa riskienhallinnan ilmoitettiin tukevan myös organisaation strategista päätöksentekoa. Puolassa riskienhallintaa ei ole sidottu muodollisuuksiin, mutta saadun vastauksen mukaan riskienhallintaa on sitäkin voimakkaammin integroitu yksikköjen jokapäiväiseen toimintaan, jota ohjaa jatkuva kehittymisen tavoite. Keveimmillään riskienhallintatoiminta on Unkarin parlamentissa, jossa ainoastaan tietoturvallisuudesta vastaava virkamies soveltaa riskienhallinnallisia toimenpiteitä.

Saatujen vastausten perusteella voidaan todeta, että riskienhallintaa edes jollakin asteella soveltavissa parlamenteissa toiminnan painopisteitä ovat toiminnan jatkuvuussuunnittelu, pelastustoiminta, työturvallisuus, kiinteistö- ja toimitilaturvallisuus sekä henkilöturvallisuus. Kriisi- ja poikkeustilanteet on huomioitu myös, sillä osassa parlamenteja niiden varalta on laadittu erilliset ohjeet. Ohjeistukset mainitaan useasti, mutta ainoastaan Slovakian parlamentti mainitsi ohjeistuksen mukaisen toiminnan käytännön harjoittelun. Osan parlamenteista riskienhallintatoimintaa tuntui myös ensisijaisesti ohjaavan kansallisen lainsäädännön asettama velvoite aktiivisen ja omaehtoisen tavoitteenasettelun sijaan.

Niistä kyselyyn vastanneista maista, jotka eivät omien sanojensa mukaan sovelta riskienhallintaa tilannettaan tarkemmin perustelivat Latvia, Liettua ja Saksa. Latviassa ja Saksassa projekteista vastuussa olevat vastaavat mahdollisten riskien huomioimisesta. Saksassa painopiste on lainmukaisuuden varmistamisessa. Liettuassa parlamentin strategisen suunnittelun osana on tähän mennessä sovellettu riskienhallintaa SWOT-analyysin muodossa. Strategista suunnitteluprosessia on kuitenkin muutettu, eikä uuteen, kevennettyyn malliin enää sisälly kyseisen

analyysin laatiminen. Liettuan sisäinen tarkastus toisaalta rohkaisee riskienhallintatoimintaan, mutta toistaiseksi ilman tulosta. Lisäksi Liettuan parlamentissa on työn alla julkisten organisaatioiden sisäiseen tarkastukseen kantaa ottava laki, jonka voimaan astuessa myös parlamentin itsensä on sitouduttava järjestelmälliseen riskienhallintatoimintaan.

5.3.3 Vertailuaineiston yhteenveto ja johtopäätökset

Kyselyyn jätti kokonaan vastaamatta 11 EU jäsenmaan parlamenttia, joista Tanskan ja Ruotsin voidaan olettaa soveltavan riskienhallintaa ainakin jollain tasolla (molemmat parlamentit ilmoittivat jättävänsä tietoisesti vastaamatta kyselyyn). Jos näin todellisuudessa on, olisi riskienhallintaa soveltavien EU jäsenmaiden osuus kaikista jäsenmaista hieman yli puolet (52 prosenttia). Vastaamatta jättäneiden maiden parlamenttien riskienhallinnan tilaa on vaikea arvioida ainoastaan kyseisten maiden sisäpoliittisen historian valossa. Oletettavaa on, että ainakin tietoturvallisuuden puolella riskienhallintaa esiintyy myös vastaamatta jättäneiden joukossa – sitä vaatii osaltaan jo unionin sisäinen yhteistyö.

Riskienhallinnan käytännön toteutus vastanneissa parlamenteissa vaihtelee melkoisesti esimerkiksi raportoinnin, standardien hyödyntämisen, siihen osoitettujen henkilöstöressurssien ja järjestelmällisyyden suhteen. Tämä on toisaalta luonnollista, sillä tuleehan riskienhallintatoiminta rakentaa aina kohdeorganisaation ehdoilla ja sen tarpeita parhaiten vastaavaksi kokonaisuudeksi.

Nyt toteutetulla kyselyllä saadaan korkeintaan esimakua siitä, mitkä parlamentit saattaisivat olla potentiaalisia parhaiden käytänteiden keräämisen suhteen. Toisaalta tästä syystä on myös erityisen valitettavaa, että Pohjoismaiset parlamentit eivät vastanneet kyselyyn sisällöllisesti. Pohjoismaisten parlamenttien kokemusten hyödyntäminen olisi luontevaa yhteiskuntarakenteiden, maantieteellisten olosuhteiden, poliittisten rakenteiden samankaltaisuuden ja toisaalta verrokiparlamenttien turvallisuusympäristön haasteellisuuden vuoksi. Näin ollen niihin suunnattu erillinen, luottamuksellinen ja kohdeorganisaation hyväksymä tutkimus tai opintomatka olisi varmasti paikallaan.

Turvallisuustoiminnan ja riskienhallinnan kehittämisen osalta päätös kyselyn tulosten soveltamisesta on tehtävä eduskunnan kansliassa. Päätöstä tehdessä olisi kuitenkin hyvä kiinnittää huomiota ainakin seuraaviin asioihin

- mihin kysymyksiin parhaiden käytänteiden avulla voidaan saada ja halutaan vastauksia
- mihin kysymyksiin parhaat käytänteet eivät vastaa
- mitkä parlamentit sopisivat parhaiten parhaiden käytänteiden lähteiksi ja miksi
- vertauskohteiden valinta ja jatkotoimenpiteiden suunnittelu.

On lisäksi muistettava, että parhaiden käytänteiden soveltaminen organisaatioturvallisuuden ja riskienhallintatoiminnan kehittämiseen on haasteellista. Kumpikin edellä mainituista on aina voimakkaasti sidottu kohdeorganisaatioonsa ja on muodoltaan ja sisällöltään kutakin organisaatiota parhaiten palveleva. Parhaiden käytänteiden soveltaminen on näin ollen tarkoituksenmukaista riskienhallintaa koskevissa osakokonaisuuksissa kuin kokonaista järjestelmää tai toimintapolitiikkaa koskevissa kysymyksissä. Organisaatioturvallisuuteen liittyvissä käytännön ratkaisussa parhaita käytäntöjä sen sijaan voitaisiin hyödyntää esimerkiksi toimitilaturvallisuuden, tietoturvallisuuden, ulkomaantoimintojen turvallisuuden ja turvallisuuskulttuurin liittyvien ratkaisujen osalta.

Organisaatioturvallisuuden ja riskienhallinnan kehittämisen ja parhaiden käytänteiden soveltamisen suhteen on kuitenkin se, että muualta hankitut ratkaisut eivät missään tapauksessa saa korvata organisaatiossa itsessään tehtävää ideointia, suunnittelutyötä ja päätöksentekoa. Organisaatiossa tehty riskienhallinnan ja organisaatioturvallisuuden suunnittelutyö on välttämätön osa näiden alojen ammattitaidon kehittymistä niin riskienhallinnan ja turvallisuuden vastuuhenkilöinä työskentelevien kuin myös muun henkilöstön kannalta. Se on lisäksi ainoa tapa varmistaa, että tehdyt ratkaisut palvelevat parhaiten juuri kyseistä organisaatiota.

6 Johtopäätökset

Eduskunnan kanslian turvallisuustoiminnan nykytilaa ja turvallisuusympäristön mahdollisia kehityssuuntia käsittelevien osalukujen perusteella voidaan todeta, että turvallisuuteen liittyvät haasteet kasvavat tulevaisuudessa, näihin haasteisiin vastaaminen vaatii kokonaisvaltaista organisaatioturvallisuutta ja että riskienhallintatoiminnan käynnistäminen eduskunnan kansliassa mahdollistaisi tulevien haasteiden tunnistamisen ja haasteisiin varautumisen ennakoita. Riskienhallinta tukisi näin ollen eduskunnan kanslian organisaatioturvallisuuden kehittämistä.

6.1 Eduskunnan kanslian turvallisuusympäristö muuttuu haasteellisemmaksi

Eduskunnan kanslian turvallisuusympäristö muuttuu haasteellisemmaksi. Kerätyn tulevaisuustiedon mukaan (osaluku 5.2.1) muutokset johtuvat globaaleista, kansainvälisistä ja kansallisista ilmiöistä. Tässä kehittämistyössä muotoillut skenaariot eivät ole tyhjentyviä. Riippumatta kuitenkin kehityksen konkreettisista ilmenemismuodoista tai vauhdista, suunta tuntuu olevan yhä enemmän kohti kovenevia arvoja, ahdasmielisiä asenteita ja harkitsevuuden sijaan reagoitua ja lyhytjänteisyyttä. Turvallisuusympäristön muutoksista kieliviä indikaatioita on ollut esillä jo useamman vuoden ajan (Liite 6).

Eduskunnan kanslian kannalta erityisen huolestuttavaa olisi se, että kansalaisten turhautuminen purkautuisi jatkossa julkisia kohteita ja valtionhallinnon organisaatioita tai niitä edustavia ihmisiä kohtaan. Lisäksi tietoturvallisuus (mukaan lukien poliittinen vakoilu) vaatii tulevaisuudessa yhä enemmän huomiota ja resursseja etenkin silloin, jos kansainvälinen ilmapiiri kiristyy entisestään.

Turvallisuustoimintaa tulisi johtaa näkökulmasta, joka varautuu myös kaikkein vaikeimpiin olosuhteisiin. Tämä ei kuitenkaan tarkoita pessimististä näkökulmaa vaan tavoitteena tulisi olla kyky realistisesti arvioida ja viestittää toimintaympäristön muutoksista organisaation sisällä.

6.2 Todellinen turvallisuus vaatii kokonaisvaltaista lähestymistapaa

Kun turvallisuuden ei koeta olevan uhattuna, voi turvallisuustoiminnan arvostus organisaatiossa jäädä vähäiseksi. Turvallisuus ei kuitenkaan toteudu syntyneiden vahinkojen korjaamisesta, vaan niihin varautumisesta ennakkoon. Näin ollen turvallisuudesta vastaavien erityinen tehtävä on huolehtia organisaation sisäisestä markkinoinnista, jotta turvallisuustoiminnalle osoitetaan sille kuuluvat resurssit myös ennalta ehkäisevän työn mahdollistamiseksi.

Aikaisemmat luvut ovat osoittaneet, että turvallisuus vaatii kokonaisvaltaista lähestymistapaa. Toimitilaturvallisuus on vain yksi osa-alue kymmenestä, eikä kulunseurannalla tai videovalvonnalla kyetä pysäyttämään turvallisuusuhkia nyt, saati tulevaisuudessa. Tietoturvallisuuden painottuessa tekniisiin ratkaisuihin täytetään vain pieni osa tietoturvallisuuden vaatimuksista, joita ovat tiedon saatavuus, tiedon eheys ja tiedon luotettavuus. Tekninen tietoturvallisuus on henkilöstölle pitkälti näkymätöntä toimintaa, eikä se ohjaa tiedon oikeanlaiseen käsittelyyn - jakamiseen, säilyttämiseen ja hävittämiseen. Turvallisuuskulttuurin puuttuessa myös ymmärrys tehtyjen tietoteknisten ratkaisujen tarpeellisuudesta on puutteellista. Näin ollen tietoturvaan koskevat ohjeet ja toimintasuositukset voidaan kokea rajoituksina, byrokraattiana tai tarpeettomana valvontana kaikkia koskevan turvallisuuden eteen tehtävän työn sijaan. Tämän lisäksi ohjeistusten ollessa ristiriidassa käytettävissä olevien välineiden ja ohjelmien suhteen on omiaan lisäämään turhautumista. Turvallisuuden toteuttamisen tulee yksittäisen työntekijän näkökulmasta olla vaivatonta ja kannattavaa.

Eduskunnan kanslian turvallisuustoiminnan SWOT-analyysi suhteessa laadittuihin neljään skenaarioon on hahmoteltu taulukkoon 17.

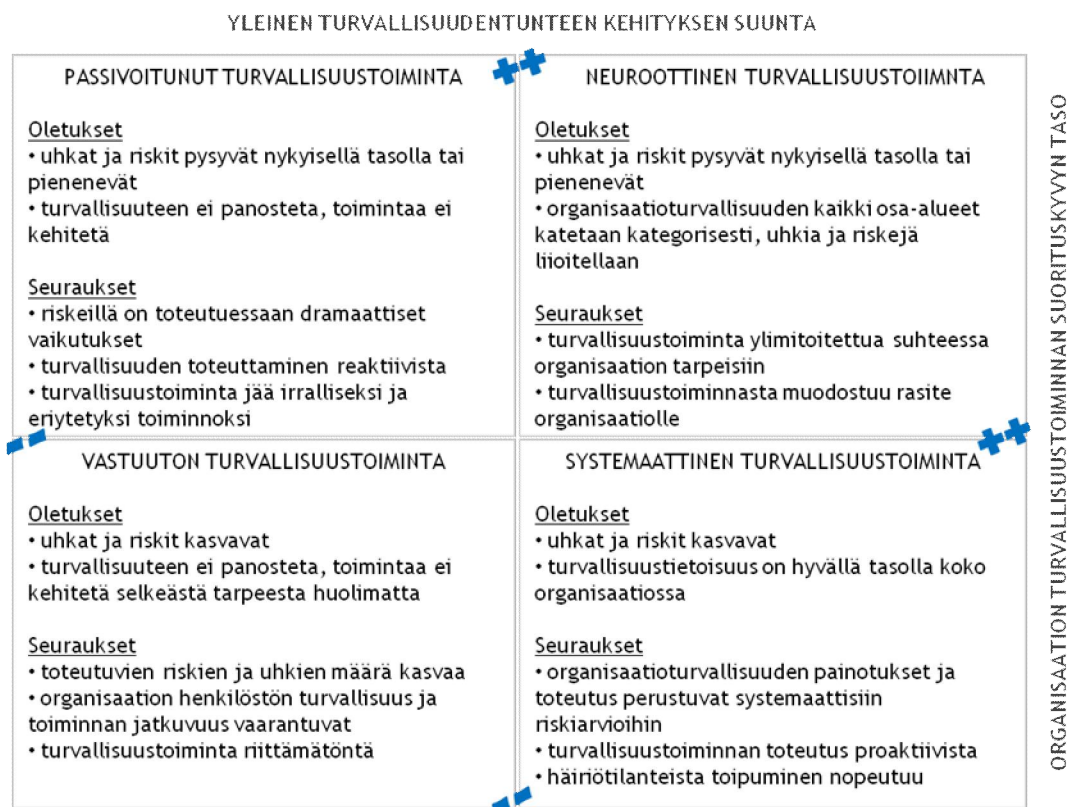
Eduskunnan kanslian turvallisuustoiminnan suorituskyky suhteessa skenaarioihin		
SKENAARIO	HEIKKOUEDET	VAHVUUDET
Kriittinen kotipesä	<ul style="list-style-type: none"> • henkilöstön huono turvallisuustietoisuus • turvallisuustoiminnan yksipuolisuus • huono maine • jatkuvuussuunnittelu 	<ul style="list-style-type: none"> • tekninen tietoturvallisuus • työterveydenhoito • työsuojelu • henkilöstöryhmien sisäinen koheesio
Teknokraattien anarkia	<ul style="list-style-type: none"> • turvallisuuskulttuurin puute • kriisiviestintä • passiivinen maineenhallinta • jatkuvuussuunnittelu 	<ul style="list-style-type: none"> • tekninen tietoturvallisuus • kiinteistö- ja toimitilaturvallisuus • viranomaisyhteistyö
Valtarakenteet maalitauluina	<ul style="list-style-type: none"> • henkilöstön huono turvallisuustietoisuus (erityisesti tietoturvallisuus) • turvallisuuskulttuurin puute • passiivinen maineenhallinta • jatkuvuussuunnittelu 	<ul style="list-style-type: none"> • tekninen tietoturvallisuus • kiinteistö- ja toimitilaturvallisuus • viranomaisyhteistyö
Yhteiskuntarauha järkkyy	<ul style="list-style-type: none"> • henkilöstön huono turvallisuustietoisuus (tietoturvallisuus) • turvallisuuskulttuurin puute • jatkuvuussuunnittelu 	<ul style="list-style-type: none"> • kiinteistö- ja toimitilaturvallisuus • viranomaisyhteistyö

