LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Harjoitusmallin kehittäminen valtiohallinnon häiriöhallintaryhmälle

Muttilainen, Mikko

2015 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Harjoitusmallin kehittäminen valtiohallinnon häiriöhallintaryhmälle

Mikko Muttilainen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Mikko Muttilainen

Harjoitusmallin kehittäminen valtiohallinnon häiriöhallintaryhmälle

Vuosi 2015 Sivumäärä 43

Opinnäytetyön tutkimuskohteena oli poikkihallinnollista kyberturvallisuusyhteistyötä kehittävän valtiohallinnon häiriöhallintaryhmän harjoitustoiminta. Tutkimusongelma oli se, että valtiohallinnon häiriöhallintaryhmän harjoitustoimintaa tai harjoitusten luomisprosessia ei ollut vakiinnutettu. Tutkimuksen tavoitteena oli luoda häiriöhallintaryhmälle harjoitusmalli, jonka avulla ryhmälle saataisi luotua tehokkaasti ja helppokäyttöisesti kevyitä harjoituksia. Työn tilaajana toimi Valtiovarainministeriön alaisuudessa toimiva SecICT-hanke, mistä syystä tutkimus rajattiin koskemaan nimenomaisesti viranomaistoimintaa.

Tutkimuksellinen lähestymistapa työhön oli kvalitatiivinen. Tiedonkeruumenetelminä käytettiin kyselyä, teemahaastattelua sekä havainnointia. Tutkimuksen aikana suoritettiin kaksi harjoitusta, joiden onnistumista mitattiin kyselyjen avulla. Harjoitustilanteen aikaista toimintaa havainnoitiin toimintaa varten räätälöidyn havainnointilomakkeen avulla. Kokemuksia menneistä kansallisista sekä kansainvälisistä kyberharjoituksista haluttiin kerätä ja hyödyntää haastattelemalla kolmea valtiohallinnon tieto- ja kyberturvallisuuden asiantuntijaa.

Ensimmäinen versio harjoitusmallista kehitettiin ensimmäisen harjoituksen ja tiedonkeruuvaiheen jälkeen, minkä jälkeen mallin toimivuutta testattiin järjestämällä toinen harjoitus. Harjoituksen suunnittelussa pyrittiin hyödyntämään tutkimusprosessin kautta löydettyä uutta tietoa. Harjoitusmallin taustavaikutusta toisen harjoituksen onnistumiseen mitattiin harjoituksen jälkeen toteutetulla kyselyllä.

Häiriöhallintaryhmän sisäiset harjoitukset koettiin toimintaan osallistuvien asiantuntijoiden näkökulmasta tärkeäksi tavaksi kehittää poikkihallinnollista yhteistoimintaa. Harjoitusmallin soveltamisella harjoitusten luomiseen sekä toiminnan kehittämiseen saatiin alustavia positiivisia tuloksia. Mallin käyttöönotto myös muualla valtiohallinnossa herätti kiinnostusta. Jatkotutkimusaiheena voitaisiin pitää tämän työn ulkopuolelle rajattua yksityisen sektorin kiinnostusta vastaavalle mallille etenkin suurissa yrityksissä tai konserneissa.

Asiasanat: harjoitusmalli, pöytäharjoitus, kyberturvallisuus, viranomainen

Laurea University of Applied Sciences **Abstract**
Leppävaara
Bachelor's Degree Programme in Security Management

Mikko Muttilainen

Developing an Exercise Framework for the Virtual Incident Response Team

Year 2015 Pages 43

The research subject of this thesis was the development of cross-governmental cyber security training exercises held by the Virtual Incident Response Team. The research problem of the thesis was that the creation and development processes for the exercises hadn't been established. The main objective of the study was to create an exercise framework that would allow the team to create lightweight exercises efficiently and effectively. The subject for the study originally came as a request from the SecICT-project, which operates under the Ministry of Finance of Finland.

The scientific approach to the study was qualitative. The methods used in this study were enquiry, interviews and observation. Two cyber security training exercises were held during the study period and the effectiveness of those exercises was measured with enquiries. The operational success of the exercises was observed and documented by using a custom observation form. The information and experiences from past national and international cyber security exercises were gathered by interviewing three cyber security experts working within the government.

The first version of the exercise framework was developed after the first exercise and some data had been gathered by using the research methods. The framework was then tested by trying to utilize the newfound information in the development process of the next exercise. The success of the second exercise was then measured by using an enquiry.

The lightweight cyber security training exercises were found to be a useful way to develop cross-governmental co-operation. The effect of the exercise framework on the quality of the exercises was found to be positive. Other government agencies were also interested in utilizing the framework within their own organizations. A subject for further research could be to investigate the need and interest for these types of exercises in the private sector.

Keywords: exercise framework, tabletop exercise, cyber security, authority

Sisällys

1 Johdanto

Opinnäytetyön kehittämiskohteena oli vuoden 2014 lokakuussa perustetun valtiohallinnon häiriöhallintaryhmän harjoitustoiminta. Työn tavoitteena oli luoda häiriöhallintaryhmälle pöytäharjoituksiin keskittyvä harjoitusmalli, jonka avulla ryhmälle voitaisiin luoda yksinkertaisesti ja tehokkaasti eri tilanteisiin soveltuvia harjoituksia. Ensisijaisesti harjoitusmallia tulisi hyödyntämään valtiohallinnon häiriöhallintaryhmä, mutta se soveltuu myös muualle valtiohallintoon tai muiden organisaatioiden hyödynnettäväksi.

Opinnäytetyöprosessin lähtökohtana oli se, että työn lopputulos vastaisi mahdollisimman hyvin työn tilaajan tarpeita sekä monipuolisia toimintaympäristön haasteita. Erityisesti harjoitusmallilta toivottiin helppokäyttöisyyttä sekä harjoitusten skaalautuvuutta. Näin harjoitusmalli saataisiin myös jatkossa hyödynnettyä niin häiriöhallintaryhmän kuin muidenkin toimijoiden toimesta, välttäen päällekkäistä työtä valtiohallinnossa.

Tutkimuksellinen lähestymistapa opinnäytetyöhön oli kvalitatiivinen ja pääpainopisteen nähtiin olevan työelämälähtöisessä toiminnan kehittämisessä. Tiedon keruu- ja analyysimenetelmät valittiin tukemaan asiantuntijoilta saatavaa arvokasta palautetta ja soveltumaan myös tulevaisuudessa häiriöhallintaryhmän harjoitustoiminnan kehittämiseen. Noin muutaman kymmenen hengen suuruinen tietoturvallisuuteen suuntautunut asiantuntijajoukko pystyy näin parhaiten kehittämään valtiohallinnon kybervarautumisen tasoa niin omilla hallinnonaloillaan kuin myös yhteistyössä toistensa kanssa.

Aiheen valinta oli niin mielenkiintoinen kuin ajankohtainenkin. Kyberturvallisuuden tärkeyttä on lähiaikoina korostettu monelta taholta ja sen rooli tulee kasvamaan jatkossakin alati verkottuvan ja tietoliikenteeseen painottuvan yhteiskunnan kehittyessä. Näin ollen myös valtiohallinnon kyberuhkiin varautumisen tulee olla ajan tasalla. Toimia tämän edistämiseksi onkin jo tehty: esimerkiksi Liikenne- ja viestintäministeriön alaisuudessa toimiva Kyberturvallisuuskeskus aloitti toimintansa tammikuussa 2014 (Viestintävirasto 2014).

Opinnäytetyön aihe oli myös siitä erikoinen, ettei nimenomaisesti kyberturvallisuuteen liittyvästä harjoitustoiminnasta ole ennen tehty aikaisempia opinnäytetöitä. Kyberturvallisuuden ollessa itsekin vielä lapsenkengissä, on valtiohallinnolla nyt hyvä mahdollisuus kehittää toimintaansa yhdessä uuden häiriöhallintaryhmän perustamisen myötä. Yhdessä harjoittelu tuo usein esiin odottamattomia ja toimintaa haittaavia ongelmia ja tästä näkökulmasta katsottuna voitiinkin odottaa, että harjoitusmalli tulisi olemaan käyttökelpoinen ja tarpeellinen työkalu yhteistoiminnan kehittämiseen.

1.1 Käsitteet

Työssä käytetään termejä ja käsitteitä jotka eivät välttämättä ole maallikolle tuttuja. Tästä syystä koettiin tarpeelliseksi avata työssä käytettyjä käsitteitä. Myös tieteellisestä näkökulmasta tämä on oleellisesta, sillä työssä tehdyt havainnot saattavat jäädä merkityksettömiksi ilman käsitteiden määrittelyä. Käsitteiden tarkka määrittely myös vähentää väärinymmärryksiä sekä antaa tekstille tiettyä legitimiteettiä. Osa käytetyistä käsitteistä voitaisiin käsittää monella tavalla, mistä syystä termien selitys kontekstiin liittyen on vielä korostuneemmassa asemassa. (Hirsjärvi, Remes & Sajavaara 2013, 146-149)

HARJOITUSMALLI
Tämän opinnäytetyön kontekstissa harjoitusmallilla tarkoitetaan viitekehystä, jonka avulla voidaan luoda helppokäyttöisesti ja tehokkaasti eri tarpeisiin soveltuvia harjoituksia. Harjoitusmalli pitää sisällään ohjeet harjoituksen tekoon, havainnointilomakkeen, toteutusaikataulun sekä esimerkkiharjoituksen.

KYBERTURVALLISUUS
Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristöä käytetään käsitteenä, kun pyritään kuvaamaan modernia sähköistettyä ja verkottunutta yhteiskuntaa. (Turvallisuuskomitean sihteeristö 2013)

PÖYTÄHARJOITUS
Pöytäharjoituksella (engl. tabletop exercise) tarkoitetaan yksinkertaista ja kestoltaan lyhyttä harjoitusta, jossa pyritään löytämään ratkaisuja tosielämän ongelmatilanteisiin keskustelemalla ryhmässä. Harjoituksessa on tyypillisesti yksinkertainen käsikirjoitus sekä syötteitä keskustelun aktivoimiseksi. (Phelps 2010,13)

SKENAARIO
Skenaariolla tarkoitetaan harjoituskontekstissa jonkinlaista kuvausta tapahtumasta, onnettomuudesta, hyökkäyksestä tai muusta tapahtumaketjusta, jossa jokainen vaihe kuvataan tarkasti tarinan ja harjoitustekniikan avulla. (Phelps 2010, 47)

VIRTUAL INCIDENT RESPONSE TEAM (VIRT)
Virtual Incident Response Team eli valtiohallinnon häiriöhallintaryhmä on tietoturvallisuuteen erikoistuneista asiantuntijoista koostuva poikkihallinnollinen yhteistyöelin. Vuonna 2014 perustettu ryhmä pyrkii parantamaan valtiohallinnon kybervarautumisen tasoa ja tiivistämään hallinnonalojen välistä yhteistyötä vakavissa- ja laajavaikutteisissa häiriötilanteissa. (Valtiovarainministeriö 2014, 3)

1.2 Työn tilaaja

Opinnäytetyön tilaajana toimi Valtiovarainministeriön rahoittama SecICT-hanke. Valtiovarainministeriö toimii valtiohallinnossa talous – ja finanssipolitiikan sekä veropolitiikan asiantuntijaorganisaationa. Se vastaa julkishallinnollisen sektorin, kuntahallinnon lainsäädännön sekä kunnallistalouden kehittämisestä. Ministeriön toiminnan tavoitteena on taloudellisen vakauden ja kasvun edistäminen, verojärjestelmän kilpailukykyisyyden takaaminen sekä julkishallinnon palvelu – ja kilpailukyvyn turvaaminen. (Valtiovarainministeriö 2015)

JulkICT-toiminto vastaa julkishallinnon tietojärjestelmien- ja hallinnon kehittämisestä. ICT:tä käytetään lyhenteenä informaatio- ja kommunikaatioteknologialle (Burdett & Bowen 2013, 3). JulkICT-toiminto pyrkii myös edistämään kansalaisten sähköisiä asiointipalveluja sekä avata avoimen datan tietovarantoja. Toiminto vastaa myös julkishallinnon tietoturvallisuuden ohjaamisesta ja kehittämisestä. (Valtiovarainministeriö 2015)

SecICT-hanke (valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke) on JulkICT-toiminnon Kyberturvallisuus ja Infrastruktuuri-yksikön alaisuudessa toimiva kehittämishanke. Hanke käynnistettiin vuonna 2013 ja sen hankepäällikkönä toimii erityisasiantuntija Kirsi Janhunen. Hankkeen on määrä päättyä vuoden 2015 loppuun mennessä. Hankkeen tehtävänä on suunnitella viranomaisyhteistyönä ja valituilta osin pilotoida valtionhallinnon tietoturvaloukkausten havainnointi, tietoturvapoikkeamiin reagointi ja tietoturvallisuuden tilannekuvan hallinta sekä toimintamallit hyödyntäen valtion keskitettyjä ICT-palveluita. (Hankerekisteri 2015)

Osana hankkeen tavoitetta lähentää viranomaisten yhteistyökykyä, perustettiin hankkeen kautta valtionhallinnon häiriöhallintaryhmä eli VIRT. Opinnäytetyöprosessissa kehitettävä harjoitusmalli tulee tämän häiriöhallintaryhmän käyttöön. VIRT:n jäsenistö koostuu valtiohallinnon asiantuntijarooleissa työskentelevistä virkamiehistä, jotka vastaavat omissa organisaatioissaan kyberhäiriötilanteiden hallinnasta. Asiantuntijat valittiin ryhmään lähettämällä nimityspyyntö kuhunkin organisaatioon. Toiminnan alkuvaiheessa asiantuntijoita toimintaan on pyydetty pääasiassa turvallisuusviranomaisista, mutta ryhmää on sittemmin pyritty laajentamaan kattamaan kaikki hallinnonalat. (Valtiovarainministeriö 2014, 3)

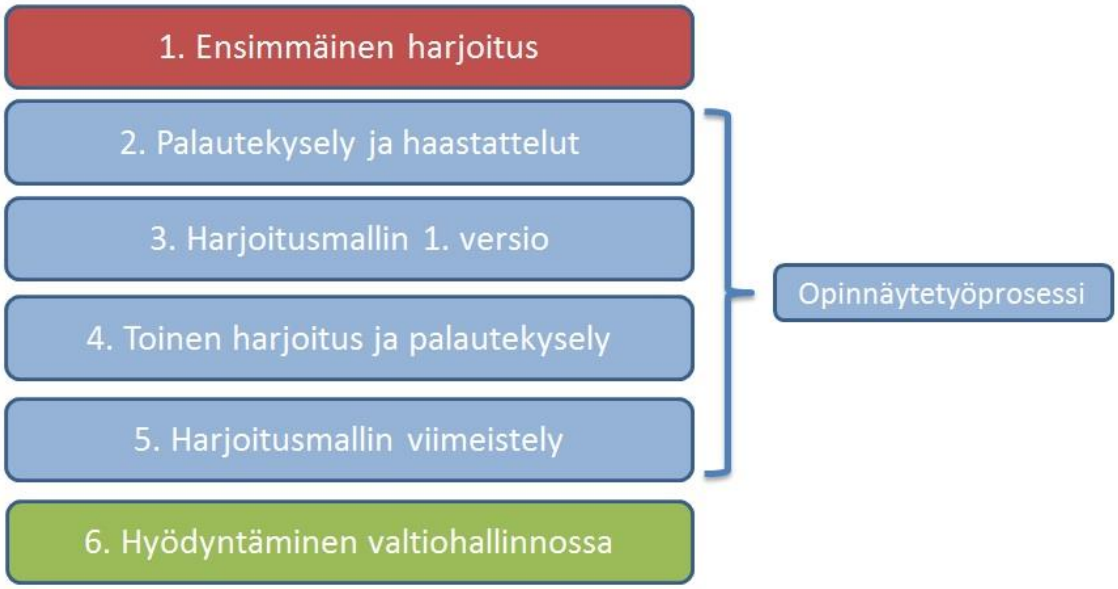
Toimintaan osallistuvat asiantuntijat ovat omissa organisaatioissaan tyypillisesti tietoturvapäälliköitä, tietoturva-asiantuntijoita, turvallisuuspäälliköitä tai työskentelevät riskienhallintaan liittyvissä rooleissa. Jos organisaatiolla niin sanottu SOC (Security Operations Center), on VIRT:iin osallistuva asiantuntija tyypillisesti tämän vetäjä. Tällä valintamenettelyllä on pyritty siihen, että tällä hetkellä erillään toimivat SOC:t saataisiin jakamaan keskenään tietoa ja muodostamaan valtiohallintoon parempaa kyberturvallisuuden tilannekuvaa.

1.3 Työn rakenne ja kehittämisprosessi

Opinnäytetyön rakenne mukailee loogisesti ja kronologisesti edennyttä kehittämisprosessia. Hirsjärven ym. (2013, 54-55) mukaan opinnäytetyön rakenteen tulisi olla selkeä ja sen tulisi muodostaa työstä tasapainoinen kokonaisuus. Ensimmäisessä kappaleessa esitellään työlle olennaisten käsitteiden määrittelyt, työn tilaaja sekä käydään läpi työn rajaukset ja prosessi. Tästä siirrytään käytettyjen tutkimusmenetelmien esittelemiseen ja tutkimuksellisen viitekehyksen avaamiseen. Tämän jälkeen työn loppuosa mukailee tyypillisen konstruktiivisen tutkimuksen prosessia (Ojasalo, Moilanen & Ritalahti 2014, 67).

Konstruktiivisen tutkimuksen prosessissa aloitetaan mielekkään ongelman etsimisellä, josta siirrytään tiedonhankintaprosessiin. Tämän jälkeen pyritään keksimään ongelmalle käytännön ratkaisu ja testaamaan ratkaisun toimivuutta. Lopuksi pyritään osoittamaan ratkaisun toimivuuden ja teoriakytkentöjen yhteys sekä kartoittamaan ratkaisun soveltamisalueen laajuus. (Ojasalo ym. 2014, 67)

Tämän työn kehittämisprosessi on kuvattu alla kuviossa 1. Ongelma tunnistettiin ensimmäisen harjoituksen pitämisen jälkeen ja tästä alkoi varsinainen opinnäytetyöprosessi. Tämän jälkeen kerättiin aiheeseen liittyvää teoreettista ja käytännön tietoa tiedonkeruumenetelmiä käyttäen ja luotiin alustava harjoitusmalli. Harjoitusmallia testattiin hyödyntämällä sitä toisen harjoituksen tekemiseen. Tämän jälkeen mallia jatkokehitettiin toisen kyselyn avulla. Lopuksi pyrittiin kartoittamaan harjoitusmallin hyödynnettävyyttä muualla valtiohallinnossa.



Kuvio 1. Harjoitusmallin kehittämisprosessi

1.4 Tutkimuskysymys ja rajaukset

Opinnäytetyöprosessin alkuvaiheessa oli selvää, että aihe tulee olemaan hyvin käytännönläheinen ja lopullinen tuotos tulisi ainakin ensin vain pienen asiantuntijajoukon käyttöön. Tutkimuskysymystä määrittäessä syntyi ristiriitaa siitä, tulisiko työn olla puhtaasti konstruktiivinen tutkimus vai onko työssä pidemmän aikavälin kehittämisen elementtejä. (Ojasalo ym. 2014, 65) VIRT-toiminta oli kirjoitushetkellä ollut käynnissä vasta puoli vuotta ja sen jatkuvasti toimintaa kehittävän luonteen vuoksi myös kehittämisprosessin tuli joustaa.

Hirsjärven ym. (2013, 126) mukaan tutkimuksessa pyritään esittämään yksi pääongelma, joka pyritään rajaamaan ja selittämään mahdollisimman hyvin. Tämän työn osalta ongelma löytyi harjoitustoiminnan jatkuvuudesta; VIRT-toiminnalle oli tehty yksi harjoitus ja sen myötä hyvää pohjatyötä, jota voitaisiin hyödyntää myös jatkossa. Pohjatyötä tai harjoituksen luomisprosessia ei ollut kuitenkaan dokumentoitu ja mahdollisten henkilöstömuutosten tapahtuessa saattaisi tämä tieto kadota kokonaan. Tästä ongelmasta saatiinkin johdettua tutkimuskysymys: kuinka valtiohallinnon häiriöhallintaryhmän harjoitustoiminta saadaan vakiinnutettua ja harjoitusten tuloksellisuutta seurattua?

Onnistuneelle opinnäytetyölle olennaista on riittävän tiukka aiheen rajaus. Tyypillisiä sudenkuoppia opinnäytetyön aiheen valitsemisessa ovat liian laajan tutkimusaiheen valitseminen, lähdemateriaalin olemattomuus sekä aiheen epämääräisyys. Joskus myös tutkijan valitsemasta aiheesta on jo kirjoitettu aikaisempi työ, jolloin tutkimukselle täytyy vähintään löytää uusi näkökulma tai hylätä aihe tyystin. Rajauksen tukena voidaan käyttää opinnäytetyön viitekehystä ja annettua tehtävänantoa. (Hirsjärvi ym. 2013, 83-84)

Tämän työn kannalta rajaukset ovat olleet pääosin alusta asti selkeät. Työn kautta kehitettävän mallin kohderyhmä on valtiohallinnossa toimiva pieni asiantuntijajoukko. Työn lopussa on kuitenkin myös kartoitettu mallin hyödyntämistä muualla valtiohallinnossa, sillä se on olennainen osa konstruktiivista tutkimusta. Opinnäytetyöprosessin aikana on pyritty tarkoituksellisesti keskittymään vain valtiohallintoon eikä yksityiseen sektoriin.

Työn tilaajan toiveena oli myös, että mallin tulisi myös tukea kevyttä ja helppokäyttöistä harjoitusten muodostamista, joten taustalla olevan myös teorian ja harjoituksen tekemiseen käytettävän vaivan määrä on pyritty minimoimaan (Janhunen 2015). Lopputuloksen toivottiin olevan käytännönläheinen. Harjoitusmallissa keskitytään nimenomaan pöytäharjoitusten suunnitteluun eikä muita harjoitustyyppejä ole sisällytetty tutkimukseen.

2 Tutkimusasetelma

Tässä luvussa kuvataan opinnäytetyön teoreettinen viitekehys, lähestymistapa sekä käydään läpi aikaisempaa tutkimustietoa sekä työssä käytetyt tiedonkeruumenetelmät. Teoreettisen viitekehyksen ja käytettyjen menetelmien kuvaaminen on olennainen osa opinnäytettä ja niillä pyritään myös vahvistamaan työn reliabiliteettia ja toistettavuutta. Tarkoituksena on kuvata se, mitä tutkimuksessa tehtiin ja kuinka tehdyt toimenpiteet suoritettiin (Hirsjärvi ym. 2013, 261). Tavoitteena on kuvata koko prosessi mahdollisimman selkeästi ja tarkasti siten, että lukijalle selkeytyy tutkimuksen taustalla oleva johtoajatus ja se, kuinka käytetyt menetelmät tukevat tutkimuksen lopputavoitteeseen pääsyä.