SKENAARIO	UHKAT	MAHDOLLISUUDET
Kriittinen kotipesä	<ul style="list-style-type: none"> • henkilöstön tyytymättömyyden kärjistymisen työnseisauksiin tai vahingontekoihin • uuden työvoiman rekrytointi epäonnistuu • lainsäädäntötyö seisahtuu tietoliikenteen häiriöiden vuoksi • tietoturvaluottelu vaarantuu vakoilun, sosiaalisen hakkeroinnin tai työntekijöiden tahallisen tietovuodon vuoksi 	<ul style="list-style-type: none"> • työnantajakuvan parantaminen • työyhteisön uudistaminen ja siitä saatava kilpailuvaltti valtionhallinnon työnantajana • tietoturvaluottelun kehittäminen yhteistyössä ja yhdenmukaisesti muun valtionhallinnon kanssa • riskienhallintatoiminnan ja organisaatioturvaluottelun myötä työntekijöiden aktiivisuus tietoturvaluottelun ylläpitämisessä tehostuu ja turvaluottelukulttuuri vahvistuu
Teknokraattien anarkia	<ul style="list-style-type: none"> • henkilöturvaluottelun heikkeneminen • vieraantuminen nopeissa sykleissä muuttuvasta yhteiskunnasta hitaan reaktiokyvyn vuoksi • tietojärjestelmiin, fyysiseen omaisuuteen ja henkilöstöön/sidosryhmiin yhtäaikaaisesti kohdistuvat hyökkäykset 	<ul style="list-style-type: none"> • riskienhallinta ja turvaluottelutoiminta ylläpitävät tehokkaasti tilannetietoisuutta • turvaluottelusuhteisiin kyetään varautumaan ennalta kokonaisvaltaisen organisaatioturvaluottelun, riskienarvioinnin ja viranomaisyhteistyön voimin • kehittyneen turvaluottelukulttuurin myötä tieto henkilöstön havaitsemista hyökkäysyrityksistä tai turvaluotteluun liittyvistä puutteista saadaan tehokkaasti käyttöön • organisaatiojohdon sitoutumisen ja lisääntyneen tilannetietoisuuden myötä turvaluottelutoiminnalle osoitetaan sen tarvitsemat resurssit
Valtarakenteet maalitauluina	<ul style="list-style-type: none"> • henkilöturvaluottelun heikkeneminen • tietojärjestelmiin, fyysiseen omaisuuteen ja henkilöstöön/sidosryhmään yhtäaikaaisesti kohdistuvat hyökkäykset • poliittiseen vakoiluun yhdistyvät kiristykset, kaappaukset tai muut uhkaukset 	<ul style="list-style-type: none"> • sähköisen toimintatavan aktiivinen kehittäminen ja proaktiivinen asenne yhteiskunnan teknologisiin ja tietoteknisiin muutoksiin • uusien toimintatapojen ja vaikutuskanavien sitouttaminen kansalliseen työhön • tietoturvaluottelun kaikkien tavoitteiden toteuttaminen ja edelläkävijyys valtionhallinnossa • riskienhallinnan soveltaminen turvaluotteluun ja toimintaympäristön muutoksiin liittyvän tilannetietoisuuden takaamiseksi • kokonaisvaltaisen organisaatioturvaluottelun sijoitettujen resurssien palautuminen turvaluottelusuhteiden torjunnalla

Yhteiskuntarauha järkkyy	<ul style="list-style-type: none"> • henkilöturvallisuus vaarassa • toiminnan jatkuvuus vaarassa • suurten tuho vaikutusten hyökkäykset • tietojärjestelmiin, fyysiseen omaisuuteen ja henkilöstöön/sidosryhmään yhtäaikaisesti kohdistuvat hyökkäykset • poliittiseen vakoiluun yhdistyvät kiristykset, kaappaukset tai muut uhkaukset 	<ul style="list-style-type: none"> • riskienhallinnan soveltaminen turvallisuuteen ja toimintaympäristön muutokseen liittyvän tilannetietoisuuden takaamiseksi • kokonaisvaltaisen organisaatioturvallisuuden sijoitettujen resurssien palautuminen turvallisuusuhkien torjunnalla • parempi maineenhallinta aiheuttaa muusta valtionhallinnosta erottuvan kunnioitetun aseman • viranomaisyhteistyön syventäminen
--------------------------	--	--

Taulukko 17: Eduskunnan kanslian turvallisuustoiminta suhteessa skenaarioihin

Organisaatioturvallisuuden kokonaisvaltaisuus ja riskienhallintatoiminnan laatu heijastavat osaltaan organisaation yleistä kypsyystasoa. Kuvioon 21 on hahmoteltu kärjistetyt esimerkit organisaatioturvallisuuden erilaisista toteutuksista suhteessa organisaation turvallisuusympäristöön. Esimerkkien mukaan organisaatiossa työskentelevien turvallisuudentunteen pysyessä samana tai sen parantuessa organisaatiota rasittaa eniten neuroottinen tai passivoitunut turvallisuustoiminta (Kuvio 21).



Kuvio 21: Organisaation turvallisuustoiminnan suorituskyvyn riittävyys

Neuroottisessa turvallisuustoiminnassa riskienhallinnan ylimitoitettun toteutuksen taustalla voivat vaikuttaa esimerkiksi yksityisen turvallisuusyhteisön painostus tai yksittäiset vaikutusvaltaiset henkilöt. Vaikuttaminen turvallisuutta koskeviin päätöksiin tapahtuu epävirallisilla foorumeilla. Riskienhallinnasta päättävän tahon intressit priorisoidaan yli kohdeorganisaation intressin. Passivoituneessa turvallisuustoiminnassa turvallisuustoiminta nojaa hyvään tuuriin. Turvallisuustoiminta nojaa verkostoihin, joiden jäsenet jatkavat toimintaansa kehittymättä ja toimivat toistensa tukena ja vahvistajina. Toteutuneista riskeistä toivotaan otettavan opiksi, mutta konkreettinen toiminnan kehittämisvastuu osoitetaan vain näennäisesti organisaation sisällä. Resursseja toteutukseen ei anneta, eikä osata perustellusti pyytää.

Organisaatioturvallisuuden osalta vakavin tilanne syntyy vastuuttomassa turvallisuustoiminnassa. Siinä selkeästä tarpeesta huolimatta riskienhallintaa ei toteuteta missään muodossa. Kehityksen esteenä on pahimmillaan yksittäinen vaikutusvaltainen taho ja järkiperusteiden sijaan pelon ja ylpeyden tunteet. Vastuuttomasti hoidetun organisaatioturvallisuuden seurauksena riskit ovat toteutuessaan murskaavia ja toiminnan jatkuvuutta uhkaavia. Kehittämis-toimenpiteiden sijaan organisaatiossa alkaa syyllisten etsintä ja vastuun välttely.

lhannetilanteessa turvallisuustoiminta on systemaattista. Tulevaisuudessa se voi tarkoittaa virtuaalisesti verkostoituneista ja aktiivisista yksilöistä koostuvan yhteisön tukea yksittäisen organisaation riskienhallinnan suunnittelussa ja toteutuksessa. Toimintaympäristön hallinnan vaikeutumisen rinnalla myös tiedonhankintamahdollisuudet lisääntyvät ja niitä hyödynnetään aktiivisesti. Turvallisuustoiminta perustuu suunnitelmiin ja riskianalyysiin osoitetut resurssit ja organisaatiojohdon riskienhallintaa ja turvallisuutta koskevat linjaukset huomioiden. Toteutuneet riskit hyödynnetään aktiivisesti kehittämistyöhön.

6.3 Riskienhallinta tukee eduskunnan kanslian turvallisuuden kehittämistä

Riskienhallinnan ja organisaatioturvallisuuden välillä on kiinteä yhteys ja synergia. Niitä yhdistää erityisesti proaktiivisuuden ja suunnitelmallisuuden fundamentit.

Riskienhallintaprosessi yhtenäistää ja systematisoi organisaation turvallisuustoimintaa. Sillä on vaikutusta myös turvallisuuteen liittyvään termistöön. Yhtenäiset toimintatavat ovat tärkeitä organisaation sisäisen turvallisuuskulttuurin kehittämisessä ja erityisesti viranomaisyhteistyön sujuvuuden kannalta. Riskienhallintaprosessin termistön yhteneväisyys ja toiminnan mitattavuus luovat hyvän perustan myös eduskunnan kanslian turvallisuustoiminnan tason mitattavuudelle ja kehittämiselle.

Yhteistyö korostuu erityisesti poikkeustilanteissa ja kansallisissa hätätilanteissa. Organisaation tilannetietoisuus on edellytys hyvälle yhteistyölle viranomaisten kanssa ja mahdollistaa te-

hokkaammin maineenhallinnan kriisiviestinnän muodossa. Lisäksi on huomioitava, että organisaatiokohtaiset tilannetiedot voivat joissain tilanteissa olla merkittävä osa laajempaa tilannekuvaa, jolloin viestinnän oikea sisältö, oikea-aikaisuus ja oikea muoto ovat tärkeitä.

Laadukas riskienhallintatoiminta ja organisaatioturvallisuus tukevat poikkeustilanteiden hallintaa ja kriisiviestintää. Kokonaisvaltaiseen riskienhallintaan kuuluvat toiminnan jatkuvuus-suunnittelu (business continuity management), häiriötilanteista toipumissuunnitelmat (disaster recovery planning) ja (liike-) toiminnan vaikutusanalyysi (business impact analysis) ovat kaikki osa poikkeustilanteisiin valmistautumista. Niiden pohjalta kerätty ja analysoitu tieto auttaa organisaatiojohtoa reagoimaan nopeammin, arvioimaan tilannetta paremmin tiedoin ja toimimaan järjestelmällisesti poikkeustilanteissa. Riskienhallintaprosessiin käynnistämiseen liittyvät johto-, vastuu- ja viestintäkanavien määrittely, käyttäminen ja harjoitusmuotoinen testaus voisivat eduskunnan kansliassa toimia pohjana poikkeustilanteiden hallinnassa ja kriisiviestinnässä.

Riskienhallintaprosessiin sisältyvät toimintatavat, työkalut ja raportointi tukevat ja kehittävät väistämättä organisaatioturvallisuutta. Riskienhallinta voidaan tietoisesti valjastaa ensisijaisesti turvallisuuden kehittämiseen. Yksi merkittävistä hyödyistä on silloin toiminnan kokonaisvaltaisuus – riskien ja uhkien moninaisuus, niiden lähteet ja vaikutukset huomioiden myös organisaatioturvallisuutta on väistämättä tarkasteltava sen kaikkien osa-alueiden osalta. Vaikka riskienhallinta sisältää organisaatioturvallisuuden lisäksi muita tavoitteita, voidaan se siis erinomaisesti valjastaa turvallisuuden kehittämiseen. Turvallisuus on tärkeä tavoite jokaisessa organisaatiossa.

7 Riskienhallintatoiminnan käynnistäminen eduskunnan kansliassa

Riskien huomioiminen toiminnassa ei valtionhallinnon organisaatioiden osalta saa jäädä viitsimisen jalkoihin, sillä jo hyvän hallintotavan ja yhteiskunnan turvallisuusstrategiainkin toimivuuden näkökulmasta aktiivisen riskienhallinnan on oltava osa niiden jokapäiväistä toimintaa.

Riskienhallinnalla on selvästi pidemmät perinteet julkisen sektorin toiminnassa kuin turvallisuusjohtamisella; riskienhallintaa koskeva ohjeistus on kattavampaa ja sen kehitysvaiheet pidemmällä. Riskienhallinnan on ilmeisesti koettu olevan turvallisuusajattelua luonnollisempi tai relevantimpi osa-alue julkisen organisaation toiminnassa. Toisaalta on myös mahdollista, että riskienhallinnan on julkisella sektorilla ajateltu edustavan turvallisuustoimintaa.

Turvallisuusajattelun hajanainen kehittyminen julkisella sektorilla selittyy osaksi sillä, että organisaatioiden toimintaa eivät yhtä olennaisesti ohjaa voiton tavoittelu tai toimintaympäristön vahva kilpailu. Eduskunnan kanslian kohdalla riskienhallintatoiminnan käynnistäminen palvelisi kuitenkin erityisesti turvallisuustoiminnan kehittämistä, turvallisuuskulttuurin rakentamista ja parantaisi poikkeustilanteiden johtamisen edellytyksiä.

Julkisen organisaation turvallisuusjohtaminen sisältää yksityiseen sektoriin nähden samat osa-alueet, mutta henkilöstön hyvinvointiin ja motivaatioon, tietoturvallisuuteen sekä laillisuuteen liittyvät uhkat ja riskit korostuvat julkisella sektorilla. Sen sijaan varsin vähän huomiota lähdekirjallisuudessa sai julkisen sektorin organisaatioihin liittyvät maineriskit. Niiden arvioimiseen ja hallitsemiseen olisi syytä panostaa juuri julkisella sektorilla, jossa toiminnan luotettavuus ja legitimitetti perustuvat ensisijaisesti hyvään maineeseen ja kansalaisten luottamukseen. Mainerikit ovat lisäksi vaikeimmasta päästä hallita; niitä ei voida siirtää tai kokonaan poistaa eikä niiden varalle voida ottaa vakuutusta. Mainerikin toteutuessa toiminnan jatkuvuus voi olla koetuksella, sillä luottamus on helppo menettää, mutta äärimmäisen työläs (ja joissain tapauksissa mahdotonta) palauttaa.

Aikaisemmat luvut käsittelevät riskienhallintaa ja eduskunnan turvallisuusympäristön muutoksia ja toimivat siten osaltaan perusteluina turvallisuustoiminnan kehittämisen tarpeelle ja toisaalta esittelevät riskienhallinnan hyödyntämismahdollisuuksia organisaatioturvallisuuden parantamiseksi. Tässä luvussa käsitellään riskienhallinnan käynnistämistä eduskunnan kansliassa. Eduskunnan kansliassa tehtävä riskienhallintaa koskeva suunnittelutyö ja päätökset ovat korvaamattoman tärkeitä yhtäältä henkilöstön riskienhallintaosaamisen karttumisen ja toisaalta kanslian turvallisuustoiminnan omaehtoisen kehittämisen kannalta.

7.1 Riskienhallinnan tavoitteet eduskunnan kansliassa

Tämän kehittämistyön näkökulmasta riskienhallintatoiminnan käynnistäminen eduskunnan kansliassa liittyy erityisesti organisaatioturvallisuuden kehittämiseen. Riskienhallintaprosessi tuottaa turvallisuusjohtamisen tueksi muun muassa järjestelmällisyyttä, suunnitelmallisuutta, riskitietoisuutta ja syvempää organisaation tuntemusta. Turvallisuusjohtamisen ja riskienhallinnan tavoitteiden ja johtamisen ollessa selkeästi samansuuntaiset, olisi niiden välillä vallitsevan synergian hyödyntäminen viisasta vastakkainasettelun sijaan.

Myös eduskunnan kanslian osalta riskienhallinnan tavoitteita ovat vaatimustenmukaisuus ja sidosryhmäodotukset. Valtioneuvosto, valtion hallintoviranomaiset, valtion liikelaitokset, muut valtion viranomaiset ja kunnat ovat valmiuslain perusteella velvollisia varautumaan poikkeusoloihin ja tekemään valmiussuunnitelmia. Varautumista johtaa, valvoo ja koordinoi valtioneuvosto, jonka viestintäyksikkö vastaa valtioneuvostotason yhteystoiminnan kehittämisestä. (Valtioneuvoston kanslia 2007, 19–23.) Kansakunnan ylin päätöksenteko- ja lainsäädäntöelin kuuluu yhteiskunnan elintärkeisiin toimintoihin. Eduskunnan kansliassa toiminnan jatkuvuussuunnitelmien tulisi koskea koko organisaatiota, ei ainoastaan täysistuntoa. Jatkuvuussuunnittelun on oltava ajan tasalla riippumatta siitä, millaisessa asemassa turvallisuustoiminta tai riskienhallinta organisaatiossa muutoin ovat.

Valtionhallinnon organisaatiossa riskienhallinnan tuoma hyöty liittyy ennen muuta lisääntyvään toiminnan tehokkuuteen (Hopkin 2010, 231). Taloudellisten mittareiden lisäksi tämä tarkoittaa toiminnan laatua ja esimerkiksi organisaation sisällä esiintyviin haasteisiin liittyen ongelmien todellisen syyn löytämistä ja ratkaisemista. Organisaation riskienhallintatoiminnan laajuuden on oltava oikeassa suhteessa organisaatiota koskevien riskien luonteeseen, kokoon ja kompleksisuuteen nähden. Käytännössä tämä tarkoittaa sitä, että riskienhallintakeinoista aiheutuvia kustannuksia on verrattava riskin toteutumisesta aiheutuviin kustannuksiin.

Eduskunnan kanslian riskienhallinnasta kustannuksia syntyy ensisijaisesti riskienhallinnan asiantuntijan tehtävään perustamisesta ainakin palkkauksen ja koulutuksen osalta. Ylimmän virkamiesjohdon riskienhallintakoulutus voidaan järjestää riskienhallinnan asiantuntijan toimesta ja muun virkamiesjohdon osalta se voidaan sisällyttää ulkoistettuihin esimieskoulutuksiin, kuten virkamiesjohto itse ehdotti sisäisen tarkastuksen vuonna 2010 toteuttamassa kyselyssä (Eduskunnan kanslia 2010c). Riskienhallintajärjestelmän rakentaminen ei välttämättä vaadi suuria investointeja, mutta organisaation osaamisen kehittyessä ja sen myötä riskienhallinnan tavoitteiden tarkentuessa on mahdollista, että kuluja syntyy esimerkiksi tieto- tai johtamisjärjestelmien kehittämiseen tai valittujen riskienhallintakeinojen (henkilöstön koulutus, rekrytointi, vakuuttaminen, laitteet ja koneet, muu välineistö) liittyen.

Organisaation taloussuunnitteluun liittyy myös arvokysymyksiä. Johto on yleensä, ja vaikeina taloudellisina aikoina erityisesti, kiinnostunut juuri toiminnan tehokkuuden lisäämisestä. Hopkinin mukaan riskienhallinnan taloudellisen hyödyn mittaamisen osalta on haasteellista kuitenkin absoluuttisesti arvottaa estetty riski ja siitä syntynyt hyöty. Lisäksi riskienhallinnasta koitua hyötyä on usein tulevaisuudessa mahdollisesti toteutuva, ei niinkään heti nähtävissä oleva hyötyä tuottava tai kustannuksia vähentävä tapahtuma. (2010, 115.) Eduskunnan kanslian osalta tämä koskee erityisesti strategisia ja operatiivisia riskejä sekä työturvallisuutta. Henkilöstön hyvinvointi edellyttää ennaltaehkäiseviä satsauksia, jotka puolestaan heijastavat organisaation todellista sitoutumista henkilöstöönsä tärkeimpänä suojattavana arvonaan.