Tutkimuksellinen lähestymistapa kehitystyöhön oli laadullinen eli kyseessä on kvalitatiivinen tutkimus. Tarkemmin määriteltynä voidaan puhua myös konstruktiivisesta tutkimuksesta. Ojasalon ym. (2014, 65) mukaan konstruktiivisesta tutkimuksesta voidaan puhua silloin, kun tutkimuksen tavoitteena on luoda jonkinlainen konkreettinen tuotos, esimerkiksi suunnitelma, mittari tai malli. Ojasalo ym. (2014, 65-66) lisäävät, että konstruktiivisen tutkimuksen tavoitteena on löytää käytännön ratkaisu käytännön ongelmaan sekä tuottaa samalla uutta tietoa. Työstä saatavan uuden tiedon levittäminen muualle valtiohallintoon on ollut myös työn tilaajan toiveena.

2.1 Aikaisemmat tutkimukset

Ojasalon ym. (2014, 30) mukaan kehitystyössä on erittäin oleellista tutustua olemassaolevaan tutkimustietoon ja julkaisuihin. Aikaisemman tutkimustiedon etsiminen aiheesta aloitettiinkin ammattikorkeakoulujen opinnäytetyötietokannan eli Theseuksen sekä Kansalliskirjaston ylläpitämän julkaisuarkiston, Dorian, selaamisella. Yllämainituista tietokannoista pyrittiin etsimään aikaisempia julkaisuja, joiden aihe tai sisältö voisi liittyä tämän tutkimuksen aihepiiriin. Hakusanoina käytettiin työn keskiössä olevia termejä, kuten ”harjoitusmalli”, ”pöytäharjoitus” ja ”kyberturvallisuus”.

Dorian aineistoista ei löytynyt aihetta hyödyttäviä tutkimuksia hakusanoilla ”harjoitusmalli” tai ”pöytäharjoitus”. Kyberturvallisuutta oli puolestaan tutkittu erityisesti lähivuosina paljonkin monesta eri näkökulmasta. Kyberturvallisuutta tutkineet opiskelijat olivat lähes poikkeuksetta Maanpuolustuskorkeakoulun opiskelijoita. Tämän työn tavoitteena ei ollut kuitenkaan kyberturvallisuuden substanssin tutkiminen, joten edellä mainittujen töiden hyöty tähän tutkimukseen nähden koettiin pintapuoleisseksi.

Lähiten aihetta sivusi Aholan (2014) pro gradu-tutkielma ”Valmiusharjoitusten onnistumiseen vaikuttavat tekijät osallistujien näkökulmasta”. Tutkimuksen kohteena olivat aluehallintovi-

rastojen sekä Pelastusopiston järjestämät valmiusharjoitukset, joiden onnistumista Ahola pyrki mittaamaan kyselytutkimuksen ja haastatteluiden avulla (Ahola 2014, 23). Tutkimus eroaa tämän työn aiheesta siten, että näkökulma on osallistujan mielipiteessä harjoituksen onnistumisesta. Tutkimuksen kohteena olleet harjoitukset ovat olleet myös luonteeltaan huomattavasti laajempia sekä toiminnallisempia kuin tässä työssä käsiteltävät harjoitukset.

Theseuksesta etsittäessä hakutuloksina saatiin pääasiassa toiminnalliseen lihasharjoitteluun liittyviä harjoitusmalleja käsitteleviä opinnäytetöitä. Pöytäharjoitukset mainitsevat puolestaan Laine (2011, 14) ja Tuomikoski (2014, 50) varautumis- ja jatkuvuussuunnitteluun liittyvissä tutkimuksissaan. He mainitsevat pöytäharjoitukset pintapuolisesti yhtenä välineenä organisaatioiden valmiuden testaamiseen erilaisiin kriisitilanteisiin liittyen.

Theseuksen ja Dorian lisäksi aikaisempaa tutkimustietoa pyrittiin etsimään myös kansainvälisistä lähteistä. Etenkin monipuolista kirjallisuutta aihepiirin tiimoilta löytyi runsaastikin, mutta suurin osa näistä lähteistä kosketti pelastusviranomaisten toimintaa tai muuta kriisivarautumista. Aiheet käsittelivät pääasiassa fyysisiä uhkia, kuten esimerkiksi luonnonkatastrofeja, kemikaalivuotoja tai bioterrorismia. Siinä missä monestakin näistä lähteistä olisi voinut soveltaa tietoa tätä tutkimusta varten, valittiin löydetystä aineistosta kaksi eniten potentiaalista hyötyä tuovaa lähdettä.

Ensimmäisen harjoituksen suunnitteluun oli jo ennen opinnäytetyöprosessia käytetty lähteenä FEMA:n kyberturvallisuusaiheista pöytäharjoitusta, joka järjestettiin vuonna 2012. FEMA eli Federal Emergency Management Agency on Yhdysvaltojen virasto, joka on keskittynyt vastaamaan nopeasti luonnonkatastrofeihin tai muihin laajoihin hätätilanteisiin. (FEMA 2012) Edellämainitun harjoituksen materiaalit koettiin erittäin havainnollistaviksi ja hyödyllisiksi, minkä takia materiaaleja haluttiin hyödyntää myös tutkimuksessa.

Toisena tärkeänä lähteenä päätettiin käyttää Phelpsin (2010) teosta ”Emergency Management Exercises”. Vaikka kirjan nimi viittaakin jälleen tyypillisten hätätilanteiden hallintaan, löytyy teoksesta erittäin kattavasti erityyppisiä harjoituksia ja tarkat kuvaukset kustakin harjoitustyypistä. Teosta hyödynnettiin opinnäytetyöprosessin aikana runsaasti etenkin eri lomakkeiden suunnittelussa.

Tutkimuksen aiheeseen peilaten oli selkeää, että kirjallisen ja sähköisen lähdemateriaalin pääasiallinen soveltumattomuus työhön oli huomattavaa. Tästä syystä menetelmien valinnassa jätettiin ulkopuolelle muunmuassa kirjallisuuskatsaus sekä dokumenttianalyysi. Työssä haluttiin myös keskittyä hyödyntämään VIRT-toiminnassa mukana olevien asiantuntijoiden ammattitaitoa ja laadullisia menetelmiä käyttäen mahdollisesti jopa keksiä innovatiivisia ja uusia ratkaisuja harjoitusten luomiseen.

2.2 Tiedonkeruumenetelmät

Tiedonkeruumenetelmien valinta pyrittiin toteuttamaan siten, että niiden tuottama tieto olisi työn kannalta relevanttia, hyödynnettävää ja sellaista, millä kohderyhmän toimintaa saataisiin kehitettyä myös jatkossa. Koska häiriöhallintaryhmä on pieni asiantuntijoista koostuva joukko, voitiin alusta saakka sulkea pois suurin osa kvantitatiivisista menetelmistä ja keskittyä muutamaan asiantuntijoiden arvokkaiden kokemusten tallentamiseen soveltuvaan menetelmään. Tämä kuvastaa myös hyvin laadullisen tutkimuksen luonnetta – tutkimuksen kohteena ovat ihmiset ja kerättävä tieto kuvaa kohdejoukon mielipiteitä, kokemuksia ja muita näkökulmia (Hirsjärvi ym. 2013, 164).

Tiedonkeruumenetelmiksi valittiin kolme menetelmää: kysely, haastattelu sekä havainnointi. Uuden tiedon löytämiseksi oli tärkeää, että tietoa kerätään monipuolisin menetelmin (Ojasalo ym. 2014, 68). Kvalitatiiviselle tutkimukselle tyypillistä on myös se, että menetelmien tuloksena saatava tieto on ennestään tuntematonta ja siksi tutkimukselle ei ole olennaista antaa ennalta asetettua hypoteesia (Hirsjärvi ym. 2013, 164). Menetelmät valittiinkin tukemaan toisiaan niin sanotun ”hiljaisen tiedon” löytämiseksi ja hyödyntämiseksi työssä.

2.2.1 Kysely

Ensimmäinen käytetyistä tutkimusmenetelmistä oli kysely. Kyselyitä tehtiin kaksi ja ne olivat keskenään lähes samanlaisia referenssitason määrittämiseksi. Kyselyä käytettiin palautteen keräämiseksi kahdesta harjoituksesta. Ensimmäisellä kyselyllä pyrittiin kartoittamaan yleisiä kokemuksia harjoitusformaatista, mittaamaan harjoituksen onnistumista asiantuntijoiden näkökulmasta sekä kartoittamaan toivottuja aiheita tulevilla harjoituksille. Tässä yhteydessä voitaisiinkin käyttää termiä ”palautekysely”. Kyselyn toteuttamiseen käytettiin Laurean käytössä olevaa e-lomake-työkalua. Kysymykset löytyvät liitteestä 1.

Kyselyn käyttämisessä tiedonkeruumenetelmänä on niin hyviä kuin huonojakin puolia. Ilmeisimmät vahvuudet kyselylle löytyvät sen helppokäyttöisyydestä, tutkijan ajan säästämisestä ja tunnettuudesta. Myös kyselyn levittäminen etenkin sähköisesti on erittäin helppoa. Kyselyn kustannusvaikutukset ovat myös minimaaliset sekä sen jatkohyödyntäminen on helppoa. (Hirsjärvi ym. 2013, 193-195)

Eniten haastetta kyselyn tekemisessä aiheuttavat usein oikeiden kysymysten löytäminen sekä vastausvaihtoehtojen valitseminen. Tätä työtä varten valittiin viisiportainen vastausmalli, sillä se sopii hyvin mahdollisimman neutraalien vastausvaihtoehtojen valintaan. Myös kysymysten tulisi olla asettelultaan sellaisia, etteivät ne sanankäänteillään ohjaa vastaajaa mihinkään suuntaan. (Ojasalo ym. 2014, 130-131) Tärkeää on myös kyselyn pituuden määrittelemi-

nen – työn tilaajalla oli vahva toivomus siitä, että kysely pidetään tiiviinä ja että siihen liittyviä kysymyksiä olisi korkeintaan 15 kappaletta. Virkamiesten koettiin täyttävän vuosittain kymmenittäin erilaisia kyselyitä ja täten lyhyenä mainostettu kysely tuntuisi houkuttelevammalta vastaamisen kannalta.

Kyselyssä kaikkien potentiaalisten vastaajien joukkoa kutsutaan perusjoukoksi (Ojasalo ym. 2014, 122). Perusjoukko oli molemmissa kyselyissä järin pieni; ensimmäisessä harjoituksessa potentiaalisia vastaajia oli noin 20 ja toisessa noin 12. Pieni perusjoukko korreloi täysin harjoituksiin osallistuneiden asiantuntijoiden määrän kanssa, sillä kyselyyn voivat vastata vain ne henkilöt, jotka ovat harjoitukseen osallistuneet. Tämä onkin tyypillinen ongelma kvalitatiivisten tutkimusten kyselyissä. Pieni otanta johtaa myös siihen, ettei vastaustuloksista voida vetää kuin suuntaa-antavia johtopäätöksiä (Ojasalo ym. 2014, 129).

Kyselyyn vastaamisen kynnyksen laskemiseksi on myös usein tarpeellista luoda kyselyä varten saatekirje. Saatteessa kuvaillaan ainakin kyselyn tarkoitus, kysymysten määrä sekä arvioitu vastausaika. (Hirsjärvi ym. 2013, 204) Näitä kyselyjä varten kyselystä mainittiin jo sen lähettämistä edeltävässä kokouksessa sekä saatekirjeenä toimivan sähköpostin lähetti työn tilaaja, ei allekirjoittanut.

2.2.2 Teemahaastattelu

Kyberturvallisuus on Suomessa erittäin tuore ilmiö ja siihen liittyvä asiantuntemus on näin ollen harvojen ja valikoitujen henkilöiden käsissä. Tästä syystä työhön päätettiin ottaa toiseksi tiedonkeruumenetelmäksi haastattelu. Haastattelujen avulla pyrittiin löytämään jo hyödyllisiksi koettuja toimintatapoja edellisistä kyberharjoituksista niin Suomessa kuin ulkomaillakin. Lisäksi koettiin tarpeelliseksi haastatella työn tilaajan roolissa olevaa hankepäällikköä, jotta saataisiin dokumentoitua työn tavoitteet, VIRT-toiminnan tausta sekä se, mitä harjoitusmallilta halutaan. Haastatteluissa käytetyt kysymykset löytyvät liitteestä 2.