Eduskunnan kansliassa toteutettavan riskienhallintatoiminnan merkittäviä tavoitteita ja hyötyjä ovat ainakin (soveltaen myös sisäisen tarkastuksen virkamiesjohdolle jo vuonna 2008 tekemän kyselyn tuloksia)

- toimintaprosessien tehostuminen, toimintokohtaiset riskikuvat
- henkilöstön yleinen riskitietoisuus, turvallisuuskulttuurin rakentuminen
- strategiseen päätöksentekoon ja organisaation johtamiseen tarvittavan analysoidun tiedon lisääntyminen,
- poikkeustilanteiden toiminta- ja johtamisvalmiuksien paraneminen
- kanslian eri yksiköiden välisen yhteistoiminnan lisääntyminen, organisaatiokulttuurin vahvistuminen
- henkilöstön osaamisen ja kehittämisideoiden tehokkaampi hyödyntäminen
- johtamisen ja johtamisjärjestelmän kehittäminen, hyvä hallintotapa
- hyvinvoiva henkilöstö
- eduskunnan maineen suunnitelmallinen ja kokonaisvaltainen hallinta
- turvallisuustoiminnan kehittyminen kohti kokonaisvaltaista organisaatioturvallisuutta.

Schroderus ehdotti eduskunnan kanslian turvallisuustoimintaa käsitelleessä lopputyössään jatkotutkimuksen aiheeksi johdonmukaisen viestintätavan luomisen turvallisuustoiminnan kehittämistarpeiden viestittämiseksi eduskunnan poliittiselle johdolle ja turvallisuustoiminnan jalkauttamiseksi työntekijätasolle (Schroderus 2008, 29, 46). Riskienhallintaprosessi vastaisi erinomaisesti myös edellä mainittuihin tavoitteisiin.

Riskienhallinta mahdollistaa eduskunnan kanslian toimintaan liittyvien riskien ja uhkien aktiivisen havainnoinnin, eri riskilajien ja organisaatioturvallisuuden osa-alueiden realistisen painottamisen ja resurssien käytön pitkäjänteisen suunnittelun. Viimeisen työtyytyväisyyskyselyn (2011) mukaan henkilöstö kokee suurimpien haasteiden olevan johtamisessa ja viestinnässä. PESTE-analyysin, virkamiesjohdon kyselyn ja yhteiskunnan turvallisuusstrategian perusteella tärkeimmiksi kehittämiskohteiksi nousevat puolestaan henkilö- ja tietoturvallisuus sekä valmiussuunnittelu.

Liittyipä eduskunnan kanslian haaste tai ongelma mihin riskilajiin tai organisaatioturvallisuuden osa-alueeseen hyvänsä, riskienhallintatoiminta mahdollistaa todellisten syiden selvittämisen tehostaen samalla kestäväen ratkaisun löytämistä. Riskienhallinnalla olisi myös eduskunnan kansliaa yhdistävä ja kokoava vaikutus erityisesti käynnissä olevien ja pienryhmissä toteutettavien, koko eduskunnan kansliaa koskevien kehittämisprojektien osalta (esimerkiksi asiakirjaturvallisuus ja kriisiviestintä, tasa-arvotutkimukset, työhyvinvointikyselyt ja työhyvinvoinnin kehittäminen).

7.2 Riskienhallinnan integrointi eduskunnan kanslian toimintaan

Ennen riskienhallintatoiminnan käynnistämistä eduskunnan kansliassa on laadittava riskienhallintaa ohjaava asiakirja. Toimintaa ohjaavan asiakirjan laatimista olisi aiheellista järjestää eduskunnan kanslian johdolle koulutusta riskienhallinnan periaatteista, tavoitteista ja toteutusperiaatteista, jotta heidän olisi paremmin mahdollista osallistua asiakirjan laadintaan. Riskienhallintaa ohjaava asiakirja olisi hyvä luonnostella etukäteen riskienhallinnan asiantuntijan toimesta, mutta sen lopullinen muotoilu vaatii kanslian ylimmän johdon osallistumista ja hyväksynnän. Ylimmän virkamiesjohdon laatima riskienhallintapolitiikan tulee ilmaista riskienhallintaan liittyvän tahtotilan ja tavoitteet.

Riskienhallinnan ohjausasiakirjat voidaan eriyttää pienemmille ryhmille sopiviksi laatimalla yksiköiden tasolle erilliset asiakirjat, joissa koko organisaatiotason tavoitteet on jaettu edelleen osatavoitteisiin. Tällöin henkilöstö saa tarkemman käsityksen oman vastuualueensa riskienhallintatoiminnasta ja menetelmistä. Henkilöstön osallistaminen riskienhallintaprosessiin on erityisen tärkeää viimeistään tässä vaiheessa, jotta laadittujen ohjeiden jalkautus riskien tunnistamis- ja arviointityön muodossa on henkilöstön näkökulmasta mahdollisimman mielekästä ja motivoivaa.

Ohjaavan asiakirjan lisäksi eduskunnan kanslian riskienhallintatoiminnan käynnistäminen vaatii sopivien työkalujen valintaa. Työkalujen tarkoituksenmukaisuus on ratkaisevan tärkeää ja niiden suunnitteluun tulee käyttää riittävästi aikaa. Riskien tunnistamisen ja arvioinnin työvälineitä ovat esimerkiksi riskikartat ja riskiprofiilit. Työkalujen avulla organisaatiossa muodostetaan riskikuva, jota on seurattava ja päivitettävä säännöllisesti. Riskien arvioinnissa yleisesti käytettyjä tekniikoita puolestaan ovat kyselylomakkeet, tarkistuslistat, työryhmätyöskentely, aivoriihi, PESTLE- ja SWOT-analyysit sekä riippuvuusanalyysit (Hopkin 2010, 123).

Riskienhallinnan integroiminen organisaation strategiatyöhön ja olemassa oleviin johtamisjärjestelmiin on tärkeää. Riskienhallinnalle asetetut tavoitteet, aikataulu, organisaation strategiasuunnittelun sykli, johtamisjärjestelmät sekä riskienhallinnan organisointi vaikuttavat siihen, miten integrointi toteutetaan. Juvosen mukaan vaihtoehtoja ovat erillinen riskienhallin-

nan kehittämisprojekti tai strategiasuunnittelun yhteyteen rakennettu projekti, jossa riskienhallinta integroidaan osaksi tai kokonaan käytössä oleviin johtamisjärjestelmiin. (Juvonen ym. 2005, 192.)

Koska riskienhallintatoiminta on eduskunnan kanslian henkilöstölle suhteellisen vieras asia, olisi se hyvä käynnistää hallitusti pienemmissä kokonaisuuksissa. Silloin on mahdollista paremmin varmistaa, että toiminta perustuu yhtenäisiin ohjeisiin ja käytäntöihin. Lisäksi toiminnan alkuvaiheessa havaittavat kehittämiskohteet saadaan heti työstettyä. Käytännössä tämä tarkoittaa sitä, että riskienhallintatoiminta käynnistetään ensin yhdessä yksikössä. Yksikön/osaston valinta voidaan tehdä esimerkiksi sen kohdalla tunnistettujen ja priorisoitavien kehittämistarpeiden vuoksi tai yksikön itsensä ilmaiseman halukkuuden perusteella.

Riskienhallinnan integrointi tarkoittaa koko henkilöstön osallistumista sen suunnitteluun ja toteutukseen. Toiminnan käynnistäminen ja kehittäminen yksiköittäin tukee myös yksikkötason osaamisen ja turvallisuuskulttuurin kehittymistä. Riskienhallinnan asiantuntijan rooli on toiminnan alkuvaiheessa varsin vahva, mutta ajan myötä ja yksikköjen osaamisen karttuessa hänen tehtävänä on ennen muuta tukea, ohjata ja kehittää riskienhallintatoimintaa koko organisaation tasolla. Tehtäviin kuuluu lisäksi toimia sisäisen tarkastuksen rinnalla eduskunnan kanslian ylimmän johdon esikuntana, tarkoittaen käytännössä yhtenäisen riskikuvan rakentamista yksikkökohtaisten raporttien pohjalta, riskienhallinnasta raportointia ja asiantuntija-avun tarjoamista ylimmälle johdolle. Lisäksi riskienhallinnan asiantuntijan tehtävänä on osallistua turvallisuusjohtajan rinnalla sidosryhmätyöskentelyyn erityisesti viranomaisyhteistyön osalta.

Varsinainen riskien tunnistaminen ja niiden arviointi sekä hallintatyö tapahtuisivat näin ollen yksiköissä riskienhallinta-asiantuntijan tukemana ja riskienhallintastrategian tai -politiikan linjausten mukaisesti. Eduskunnan kanslian kuuden eri yksikön toiminta ja riskit poikkeavat toisistaan, mutta niistä jokaisen tulisi huolehtia ainakin henkilö-, toimitila-, tieto- ja ympäristöturvallisuuteen liittyvistä riskeistä sekä pohtia omalta osaltaan pelastustoimintaa ja varautumissuunnitelmaa. Yksiköiden osaamisalueet tulisi ottaa hyödyntää koko organisaation riskienhallinta- ja turvallisuustoiminnassa, esimerkiksi tieto- ja viestintäyksikkö voisi osallistua kriisiviestinnän käytännön harjoitusten suunnitteluun ja toteutukseen.

Yksiköiden riskienhallinnan mahdollisia painotuksia on eritelty tarkemmin liitteessä seitsemän. Kanslian kunkin yksikön osalta tulisi ainakin arvioida henkilö-, tieto- ja työturvallisuuden tilanne, pelastustoiminta ja toiminnan jatkuvuussuunnittelun tila. Eduskunnan kanslian kehittämistarpeet syntyvät osaltaan eri yksiköiden tarpeiden synteesinä, mutta sen lisäksi tulisi arvioida erityisesti jatkuvuussuunnittelun, kriisiviestinnän ja turvallisuuskulttuurin kehittämisen tarpeet. Yksittäisten riskien lisäksi olisi tärkeää työstää organisaation eri toimintojen ja

rakenteiden keskinäiset riippuvuussuhteet – miten yksittäisen yksikön tai toiminnon keskeytyminen tai lamaantuminen vaikuttaa muuhun organisaatioon? Löytyykö toisten yksiköiden väliltä merkittävämpiä riippuvuuksia kuin toisten? Pitäisikö riippuvuussuhteisiin pyrkiä vaikuttamaan? Voidaanko niihin ylipäätään kustannustehokkaasti vaikuttaa?

Riskienhallintatoimintaan liittyvien vastuiden tulee olla selvät. Ilmosen mukaan suurempiin organisaatioihin perustetaan riskienhallinnan ohjausryhmä, johon kuuluvat yrityksen ylin johto, operatiivinen johto sekä riskienhallinnasta vastuulliset tahot (Ilmonen ym. 2010, 57). Riskienhallinnan vastuut jakautuvat eduskunnan pääsihteerille, yksikkötason esimiehille, henkilökunnalle, riskienhallinnan asiantuntijalle, turvallisuusjohtajalle ja sisäiselle tarkastukselle. Esimiesasemassa toimivien tulisi mieltää riskienhallinta yksikkönsä ydintehtäviin ja toimintoihin luonnollisesti kuuluvana vastuuna sen sijaan, että sitä lähestyttäisiin ”oikeasta” toiminnasta erillisenä, irrallisenakin toimintona (Hopkin 2010, 87–88). Puhemiesneuvostosta on mahdollista nimetä yksi henkilö riskienhallinnan suojelijaksi (guardian) (Hopkin 2010, 90), jolloin myös eduskunnan kanslian poliittinen johto olisi paremmin tietoinen kehittämistarpeista ja sitoutunut niiden edellyttämien resurssien varmistamiseen (mukaan lukien tahtotila). Eduskunnan kanslian toimintaan vaikuttava poliittinen johto olisi tavalla tai toisella hyvä sitoa riskienhallintatoimintaan, sillä kansanedustajiin kohdistuvat uhkat vaikuttavat myös kansliaan ja kanslian turvallisuusyksikkö on yhtäläillä myös heistä. Riskienhallinnan neuvottelukunnan perustaminen on tästä syystä myös yksi vaihtoehto.

Yhteismitallisen kuvan saaminen organisaation riskeistä edellyttää yhtenäisen riskienhallintajärjestelmän käyttöönottoa. Sopivan viitekehyksen löytäminen voi eduskunnan kanslian kohdalla olla haasteellista. Riskienhallintaan liittyviä standardeja on erilaisia, mutta ne noudattavat yleensä samaa perusrunkoa. Riskienhallintastandardien käytön puolesta puhuu myös se, että ne luovat yhteisen riskienhallintasanaston ja metodin, mikä puolestaan mahdollistaa organisaatiossa jatkuvan ja toistettavan lähestymistavan riskienhallintaan (Ilmonen ym. 2010, 30). Standardeja voidaan hyödyntää myös soveltaen. Eduskunnan kanslian osalta viitekehyksen valinnassa on huomioitava ainakin viranomaisyhteistyön asettamat vaatimukset turvallisuustason ja riskienhallinnan vähimmäistasoista. Vähimmäisvaatimuksena kuitenkin on, että riskienhallintatoiminnassa käytettävät menetelmät ja erityisesti termistö ovat eduskunnan kanslian sisällä yhteneväiset.

7.3 Turvallisuuskulttuuri ja riskitietoisuus

Suomalaisissa työyhteisössä turvallisuuskulttuuri on siinä mielessä vielä huonosti ymmärretty käsite, että turvallisuuden hoitaminen mielletään usein yksinomaan turvallisuushenkilöstön vastuuksi ja muusta toiminnasta irralliseksi. Riskienhallinta- tai turvallisuusstrategiasta ei kuitenkaan ole hyötyä, mikäli henkilöstö ei joko tiedonpuutteen tai asenteiden vuoksi niitä nou-

data. Organisaation turvallisuuden edistämistäväylät perustuvat myös Suomisen mukaan rakenteellisten ja valvontaratkaisujen ohella nimenomaan henkilöstövoimavarojen käyttöön, sillä henkilöstön asenteet ja järkevät työtavat vaikuttavat ratkaisevasti turvallisuuden edistämiseen (2003, 165–167).

Turvallisuuskulttuurin rakentaminen ja henkilöstön riskitietoisuuden parantaminen ovat eduskunnan kansliassa sekä riskienhallinnan käynnistämisen että organisaatioturvallisuuden kehittämisen kannalta kriittisiä tavoitteita. Eduskunnan kansliassa kukin yksikkö tai osasto tuntuu toimivan erillisenä kokonaisuutenaan ja niiden välinen yhteistyö on varsin vähäistä. Yhtenäisen organisaatiokulttuurin puute vaikuttaa myös turvallisuuskulttuurin kehittämiseen.

Eduskunnan kanslian riskienhallintatoiminnan käynnistämisessä tulisikin yhtäältä ottaa huomioon yksiköiden ja osastojen poikkeavat tarpeet ja toisaalta olisi pyrittävä hyödyntämään niiden välillä riskienhallintaprosessin kautta tapahtuvaa luontevaa lähentymistä esimerkiksi asiantuntemuksen jakamisen tai parhaiden käytäntöjen muodossa. Riskienhallinnan toteutuksella haetaan eri yksiköiden välillä yhtenäistä käytäntöä riskien analysoimiseen ja mittaamiseen tasapainoisen ja yhteismitallisen kuvan saamiseksi koko organisaation eri riskeistä (Kuusela & Ollikainen 2005, 135, 158). Riskienhallintaprosessi ja turvallisuuskulttuurin rakentaminen eduskunnan kansliassa voisivat näin ollen avata tien yhtenäisempään organisaatiokulttuuriin.

Turvallisuuskulttuurin kehittäminen edellyttää edellä mainituista syistä substanssiosaamisen lisäksi myös eduskunnan kanslian toimintakulttuurin ymmärrystä ja kykyä motivoida henkilöstö osallistumaan riskienhallintaan. Henkilöstölle tulee tarjota yleisen tason riskienhallinta- ja turvallisuuskoulutusta ja tarpeen mukaan yksikkö-, toiminto- tai projektikohtaista koulutusta. Koulutuksen tulisi teorian lisäksi sisältää havainnollistavia esimerkkejä ja interaktiivisia osuuksia. Interaktiivisuus mahdollistaisi henkilöstön kysymysten ja ehdotuksen aktiivisen hyödyntämisen koulutuksen ja riskienhallinnan kehittämisessä.

Eduskunnan kanslian henkilöstön osallistaminen riskien tunnistamiseen ja arviointiin sekä valittujen riskienhallintakeinojen arviointiin syventäisi riskienhallintaprosessia ja edistäisi henkilöstön riskitietoisuutta. Työryhmissä tehty työ auttaisi henkilöstöä tunnistamaan paremmin omaan toimenkuvaan liittyviä riskejä ja toisaalta madaltaa kynnystä epäkohtiin puuttumisen tai niistä raportoinnin suhteen. Lisäksi osallistuminen suunnitteluvaiheeseen vaikuttaa suotuisasti valittujen toimintamallien käytännön toimeenpanoon.

Riskien kartoittaminen ja analysointi toimivat näin ollen sellaisenaankin eräänlaisena riskienhallinnallisena keinona. Vaikka kaikkia riskejä ei voida kokonaan poistaa, on niiden läpikäyminen hyödyksi koko eduskunnan kanslialle. Henkilöstön osallistuminen riskienhallintatyöhön on välttämätöntä, mutta se ei missään tilanteessa saa korvata ylimmän johdon osallistumista,

tukea ja aktiivisuutta. Johdon sitoutuminen ja tuki riskienhallinnalle on turvallisuuskulttuurin rakentamisen elinehto (Hopkin 2010, 106).