Haastattelutyypiksi valittiin teemahaastattelu ja rakenteeksi puolistrukturoitu haastattelu. Teemahaastattelulle tyypillistä on se, että haastattelun kysymykset juontavat juurensa jonkin tietyn teeman tai aiheen ympärille. Kysymykset itsessään voivat keskittyä hyvinkin erilaisiin yksityiskohtiin, mutta taustalla oleva teema pysyy samana. Puolistrukturoidulla haastattelulla tarkoitetaan sitä, että haastattelijalla on ennalta sovitut kysymykset, mutta rakenteesta voidaan poiketa haastattelijan toimesta, jos keskustelua halutaan ohjata johonkin tiettyyn suuntaan tai saada tietoa jostain teemaan liittyvästä ennakkoon tunnistamattomasta asiasta. Samaten voidaan myös jättää kysymättä haastattelun aikana turhiksi koettuja kysymyksiä. (Ojasalo ym. 2014, 107-108; Eskola & Suoranta 2000, 86)

Haastattelut pyrittiin pitämään ohjeen mukaisesti tiiviinä ja kysymykset pyrittiin miettimään tarkasti etukäteen, että haastattelun vaikuttavuus olisi mahdollisimman suuri (Metsämuuronen 2001, 42-43). Kaikki haastattelut nauhoitettiin haastatteluhetkellä ja tämän jälkeen kirjoitettiin auki eli litteroitiin. Tällä tavoin haastattelija pystyi keskittymään täysin siihen mitä haastateltava hänelle kertoo. Litterointi on tyypillisesti hyvä tehdä mahdollisimman pian haastattelutilaisuuden jälkeen. Näin haastattelussa käsiteltävät asiat ovat tuoreena mielessä. Litteroinnin tulisi myös olla mahdollisiman sanatarkkaa, sillä haastattelun analyysissä pienetkin litteroinnissa tapahtuneet virheet voivat johtaa virheanalyyseihin tai väärinkäsityksiin. (Ojasalo ym. 2014, 107)

Hirsjärven ym. (2013, 206) mukaan teemahaastattelun pituuden tulisi olla vähintään tunti. Tämän työn kontekstissa haastatteluiden aiheet olivat kuitenkin erittäin rajattuja ja täten haastattelujen pituudet vaihtelivat noin puolesta tunnista tuntiin. Haastattelutilaisuuksia ei myöskään haluttu keinotekoisesti pidentää.

Haastateltavat pyrittiin valitsemaan tarkasti, jotta kaikki työn kannalta tarpeelliset näkökulmat tulisi tutkittua. Gillhamin (2005, 78-79) mukaan asiantuntijoiden haastattelussa on erityistä se, että asiantuntijoilla on henkilökohtaista ja usein dokumentoimatonta tietoa oman erikoisosaamisensa alueelta. Tähän tietoon haastatteluilla pyrittiin pääsemään käsiksi.

2.2.3 Havainnointi

Kolmantena tiedonkeruumenetelmänä käytettiin havainnointia. Havainnointi on hyvä tiedonkeruumenetelmä havaintojen tekemiseen tapahtumien luonnollisissa ympäristöissä. Havainnointi vaatii myös huolellista valmistautumista ennen itse tapahtumaa. Havaintojen tekijän eli havainnoijan roolin voi vaihdella ulkopuolisesta tarkkailijasta aktiivisesti osallistuvaan rooliin, kunhan tapahtumaan osallistuminen ei häiritse havaintojen tekemistä ja dokumentointia. (Ojasalo ym. 2014, 114-116; Vilkka 2006, 43-44)

Havainnoinnissa olennaista on systemaattinen tarkkailu ja havaintojen dokumentoiminen. Dokumentointia varten on usein tarpeellista luoda etukäteen jonkinlainen tiedonkeruulomake, johon havainnot kerätään. Havainnoijan tulisi myös olla tilaisuudessa objektiivisessa asemassa ettei havainnoinnin tulokset vääristy tarkkailijan ennakkoasenteet vääristä tuloksia. Koska havainnoija ei pysty havainnoinnin aikana kirjaamaan jokaikistä asiaa ylös, on havainnoijalla oltava kyky ymmärtää mitkä ovat kulloinkin olennaiset kirjattavat asiat. Havainnoijalla tulee usein siis myös oltava jonkinasteista asiantuntemusta aiheesta. Havainnoijan tulisi kuitenkin mahdollisimman hyvin pitää erillään havainnot sekä omat tulkintansa ja mielipiteensä havainnointavista aiheista. (Hirsjärvi ym. 2013, 213-214; Ojasalo ym. 2014, 115-116)

Tässä työssä havainnointia käytettiin tiedonkeruumenetelmänä harjoitusten aikana. Ennen harjoituksia luotiin harjoituksia varten räätälöity havainnointilomake, jota havainnoija käytti tiedon keräämiseen. Havainnointilomake oli yksinkertaistettu versio esimerkiksi FEMA:n (2012) ja Phelpsin (2010, 160-161) käyttämistä havainnointilomakkeista. Havainnointilomakkeen ja harjoituksissa esitettyjen PowerPoint-esitysten välille myös luotiin värikoodattu numerointijärjestelmä, jotta havainnoija tietäisi kokoajan missä kohtaa harjoitusta mennään. Havainnointilomake löytyy liitteestä 3.

Phelpsin (2010, 160-161) mallissa käytetään yhdistettyä ”inject listiä” eli syötelistaa ja havainnointilomaketta. Syötelista on tarkoitettu harjoituksen vetäjälle eli fasilitaattorille syötekohtaisia muistiinpanoja varten, joiden avulla hän pyrkii kertomaan käsikirjoituksen mukaista pohjatarinaa tilaisuuteen osallistuville. Havainnointilomake on tyypillisesti tästä erillinen työkalu, joka ei sisällä muuta kuin yksinkertaisen kuvauksen syötteestä.

FEMA:n (2012) mallissa havainnointilomake on erillään fasilitaattorin muistiinpanoista. Tässä mallissa havainnointilomake on kuitenkin monisarakkainen ja vaikeakäyttöinen, joten lomaketta oli tarpeen yksinkertaistaa. Koettiin, että harjoitustilanteessa ei ole aikaa täyttää monta eri saraketta, etenkin jos keskusteluvuorot vaihtuvat usean puhujan välillä. Lisäksi havainnoijalla oli harjoitusten aikana puoliaktiivinen rooli, minkä vuoksi mahdollisimman yksinkertainen havainnointilomake koettiin parhaaksi vaihtoehdoksi.

2.3 Analysointimenetelmät

Tiedonhakumenetelmien tuottamia tuloksia pyrittiin analysoimaan laadulliselle tutkimukselle tyypillisiä analysointimenetelmiä käyttäen. Hirsjärven ym. (2013, 224-225) mukaan laadullisen tutkimuksen analyysimenetelmien käyttämisessä pääpainona on aineiston ymmärtäminen. Hirsjärvi ym. (2013, 224) lisäävät, että aineistosta saaduilla tuloksilla ei useimmissa tapauksissa voida selittää ilmiöitä, vaan korkeintaan antaa suuntaa sille, kuinka tutkittua ilmiötä kannattaa tulkita. Laadullisen näkökulman vuoksi esimerkiksi kyselyn ja havainnoinnin osalta sopivien analyysimenetelmien löytäminen oli haastavaa.

Kyselyiden tulosten analyysissä suurimpana ongelmana oli se, että niin perusjoukon kuin vastanneiden lukumäärät olivat pieniä puhtaasti asiantuntijajoukon lukumäärän vuoksi. Tämän takia kaikki kvantitatiiviset analyysimenetelmät suljettiin pois käytöstä. Aineiston ymmärtämisen parantamiseksi saadut vastaukset siirrettiin kyselytyökalusta Excel-taulukkoon, jolloin tietoa pystyttiin tarkastelemaan tarkemmin sekä visualisoimaan. Tulosten visualisointi kuvioiksi tai taulukoiksi koettiin työn tilaajan näkökulmasta tärkeäksi, sillä kyselyn tuloksia päästiin sitä kautta esittelemään seuraavassa häiriöhallintaryhmän kokouksessa.

Haastattelujen osalta analyysimenetelmänä käytettiin teemoittelua. Haastattelumateriaalin analyysissä käytettiin Ojasalon ym. (2014, 110-111) ohjetta tiedon käsittelystä, analysoinnista ja tulkinnasta. Haastatteluiden analyysissa ensimmäisenä vaiheena oli äänitteiden auki kirjoittaminen eli litterointi. Litterointi pyrittiin tekemään mahdollisimman pian haastattelun jälkeen. Litteroinnin jälkeen aineistoa pyrittiin luokittelemaan aihealueittain ja teemoittain, minkä jälkeen voitiin paremmin hahmottaa linkki aiheyhteyteen ja hyödyntää haastattelussa hyödylliseksi aineistoksi koettua tietoa. Huomionarvoista oli kuitenkin se, että haastateltavat pyrittiin kuitenkin valitsemaan siten, että jokaisella olisi harjoitusmallin kehittämisen kannalta annettavanaan erilainen näkökulma oman erityisasiantuntemuksensa takia.

Havainnoinnin kannalta analyysimenetelmänä käytettiin aineiston pelkistämistä sekä tulkitsemista (Ojasalo ym. 2014, 119). Yksikin harjoitus tuottaa havainnoinnin kautta hyvin monipuolista ja rönsyilevää tietoa, minkä takia tärkeimpien havaintojen ja suuntaviivojen löytäminen kerätyn aineiston joukosta oli erittäin tärkeää. Tärkeimpien havaintojen löytämisen jälkeen tietoa pyrittiin tulkitsemaan yhteistyössä työn tilaajan kanssa.

Havainnoinnin tulosten analyysillä oli kaksi vaikutusta. Ensimmäisenä vaikutuksena oli antaa opinnäytetyöprosessiin viitteitä siitä, kuinka hyvin pöytäharjoitus toimii harjoitteluvälineenä ja miten hyvin se toimii keskustelun herättäjänä. Toinen vaikutus oli tärkeä VIRT-toiminnan kehittämisen kannalta, sillä havainnoinnin tuloksena harjoituksista saatava tieto saatiin dokumentoitua ja myöhemmin hyödynnettyä.

3 Harjoitusmallin luominen

Tässä luvussa kuvataan niitä askelia mitä opinnäytetyöprosessin aikana tehtiin kohti harjoitusmallin ensimmäistä versiota. Ensin luvussa kuvataan millä taustalla kirjoittaja loi ensimmäisen työssä kuvatun harjoituksen ja kuinka se toteutettiin. Tämän jälkeen on kuvattu mitä tuloksia harjoituksen jälkeen tehdyllä palautekyselyllä ja haastatteluilla saatiin.

3.1 Työharjoittelu Valtiovarainministeriössä

Kirjoittaja aloitti Valtiovarainministeriössä harjoittelijana heinäkuussa 2014. Työharjoittelun oli määrä kestää noin kymmenen viikkoa ja toimia toisena Laurean harjoittelujaksoista. Harjoittelun pituutta lopulta kuitenkin jatkettiin kolmella kuukaudella, jatkuen vuoden loppuun saakka.

Sijoittautuminen ministeriössä tapahtui Julkisen hallinnon tieto- ja viestintätekniseen toimintoon ja sen alaisuudessa toimivaan Vaatimukset ja suositukset-yksikköön (nyk. Kyberturvallisuus ja infrastruktuuri-yksikkö). Työnkuva ministeriössä koostui pääasiassa SecICT-

hankkeeseen liittyvistä avustamistehtävistä sekä tiedonkeruusta. Tämän lisäksi harjoitteluun sisällytettiin myös VAHTI-toimintaan littyviä työtehtäviä.

Harjoittelun pituuden pidennyksen jälkeen koettiin, että harjoittelun loppuajalle olisi mielekästä saada jonkin laajempi projekti, joka tukisi itsenäistä työskentelyä ja innovointia. Tässä vaiheessa VIRT-ryhmän toiminta oli juuri käynnistetty ja alustavia suunnitelmia ensimmäisestä harjoituksesta oli jo tehty. Näin ollen tehtäväksi asetettiin harjoituksen luominen VIRT-ryhmälle, mikä järjestettiin työharjoittelun loppupuolella joulukuussa 2014.

3.2 Ensimmäinen harjoitus

Harjoituksen aihioksi valittiin pöytäharjoitus, sillä se koettiin VIRT-ryhmän kokoon nähden soveltuvimmaksi, kustannustehokkaimmaksi ja kevyimmäksi tavaksi harjoitella yhdessä. Myös Phelpsin (2010, 151) mukaan yksinkertainen pöytäharjoitus on yksi helpoimmista tavoista järjestää harjoitus pienelle ihmisjoukolle. Pöytäharjoitus on nimensä mukaisesti harjoittelutyyppi, jossa harjoitettava joukko istuu kirjaimellisesti tai kuvainnollisesti yhden pöydän ääressä. Yksinkertainen pöytäharjoitus ei täten tyypillisesti pidä sisällään suuremmille harjoituksille tyypillisiä simulaatioelementtejä tai ns. ”hands-on” toimintaa.

Ensimmäiselle harjoitukselle oli varattu aikaa noin kolme tuntia, mikä osoittautui suunnittelun kannalta melko pitkäksi ajaksi. Arvioitiin, että itse harjoitusosio tulisi kestämään noin kaksi ja puoli tuntia, kun otettaisiin huomioon tilaisuuden aloitus, tauko sekä palauttelle varattu aika. Näinkin pitkä aika harjoittelulle tarkoitti täten sitä, että harjoiteltavia skenaarioita tulisi olla useampia ja niiden tulisi olla kysymysten asettelultaan monitahoisia. Perusrakenteeltaan harjoituksesta tehtiin yksinkertainen. Esitysvälineeksi valittiin valtiohallinnossa yleisesti käytössä oleva Microsoft PowerPoint-työkalu.

Esityksen alussa käytiin läpi harjoituksen tavoiteet, osallistujat sekä muutamia ohjeita ”pelin” pelaamiseen. Itse harjoitusosio käynnistyi harjoituksen maailman kuvauksella, mikä tyypillisesti tapahtuu näyttämällä harjoitusta varten tehtyjä kuvia tai uutisartikkeleita, joilla pyritään luomaan harjoitukselle taustatarinaa sekä johdattaa ensimmäiseen syötteeseen.

Syötteellä tarkoitetaan tiettyyn skenaarioon liittyvää esitettävää tilannetta, johon harjoitukseen osallistuvat reagoivat. Koska pöytäharjoituksessa syötteisiin ei voida reagoida toiminnallisesti, seuraa syötteen jälkeen keskusteluosio skenaarion pohjalta. Harjoitusta suunnitellessa huomattiin, että syötteen jälkeisten keskusteluun johdattavien kysymysten suunnitteluun kannattaa varata runsaasti aikaa, sillä ne ovat pöytäharjoituksessa primäärinen keskustelua ohjaava voima. Harjoituksen vetäjän rooli korostuu, jos kysymykset ovat puuttellisia eivätkä ohjaa keskustelua asetettujen tavoitteiden suuntaan.

Koska VIRT:n fokuksena on keskittyä kehittämään valtiohallinnon keinoja ja yhteistyökykyä kyber- ja tietoturvallisuuden uhkia vastaan, keskityttiin skenaarioiden luomisessa lähinnä tietoverkkoihin- ja järjestelmiin kohdistuviin uhkiin eikä esimerkiksi fyysiseen turvallisuuteen liittyviin uhkiin. Asiantuntijoiden korkea tietotaidon taso merkitsi myös sitä, että skenaarioiden pitäisi pureutua arkaluontoisempiin ja merkittävämpiin aiheisiin kuin esimerkiksi palvelunestohyökkäyksiin tai muihin ”arkipäiväisiin” uhkiin, joihin on jo varauduttu monen vuoden ajan.

Ensimmäisen harjoituksen kantavaksi teemaksi tulivatkin APT (Advanced Persistant Threat)-tyyppiset hyökkäykset, joissa hyökkääjällä olisi aikaisempaa tietoa esimerkiksi valtiohallinnon tietojärjestelmien verkkoarkkitehtuurista tai prosesseista. APT-hyökkäyksellä tarkoitetaan kohdistettua haittaohjelmahyökkäystä, missä hyökkääjä on huolellisesti suunnitellut iskevänsä juuri tiettyyn kohteeseen. (Mowbray 2014, 29)

Lopulliseen harjoitukseen kehitettiin lopulta noin kymmenen eri skenaariota. Skenaarioiden kehittämisessä käytettiin apuna muun muassa Yhteiskunnan turvallisuusstrategiaa (Puolustusministeriö 2010) sekä Kyberturvallisuusstrategiaa (Turvallisuuskomitean sihteeristö 2013). Näistä strategioista löytyi hyviä suuntaviivoja skenaarioiden kehittämiseen, etenkin useampien eri hallinnonalojen näkökulmien huomioonottamisessa. Harjoitukseen osallistuvien kannalta tämä on myös merkittävä asia – toimintaan kuuluvien asiantuntijoiden roolit voivat poiketa hyvin paljon toisistaan, mikä tarkoittaa sitä, että skenaarioiden keskusteluosuuksissa voidaan löytää hyvin erityyppisiä näkökulmia tai kokemuksia erilaisiin tilanteisiin.

3.3 Palautekyselyn tulosten analyysi

Ensimmäisen harjoituksen jälkeen harjoituksessa mukana olleille lähetettiin sähköpostitse pyyntö vastata palautekyselyyn koskien pidettyä harjoitusta. Palautekyselyssä oli yhteensä 14 kysymystä, joista yksi oli avoin kysymys ja loput monivalintakysymyksiä. Vastaajamäärä tässä kyselyssä oli yhdeksän henkilöä, mikä tarkoittaa sitä, että noin puolet potentiaalisista vastaajista saavutettiin kyselyllä. Tämä koettiin työn tilaajan näkökulmasta kelvolliselta vastausmäärältä valtiohallinnossa. Myös Vehkalahden (2014, 44) mukaan kyselytutkimusten vastausprosentti saattaa useinkin jäädä alle 50 % prosentin.

Tulosten esittelyyn on valittu muutamia palautekyselyn tulosten kuvastavimpia kysymyksiä kuvioiksi. Kysymykset olivat jaettu viiteen eri kategoriaan: skenaariot, keskustelu, tavoitteeseen pääseminen, kokonaisuus sekä harjoituksen pituus. Skenaario-kategoriassa kysyttiin kysymyksiä liittyen skenaarioiden realistisuuteen, ajankohtaisuuteen ja relevanssiin asiantuntijan organisaatioon nähden. On huomionarvoista, että skenaarioita oli lähes kymmenen ja ne vaihtelivat toisistaan paljonkin. Kyselyn kysymykset löytyvät liitteestä 1.

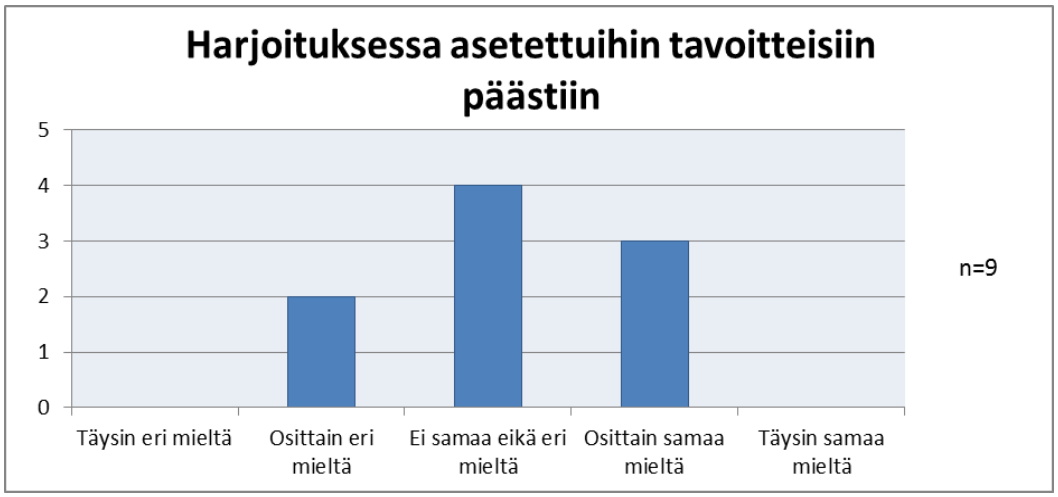
Skenaarioiden ajankohtaisuus on toiminnan kannalta välttämätöntä. Häiriöhallintaryhmän kannalta olisi ajan haaskausta harjoitella skenaarioita, joihin on jo valmiiksi mietittyjä ratkaisuja tai uhat ovat vakavuusasteeltaan matalasta päästä. Kyselyyn vastanneista asiantuntijoista jokainen oli vähintään osittain samaa mieltä väittämästä ”harjoituksen skenaariot olivat ajankohtaisia”. Parantamiseenkin jäi vielä varaa, mutta on huomionarvoista että erinomaisten skenaarioiden luomiseen tarvittaisiin erittäin syvällistä tietoa valtion kybertoimintaympäristöjen heikkouksista.

Yhdeksi kyselyn tärkeäksi näkökulmaksi haluttiin ottaa asiantuntijoiden kokemus siitä, onko harjoittelusta hyötyä heidän omille organisaatioilleen. Kuten jo aikaisemmin mainittiin, harjoitusten skenaariot vaihtelivat laidasta laitaan, joten skenaarioiden omakohtaisuus saattoi vaihdella skenaarioittain. Vastaustulokset (kuvio 2) antoivat kuitenkin positiivisen kuvan siitä, että harjoituksessa harjoiteltiin oikeansuuntaisia ja laajavaikutteisia häiriötilanteita.

Kuvio 2. Ensimmäinen kysely - skenaarioiden omakohtaisuus

Tavoitteiden asettaminen ja niihin pääseminen ovat harjoituksen kulmakiviä onnistumisen mittaamisessa. Kyselyssä kysyttiin monia harjoituskokemukseen liittyviä kysymyksiä, mutta tärkeimpinä kysymyksinä kaikista olivat kaksi tavoitteisiin pääsemiseen liittyvää kysymystä. Kuten kuviosta 3 voidaan tulkita, on tavoitteisiin pääsemisen onnistumiseen vastattu niin kielteisesti kuin positiivisestikin.