Riskienhallintaan ja organisaatioturvallisuuden kehittämiseen liittyvät käsitteet riskinottohalukkuus (risk appetite) ja riskin kantokyky (risk capacity). Organisaatiojohto määrittelee riskinottohalukkuuden, joka ei välttämättä kuitenkaan ole sama, kuin organisaation todellinen riskin kantokyky (Hopkin 2010, 233–242). Molemmat vaikuttavat osaltaan turvallisuuskulttuurin muodostumiseen ja henkilöstön riskitietoisuuden kehittymiseen. Yleinen turvallisuudentunne ja organisaation turvallisuustoiminnan suorituskyky vaikuttavat nekin organisaation turvallisuuskulttuuriin ja erityisesti siihen, mitkä organisaatioturvallisuuden osa-alueista koetaan tärkeimpinä. Organisaatioturvallisuuden käytännön toteutuksen tulee olla tasapainossa organisaatioon kohdistuvien riskien ja niiden hallintaan käytettävissä oleviin resursseihin nähden. Epäonnistunut painotus vaikuttaa henkilöstön suhtautumiseen ja siten myös turvallisuuskulttuuriin.

Organisaatio- ja turvallisuuskulttuurin, kuten minkä tahansa kulttuurin muuttaminen on vaikeaa ja varsin hidasta. Vastahakoisiin asenteisiin ja tunteisiin on erityisen vaikea vaikuttaa ainoastaan tietoa jakamalla tai logiikkaa käyttäen. Täysin mahdotonta se ei kuitenkaan ole, sillä usein henkilökohtaiset kokemukset muuttavat juuri asenteita ja tuntemuksia. Turvallisuutta ei tule edistää pelon avulla, mutta havainnolliset esimerkit tosielämän tilanteista ovat edellisen perusteella oleellinen osa koulutusta. Myös hahmotelmat turvallisuustoiminnan toteutuksesta suhteessa turvallisuusympäristön vaatimuksiin auttavat henkilöstöä ymmärtämään muutoksen tarpeen (Kuvio 21).

Turvallisuuskulttuurin kehittäminen vaatii paljon työtä. Eduskunnan kanslian turvallisuusyksiköllä ja toisaalta myös riskienhallinnan asiantuntijalla tulisi olla aktiivisesti turvallisuuskulttuuria edistävä rooli. Koko organisaatiota koskevien vuosittaisten turvallisuuskatsausten tai koulutustilaisuuksien lisäksi eduskunnan kanslian eri yksikköjen osalta tulisi huolehtia säännöllisestä ja kohdennetusta turvallisuuteen ja riskienhallintaan liittyvästä yhteydenpidosta. Vastuu aktiivisuudesta on ensisijaisesti turvallisuudesta ja riskienhallinnasta vastaavilla tahoilla. Myös eri yksikköjen motivointi ja osallistaminen on edellä mainituissa yksiköissä työskentelevien ammattilaisten tehtävä.

Jos käytännön riskienhallintatyö käynnistetään eduskunnan kansliassa yhdestä yksiköstä, tulisi tämän yksikön osalta huomioida itse riskienhallintaprosessin lisäksi turvallisuuskulttuurin kehittäminen. Tiedot, taidot, arvot, asenteet ja kokemukset tulisivatkin heti koulutuksen alkuvaiheessa yhdistää, jotta eduskunnan kanslian riskienhallinta ja turvallisuustoiminta saavat kestävä perustan. Käytännössä kukin työntekijä on oman yksikkönsä osalta paras riskienhallinnan asiantuntija ja organisaatioturvallisuuden toimeenpanija. Ammatillaisen tehtäväksi jää

riskienhallintatyössä tarvittavien rakenteiden ja työkalujen tuottaminen, työnohjaus, asiantuntija-avun tarjoaminen sekä riskienhallintatoiminnan kehittäminen.

7.4 Kriisiviestintä ja poikkeustilanteiden johtaminen

Eduskunnan viestintää ohjaa lokakuussa 2011 valmistunut Eduskunnan kanslian viestintästrategia 2011–2014. Eduskunnan kanslialla valmiudet viestinnän tehokkaaseen toteuttamiseen ovat erinomaiset. Sen viestintäyksikössä työskentelee toistakymmentä viestinnän ammattilaista, joiden käytössä on monipuoliset viestintäkanavat, kuten eduskunnan kotisivut, televisio (uutiset, täysistuntolähetykset, haastattelut ja ajankohtaisohjelmat), painettu media, intranet ja sähköinen työtila, sisäinen lehti, sähköposti, mediaa edustavat talon ulkopuoliset toimittajat sekä muun muassa valtiolle.fi ja valtioneuvoston verkkosivustot. Lisäksi se on organisaationa suuren yleisön erityisen mielenkiinnon kohteena.

Työtyytyväisyyskyselyn mukaan eduskunnan kanslian henkilöstö on kuitenkin osittain tyytymättömän talon sisäiseen tiedonkulkuun (Eduskunnan kanslia 2011c, 12). Organisaation ylimmän johdon ja lähimpien esimiesten aloitteellinen, nopea, rehellinen ja oikein ajoitettu kommunikatio on henkilöstön kannalta keskeistä. Kriisitilanteen hoitoon osallistuva virkamies on osaltaan vastuussa sisäisen viestinnän aktiivisuudesta ja tehokkuudesta. (Seeck 2009, 27; Valtioneuvoston kanslia 2007, 20–21.) Toimiva sisäinen viestintä yhtenäistää ulkoista viestintää ja voi parhaimmillaan estää vahinkojen syntymistä esimerkiksi henkilöstön pelastautumista vaativissa tilanteissa. Viestintästrategiassa sisäisen vuorovaikutuksen parantaminen onkin nimetty yhdeksi painopisteeksi (Eduskunnan kanslia 2011e, 3).

Normaaliolojen viestintä luo perustan kriisiviestinnälle. Eduskunnan kanslian kriisiviestintäohjeen luonnos julkaistiin intranetissä joulukuussa 2011. Kriisiviestintäohje käsittelee kriisiviestintämalleja, viestinnän keinoja, kriisiviestinnän dokumentointia ja jälkiarviointia. Lisäksi se sisältää muun muassa muistilistan ja yhteystietoja sekä kriisiviestinnän periaatteet sisältävän huonetaulun. Ohjeessa otetaan kantaa myös kriisiviestinnän vastuisiin ja organisointiin tila-vaatimukset mukaan lukien. (Eduskunnan kanslia 2011d.) Viestinnän ja johtamisen tärkeä yhteys ja vuorovaikutus jäävät kuitenkin sekä kriisiviestintäohjeessa että viestintästrategiassa varsin vähälle huomiolle.

Olkoonkin, että viestintä ja johtaminen ovat toisistaan erottamattomat, ei niiden saumaton yhteensovittaminen silti ole itsestäänselvyys. Yhteensovittaminen alkaa normaaliolojen viestinnästä ja myös eduskunnan kanslian arkeen sisältyy tilanteita, joissa johdon olisi oltava tilannetietoinen ja kykeneväinen sisällöltään onnistuneeseen ja prosessien puolesta tehokkaaseen viestintään. Poikkeustilanteiden johtamista harjoiteltaessa olisi viestintään kiinnitettävä aivan erityistä huomiota.

Viestinnän ja johtamisen yhteyden vakiintumiseen liittyy eduskunnan kanslian osalta kieltämättä haasteita. Aktiivista viestintää vaativia prosesseja on jatkuvasti käynnissä useilla eri foorumeilla sitoen viestintäyksikön resursseja pois organisaation sisäisestä kehittämis- ja kouluttamistyöstä. Strateginen suunnittelu on vasta aloitettu, eikä organisaation kaikista kriittisistä toiminnoista ole vielä laadittu toimintatapoja selkiinnyttäviä yleisiä politiikkoja.

Lisäksi eduskunnan kanslian johtamiseen osallistuu normaalioloissa ja poikkeustilanteissa virkamiesjohto ja poliittinen johto. Viranomaisviestintä voidaan jakaa poliittiseen ja hallinnolliseen viestintään. Hallinnosta vastaava viranomainen toimii virkavastuulla ja perustaa viestintä faktoihin. Poliittisella vastuulla toimiva voi helpommin kertoa arvioita, näkemyksiä ja vahvistamattomiakin huonoja uutisia. (Huhtala & Hakala 2007). (Seeck ym. 2008, 128.) Haasteena on se, etteivät nämä roolit saa sekoittua keskenään. Eduskunnan kanslian kriisiviestinnässä voitaisiin hyödyntää virkamiesten ja poliittisten viestittäjien käytön mahdollisuutta. Poliittinen viestijä voisi keskittyä henkiseen johtamiseen ja virkamiehet faktoista tiedottamiseen. Viestintävastuista ja rooleista olisi tältä osin sovittava etukäteen ja yhteistoimintaa harjoiteltava. Lisäksi vuorovaikutus näiden viestittäjäryhmien välillä on tärkeää ulospäin suuntautuvan viestinnän johdonmukaisuuden vuoksi.

Eduskunnan kanslian ulkoisen viestinnän johdonmukaisuuden merkitys ja aktiivisuus korostuukin erityisesti maineriskien osalta. Kokonaisvaltainen viestintä puhuttelee yleisöä sekä asiattä tunnetasolla. On tärkeää, että viestintä toteutetaan sidosryhmät huomioiden ja heidän tarpeitaan silmälläpitäen. Eduskunnan toimivalta yleensäkin on riippuvainen kansalaisten sille osoittamasta luottamuksesta ja siten toiminnan legitimitetistä. Eduskunta ja eduskunnan kanslia ovat viime vuosien aikana kärsineet lukuisten maineriskien toteutumisesta (Liite 5). Osa virkamiehistä ei omien sanojensa mukaan uskalla vapaa-ajallaan ollessaan kertoa uusille ihmisille missä ovat töissä.

Ihmisten kriisitilanteissa kokema tuska ja huoli vaativat asiallista, oikea-aikaista ja myötäelävää viestintää. Viestinnän sisällön rinnalla huomiota tulee kiinnittää myös viestinnän muotoon muun muassa kielilain osalta. Lisäksi viranomaisen tai virkamiehen tiedotusvälineissä tai tiedotustilaisuudessa antamista tiedoista voi aiheutua vahingonkorvausvastuu, myös silloin, kun tiedottamisessa ei ole suoranaisesti ole kysymys julkisen vallan käytöstä. (Seeck ym. 2008, 132.)

Juuri viestinnän laatu lopulta ratkaisee, onko siitä hyötyä vai haittaa organisaatiolle poikkeustilanteen hoitamisessa. Kriisiviestintä voi onnistua silloinkin, jos huonoista puitteista tai puutteellisesta ennakkosuunnittelusta huolimatta viestinnän sisältö on laadullisesti hyvää. Kriisiviestinnän osalta tärkeää on erityisesti henkilöiden valinta ja koulutus, kriisiviestintäjärjes-

telmän rakentaminen ja harjoitusten suunnittelu ja toteuttaminen sekä yhteistoimintajärjestelyt eri viranomaisten välillä. (Seeck 2009, 8; Valtioneuvoston kanslia 2007, 24.)

Riskienhallinta ja organisaatiturvallisuuden kehittäminen vaativat käytännön harjoittelua. Poikkeustilanteiden johtaminen ja kriisiviestintä yhdessä ovat oleellinen osa riskienhallintaa ja organisaatiturvallisuuden toteuttamista. Eduskunnan kanslian riskienhallintaan liittyvää vuosisyklää suunniteltaessa olisi näin ollen huomioitava myös johtamisen ja viestinnän harjoittelun tarpeet ja mahdollisuudet.

8 Työn arviointi

Tutkimuksellisen kehittämistyön arvioinnissa tulee Ojasalon ym. mukaan käsitellä kehittämistyön panoksia, muutosprosessia ja lopputulosta sekä niiden välistä suhdetta (2009, 47). Virallisen arvioinnin lisäksi kehittämistyön toimeksiantajan ja tutkijan näkemykset työn onnistumisesta ja käyttökelpoisuudesta ovat tärkeitä.

8.1 Kehittämistyöhön liittyvät eettiset kysymykset

Tutkijalla on, sen alusta lähtien, ollut nöyrä asenne kehittämistyötä kohtaan. Kohdeorganisaatio on tärkeä osa suomalaista yhteiskuntaa ja sen toiminnasta päättävät ihmiset kokeneita ja vaativia. Kehittämistyö on tärkeä myös siksi, että sillä voi parhaimmillaan olla muitakin valtionhallinnon tai julkisen sektorin organisaatioita kehittävä vaikutus.

Kehittämistyön aiheeseen on laajan toimeksiannon rinnalla vaikuttanut tutkijan näkemykset siitä, minkälaisia asioita riskienhallintaa ensi kertaa vaativalle yleisölle avaavan työn tulisi sisältää. Aiheen omaehtoinen täsmentäminen oli mahdollista siksi, että turvallisuusyksikön toimeksianto oli väljä, eikä tutkijan ehdottamiin sisältöihin ehdotettu muutoksia. Kehittämistyön sisällöstä käytiin keskustelua eduskunnan kanslian turvallisuusyksikön lisäksi riskienhallinnan asiantuntijan ja eduskunnan apulaispääsihteerin kanssa. Työn tavoitteet, sisältö ja toteutus ovat edellä mainittujen kesken yhteisesti hyväksytyt.

Kehittämistyössä käytettyjen aineistonkeruumenetelmien osalta on kiinnitetty erityistä huomiota siihen, että haastatteluissa ja kyselyissä selviää, mitä kysymyksillä tarkoitetaan, miksi kysymyksiä esitetään ja minkälaiseen kokonaisuuteen ne liittyvät. Aineiston keruu on suoritettu anonyymisti ja tarvittaessa erilaisen materiaalin käyttöön on kysytty erikseen lupa. Kehittämistyössä ei käytetty turvaluokiteltua materiaalia, eikä salassapitosopimuksia tarvinnut tehdä.

Vaikka tutkimuksen tulokset osoittavat selviä kehittämisen kohteita eduskunnan kanslian turvallisuustoiminnassa, on työn tekoa ohjannut ennen muuta aito organisaation kehittämiseen tähtäävä tavoite syllistämisen sijaan. Sama koskee työn toimeksiantoa; tutkijan valintoja on työn kaikissa vaiheissa ohjannut tavoite eduskunnan kanslian kokonaisvaltaisesta kehittämisestä. Kehittämistyötä ei näin ollen saa käyttää väärin eduskunnan kanslian yksittäisen yksikön tai siinä työskentelevien henkilöiden aseman muuttamisen perusteluna yli organisaatiotaan edun.

8.2 Tavoitteenasettelu ja tulokset

Kehittämistyön tavoitteena oli selvittää eduskunnan kanslian turvallisuustoiminnan kehittämistarpeet ja riskienhallintatoiminnan soveltuvuus turvallisuuden kehittämisessä. Osatavoitteen on eduskunnan kanslian ylimmän virkamiesjohdon motivointi riskienhallintatoiminnan käynnistämiseen ja riskienhallinnan asiantuntijan työn tukeminen. Asetetut tavoitteet ovat laajoja ja sisältävät erityisen haasteen asenteiden ja kulttuurin muutosvaatimustensa suhteen. Kohdeorganisaation kannalta tärkeää on erityisesti motivoiva osuus, sillä muutosten läpivienti eduskunnan kanslian kaltaisessa organisaatiossa vaatii pitkäjänteisyyttä ja aitoa innostusta.

Kokonaisvaltainen viitekehys ja monipuolisesti valitut lähestymistavat auttavat edellä kuvatun laajan tavoitteen saavuttamisessa. Kehittämistyön teoreettinen osuus osoittaa strategisen johtamisen, organisaatioturvallisuuden ja riskienhallinnan välisen yhteyden ja synergiaedut. Samalla se valaisee turvallisuuteen liittyviä todellisia vastuita ylimmän virkamiesjohdon näkökulmasta. Tutkimustyypit tukevat toisiaan ja mahdollistavat monipuolisen ja objektiivisemmän lähestymistavan aiheeseen.

Eduskunnan kansliassa on kehittämistyön valmistumiseen mennessä ehditty ilmaisemaan suotuisa tahtotila riskienhallinnan suhteen. Tätä tahtotilaa heijastavat muun muassa vuoden 2011 sisäisen tarkastuksen vahvistuslauseke ja riskienhallinnan asiantuntijan viran perustaminen. Kehittämistyön vaikutuksia ylimmän johdon riskienhallinnalliseen tietotasoon ja asenteisiin riskienhallintatyötä kohtaan on vaikea arvioida lyhyellä aikavälillä. Vaikutukset tulevat mitä todennäköisimmin esiin vasta, jos ja kun riskienhallintatoimintaa aletaan todella käytännön tasolla toteuttaa.

Turvallisuusyksiköltä saatu palaute on sen sijaan välitöntä (Liite 8). Toimeksiantajan mielestä kehittämistyö on ylittänyt sille asetetut tavoitteet ja sitä tullaan soveltamaan eduskunnan kanslian riskienhallintatoiminnan käynnistämisen tukena. Riskienhallinnan asiantuntijan mukaan kehittämistyö tulee olemaan oleellinen työkalu toiminnan suunnittelun ja toteutuksen aikana.

Työ merkitystä lisää myös sen valmistumisen ajankohta. Viimeisten kahden vuoden aikana on Suomen lähialueillakin tapahtunut useita yleiseen turvallisuudentunteeseen vaikuttavia tapahtumia, jotka ovat osaltaan lisänneet eduskunnan kansliaan paineita organisaatioturvallisuuden ja riskienhallinnan kehittämisen suhteen. Hyvään ajoitukseen liittyy myös eduskunnan kansliaan vuonna 2011 perustetun riskienhallinnan asiantuntijan toimen perustaminen. Tehtävää hoitavan asiantuntemusta rakennetaan parhaillaan ja kehittämistyötä ehditään hyvin prosessoimaan ja käyttämään hyödyksi, ennen kuin eduskunnan riskienhallintatoiminta todella

käynnistyy. Toisaalta ajoitus on hyvä siitäkkin syystä, että eduskunnan kanslian riskienhallinta-toiminnan aloittaminen ennaltaehkäisevänä työnä ei vielä ole liian myöhäistä.