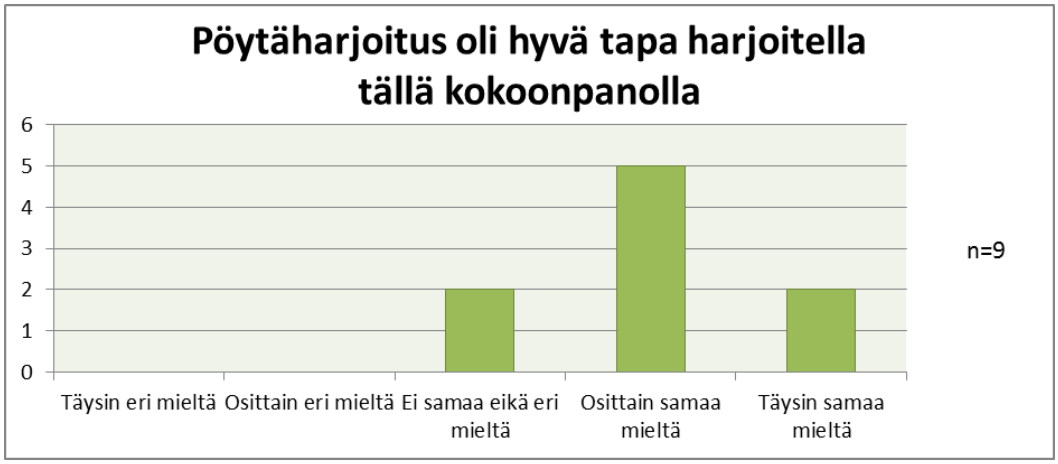
Poikkeuksellisesti moni oli myös vastannut keskimmäisen vaihtoehdon, mikä voi kieliä monesta eri asiasta. Työn tilaajan kanssa asiasta keskustellessa tultiin siihen johtopäätökseen, ettei harjoituksen tavoitteita oltu rajattu tarpeeksi selkeästi ja että rajausta tulisi ehdottomasti parantaa seuraavaan harjoitukseen.



Kuvio 3. Ensimmäinen kysely - tavoitteisiin pääseminen

Harjoituksen onnistumista haluttiin myös mitata kokonaisuutena, mihin sisältyy niin harjoituksen sisällön lisäksi myös tilan soveltuvuus, laitteiden toimivuus, harjoituksen pituus ynnä muita seikkoja. Kyselyyn vastanneista asiantuntijoista suurin osa (7/9) oli osittain samaa mieltä väittämän ”harjoitus oli kokonaisuutena onnistunut” kanssa. Loput kaksi vastaajaa olivat väittämän kanssa täysin samaa mieltä.

Kuviossa 4 on esitetty tulokset kyselyssä kysyttyyn kysymykseen pöytäharjoituksen soveltuvuudesta häiriöhallintaryhmän harjoitteluvälineeksi. Suurin osa vastaajista on jälleen kokenut pöytäharjoituksen ainakin osittain soveltuvaksi välineeksi harjoitteluun. Kovin moni ei kuitenkaan ole ollut väitteen kanssa täysin samaa mieltä.

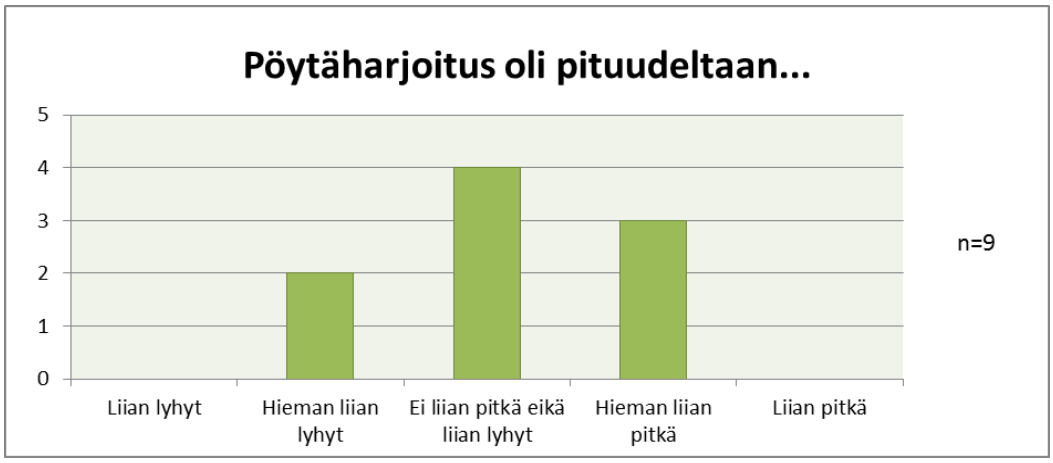


Kuvio 4. Ensimmäinen kysely - pöytäharjoituksen soveltuvuus

Työn tilaajan kanssa tehdyn pohdinnan jälkeen tultiin siihen tulokseen, että pöytäharjoituksen ei tulisi olla ainoa käytössä oleva harjoitteluväline, vaan sen lisäksi voitaisi kehittää täy-

dentäviä harjoittelumenetelmiä. Muut harjoitusmenetelmät voisivat olla pöytäharjoitusta suppeampia että laajempia toiminnallisia keinoja harjoitella.

Kyselyn viimeisenä kysymyksenä esitettiin kysymys harjoituksen pituudesta. Ensimmäisen harjoituksen pituus oli vajaa kolme tuntia tauot mukaanluettuna. Kuviossa 5 esitetyt vastaustulokset ovat hajaantuneet kolmen vastauksen kesken. Suurin osa vastaajista koki harjoituksen pituuden sopivaksi, mutta myös huomattava osa koki harjoituksen liian pitkäksi. Tästä syystä seuraavan harjoituksen kohdalla päätettiin kokeilla lyhyempää mallia. Toisen harjoituksen päätteeksi tehdyssä kyselyssä kysyttiin sama kysymystä, mistä voitiin tehdä täten jatkopäätelmiä sopivasta harjoituksen pituudesta.



Kuvio 5. Ensimmäinen kysely - harjoituksen pituus

3.4 Teemahaastatteut

Työssä haastateltiin kolmea valtiohallinnon asiantuntijaa kolmesta eri organisaatiosta. Haastateltavien valinnat tehtiin siitä näkökulmasta katsoen, että haastatteluista saataisiin mahdollisimman monipuolista tietoa harjoitustoiminnan kehittämisen kannalta kriittisistä aiheista. Haastatteluiden tarkoituksena oli kerätä tietoa Suomessa ja ulkomailla järjestetyistä kyberharjoituksista, niihin liittyvistä kokemuksista ja hyväksi todetuista käytännöistä harjoitusten suunnittelussa. Haastatteluista kerätty aineisto luokiteltiin alla olevien kappaleotsikoiden mukaisesti. Haastattelukysymykset löytyvät liitteestä 2.

3.4.1 Haastatellut asiantuntijat

Kirsi Janhunen on Valtiovarainministeriön JulkICT-toiminnon alaisuudessa toimivan SecICT-hankkeen hankepäällikkö ja toimii ministeriössä erityisasiantuntijana. Hän on toiminut hankkeen vetäjänä vuodesta 2013 asti. Janhusella on yli kymmenen vuoden työkokemus erilaisista työtehtävistä tieto- ja kyberturvallisuuden osa-alueilla. Ennen Valtiovarainministeriöön tulo-

aan hän toimi Valtion IT-palvelukeskuksessa (nyk. Valtion tieto- ja viestintätekniikkakeskus Valtori) tietoturvallisuusasiantuntijana. Hänen työnkuvaansa kuuluvat laajat julkisen hallinnon ICT-ohjaukseen liittyvät asiantuntijatehtävät.

Antti Sillanpää toimii Turvallisuuskomitean sihteeristössä erikoistutkijana. Hän on toiminut aikaisemmin erikoistutkijana Puolustushallinnossa sekä Maanpuolustuskorkeakoulussa. Koulutustaustaltaan hän on tekniikan tohtori, minkä lisäksi hän on suorittanut maisterin tutkinnot Helsingin kauppakorkeakoulusta pääaineenaan laskentatoimi sekä Helsingin yliopistosta, missä hänen pääaineenaan oli kansainvälinen politiikka. Sillanpään osallistuminen kyberturvallisuuden kehittämiseen valtiohallinnossa perustuu Turvallisuuskomitean kirjoittamaan Kyberturvallisuusstrategiaan, jonka toimeenpanoa Turvallisuuskomitean sihteeristö valvoo.

Antti Kiuru toimii Kyberturvallisuuskeskuksessa tilannekeskusryhmän päällikkönä. Hän on ollut Viestintäviraston palveluksessa noin seitsemän vuoden ajan ja nykyisessä työssään noin kaksi ja puoli vuotta. Aikaisemmin hän on työskennellyt muunmuassa tietoturva-asiantuntijana. Hänen tämänhetkiseen työnkuvaansa kuuluu tilannekeskusryhmän johtaminen, toiminnan suunnittelu sekä Viestintäviraston yhteyspisteen ympärivuorokautisen tilannekuvan ylläpitämisen varmistaminen.

3.4.2 Kokemukset kansallisista kyberharjoituksista

Kaikki asiantuntijat nostivat kansallisista harjoituksista päällimmäiseksi kolme eri harjoitusta; TIETO-harjoituksen, VALHA-harjoituksen sekä KYHA-harjoituksen. Näistä TIETO- ja KYHA-harjoitukset keskittyvät olennaisesti tieto- ja kyberturvallisuuteen liittyvien asioiden harjoittelemiseen. Näissä myös vetovastuu on ollut pääasiassa Puolustusvoimien harteilla.

VALHA-harjoitus on valtiohallinnon valmiusharjoitus, jonka tehtävänä on harjoittaa valtion ylintä johtoa ja virkamiesjohtoa yhteiskunnan poikkeustilanteissa toimimiseen. Luonteeltaan VALHA on pitkälti päätöksentekoon keskittyvä harjoitus ja se järjestetään vain kerran hallituskauden aikana. Virkamiesjohdon näkökulmasta harjoitus kestää noin viikon, kun taas valtionjohto on paikalla vain osan ajansta. Vuoden 2013 VALHA-harjoituksen pääteemana oli ensi kertaa kyberturvallisuus. (Sillanpää 2015)

TIETO-harjoitus on edellämainituista erityisesti tietoturvallisuuden ja viestintäalan kriisivalmiuden vahvistamiseen suunnattu tekninen harjoitus. Se järjestetään joka toinen vuosi. Harjoitukseen osallistuvat pääsääntöisesti asiantuntijat, jotka ovat mukana käytännön toiminnassa taktisella tasolla, esimerkiksi tekemässä korjaustoimenpiteitä. Harjoitus kestää tyypillisesti noin kolmesta neljään päivään. Harjoituksen keskeisenä toimijana on Puolustusvoimien lisäksi Liikenne- ja viestintäministeriö. (Kiuru 2015; Sillanpää 2015)

KYHA-harjoitus on nimenomaisesti kyberturvallisuuteen liittyvä harjoitus, joka järjestettiin ensi kertaa vuonna 2013. Harjoituksen järjestää Puolustusvoimat yhteistyössä Jyväskylän Ammattikorkeakoulun kanssa ja se kestää noin viisi päivää. Harjoitus on tarkoitus järjestää jatkossa joka toinen vuosi. (Sillanpää 2015)

Yleisesti haastateltavat kokivat, että kokonaisuutena kansallisista kyber-ja tietoturvallisuuteen liittyvistä harjoituksista on ollut hyötyä ja niiden merkitys on erittäin tärkeä valtiohallinnossa. Harjoituksissa päästään työskentelemään muiden viranomaisten kanssa ja luomaan verkostoja. Harjoitukset voivat myös olla hyvin herättäviä kokemuksia joillekin organisaatioille, joille esimerkiksi kyberturvallisuuteen liittyvät asiat eivät ole arkipäivää. Poikkihallinnollisuus nähtiin yleisesti positiivisena seikkana; muiden kuuleminen ja toisten toimintatapojen oppiminen koettiin hyödyllisenä. Teknisen puolen asiantuntijat myös oppivat siitä, millaista tilannekuvaa ylempi johtoporras tarvitsee päätöksenteon tueksi. (Janhunen, 2015; Kiuru 2015; Sillanpää 2015)

Parannettavaa kansallisista harjoituksista asiantuntijat löysivät monelta eri osa-alueelta. Janhusen (2015) mukaan viimeisimmissä harjoituksissa on törmätty usein samantyyppisiin ongelmiin, ja näihin pääasiassa hallinnollisiin ja kommunikaatioon liittyviin seikkoihin tulisi kiinnittää enemmän huomiota harjoitusten suunnittelussa. Myös yllämainittujen harjoitusten ja pöytäharjoitusten väliin toivottiin laajuudeltaan jotain välimallin harjoitusta. Sillanpään (2015) mukaan ongelmana on myös ollut se, että harjoitukseen saapuvat asiantuntijat eivät ole aina niitä henkilöitä joiden tosiasiassa pitäisi olla paikalla. Hänen mukaansa harjoituksiin pitäisi saada aina organisaatioista sellaisia ihmisiä, jotka tosiasiassa voivat vaikuttaa mielipiteisiin omassa organisaatiossaan. Yleisen tietoisuuden lisäämisen näkökulmasta ei siis ole aina parasta, että harjoituksissa on paikalla esimerkiksi organisaation tietoturvapäällikkö.

3.4.3 Kokemukset kansainvälisistä kyberharjoituksista

Suomen edustajat kansainvälisiin kyberharjoituksiin ovat tulleet perinteisesti pääasiassa Viestintävirastosta ja nykyään sen alaisuudessa toimivasta Kyberturvallisuuskeskuksesta. Kiurun (2015) mukaan Suomella on ollut edustusta pääasiassa neljässä eri harjoituksessa: ENISA:n järjestämässä Cyber Europe-harjoituksissa, Pohjoismaiden CERT-yhteistyön harjoituksissa sekä NATO:n jäsenmaiden sekä NATO:n rauhankumppanuusmaiden yhteisissä Cyber Coalition- ja Locked Shields-harjoituksissa. Näiden lisäksi järjestetään joukko pienempiä kommunikaatioharjoituksia, jotka sisältävät pienimuotoista yhteydenpidon harjoittelua ja testausta.

Harjoitukset ovat olleet hyvinkin erityyppisiä ja ne ovat keskittyneet niin teknisen puolen harjoitteluun kuin myös operatiivisen ja strategisen tason päätöksenteon harjoitteluun. Yllä mainittuja harjoituksia järjestetään useimmiten joka vuosi tai joka toinen vuosi. Harjoituksiin on

usein varattu paljon resursseja ja puitteet ovat olleet ensiluokkaa. Harjoitukset sitovat resursseja vastavuoroisesti myös osallistujamaalta. Kyberturvallisuuden teemalla kulkevat harjoitukset ovat yleistyneet 2010-luvulle siirryttäessä. (Kiuru 2015)

Kokemukset kansainvälisistä harjoituksista ovat olleet lähes poikkeuksetta positiivisia. Tärkeimpänä hyötynä pidettiin asiantuntijoiden tutustumista ulkomaisiin kolleegoihin ja etenkin uusiin toimintatapoihin. Usein tapahtumissa on kohdattu työskentelytapoja tai välineitä mitä kotimaassa ei ole koskaan kohdattu tai hyödynnetty. (Kiuru 2015)

3.4.4 Hyödynnettävyys VIRT-toimintaan

Kaikki kolme asiantuntijaa pitivät VIRT-toimintaa sekä siihen liittyvää harjoitustoimintaa hyödyllisenä. Pöytäharjoitusten järjestäminen kyseisellä kokoonpanolla nähtiin hyvänä lisänä isommille kansallisille harjoituksille ja vastaavien pienempien harjoitusten hyöty koettiin suurena. Asiantuntijat kokivat myös, että VIRT:n tyyppinen poikkihallinnollinen kommunikaatioväylä on ennen puuttunut ja että keskietyn tiedon saatavuus poikkeusoloissa helpottaisi kommunikaatiota merkittävästi. Negatiivisena asiana pidettiin osittain sitä, että häiriöhallintaryhmään osallistuvat asiantuntijat eivät välttämättä ole joka kerralla samat muista työkiireistä johtuen.

Monipäiväiset ja suunnitteluprosessiltaan usein jopa kokonaisia henkilötyövuosia vaativat harjoitukset ovat luonteeltaan hyvin erilaisia kuin tässä työssä käsitellyt kevyet harjoitukset, joten niistä saatuja kokemuksia ei välttämättä voida hyödyntää täysin pöytäharjoitusten suunnitteluun. Asiantuntijat halusivat kuitenkin korostaa kaikissa harjoituksissa suunnittelutyön tärkeyttä ja työpanoksen keskittämistä kiinnostavan ja ajankohtaisen käsikirjoituksen luomiseen.

Harjoitusten tulisi myös tuoda asiantuntijoille joka kerta jotakin uutta, sillä muutoin toiminta lakkaa olemasta hyödyllistä ja osallistujienkin kiinnostus laskee. Myös tosielämän caseesimerkkien tuomista harjoituksiin koettiin hyvänä tapana sitouttaa harjoitussisältö tosielämän organisaatiorakenteisiin ja toimintatapoihin. Yhdistelmä salassapidettävästä tiedosta, tilannekuvatiedosta sekä julkisesta tiedosta harjoituksessa nähtiin hyvänä ja innostavana tapana esitellä skenaarioita.

Uudenlaisena työtapana korostettiin myös tutkimusongelmalähtöistä harjoittelua ja ylipäätään selkeiden tavoitteiden asettamisen tärkeyttä jo aikaisin suunnittelutyössä. Usein olemassa olevat ongelmat ovat jo tiedossa, joten niihin tarttuminen ja läpiluotaava analysointi asiantuntijoiden kesken voisi auttaa ongelmien ratkaisemisessa.

4 Harjoitusmallin soveltaminen

Tässä luvussa kuvataan kuinka luotua harjoitusmallia sovellettiin seuraavan harjoituksen luomiseen ja yleiseen harjoitustoiminnan kehittämiseen. Toiseen harjoitukseen osallistuneille lähetettiin harjoituksen jälkeen vastauspyyntö palautekyselyyn, jolla mitattiin jälleen harjoituksen onnistumista ja tavoitteisiin pääsemistä. Uusina kysymyksinä kyselyyn tuotiin harjoitusmalliin liittyvän kiinnostuksen mittaamiseen suunnattuja kysymyksiä.

4.1 Toinen harjoitus

Ensimmäisen harjoituksen sekä tiedonkeruuvaiheen jälkeen oli tärkeää päästä hyödyntämään löydettyä uutta tietoa. Paras tapa testata harjoitusmallin toimivuutta ja uuden tiedon paikkaansapitävyyttä oli järjestää uusi harjoitus. Ensimmäisen harjoituksen jälkeen annetun palautteen sekä asiantuntijahaastatteluiden pohjalta oli selvää, että harjoituksen suunnitteluun tulisi kiinnittää entistä enemmän huomiota. Myös harjoituksen tavoitteiden tulisi olla selkeämmät ja konkreettisemmat, jotta niiden mittaaminen olisi helpompaa. Tavoitteiden määrittämisen lisäksi harjoitukselle asetettiin tutkimusongelma.

Palautekyselyn tulosten perusteella myös päätettiin, että toinen harjoitus tulisi olemaan noin puolitoista tuntia pitkä, noin tunnin lyhyempi kuin ensimmäinen harjoitus. Harjoitukseen tuotiin myös uutena elementtinä asiantuntijoiden osallistuminen harjoitukseen etäyhteyden avulla. Harjoitukseen osallistui hieman vähemmän asiantuntijoita ja harjoitukselle valittu tila oli pienempi verrattuna ensimmäiseen harjoitukseen. Pienemmän tilan valinnalla mahdollistettiin etäyhteyksien käyttö, mutta sen toivottiin myös vapauttavan keskustelua ja luomaan tilaisuuteen rennompaa tunnelmaa.

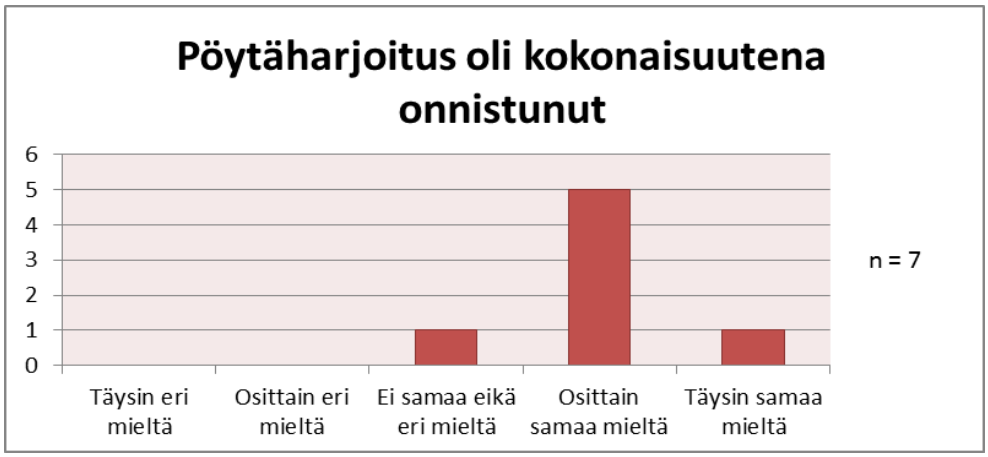
Skenaarioiden määrää laskettiin lyhentyneen ajan vuoksi sekä keskusteluille varattiin enemmän aikaa. Yhteensä harjoituksessa oli neljä skenaariota, joista kullekin varattiin aikaa noin kaksikymmentä minuuttia. Skenaariot pyrittiin jälleen linkittämään toisiinsa taustatarinan ja käsikirjoituksen avulla, luoden harjoittelutilanteeseen jonkinasteista immersiota. Skenaarioissa pyrittiin myös käyttämään paljon kuvia harjoitukseen osallistuvien asiantuntijoiden aktivoimiseen.

Tiedonkeruun pohjalta oli selkeää myös, että aiheen tai teeman valinnan tulisi tuoda tuoretta näkökulmaa VIRT-yhteistoimintaan ja käsittelemään uudentyyppisiä haasteita ensimmäiseen harjoitukseen verrattuna. Työn tilaajan kanssa käydyn keskustelun jälkeen teemaksi valittiin aihe, joka oli erittäin ajankohtainen kybervarautumisen kannalta. Harjoituksen hyökkääjätaho oli tosielämässä esittäny uhkauksia juuri harjoituksen alla, mistä syystä teema sopi harjoittelun aiheeksi erittäin hyvin.

4.2 Toisen palautekyselyn tulosten analyysi

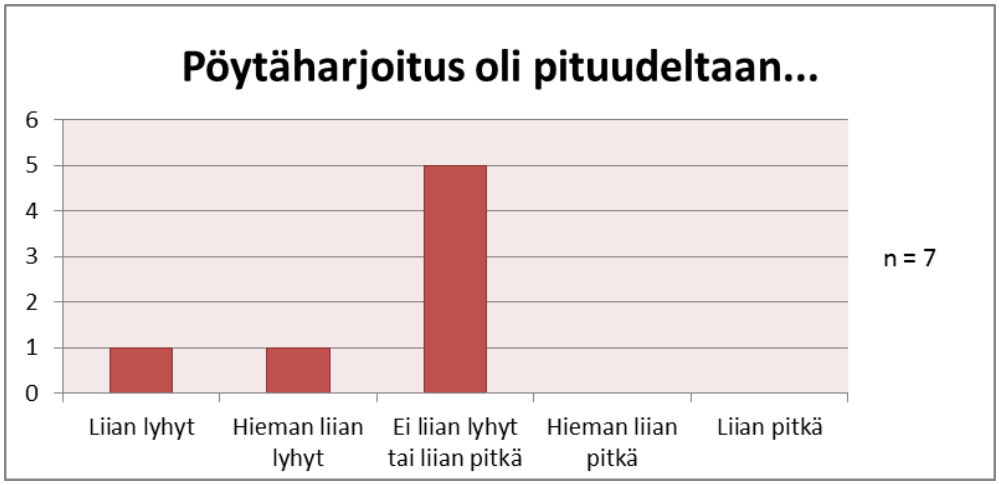
Toisen harjoituksen palautekysely oli ensimmäisen tapaan onnistunut, sillä suurin osa osallistujista vastasi siihen. Yleisesti tuloksia tarkastelemalla voitiin päätellä, että toinen harjoitus onnistui asiantuntijoiden mielestä vähintään yhtä hyvin kuin ensimmäinen ja että joillain osa-alueilla havaittiin jopa parantuneita tuloksia.