8.3 Teoreettinen viitekehys

Teoreettinen viitekehys sisältää teoriaa useista, itsessäänkin varsin laajoista kokonaisuuksista, kuten organisaatioturvallisuus, riskienhallinta, strateginen johtaminen ja oppiminen. Laajan teoriakehityksen laatiminen on kuitenkin perusteltua siksi, että kehittämistyön ensisijainen tarkoitus on tarjota eduskunnan kanslian johdolle ja riskienhallinnan asiantuntijan tehtävässä aloittaneelle henkilölle monipuolinen tietopohja toiminnan aloittamisen ja kehittämisen tueksi.

Organisaatioturvallisuuden ja riskienhallinnan välisen suhteen käsittely on tärkeää synergiaetujen havaitsemisen vuoksi. Myös niiden vaikutus strategiseen johtamiseen on tärkeä aihe, sillä sen avulla voidaan osaltaan myös perustella organisaatioturvallisuuden kehittämisen ja riskienhallintatoiminnan käynnistämisen tärkeys sekä kaikkia organisaatiotasoja koskevan vastuun merkitys.

On myös mahdollista, että laaja teoriapohja uuvuttaa lukijan. Lisäksi se voidaan kokea lannistavana sikäli, etteivät eduskunnan kanslian kokemukset systemaattisesta strategisesta suunnittelusta ole vielä kovin pitkäaikaisia. Strateginen näkemys organisaation toiminnassa on kuitenkin tärkeää toimintaympäristön muuttuessa yhä kompleksisemmaksi. Organisaatioturvallisuutta ja riskienhallintaa koskevat päätökset ovat lisäksi strategisia päätöksiä. Toisaalta riskienhallinta ja tulevaisuuden skenaariotyöskentely tukevat molemmat osaltaan ja erinomaisesti myös toisiinsa yhdistettynä organisaation strategista johtamista.

Tiedon sanotaan lisäävän tuskaa. Tämän kehittämistyön yhteydessä koottua teoreettista tietoa voidaan kuitenkin käyttää soveltuvin osin käytännöstä saatavan kokemuksen tukena. Riskienhallinnan ja organisaatioturvallisuuden asiantuntijaksi kasvaminen vie aikaa vaatien myös käytännön työkokemusta. Se vaatii paljon yhteistyötä koko organisaation tasolla varsinkin, kun aihepiiri on uusi. Näin ollen yksi kaikilla käytössä oleva kooste teoriaa, analyysiä ja johtopäätöksiä voi parhailtaan luoda pohjan organisaatiossa tapahtuvalle omaehtoiselle kehittämistyölle ja nopeuttaa oppimisprosessia.

Koska kohdeorganisaatiossa ei ole kaikki organisaatiotasot kattavaa riskienhallintatoimintaa ja siihen vaadittavaa osaamista, on aihetta perusteltua lähestyä laajemmasta näkökulmasta. Suppeammat ja syvemmät kehittämistyöt tulevat kysymykseen, kun riskienhallinnan perusteet on luotu ja kokonaisvaltaisen lähestymistavan avulla tunnistettu pienempiä kokonaisuuksia kehittämisen kohteiksi.

8.4 Lähestymistavat

Tapaustutkimus osoittaa, että näennäisesti yksityisen sektorin turvallisuuteen ja riskienhallintaan liittyvät lainalaisuudet koskevat myös julkista sektoria ja valtionhallintoa. Tulevaisuudentutkimuksen skenaariotyöskentelyllä puolestaan on erityinen rooli turvallisuuden kehittämisen motivoinnin osalta. Konstrukttiivinen tutkimus sitoo edellä mainitut tiukasti kohdeorganisaation konkreettisiin tarpeisiin.

Tapaustutkimusta tässä kehittämistyössä edustavat eduskunnan kanslian turvallisuustoiminnan nykytilaa käsittelevä osaluku ja kehittämis ehdotukset sisältävä luku. Koska turvallisuustoimintaa ja riskienhallintaa tulee aina tarkastella kohdeorganisaation ehdoilla, on tapaustutkimuksen sisällyttäminen kehittämistyöhön perusteltua, ellei jopa välttämätöntä. Eduskunnan kanslian turvallisuustoimintaa ja mahdollista riskienhallintatoiminnan käynnistämistä koskevat kyselyt kohdistettiin ainoastaan virkamiesjohtoon tai niihin liittyvissä tehtävissä toimiviin virkamiehiin. Niistä saaduissa tuloksista selviää kuitenkin vain osa totuudesta ja toimihenkilöiden mielipiteet ja ideat olisikin ehdottomasti kartoitettava ennen riskienhallintatoiminnan käynnistämistä.

Tulevaisuudentutkimuksen soveltaminen tässä kehittämistyössä on monelta osin perusteltua. Sen menetelmistä erityisesti skenaariotyöskentely auttaa hahmottamaan tulevaisuuden vaihtoehtoisia kehityskulkuja ja niihin vastaamiseen vaadittavia resursseja. Katse kohdistuu tulevaisuuteen, epätoivottujen ja toivottujen kehityssuuntien kartoittamiseen sekä toiminnan painopisteiden arvioimiseen. Skenaariotyöskentely toimii näin ollen Meristöä (1991, 42) mukaillen tässäkin työssä ennen muuta ajattelun työkaluna ja suunnittelun tukena. Vapaavuori (1993, 215) muistuttaa lisäksi, että skenaariopohjainen ajattelu korostaa tulevaisuuden ennustettavuutta ja antaa siten organisaatiolle aktiivisen toimijan roolin. Sama pätee riskienhallintaan ja turvallisuustoimintaan, sillä nykyhetkessä tehdyt päätökset ja toiminta vaikuttavat tulevaisuuteen ja muokkaavat sitä.

Kehittämistyön skenaariotyöskentely ei kuitenkaan ole täysin tyhjentävää. Laaditut skenaariot ovat yhden henkilön arvioita asioiden mahdollisista kehityskuluista, mutta skenaariotyöskentely on parhaimmillaan vasta, kun siihen osallistuu useampi henkilö. Luova ideointi voi tällöin olla syvällisempää interaktiivisuuden vuoksi ja toisaalta useamman henkilön näkökulmat auttavat hahmottamaan tulevaisuuden erilaisia kehityskulkuja ja niiden seuraamuksia monipuolisemmin. Lisäksi tässä kehittämistyössä skenaariot koostettiin ainoastaan teknologia- ja yhteiskuntasuodattimien kautta, markkinasuodattimien jäädessä tietoisesti pois. Markkinasuodattimien käyttö olisi kuitenkin syventänyt skenaarioita edelleen.

Kehittämistyön skenaariot vaikuttavat kaikki samanarvoisilta ja näin ollen niitä voidaan luonnehtia epävarmaksi tiedoksi. Niiden taustalla olevan tulevaisuustiedon perusteella voidaan kuitenkin arvioida riskienhallinnan käynnistämistä ja organisaatioturvallisuuden kehittämisen tarvetta eduskunnan kansliassa. Skenaariot muodostavat lisäksi objektiivisen näkökulman eduskunnan kanslian turvallisuustoiminnan kehittämistarpeisiin teoriatiedon, empirian ja tapaututkimuksen rinnalle. Turvallisuustoiminnan kehittämistarve kokonaisvaltaisempaan suuntaan nousikin selvästi esiin kaikissa laadituissa skenaariossa.

Konstruktiivista tutkimusta edustaa eduskunnan kansliaa koskevat kehittämis ehdotukset luvussa seitsemän. Tyypillisestä konstruktiivisesta tutkimuksesta poiketen se ei kuitenkaan sisällä konkreettista opasta tai ohjetta, saati valmiita asiakirjapohjia. Kehittämistyössä on voimakkaasti korostettu, ettei riskienhallinnan ja organisaatioturvallisuuden kehittämisen osalta ole tarkoituksenmukaista, että niitä kehitetään kritiikittömästi ulkopuolisten laatimien mallien tai asiakirjojen mukaan. Tämän kehittämistyön konstruktiivinen tavoite onkin ensisijaisesti tutkimustiedon koostamisen ja prosessoinnin avulla helpottaa ja pohjustaa riskienhallinnan ja organisaatioturvallisuuden kehittämisen eteen eduskunnan kansliassa itsessään tehtävää työtä. Toisaalta turvallisuusyksiköstä saatu suullinen ja kirjallinen (Liite 8) palaute kehittämistyön hyödyllisyydestä asettaa työn kokonaisuudessaan eräänlaiseen konstruktiivisen lopputuotteen asemaan.

8.5 Aineistonkeruumenetelmät ja analyysi

Aineistonkeruumenetelmistä eniten käytettiin haastattelua ja kyselyä. Vaikka toteutusta ei ole yksityiskohtaista selitystä tämän kehittämistyön tutkimustieteellisessä osassa, voidaan tulosten sanoa olevan hyviä vastausprosenttien ja sisältöjen käytettävyyden osalta. Haastattelujen ja kyselyjen merkitys korostuu kohdeorganisaation osallistamisen vaatimuksen myötä, koska kehittämistyötä ei ole tarkoituksenmukaista rakentaa pelkästään teoriatiedon tai tutkijan päättelyn varaan. Edellä mainittujen aineistonkeruumenetelmien kohdalla tärkeäksi nousee myös luottamuksellisuus, josta tutkija on pitänyt erityisen tarkasti huolta.

Aineiston analyysissä on käytetty laadullista ja määrällistä menetelmää. Suurimmassa osassa analyysiä ne korvaavat toisensa, mutta eurooppalaisen vertailuaineiston osalta niitä käytetään toisiaan tukemassa. Suurin osa tämän kehittämistyön analyyseistä on tehty laadullisin menetelmin. Tämä on toisaalta perusteltua tehtävän luonteen vuoksi, sillä laadullinen analyysi mahdollistaa parhaiten kohdeorganisaation ymmärtämisen ja kehittämistarpeiden kokonaisvaltaisen kartoittamisen.

Aineistonkeruumenetelmien ja aineiston analyysin voitaneen todeta olevan tarkoituksenmukaisia ja riittävällä tasolla kehittämistyön tavoitteisiin nähden.

8.6 Ehdotuksia jatkotutkimusten aiheiksi

Riskienhallintatoiminnan aloittaminen eduskunnan kansliassa vaatii tahtotilan ja tiedon lisäksi oikeita riskienhallintatyökaluja. Tässä kehittämistyössä on kerrottu riskienhallinnan menetelmistä yleisellä tasolla. Menetelmien menestyksekkäs soveltaminen vaatii kuitenkin niiden räätälöimistä kohdeorganisaation tarpeita ja riskejä vastaaviksi. Näin ollen eduskunnan kansliaan parhaiten sopiviin riskien tunnistustekniikoihin, arviointitapaan, luokitteluun ja hallintakeinoihin sekä riskirekisterin sisältöön, ja riskienhallinnan käytännön raportointiin kantaaottava työ (esim. toimintatutkimus) olisi ehdottomasti tarpeen.

Kriisiviestinnän ja poikkeustilanteiden johtamisen yhteys on selvä. Niiden tarkasteleminen yhtenä kokonaisuutena olisi tarpeen myös eduskunnan kanslian osalta. Kriisiviestinnän merkitys yhtäältä eduskunnan kanslian johtamiselle ja toisaalta maineriskien hallinnassa olisi niin ikään hyvä selvittää. Henkilöstön koulutukseen ja erityisesti käytännön harjoitteluun tulisi panostaa, jotta ohjeistus saadaan vietyä käytäntöön. Uusi kehittämistyön aihe olisikin suunnitella kriisiviestinnän ja poikkeustilanteiden johtamista varten koulutus- ja harjoittelumoduulit.

Tämän kehittämistyön valmistumisen myötä organisaatioturvallisuutta on kartoitettu eduskunnan kanslian virkamiesjohdon näkökulmasta. Eduskunnan kanslian muun henkilöstön turvallisuustietoisuuden kartoittaminen ja heidän turvallisuuteen liittyvien kokemustensa kerääminen toisi merkittävän lisän turvallisuustoiminnan ja riskienhallinnan kehittämiseen. Eri yksiköiden ja osastojen henkilöstön kokemusten myötä riskienarviointiin saadaan syvyyttä ja organisaatioturvallisuuden eri osa-alueiden todellinen painottuminen selkiintyy. Lisäksi koko henkilöstön kokemusten keräys saattaisi – huolella toteutettuna – jo itsessäänkin lisätä organisaatiossa riskitietoisuutta. Yksikkö- ja osastotasolta muodostuvat riskikuvat luovat lisäksi pohjan kohdistetulle koulutukselle (mukaan lukien mielekkäät harjoitukset).

ECPRD -verkoston kautta saadut vastaukset riskienhallinnan toteuttamisesta eurooppalaisissa parlamenteissa jäivät varsin pintapuolisiksi. Vastauksien perusteella olisi mahdollista jatkotutkimuksessa selvittää, miltä osin riskienhallintatoimintansa pitkälle vieneiden maiden toimintaa voidaan hyödyntää eduskunnassa. Tanska ja Ruotsi voisivat olla eduskunnan kanslian kannalta merkittäviä mentoreita, ottaen huomioon samankaltaiset parlamentaariset ja yhteiskuntarakenteet sekä edellä mainittujen parlamenttien turvallisuusympäristön haasteellisuuden liittyvät kokemukset. Niiden osalta voisi näin ollen olla tarkoituksenmukaista toimeenpanna erillinen, kohdeorganisaation suostumuksella ja luottamuksellisesti toteutettu tutkimus.

Lähteet

Arnell, J. 2010. Viestintäviraston kokonaisvaltaisen riskienhallinnan kehittäminen. Laurea-ammattikorkeakoulu. Turvallisuusosaamisen koulutusohjelma. YAMK opinnäytetyö. Tulostettu 1.3.2011. <http://urn.fi/URN:NBN:fi:amk-201002262580>

Asetus valtion talousarviosta 11.12.1992/1243. Finlex. Tulostettu 1.3.2011. <http://www.finlex.fi/fi/laki/ajantasa/1992/19921243>

Doz, Y. & Kosonen, M. 2008. Fast Strategy - how strategic agility will help you stay ahead of the game. Harlow: Wharton School Publishing.

Eduskunnan kanslia. 2011a. Eduskunnan kanslian strategialuonnos 21.9.2011.

Eduskunnan kanslia. 2011b. Eduskunnan kanslian vuoden 2011 työtyytyväisyyskyselyn palaute-tilaisuus henkilöstölle. 5.9.2011. Eduskunnan lisärakennuksen auditorio.

Eduskunnan kanslia. 2011c. Eduskunnan kanslian työtyytyväisyys 2012–2011. Työskentelyaineisto eduskunnan kanslian johdon neuvottelupäiville 25.–26.8.2011. Talent Partners Public Consulting.

Eduskunnan kanslia. 2011d. Eduskunnan kanslian kriisiviestintäohjeisto. Luonnos/marraskuu 2011. Eduskunnan intranet. Tulostettu 12.12.2011.

Eduskunnan kanslia. 2011e. Eduskunnan kanslian viestintästrategia 2011–2014. Luonnos/lokakuu 2011. Eduskunnan intranet. Tulostettu 12.12.2011.

Eduskunnan kanslia. 2011f. Eduskunnan kanslian strategia 2012–2015. Eduskunnan kanslian sisäinen julkaisu.

Eduskunnan kanslia. 2010a. Eduskunnan toiminnan, talouden ja hallinnon valvonnan ja tarkastuksen mahdolliset ongelmat, kehittämishaasteet ja rakenteelliset kehittämismallit. 18.5.2010.

Eduskunnan kanslia. 2010b. Eduskunnan kanslian toimintakertomus 2010. Viitattu 18.8.2011. <http://web.eduskunta.fi/dman/Document.php?documentId=bm13611132128695&cmd=download>

Eduskunnan kanslia. 2010c. Sisäisen tarkastuksen asiakirjat. Neuvotteleva virkamies Mauri Lehmusto antoi tulostetut asiakirjat tutkijalle vapaaseen käyttöön 15.6.2011.

Eduskunnan kanslia. 2008a. Eduskunnan kanslian toiminta- ja taloussuunnitelma 2010–2013, talousarvioesitys 2010 ja taloussuunnitelma 2009.

Eduskunnan kanslia. 2008b. Eduskunnan kanslian toimintakertomus 2008. Viitattu 1.10.2010. <http://web.eduskunta.fi/dman/Document.php?documentId=ea14809143006885&cmd=download>

Eduskunnan kanslia. 2008c. Eduskunnan kanslian yksiköiden johtajahaastatteluissa esiin tulleita näkemyksiä ja ehdotuksia. Sisäisen tarkastuksen laatima liite 16.5.2008.

Eduskunnan kanslia. 1987. Eduskunnan kanslian ohjesääntö 1987/320. Tulostettu 1.4.2011. <http://web.eduskunta.fi/dman/Document.php?documentId=zy17006142638225&cmd=download>

Eduskunnan kanslian hallintotoimisto. 2011. Suni, Marja. 2011. Pyytämäsi tiedot. anna.scherf@eduskunta.fi. Tulostettu 5.8.2011.

Eduskunnan kanslian hallintotoimisto. 2010. Laitinen, Hannu. 2010. VS: Strategia -asiakirjat. anna.scherf@eduskunta.fi. Tulostettu 12.10.2010.

Eduskunnan kanslian ohjesääntö. Tulostettu 3.12.2010.
<http://www.finlex.fi/fi/laki/alkup/1987/19870320>

Eduskunnan kiinteistötoimisto. 2011a. Eduskunnan intranet. Viitattu 9.8.2011.

Eduskunnan kiinteistötoimisto. 2011b. Eduskunnan intranet. Lupa kuvan käyttöön saatu turvallisuusyksiköstä 9.8.2011.

Eduskunnan työjärjestys. 17.12.1999/40 v. 2000. Tulostettu 1.7.2011.
<http://www.finlex.fi/fi/laki/ajantasa/2000/20000040>

Eduskunta. 2011. Eduskunnan internetsivusto. Viitattu 20.6.2011 ja 9.8.2011.
<http://www.eduskunta.fi>

ESDA. 2010. European Security and Defence Assembly - Assembly of Western European Union. Press Release No. 39/2010. Tulostettu 1.6.2011. http://www.eurodefense.nl/wp-content/uploads/2010/10/2010-09-29-AESD-ESDA-Press-39_2010_Eng.pdf

Eskola, J. & Suoranta, J. 2000. Johdatus laadulliseen tutkimukseen. 4. painos. Tampere: Osuuskunta Vastapaino.

EUISS. 2010. Global Governance 2025: At a Critical Juncture. Pariisi: EU Institute for Security Studies. Tulostettu 10.9.2011.
http://www.iss.europa.eu/uploads/media/Global__Governance_2025.pdf

EVA. 2010. Työelämän kulttuurivallankumous. EVA:n arvo- ja asennetutkimus 2010. Taloustieto. Tulostettu 10.1.2011.
http://www.eva.fi/wp-content/uploads/2010/06/tyoelaman_kulttuurivallankumous1.pdf

Eyeline. 2011. SWOT Analysis and C2S. Viitattu 27.7.2011.
<http://eyeline.mobi/blog/mobile-marketing-swot-analysis-and-c2s/>

Heinonen, S. 2008. Riskikäsitteen moniulotteisuus tulevaisuudentutkimuksessa. Futura -lehti 3/2008. Helsinki: Tulevaisuuden tutkimuksen seura ry.

Herrainsilta, J. 2006. Riskienhallinta valtionhallinnossa ja valtiokonttorin riskienhallintametselmän käyttöönotto. Tampereen yliopisto. Oikeustieteiden laitos. Pro gradu-tutkielma. Tulostettu 20.10.2010. <http://www.valtiokonttori.fi/Public/default.aspx?nodeid=19619>

Hirsjärvi, S., Remes, P. & Sajavaara P. 2010. Tutki ja kirjoita. 15.–16. painos. Helsinki: Kustannusosakeyhtiö Tammi.

Hopkin, P. 2010. Fundamentals of Risk Management – understanding, evaluating and implementing effective risk management. Verkkojulkaisu. Tulostettu 5.10.2011.
<http://lib.myilibrary.com.nelli.laurea.fi/>

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2010. Johda riskejä - käytännön opas yrityksen riskienhallintaan. Helsinki: Kustannusosakeyhtiö Tammi.

Isoaho, T. 2011. Poliittisten luottamushenkilöiden turvallisuus. Laurea-ammattikorkeakoulu. Turvallisuusosaamisen koulutusohjelma. YAMK opinnäytetyö. Tulostettu 1.8.2011.
<http://urn.fi/URN:NBN:fi:amk-201105208970>

Juvonen, M., Korhonen, H., Ojala, V., M., Salonen, T., Vuori, H. 2005. Yrityksen riskienhallinta. Helsinki: Suomen vakuutusalan koulutus ja kustannus.

- Kaivo-oja, J. 2011. Näkökulmia tietoyhteiskunnan ja viestinnän tulevaisuuteen. Blogi-kirjoitus Kansallisen ennakointiverkoston internet-sivustolla 8.8.2011. Viitattu 10.9.2011. <http://www.foresight.fi/2011/08/08/nakokulmia-tietoyhteiskunnan-ja-viestinnan-tulevaisuuteen/>
- Kamensky, M. 2008. Strateginen johtaminen – Menestyksen timantti. Hämeenlinna: Talentum Media.
- Kamensky, M. 2000. Strateginen johtaminen. 7. tarkistettu painos. Jyväskylä: Talentum Media.
- Kerko, P. 2001. Turvallisuusjohtaminen. Porvoo: PS-kustannus.
- Koivu, E., Ranta-aho, M. & Vuoti, H. 2010. Väärinkäytösriskit hallintaan. Tallinna: Tallinna Raamaturükikoda.
- KRP. 2011. Katsaus korruptiorikollisuuteen. Keskusrikospoliisi. Tulostettu 8.9.2011. [http://www.poliisi.fi/poliisi/krp/home.nsf/files/Katsaus%20korruptiorikollisuuteen%202011/\\$file/Katsaus%20korruptiorikollisuuteen%202011.pdf](http://www.poliisi.fi/poliisi/krp/home.nsf/files/Katsaus%20korruptiorikollisuuteen%202011/$file/Katsaus%20korruptiorikollisuuteen%202011.pdf)
- KRP. 2009. Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva – Syksy 2009. Keskusrikospoliisi. Tulostettu 7.9.2011. [http://www.intermin.fi/intermin/hankkeet/turva/home.nsf/files/Syksy_2009_yrityksiin_kohdistuvan_rikollisuuden_tilannekuva/\\$file/Syksy_2009_yrityksiin_kohdistuvan_rikollisuuden_tilannekuva.20091007%5B1%5D.pdf](http://www.intermin.fi/intermin/hankkeet/turva/home.nsf/files/Syksy_2009_yrityksiin_kohdistuvan_rikollisuuden_tilannekuva/$file/Syksy_2009_yrityksiin_kohdistuvan_rikollisuuden_tilannekuva.20091007%5B1%5D.pdf)
- Kuusela, H. & Ollikainen R. (toim.) 2005. Riskit ja riskienhallinta. Tampere: Tampereen University Press.
- Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. VTT Publications 632.
- Laurea-ammattikorkeakoulu. 2008. Ylemmän ammattikorkeakoulun opinnäytetyöohje. Tulostettu 11.6.2011. <https://intra.laurea.fi>
- Lauttamus, S. 2010. Henkilöturvallisuusopas valtionhallinnon käyttöön. Laurea-ammattikorkeakoulu. Turvallisuusalan koulutusohjelma. AMK opinnäytetyö. Tulostettu 1.8.2011. <http://urn.fi/URN:NBN:fi:amk-2010111814688>
- Lecklin, O. 2002. Laatu yrityksen menestystekijänä. Kauppakamarin Enterprise Adviser -kirjasarjan nro 2. Jyväskylä: Gummerus Kirjapaino.
- Mannermaa, M. 2006. Demokratia tulevaisuuden myllerryksessä. Eduskunnan tulevaisuusvaliokunnan julkaisuja 1/2007. Tulostettu 26.9.2011. [http://www.eduskunta.fi/triphome/bin/thw.cgi/trip?\\${APPL}=erekj&\\${BASE}=erekj&\\${THWIDS}=0.24/1317044424_163246&\\${TRIPPIFE}=PDF.pdf](http://www.eduskunta.fi/triphome/bin/thw.cgi/trip?${APPL}=erekj&${BASE}=erekj&${THWIDS}=0.24/1317044424_163246&${TRIPPIFE}=PDF.pdf)
- Mannermaa, M. 2004. Heikoista signaaleista vahva tulevaisuus. 2. painos. Porvoo: WS Bookwell.
- Meristö, T. 2011. Opinnäytetyön ohjaus 26.5.2011. Leppävaara: Laurea-ammattikorkeakoulu.
- Meristö, T. 1991. Skenaariotyöskentely yrityksen johtamisessa. Helsinki: Tulevaisuuden tutkimuksen seura.
- Meristö, T & Kivelä, S. 2011. 00715 Tulevaisuuden haltuunoton menetelmät. Kurssimateriaali. Laurea-ammattikorkeakoulu.
- Meristö, T. & Tammi, M. 2003. Tulevaisuuden haasteet. Näkökulmia Suomen teknologiapolitiikan tueksi. CoFi Report No 1/2003. Turku: Åbo Akademi Univeristy.

- Miettinen, J., E. 2002. Yritysturvallisuuden käsikirja. Jyväskylä: Talentum Media.
- Mäkinen, K. 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita Prima.
- NexusSkenarix. 2011. Kotisivut. Viitattu 26.9.2011.
http://nexuskenarix.internetix.fi/fi/materiaalit/metodi/02_skenaarion_kasitteesta?C:D=534678&selres=534678
- Niemi, H. 2010. Managing in the Golden Cage. An Ethnographic Study of Work, Management and Gender in Parliamentary Administration. Publications of the Hanken School of Economics Nr 218. Helsinki: Hanken School of Economics. Tulostettu 3.5.2011.
<https://helda.helsinki.fi/handle/10227/724>
- OECD. 2003. Emerging Risks in the 21st Century. An OECD International Futures Project. Tulostettu 3.5.2011. <http://www.oecd.org/dataoecd/23/56/19134071.pdf>
- Ojasalo, J. 2010. Strategiaprosessi ja strategisen johtamisen perustekijöitä. Laurea-ammattikorkeakoulu. Laurea Leppävaara. Espoo. Luentomateriaali 11.9.2010.
- Ojasalo, K., Moilanen, T. & Ritalahti, J. 2010. Kehittämistyön menetelmät – Uudenlaista osaamista liiketoimintaan. 1.–2. painos. Helsinki: WSOYpro.
- Otala, L. 2002. Oppimisen etu – kilpailukykyä muutoksessa. 4. uudistettu painos. Porvoo: WS Bookwell.
- PNE 1/2010 vp. Puhemiesneuvoston ehdotus laiksi eduskunnan virkamiehistä annetun lain 10 ja 71 §:n, eduskunnan työjärjestyksen 73 §:n ja eduskunnan kanslian ohjesäännön muuttamisesta.
- Puolustusministeriö. 2011a. Puolustushallinnon turvallisuus. Puolustusministeriön strateginen suunnitelma 2030 – osastrategia. Tulostettu 30.8.2011.
<http://www.defmin.fi/files/1833/turvallisuusstrategia.pdf>
- Puolustusministeriö. 2011b. Puolustushallinnon yhdyskunta- ja ympäristöpolitiikka. Puolustusministeriön strateginen suunnitelma 2030 – osastrategia. Tulostettu 30.8.2011.
http://www.defmin.fi/files/1837/yhdyskunta_ja_ymparistopolitiikka.pdf
- Puolustusministeriö. 2007. Kansainvälisen järjestelmän toimijoiden ennakkointia vuoteen 2030. Pohjoismaat ja Baltia. Tulostettu 2.3.2011. <http://www.defmin.fi/index.phtml?s=394>
- Puolustusministeriö. 2006. Turvallisesti tulevaisuuteen – Puolustusministeriön strategia 2025. Puolustusministeriö.
- Saarinen, V. 2010. Turvallisuustietoisuus julkisessa organisaatiossa : tapaus Taloushallintopalvelu. Laurea-ammattikorkeakoulu. Turvallisuusalan koulutusohjelma. AMK opinnäytetyö. Tulostettu 1.8.2011. <http://urn.fi/URN:NBN:fi-fe20071153>
- Santalainen, T. & Huttunen, P. 1993. Strateginen johtaminen julkisessa hallinnossa. Jyväskylä: Valtionhallinnon kehittämiskeskus ja Weilin+Göös.
- Schroderus, J-P. 2008. Eduskunnan turvallisuustoiminnan kehittäminen 2003–2008. Dipoli-raportit B. Master of Security lopputyö. Espoo: TKK. Koulutuskeskus Dipoli.
- Schwartz, P. 1991. The Art of the Long View – Planning for the Future in an Uncertain World. New York: Bantam Doubleday Dell Publishing Group.
- Seeck, H. (toim.) 2009. Kriisit ja työyhteisöt – kriisijohtaminen työyhteisöjen tukena. Tampere: Työterveyslaitos.

Seeck, H., Lavento, H. & Hakala, S. 2008. Kriisijohtaminen ja viestintä. Tapaus Nokian vesikriisi. Helsinki: Kuntaliitto.

Sisäasiainministeriö 2010. Kansallinen terrorismintorjunnan strategia. Sisäasiainministeriön julkaisut 21/2010. Tulostettu 1.5.2011.
[http://www.intermin.fi/intermin/biblio.nsf/9F08FC352F481EE3C225773800416669/\\$file/212010.pdf](http://www.intermin.fi/intermin/biblio.nsf/9F08FC352F481EE3C225773800416669/$file/212010.pdf)

Suominen, A. 2003. Riskienhallinta. 3. uudistettu painos. Helsinki: WSOY.

SUPO. 2009. Suojelupoliisin päällikön katsaus 2009. Tulostettu 16.3.2011. www.poliisi.fi/supo

Tammi, P. 2007. Ulkoasiainhallinnon henkilöstön turvallisuuskoulutuksen tarve. Laurea-ammattikorkeakoulu. Turvallisuusalan koulutusohjelma. AMK opinnäytetyö. Tulostettu 1.8.2010. <http://urn.fi/URN:NBN:fi-fe20061455>

Tekes. 2009. Megatrendit ja me. Tekesin katsaus 255/2009. Tekes.

Tulevaisuuden tutkimuskeskus. 2011. Ehdotus viidestä teemasta ja kymmenestä kipupisteestä. Turun yliopisto. Luettu 15.5.2011 Eduskunnan sähköposti.

Tulevaisuusvaliokunta. 2007. Monen monta demokratiaa. Eduskunnan tulevaisuusvaliokunnan julkaisu 3/2007. Tulostettu 26.9.2011.
[http://www.eduskunta.fi/triphome/bin/thw.cgi/trip?\\${APPL}=erekj&\\${BASE}=erekj&\\${THWIDS}=0.48/1317044148_189059&\\${TRIPPIFE}=PDF.pdf](http://www.eduskunta.fi/triphome/bin/thw.cgi/trip?${APPL}=erekj&${BASE}=erekj&${THWIDS}=0.48/1317044148_189059&${TRIPPIFE}=PDF.pdf)

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. 1.–3. painos. Jyväskylä: Kustannusosakeyhtiö Tammi.

Ulkoasiainministeriö. 2011. "In search of a strategy for foreign and security policies of the European Union". The Villa Lante Reflection Seminar. Eduskunnalle lähetetty kokousraportti. Kesäkuu 2011.

Ulkoasiainministeriö. 2006. Ulkoministeriön tulevaisuuskatsaus 2006. Ulkoasiainministeriö: Valtiosihteerin yksikkö.

Valtioneuvosto. 2001. Periaatepäätös valtion henkilöstöpolitiikan linjasta 30.8.2001. Helsinki: Kirjapaino Snellman. Tulostettu 25.10.2010. www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/

Valtioneuvoston asetus 423/2005. Viitattu 1.6.2011.
<http://www.finlex.fi/fi/laki/alkup/2005/20050423>

Valtioneuvoston kanslia. 2010. Valtioneuvoston kanslian tulevaisuuskatsaus. Valtioneuvoston kanslian julkaisusarja 19/2010.

Valtioneuvoston kanslia. 2009. Ikääntymisraportti. Valtioneuvoston kanslian julkaisusarja 1/2009.

Valtioneuvoston kanslia. 2007. Yhdessä ja erikseen - Maailma ja Suomi 2010-luvulla. Toimintaympäristökuvaus ministeriöiden tulevaisuuskatsausten taustaksi. Valtioneuvoston kanslian julkaisusarja 33/2009. Tulostettu 10.9.2011. <http://www.vnk.fi/julkaisukansio/2009/j33-yhdessa-ja-erikseen-j03-together/pdf/fi.pdf>

Valtiovarainministeriö. 2005a. Tulosoikeuden käsikirja. Hallinnon kehittämisosasto. Julkaisusarja 2/2005. Helsinki: Edita Prima. Tulostettu 25.10.2010.
www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/

Valtiovarainministeriö. 2005b. Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta. Valtionhallinnon hyvä käytäntö ja sen toteutumisen arviointi. Valtiovarain controller -toiminto. Tulostettu 25.10.2010. www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/

Valtiovarainministeriö. 2004. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 14.12.2004. Tulostettu 25.10.2010. www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/

Vapaavuori, M. (toim.) 1993. Miten tutkimme tulevaisuutta? Helsinki: Painatuskeskus.

Yritysturvallisuus EK. 2011. Yritysturvallisuus EK:n internet-sivusto. Viitattu 11.8.2011. <http://ek2.ek.fi/ytnk08/fi/yritysturvallisuus.php>

Yritysturvallisuus EK. 2009. Yritysturvallisuuden perusteet -DVD. Elinkeinoelämän keskusliitto.

YTS 2010. Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010. Tulostettu 1.9.2011. <http://www.yett.fi/>

Kuvat

Kuva 1: Eduskuntaan kuuluvat rakennukset ja henkilöstön työskentelytilat (A–F) pois lukien Antinkatu (Eduskunnan kiinteistötoimisto 2011b)	10
--	----

Kuviot

Kuvio 1: Eduskunnan kanslian organisaatorakenne (Eduskunta 2011).....	8
Kuvio 2: Riskienhallintaprosessi Ilmonen ym. mukailten (2010, 93)	22
Kuvio 3: Riskienhallinnan kypsyyssasteet Ilmonen ym. mukailten (2010, 94)	26
Kuvio 4: Riskienarvioinnin perusmalli Ilmonen ym. mukailten (2010, 99).....	28
Kuvio 5: Riskienhallintamenetelmät Ilmonen ym. mukailten (2010, 124).....	28
Kuvio 6: Yritysturvallisuuden osa-alueet Yritysturvallisuus EK:ta mukailten (2011) .	33
Kuvio 7: Kehittämistyön teoreettinen viitekehys ja tutkimustyytit	44
Kuvio 8: Kehittämistyön prosessi käytännössä Ojasalo ym. mukailten (2010, 23) ..	47
Kuvio 9: Skenaariotyöskentely ja strateginen suunnitteluprosessi (Meristö 2011, 38)	56
Kuvio 10: Skenaariotyöskentelyn vaiheet Meristöä ja Tammea mukailten (2003, 12)	57
Kuvio 11: Aineiston analysointiprosessi Ojasalo ym. mukailten (2010, 223–224)	58
Kuvio 12: Eduskunnan kanslian yksikköjen kannalta tärkeimmät organisaatioturvallisuuden osa-alueet (virkamiesjohdon kysely 2011)	67
Kuvio 13: Eduskunnan kansliassa eniten kehittämistä vaativat organisaatioturvallisuuden osa-alueet (virkamiesjohdon kysely 2011).....	68
Kuvio 14: Eduskunnan kanslian SWOT-analyysi Eyelinea mukailten (2011)	71
Kuvio 15: Eduskunnan kanslian PESTE-analyysi	85
Kuvio 16: Skenaarioputket Meristöä & Tammea mukailten (2003)	88
Kuvio 17: Skenaario 1 – Kriittinen kotipesä.....	89
Kuvio 18: Skenaario 2 – Teknokraattien anarkia.....	91
Kuvio 19: Skenaario 3 – Viralliset valtarakenteet maalitauluina.....	92
Kuvio 20: Skenaario 4 – Yhteiskuntarauha järkkyy	93
Kuvio 21: Organisaation turvallisuustoiminnan suorituskyvyn riittävyys	105

Taulukot

Taulukko 1: Riskilajit Ilmonen, Kallio, Koskinen & Rajamäki mukailleen (2010, 71) ..	14
Taulukko 2: Organisaatioturvallisuuden osa-alueet eri riskilajeihin jaoteltuna	15
Taulukko 3: Riskienhallinta kattaa organisaation kaikki riskit (Ilmonen ym. 2010, 71)21	
Taulukko 4: Ennusteen ja skenaarion ero Schoemakeria mukailleen (Meristö 1991, 42)57	
Taulukko 5: Tutkimusstrategiset valinnat ja kehittämistyön sisältövaatimukset	60
Taulukko 6: Arvovertailu (Eduskunnan kanslia 2011f, Valtioneuvosto 2001)	65
Taulukko 7: Yksilön osaamisen osa-alueet Otalaa mukailleen (2002, 104–106)	72
Taulukko 8: Osaamisen osa-alueet ja riskienhallinnan kehittäminen.....	73
Taulukko 9: Organisaatioturvallisuuden painopisteet eduskunnan kansliassa.....	75
Taulukko 10: Esimerkkejä eduskunnan kanslian riskientunnistamistyön pohjaksi....	77
Taulukko 11: Tulevaisuustiedon tyypittely Meristöä ja Kivelää mukailleen (2011)	77
Taulukko 12: Valtionhallinnon turvallisuusympäristöön vaikuttava tulevaisuustieto	83
Taulukko 13: Eduskunnan kanslian turvallisuusympäristön suodattimet ja ajurit	87
Taulukko 14: Tunnistetut ennakointiteemat skenaariotyöskentelyn taustalla	87
Taulukko 15: Riskienhallinnan yleisyys eurooppalaisissa parlamenteissa	95
Taulukko 16: Riskienhallinnan käytännön toteutus eurooppalaisissa parlamenteissa	99
Taulukko 17: Eduskunnan kanslian turvallisuustoiminta suhteessa skenaarioihin ...	105

Liitteet

Liite 1. Virkamiesjohdon kysely organisaatioturvallisuuden osa-alueista	135
Liite 2: Eduskunnan kanslian toimintaan vaikuttavat valtionhallinnon turvallisuusympäristöä koskevaan tulevaisuustietoon perustuvat turvallisuusriskit	138
Liite 3. ECPDR -verkoston englanninkielinen esittely (sanatarkka lainaus).....	140
Liite 4. ECPRD:n kautta eurooppalaisiin parlamentteihin lähetetty kysely.....	141
Liite 5: Mainettaan parempi eduskunta?	143
Liite 6: Turvallisuusympäristöä koskevaa uutisointia 2009–2011	144
Liite 7: Riskienhallinnan sijoittuminen eduskunnan kanslian organisaatioon	145
Liite 8: Eduskunnan kanslian turvallisuusympäristön lausunto.....	146

Liite 1. Virkamiesjohdon kysely organisaatioturvallisuuden osa-alueista

EDUSKUNNAN KANSLIAN KRIITTISET ORGANISAATIOTURVALLISUUDEN OSA-ALUEET

Virkamiesjohdon kysely 29.9.2011

Kyselyn tausta ja tarkoitus

Suoritan töiden ohessa turvallisuusosaamisen ylempää ammattikorkeakoulututkintoa. Opin-
näytetyössäni esitän kehittämisehdotuksia eduskunnan kanslian turvallisuustoimintaan tavoit-
teenani rohkaista kokonaisvaltaisen turvallisuustoiminnan ja riskienhallinnan tarkoituksenmu-
kaiseen soveltamiseen. Tämän kyselyn avulla pyrin kartoittamaan organisaatioturvallisuuden
eri osa-alueiden painottumista sekä niiden toivottuja kehittämisen painopisteitä virkamies-
johdon näkökulmasta.

Kyselyn sisältö

Kyselyyn osallistuminen vie aikaa vain muutaman minuutin. Organisaatioturvallisuuden eri
osa-alueet on esitelty liitteenä olevassa taulukossa Yritysturvallisuus EK:n yleisesti suositte-
lemaa jakoa mukailten. Pyydän sinua tutustumaan taulukon sisältöön ja vastaamaan sen poh-
jalta kahteen kysymykseen

1. mitkä ovat kolme merkittävintä organisaatioturvallisuuden osa-aluetta oman yksikkösi
tai vastualueesi näkökulmasta?
2. mitkä ovat mielestäsi kolme eniten kehittämistä kaipaavaa organisaatioturvallisuuden
osa-aluetta koko eduskunnan kanslian näkökulmasta?

Vastauksesi on tärkeä

Vastaamalla kyselyyn voit vaikuttaa oman vastualueesi tarpeiden huomiointiin eduskunnan
kanslian turvallisuustoiminnan kehittämisessä. Vastaukseksi riittää pelkkä osa-alueiden ni-
meäminen – perustelut ja vapaamuotoinen kommentointi ovat vapaaehtoisia. Aineistoa käsi-
tellään ja siihen viitataan anonyymisti. Toivon, että ehtisit osallistua kyselyyn ja vastata
mahdollisimman pian minulle sähköpostilla osoitteeseen anna.scherf@eduskunta.fi. Vastaan
mielelläni myös opinnäytetyöhön tai kyselyyn liittyviin kysymyksiisi.

Parhain terveisin,

Anna Scherf, ulkoasiainvaliokunnan osastosihteeri

	Organisaatio- turvallisuuden osa-alue	Organisaatioturvallisuuden osa-alueen kuvaus tai esimerkki (Yritysturvallisuus EK, 2009)
1.	Henkilöturvallisuus	<ul style="list-style-type: none"> - henkilöstön, vierailijoiden ja asiakkaiden suojaaminen rikoksia vastaan - organisaation suojaaminen henkilöiden aiheuttamia uhkia vastaan - turvallisuusselvitykset, salassapitosopimukset, varamies-, tavoitettavuus- ja hälytysjärjestelmät, henkösuojaus, kodin ja perheen turvallisuus ja matkustusturvallisuus
2.	Kiinteistö- ja toimitilaturvallisuus	<ul style="list-style-type: none"> - toimipaikkojen ja -tilojen riskiarvioon perustuva kustannustehokas suojaaminen - turvataan luvallinen asiointi ja häiriötön työskentely, estetään tiedon ja materiaalin anastaminen - tekniset turvajärjestelyt, kulunvalvonta ja vartiointi
3.	Pelastustoiminta	<ul style="list-style-type: none"> - ihmisen, omaisuuden ja ympäristön suojaamista ja pelastamista (ml. väestönsuojelu) - vahinkojen rajoittamista - onnettomuuksien ja uhkatilanteiden seurausten lieventämistä - pelastussuunnitelma, toimintaohjeet - koulutus- ja valistustyö (ml. kansalaistaidot)
4.	Rikosturvallisuus	<ul style="list-style-type: none"> - toimintaa, henkilöstöön ja omaisuuteen kohdistuvien rikosten ennaltaehkäisy ja niiltä suojautuminen - omaisuusrikollisuus, talousrikollisuus, ulkomaantoiminoissa kohdattava rikollisuus - rikostorjuntasuunnitelma, toimintaohjeet
5.	Tietoturvallisuus	<ul style="list-style-type: none"> - fyysiset tallenteet, paperi, cd-levy, muistikku, piirustukset, nauhoitteet, puhuttu tieto, ihmisen muisti - kolme peruselementtiä tiedon käytettävyys, eheys ja luotettavuus - ohjataan tiedon käsittelyä, säilyttämistä, hävittämistä ja välittämistä - tietoturvaluokitukset - tekninen tietoturvallisuus - turvallisuustietoisuus, turvallisuuskulttuuri
6.	Tuotannon ja toiminnan turvallisuus	<ul style="list-style-type: none"> - häiriötön tuotanto ja toiminta - nopea toipuminen häiriöstä - turvalliset tuotteet ja palvelut - varmistetaan organisaation jokapäiväiset toiminnot - verkostoitumisen riskit ja häiriöalttius - tuotevastuu
7.	Työturvallisuus	<ul style="list-style-type: none"> - lakisääteinen työsuojelutoiminta - organisaation omaehtoinen toiminta - työperäisten vaara- ja haittatekijöiden syntymisen estäminen ja poistaminen - työsuojelun toimenpideohjelma, toimintaohjeet - työsuojeluvastuut - fyysinen ja henkinen hyvinvointi
8.	Ulkomaantoimintojen turvallisuus	<ul style="list-style-type: none"> - ulkomailla olevien henkilöstön ja toimintojen suojaaminen - vieraan ympäristön poikkeava lainsäädäntö, kulttuuri ja uskonto - riskien toteutumisen todennäköisyyden vähentäminen ja seuraamusten lieventäminen

9.	Valmiussuunnittelu	<ul style="list-style-type: none"> - kansallisen huoltovarmuuden turvaaminen kaikissa olosuhteissa - toiminnan jatkuvuussuunnittelu - tietoyhteiskunta, kuljetuslogistiikka, elintarvikehuolto, energiahuolto, terveydenhuolto, rahoitushuolto, kriittinen perusteellisuus - lakisäateistä ja omaehtoista
10.	Ympäristöturvallisuus	<ul style="list-style-type: none"> - ekologisesti kestävä toiminta, kestävä kehitys - henkilöstön tietoisuus ympäristöasioista - ohjeistus ja ennen muuta ohjeistuksen toteuttaminen työssä - ympäristöjärjestelmät, auditoinnit, ympäristönsuojelun tason arviointi, ympäristömerkinnät, elinkaariarviointi, kasvihuonepäästöjen hallinta, ympäristöviestintä, tuotesuunnittelun ympäristönäkökohdat

Jakelu

pääsihteeri	Seppo Tiitinen
hallintojohtaja	Pertti Rauhio
apulaispääsihteeri	Timo Tuovinen
lainsäädäntöjohtaja	Keijo Koivukangas
kv-asiain yksikön johtaja	Katriina Kuusinen
turvallisuusjohtaja	Jukka Savola
henkilöstöpäällikkö	Hannu Laitinen
tiedotuspäällikkö	Marjo Timonen
toimistopäällikkö	Martti K. Korhonen
toimistopäällikkö	Ari Apilo
toimistopäällikkö	Pertti J. Rosila
toimistopäällikkö	Ilona Nokela
tietohallintopäällikkö	Juha Suomalainen
tietopalvelupäällikkö	Antti Rautava
kirjastonjohtaja	Sari Pajula
vastaava työterveyslääkäri	Anita Pienimäki
suunnittelija	Sakari Keckman
turvallisuusesimies	Lasse Jartti
siivoustyön esimiehet	Riitta Huikari-Hyvönen, Minna Majuri
jaostopäällikkö	Simo Valkeajärvi

Liite 2: Eduskunnan kanslian toimintaan vaikuttavat valtionhallinnon turvallisuusympäristöä koskevaan tulevaisuustietoon perustuvat turvallisuusriskit

Turvallisuuden osa-alue	Mahdollisia tulevaisuustiedon käytännön ilmenemismuotoja
Henkilöturvallisuus ja rikosturvallisuus	<ul style="list-style-type: none"> • väkivaltaisuuden yleinen lisääntyminen • väkivallan kohdistuminen kansanedustajiin • väkivallan kohdistuminen virkamiehiin • eduskunnan sisäiset väkivallanteot • ulkopuolisen tiedustelun lisääntyminen ja koveneminen • maineriskien lisääntyminen ja koveneminen • turvallisuustoiminnan painottuminen teknisiin osa-alueisiin • eduskunnassa käsiteltävien asioiden merkityksen ja kiinnostavuuden lisääntyminen • terrori-iskun uhkien lisääntyminen (Helsinki/eduskunta) • terrori-iskun toteutuminen (Helsinki/eduskunta) • yleinen turvattomuudentunteen lisääntyminen
Tietoturvallisuus	<ul style="list-style-type: none"> • sähköiseen kokousmenettelyyn ja arkistointiin siirtyminen • Suomen "wikileaks" toteutuminen • tietomurron tai tietovuodon havaitseminen • turvallisuustoiminnan painottuminen teknisiin osa-alueisiin • eduskunnassa käsiteltävien asioiden merkityksen ja kiinnostavuuden lisääntyminen • korruption lisääntyminen ja/tai rakenteellistuminen • tietoturvaluokituksen laiminlyönti • turvallisuuskulttuurin luomisen laiminlyönti
Työturvallisuus ja ulkomaantoimintojen turvallisuus	<ul style="list-style-type: none"> • huonon henkilöstöhallinnon kärjistyminen • henkilöstön tyytymättömyyden kärjistyminen • eduskunnan sisäinen väkivallanteko • peruskorjaukseen liittyvä räjähdys/muu onnettomuus • riittämätön varautuminen eläköitymiseen • uusien työntekijöiden rekrytoinnin epäonnistuminen • maineriskien lisääntyminen ja koveneminen • matkustamiseen liittyvät riskit
Kiinteistö- ja toimitilaturvallisuus	<ul style="list-style-type: none"> • eduskunnan tilojen valtaus • täysistuntoon kohdistuva hyökkäys • eduskuntarakennusten vahingoittaminen • videovalvontalaitteiden väärinkäytön havaitseminen • kulkukorttien väärinkäytön havaitseminen • terrori-iskun uhka (Helsingissä/eduskunnassa) • terrori-iskun toteutuminen (Helsinki/eduskunta)
Tuotannon turvallisuus (jatkuvuussuunnittelu)	<ul style="list-style-type: none"> • toiminnan laatu heikkenee • virheistä ei opita syyttävän organisaatiokulttuurin vuoksi • toiminta keskeytyy • toiminnan häiriöstä toipuminen on hidasta

Pelastustoimi ja ympäristöturvallisuus	<ul style="list-style-type: none"> • tulipalo tai räjähdys (peruskorjaus) • rakenteiden sortuminen (peruskorjaus) • luonnonmullistus • kemiallinen tai biologinen hyökkäys • terrori-iskun uhkien lisääntyminen (Helsinki/eduskunta) • terrori-iskun toteutuminen (Helsinki/eduskunta)
Valmiussuunnittelu (jatkuvuussuunnittelu)	<ul style="list-style-type: none"> • kokonaisvaltaisen turvallisuustoiminnan puute eduskunnan kansliassa • eduskunnan kanslian johdon sitoutumattomuus turvallisuustoiminnan kehittämiseen • valmiussuunnitelmien käytännön harjoittelun puute • eduskunnan kanslian eri yksiköiden osaamisalueiden hyödyntämättömyys • valtionhallinnon organisaatioille esitetyt kansalliset laatu- ja suoritusvaatimukset (mm. VNK, Valtionkonttori, YTS) • valtionhallinnon organisaatioille esitetyt kansainväliset laatu- ja suorituskykyvaatimusten kiristyminen (mm. EU, OECD) • demokratian muutos • eduskunnan ydintehtävien muutos • eduskunnan ydintehtävien toteuttamistavan muutos • infrastruktuurin häiriöiden lisääntyminen • yhteiskunnan eriarvoistuminen ja väkivallan lisääntyminen • terrori-iskun uhkien lisääntyminen (Helsinki/eduskunta) • terrori-iskun toteutuminen (Helsinki/eduskunta) • turvallisuustoiminnan ulkoistaminen

Liite 3. ECPDR -verkoston englanninkielinen esittely (sanatarkka lainaus)

THE EUROPEAN CENTRE FOR PARLIAMENTARY RESEARCH AND DOCUMENTATION (ECPRD)

Background

Since it was first established at the request of the speakers of European Parliamentary Assemblies in June 1977, the European Centre for Parliamentary Research & Documentation (ECPRD) has been a useful tool for inter-parliamentary cooperation and information exchange. Comparative requests, seminars and surveys by individual parliaments on particular topics offer all those involved the chance to work together. The advent of the internet has made the Centre more accessible than ever.

The Centre's aims

The data generated by the Centre's members is extensive and specific information can be hard to track down. Bringing together the information, facilitating the exchange of ideas and making the retrieval of data and the circulation of studies easier is the Centre's role. The ECPRD acts as a channel for requests for information whenever one parliament would like to know more about practice and policy in other countries.

Structures

Three groups make up the ECPRD's governing structure:

- two co-directors, each of whom assisted by a co-secretary;
- the Conference of Correspondents;
- the Executive Committee.
- The co-directors, appointed by the Secretary-General of the European Parliament and of the Parliamentary Assembly of the Council of Europe, are responsible for organising all the Centre's activities.

The Secretary-General of each member parliament selects a senior official to be a representative at the annual Conference of Correspondents. Acting as a link between the Centre and their own parliament, these officials take part in determining the Centre's programme. The Executive Committee is made up of the two directors who are joined by five people elected from and by the Conference. Each year one (or two) is replaced. This brings a fresh approach without sacrificing continuity. Their job is to lay the ground work for the annual Conference of Correspondents and to keep up the impetus on the Centre's work.

Lähde: Euroopan parlamentin sisäinen internetsivusto.

Lupa tekstin julkaisemiseen saatu eduskunnan kanslian tietopalvelupäälliköltä 12.8.2011.

Liite 4. ECPRD:n kautta eurooppalaisiin parlamentteihin lähetetty kysely

RISK MANAGEMENT IN PARLIAMENTS

The Finnish Parliament intends to investigate the effect of risk management in the Finnish Parliament's strategic management. The purpose of this request is to produce comparative information on whether risk management is applied in other European Parliaments and how it is carried out in general.

In this connection we have used a broad definition of risk management (from Wikipedia 2011): "Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attacks from an adversary."

Our request is divided into two sections:

- Section A is targeted at those Parliaments that do not apply risk management in their organisation.
- Section B in turn is meant for those Parliaments that do apply risk management in their organisation. The desired persons to answer the questions are managers or specialists of security or risk management in your organisation.

We would appreciate your contributions to be submitted no later than Friday 24th of June 2011. Could you please send your replies to Antti Rautava, antti.rautava@eduskunta.fi

RISK MANAGEMENT IN THE EUROPEAN PARLIAMENTS 2011

Section A: "There is no risk management in our Parliament"

1. Has there ever been any discussion about risk management in your Parliament?
2. Is it a conscious decision not to apply risk management?
3. Why have you decided not to apply risk management?
4. Do you have other means to assess possible threats affecting your Parliament?
5. Is there any intention to apply risk management in the future?

Section B: "We do apply risk management in our Parliament"

1. How is risk management organised in practice?
(e.g. organisation level policies, number and know-how of staff, division of tasks...)
2. What are the threats you want to affect by applying risk management?
(e.g. security, safety, financial, environmental...)
3. Is your risk management based on some standard?
(If yes – which one? If no – why not?)
4. How does risk management concern your Parliaments personnel?
(e.g. level of responsibility and participation of the middle managers, participation of other officials...)
5. What is the yearly cycle of your Parliament's risk management like?
(e.g. in terms of planning, realisation, follow-up and assessment and reporting)
6. How is risk management utilised in your Parliament's strategic management?
(e.g. Is risk analysis, assessments or reports taken into account when making strategic decisions? Is risk assessment applied directly into the strategic plans themselves?)

Liite 5: Mainettaan parempi eduskunta?

- "Eduskunnan naiset seksuaalisen häirinnän uhreina - neljässä tapauksessa kymmenestä ahdistelija on kansanedustaja" (Iltalehti 24.1.2008)
- "Eduskunnan urheilukerhosta kavallettiin 135 000 euroa" (Iltalehti 19.2.2010)
- "Taas uusi skandaali – Eduskunta selvittää tieto- ja viestintäjohtajan ylityöilmoituksia" (Iltalehti 15.3.2010)
- "Eduskunnan mokaaja selville: Hän möläytti mikrofoniin" (Ilta-Sanomat 29.4.2011)
- "Kansanedustaja: Torkkupeitto tuli pyytämättä ja yllättäen" (Iltalehti 10.11.2010)
- "Kriisikokous kiusaamisesta – Kiusaamista, seksismiä ja syrjäyttämistä, väitöskirja paljastaa eduskunnan synkät kulissit" (Iltalehti 22.11.2010)
- "Taas epäselvyyksiä eduskunnassa – Tiitinen teki esitutkintapyynnön poliisille" (Iltalehti 26.11.2010)
- "Rötöspesäke – liki kymmenen prosenttia kansanedustajista on joko tuomittu rikoksesta tai parhaillaan rikosepäilyjen kohteena" (Iltalehti 24.1.2011)

2 VASTAUSTA | 88 LUKUKERTAA

 Miksi eduskunnassa on menossa aina joku kohu?

 apa66 3.4.2010 23:50

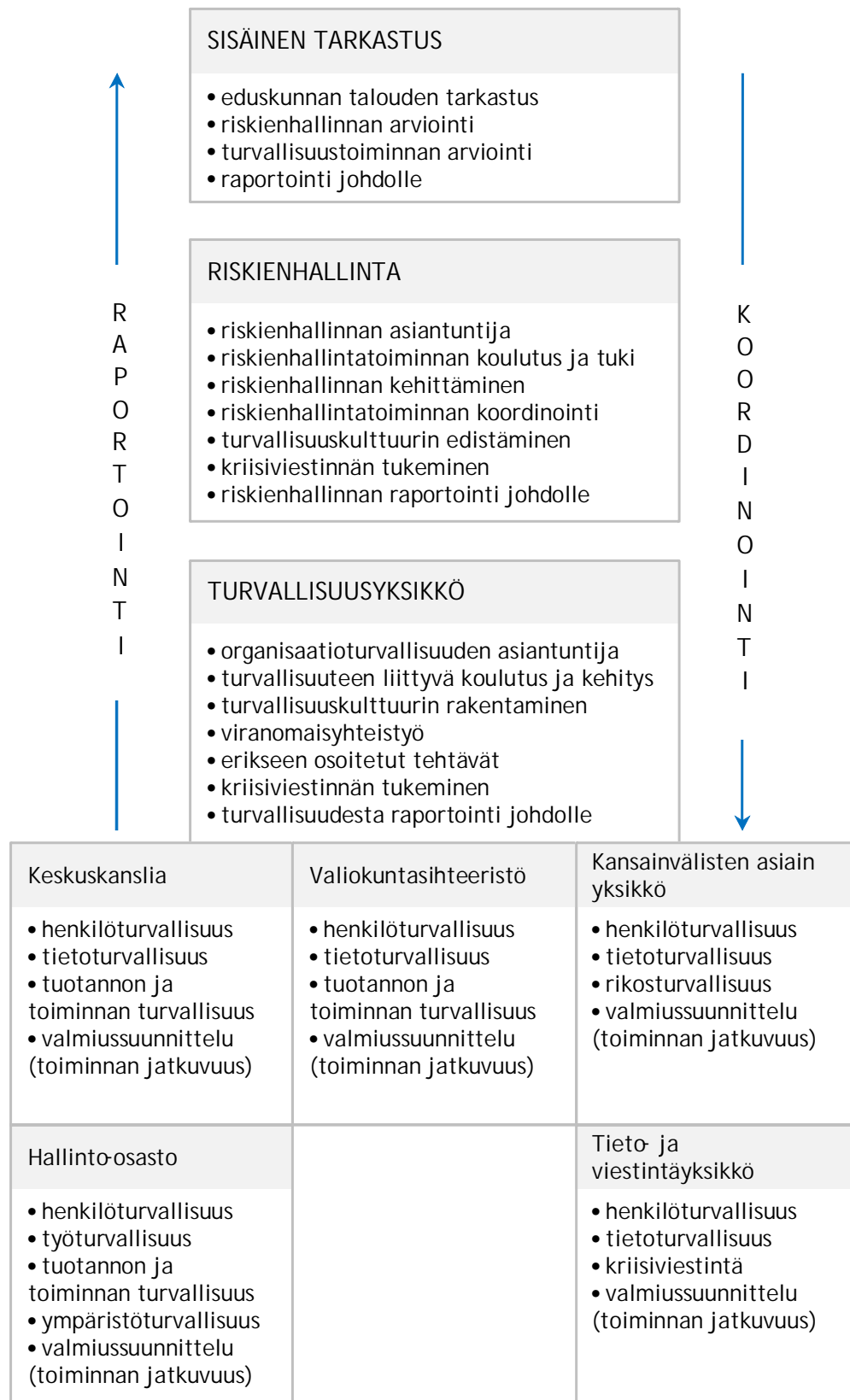
Mitä tämä on taas kuin loputonta sekoilua, aina joku kohu - tämä Marja Tiura -juttu nyt viimeisin. Mutta näitähän on riittänyt: Matti Vanhanen ja lautakasa, tekstiviestit, ym., yleinen vaalirahakohu, Ilkka Kanerva ja tekstiviestit, Rosa Meriläinen ja huumekohu, Anneli Jäätteenmäki ja Irak-sotkut, Sonera-kohu, nämä nyt vain tässä viimeisen 10 vuoden ajalta ja vain päällimmäisiä! Äh, suuri osa siis näistä on edustajien itsensä aiheuttamia. Miten tällaista peliä voidaan jatkuvasti sietää? Emmehän me ole kansanedustajia valinneet siksi, että he keskenään vain asioita sekoittaisivat ja sekoilisivat? Olen monta kertaa miettinyt mitä monia tärkeitä asioita menee kokonaan sivuitse, tai jää kokonaan käsittelemättä ja hoitamatta, kun on aina vain joku tosi typerä kohu meneillään.

 VASTAA  Jaa viesti  +1  0  Suosittele  Ilmoita asiaton viesti

Liite 6: Turvallisuusympäristöä koskevaa uutisointia 2009–2011

- "Varo, kopiokone vakoilee sinua – kopiokoneenkorjaajasta tulisi helposti vähintään yhtä kova tietovarvas kuin pahimmastakaan hakkerista" (Taloussanomat 14.12.2009)
- "Suuri osa maailman laittomasta tavarasta kulkee kohti pohjoista – Euroopan viisi merkittävää järjestäytyneen rikollisuuden kokouspaikkaa" (Helsingin Sanomat 1.10.2010)
- "Hyvästi lintukoto? – Eduskunnan turvallisuusjohtaja tyrmää kritiikin valtionhallinnon turvajärjestelyjä kohtaan" (Ilta-Sanomat 11.11.2010)
- "Ammattirikolliset yrittävät soluttautua turvafirmoihin – rikollisjengeihin kuuluvia on jo onnistunut pääsemään vartijoiksi" (Iltalehti 8.12.2010)
- "Laki eduskunnan turvatoimista ei salli ampuma-aseita turvahenkilöstölle. Ruotsissa aseistettuja suojeluvartioita on jo pitkään ollut kaikissa valtionhallinnon keskeisissä rakennuksissa" (Ilta-lehti 10.11.2010)
- "Pommimies räjäytti itsensä Tukholman keskustassa" (Helsingin Sanomat 11.12.2010)
- "Tappouhkauksia – Suomalaiset poliitikot ovat saaneet kokea kansan vihan" (Iltalehti 12.1.2011)
- "Eduskunnan turvajärjestelyt ovat lentokenttätasoa" (Iltalehti 13.1.2011)
- "Työpahoinvointi maksaa kymmeniä miljardeja" (Kauppalehti 2.3.2011)
- "Kriisinhallinnan asiantuntija kehuu Japanin pääministeriö hätätilatiedottamisesta. Suomen ylin johto ei sen sijaan saa kriisinhallintaan erikoistuneelta Timo Hellenbergiltä kiitosta" (Iltalehti 16.3.2011)
- "Äärioikeistolaiset miehet nujakoivat kokoomuksen teltalla Oulussa" (Helsingin Sanomat 10.4.2011)
- "Viha on kasvanut Suomessa" (Hanna Kaarto, Helsingin Sanomat 10.4.2011)
- "Nyt puhkesi vaaliviha: Uhkaavia iskuja ja sabotaasia" (Iltalehti 11.4.2011)
- "Iskut merkkejä ilmapiirin kiristymisestä – Asiantuntijan mukaan iskut ovat Suomessa kuitenkin lähinnä kanava turhautuneisuuden purkautumiseen" (Iltalehti 11.4.2011)
- "Tampereen oikeustalolla pommiuhka" (Iltalehti 1.4.2011)
- "Rasismitutkija varoittaa kokoomuksen vaalitulaisuudessa mellakoineesta liikkeestä – Pahimmillaan tilanne voi kääntyä vaikka kuinka pahaksi, Itä-Suomen yliopiston tutkija Vesa Puuronen sanoo" (Iltalehti 11.4.2011)
- "Turvatoimia kiristetty – Poliitikot huolestuivat väkivallasta. Iskut vaalikampanjoihin ovat lisääntyneet" (Ilta-Sanomat 11.4.2011)
- "Vaaliviha yltyy – ehdokas sai nyrkistä" (Iltalehti 12.4.2011)
- "TVO selvittää ydinvoimaloiden varautumisen luonnonkatastrofeihin" (Verkkouutiset 13.4.2011)
- "Kova paljastus Ruotsissa – CIA jäi kiinni. Amerikkalaiset harjoittivat luvaton tiedustelutoimintaa Ruotsissa maan hallituksen tietämättä, väittää Svenska Dag Bladet" (Iltalehti 23.5.2011)
- "Ydintuho paljastuu - polttoaine suli kolmessa Fukushima reaktorissa" (Ilta-Sanomat 24.5.2011)
- "Osion räjähdys vaikuttaa koko Pohjolan turvallisuustilanteen arviointiin" (Yle-uutiset 22.7.2011)
- "Valepoliisi ampui nuoria leirillä Norjassa - ainakin kymmenen kuoli" (Yle-uutiset 22.7.2011)
- "Nuoret rankkasivat työnantajia – Nuorten mielikuvissa Nokia, Lidl ja valtio ovat heikoimmin johdettuja työpaikkoja" (Iltalehti 31.8.2011)
- "HS: Huolestuttava kehitys Suomen jengeissä – Moottoripyöräjengit ovat laajentaneet toimintaansa merkittävästi viime vuosikymmeninä. Poliisi pelkää jengien välien kiristyvän edelleen" (Iltalehti 9.9.2011)
- "Nämä terroristijärjestöt uhkaavat Suomea – Tutkija paljastaa, mitkä terroristiryhmät toimivat Suomessa" (Iltalehti 19.10.2011)
- "Äärioikeistolla mystinen kokous Helsingissä - Helsingissä kokoontuu lauantaina äärioikeistoa eri maista" (Iltalehti 22.10.2011)
- "Uusi supervirus voi tappaa puolet maapallon väestöstä" (Iltasanomat 29.11.2011)

Liite 7: Riskienhallinnan sijoittuminen eduskunnan kanslian organisaatioon



Liite 8: Eduskunnan kanslian turvallisuusympäristön lausunto

Liike-elämässä riskienhallinnassa on usein kysymys yrityksen toiminnan varmistamisesta ja etenkin yritykseen sijoittaneiden omistajien tai muiden rahoittajien sijoitusten turvaamisesta sekä tuottovaatimusten täyttämisestä.

Julkisessa hallinnossa riskienhallinnan painopistealueita voivat olla 1. vahinkoriskeissä työterveys- ja työturvallisuusriskit, henkilöriskit, ympäristöriskit ja toimitilaturvallisuuden riskit, 2. operatiivisissa riskeissä johtamiseen liittyvät riskit, tietoturvallisuusriskit, toimintaan ja sen tehokkuuteen liittyvät riskit, kriisitilanteisiin liittyvät riskit ja 3. taloudellisissa riskeissä kirjanpidon ja talousraportoinnin riskit sekä 4. strategisissa riskeissä viestintäriskit.

Riskienhallinta on Eduskunnan kanslian uusi toiminnan alue. Riskienhallinta tulisi tutkimuksessa esitetyllä tavalla liittää eduskunnan kanslian normaaliin päivittäiseen toimintaan siten, että riskienhallinta tukee niin strategista kuin operatiivista johtamista ja toiminnan suunnittelua. Riskienhallinta tukee osastojen ja yksiköiden toimintaa ja tuo esiin aiempaa selvemmin eduskunnan pääsihteerin alaisuudessa osastopäälliköiden ja yksiköiden päälliköiden vastuun toimintansa sisäisestä tarkastuksesta ja kokonaisvaltaisesta suunnittelun ohjaamisesta sekä toiminnan johtamisesta. Em. toimintaan riskit huomioon ottaen liittyy talouden ja toiminnan tehokkuuden lisääminen.

Eduskunnan kansliassa riskienhallinnan tulevaisuuden haaste on riskienhallinnan saaminen hallituksi osaksi osastojen ja yksiköiden normaalia toimintaa ja johtamista. Tutkijan ehdottamat jatkotutkimukset tukevat hyvällä tavalla riskienhallinnan kokonaisuuden kehittämistä.

Tutkija on löytänyt Eduskunnan kansliaan ideaalin riskienhallinnan kokonaisjärjestelyn ja riskienhallinta on organisoitu yleisellä tasolla hyvän hallintotavan mukaisesti. Riskienhallintaa järjestettäessä tulisi kuitenkin ottaa huomioon Eduskunnan kanslian erityinen luonne ja toimintatavat niin lainsäädäntötyössä kuin sitä tukevassa hallinnollisessa toiminnassa. Eduskunnan erityisluonteen huomioon ottaminen ei millään tavalla vähennä tutkimuksen arvoa eikä käytettävyyttä.

Tutkimuksen lopputulos on ylittänyt Eduskunnan kanslian Turvallisuusyksikön toimeksiannossa asetetut vaativat tavoitteet. Työtä voidaan hyödyntää kokonaisvaltaisen riskienhallinnan kehittämässä. Turvallisuusyksikön näkökulmasta tutkimustyötä voidaan pitää erittäin korkeatasoisena opinnäytetyönä, jossa tutkija on osoittanut hallitsevansa työssä käytetyt tutkimusmenetelmät ja riskienhallinnan teoreettiset taustat. Tutkimustyöllä on saadut tulokset osoittavat tutkijan perehtyneen syvällisesti koko aihealueeseen. Työn tuloksia voidaan käyttää sellaiseen Eduskunnan kanslian riskienhallinnan kehittämässä.