Harjoituksen aiheen ajankohtaisuus koettiin asiantuntijoiden mielestä erittäinkin positiivisena ja kaikkien mielestä aihe olisi voinut edes osittain koskettaa heidän omaa organisaatiotaan. Aiheen valinta siis onnistui. Myös aiheen pohjalta syntynyt keskustelu koettiin positiiviseksi. Kuvion 6 perusteella harjoitus oli myös jotakuinkin yhtä onnistunut kuin ensimmäinenkin.



Kuvio 6. Toinen kysely – harjoituksen onnistuminen

Harjoituksen pituutta lyhennettiin ensimmäisestä harjoituksesta noin tunnilla. Alla olevasta kuviosta 7 voidaankin huomata että lyhennetty harjoituspituus lienee jo lähellä optimia. Optimaalinen pöytäharjoituksen pituus onkin näillä näkymin noin 1,5 - 2 tuntia.



Kuvio 7. Toinen kysely - harjoituksen pituus

5 Tulokset

Tässä luvussa kuvataan opinnäytetyöprosessin tuloksena syntynyttä harjoitusmallia ja sen komponentteja. Tämän jälkeen tutkittiin kehitetyn mallin sovellettavuutta valtiohallintoon. Tutkimuksen lopullisena tuotoksena syntynyt harjoitusmalli vastasi lopulta jotakuinkin sitä mitä työn tilaajan näkökulmasta oli toivottu ja mitä työn alussa oli asetettu tavoitteeksi. Harjoitusmallin toivottiin siis tukevan ja nopeuttavan harjoitusten luomisprosessia sekä antaa eväitä pitkäjänteiseen harjoitustoiminnan kehittämiseen. Itsessään sekin oli jo positiivinen tulos, että opinnäytetyöprosessin aikana järjestettiin toinen onnistunut harjoitus.

5.1 Viimeistelty harjoitusmalli

Lopullinen harjoitusmalli koostuu neljästä eri osasta. Tärkein osa harjoitusmallia on ohjeistus harjoituksen järjestämiseen, mikä on noin kahdeksansivuinen word-dokumentti. Tämän lisäksi malliin kuului oheismateriaalina harjoituksen järjestämistä helpottava aikataulu, havainnointilomake harjoituksen aikaisen havainnoinnin helpottamiseksi sekä esimerkkiharjoitus PowerPoint-esityksenä. Harjoitusmallin komponentit löytyvät osin liitteistä 3-5.

5.1.1 Ohjeistus

Ohjeistusta lähdettiin tekemään alun perin häiriöhallintaryhmän vaatimukset mielessä pitäen. Työn edetessä huomattiin kuitenkin, että työstä voisi olla hyötyä myös muille valtiohallinnon toimijoille, joten ohjeistuksesta tehtiin mahdollisimman helposti ymmärrettävä myös aiheeseen tutustumattomille. Ohjeistus alkaa tavanomaiseen tapaan kansilehdellä, sisällysluettelolla sekä esipuheella. Tämän jälkeen ohjeistuksessa kuvaillaan minkä tyyppinen harjoitus pöytäharjoitus on. Tässä kappaleessa pyrittiin erityisesti keskittymään kuvailemaan mitä ominaisuuksia pöytäharjoituksilla on, kuinka monta osallistujaa harjoituksessa voi olla, millaiset organisaatiot tyypillisesti hyödyntävät pöytäharjoituksia ja mitkä ovat pöytäharjoituksen hyvät ja huonot puolet.

Opinnäytetyöprosessin aikana oli silmiinpistävää, kuinka tärkeää perusteellinen suunnittelutyö on harjoituksen onnistumisen kannalta. Tämä seikka kävi ilmi myös kaikkien tiedonkeruumenetelmien tuottamista tuloksista. Tämän takia ohjeistukseen varattiin kokonainen kappale pelkästään harjoituksen suunnittelulle. Suunnitteluosiossa pyrittiin antamaan lukijalle selkeät ohjeet siitä, kuinka harjoituksen tavoitteita tulisi lähteä määrittämään sekä mitkä ovat parhaat tavat lähestyä harjoituksen käsikirjoituksen suunnittelua sekä skenaarioiden laadintaa. Ohjeistuksessa pyrittiin myös painottamaan sitä, kuinka paljon aikaa ja resursseja onnistuneen käsikirjoituksen laatimiseen tulee allokoida. Myös harjoituksen kohderyhmään eli osallistujiin neuvottiin kiinnittämään huomiota.

Toiseksi viimeisenä ja laajimpana kappaleena oli harjoituksen osa-alueiden kuvaaminen. Harjoituksen käytännön valmistelua lähestyttiin lukijalle helposti omaksuttavasti kronologisesella järjestyksellä; ohjeita annettiin toiminnasta ennen harjoitusta, harjoituksen aikana, sekä harjoituksen jälkeen. Näiden näkökulmien lisäksi ohjeistuksessa painotettiin myös jatkokehittämisen tärkeyttä.

Ohjeistuksessa haluttiin korostaa suunnittelutyön tärkeyden lisäksi myös harjoitusta edeltävän esivalmistelun tärkeyttä. Tähän kuuluu muun muassa selkeiden roolien asettaminen. Tässä osiossa myös kerrotaan mitkä ovat fasilitaattorin ja havainnoijan tärkeimmät tehtävät. Käytännön valmisteluihin kuuluvat myös esimerkiksi tilavarausten tekeminen, tekniikan toimimisesta huolehtiminen, esitysmateriaalin huolellinen valmisteleminen sekä kalenterikutsujen lähettäminen osallistujille.

Harjoituksen aikaisen toiminnan ohjeistamisessa korostettiin myös roolitusta. Harjoituksen aikana tärkein rooli on fasilitaattorilla, joka pyrkii toimimaan interaktiivisesti osallistujien kanssa sekä aktivoimaan keskustelua käyttämällä hyväksi käsikirjoitusta sekä hänen käytössään olevaa mediaa. Harjoituksesta saatavien tulosten näkökulmasta myös havainnoijan roolia haluttiin korostaa lukijalle, sillä havainnoija on pääasiallisessa vastuussa harjoituksessa tehtävistä muistiinpanoista.

Harjoituksen jälkeisessä toiminassa korostettiin erityisesti palautteen tärkeyttä. Parhaimman palautteen saamiseksi ohjeistuksessa neuvottiin keräämään palaute harjoituksesta mahdollisimman pian harjoituksen päättymisen jälkeen. Ohjeistuksessa myös neuvottiin mitä asioita palautekyselyssä olisi hyvä kysyä ja mitata. Ohjeistuksessa kehotettiin fasilitaattoria myös päättämään harjoitus siten, ettei harjoitukseen jäisi juonen kannalta epäselvää loppua ja että harjoitus päättyisi positiivissävytteisesti. Harjoituksen jälkeen lukijaa kehotettiin myös järjestämään harjoituksen purkutilaisuus, missä koottaisiin harjoituksesta saatu tieto sekä käytäisiin läpi harjoituksesta saatu palaute. Harjoituksesta saatuja kokemuksia ehdotettiin myös esiteltäväksi organisaation johdolle sekä osallistujille.

Viimeiseksi kappaleeksi haluttiin jättää lukijalle helpoiten ymmärrettävät ohjeet hyvän harjoituksen järjestämiseksi. Lopputuloksena syntyi kymmenen vinkin lista, mitä noudattamalla lukija saisi konkreettisia ja napakoita neuvoja harjoituksen järjestämiseen. Vinkit järjestettiin jälleen kronologiseen järjestykseen harjoituksen näkökulmasta, painottaen jälleen suunnittelutyön tärkeyttä harjoituksen onnistumisen kannalta. Vinkeissä korostettiin muun muassa selkeiden ja mitattavien tavoitteiden määrittämistä, hyvän taustatarinan ja mukaansatempaavan juonen keksimistä, ajankohtaisten skenaarioiden käyttämistä, roolien asettamista, keskustelun ohjaamista tavoitteiden suuntaan sekä palautteen keräämisen tärkeyttä.

5.1.2 Oheismateriaalit

Ohjeistuksen lisäksi harjoitusmallin sisällytettiin myös kolme lisäkomponenttia; harjoituksen toteutusaikataulu, havainnointilomake sekä esimerkkiharjoitus. Harjoituksen toteutusaikataulun esikuvana toimi Phelpsin (2010, 151-154) käyttämä malli. Havainnointilomake ja esimerkkiharjoitus suunniteltiin alusta asti toimimaan yhdessä. Havainnointilomakkeen sivussa kulkeva numerointi on esillä myös esimerkkiharjoituksen kalvoissa, millä tavalla havainnoija pystyy helposti seuraamaan missä kohtaa harjoitusta mennään. Havainnointilomaketta yksinkertaistettiin ensimmäisestä versiosta helppokäyttöisyyden parantamiseksi.

Esimerkkiharjoituksessa käytettiin yhtä aikaisemmin käytössä ollutta skenaariota ja siihen liittyviä kuvia ja kalvoja. Tämän lisäksi käsikirjoituksen tärkeimmät asiat lisättiin esityksen muistiinpanoihin seurattavuuden parantamiseksi.

5.2 Mallin hyödynnettävyys valtiohallinnossa

Kuten todettua, opinnäytetyöprosessin aikana huomattiin, että harjoitusmallia voitaisiin jalkauttaa myös muihin valtiohallinnon organisaatioihin. Työn tilaajan puolesta ehdotettiin myös sitä, että harjoitusmallin voisi siirtää Valtorin ylläpitämään valtiohallinnon tietoturvallisuuden työkalupakkiin. Tällöin kaikki valtiohallinnon tietoturvallisuuden kanssa työskentelevät asiantuntijat pääsisivät halutessaan käyttämään mallia harjoitusten tekoon.

Alla olevassa kuviossa 8 on kuvattu toisen harjoituksen palautteessa kerätty mielipide harjoitusmallin kiinnostavuudesta VIRT-harjoitukseen osallistuneilta asiantuntijoilta. Tulosten perusteella harjoitusmalli kiinnostaa myös VIRT-toimijota ja mallia tullaankin jakamaan kaikille sitä haluaville.

Kuvio 8. Toinen kysely - harjoitusmallin kiinnostavuus

6 Johtopäätökset

Tässä luvussa käsitellään opinnäytetyön onnistumista asetettuihin tavoittesiin nähden sekä arvioidaan työn luotettavuutta ja käytettävyyttä. Hirsjärven ym. (2013, 263-265) mukaan työn loppuvaiheen tarkastelujaksossa nostetaan esiin sen olennaiset seikat ja havainnot, osoitetaan niiden merkitsevyys ja rajoitukset sekä tehdään näiden perusteella johtopäätökset.

Diskussiossa eli pohdinnassa tarkastellaan erityisesti työssä löydetyn uuden tiedon merkitsevyyttä ja hyötyä kokonaiskuvaan suhteutettuna. Luvussa pohditaan myös työn jatkokehittämismahdollisuuksia sekä ehdotetaan aiheita jatkotutkimukselle. Tämän jälkeen tutkitaan työn toistettavuutta ja sitä, kuinka hyvin tutkimuksessa käytetyt menetelmät palvelivat työn lopputulosta. Lopuksi kirjoittaja käy läpi kuinka työssä onnistuttiin hänen henkilökohtaisesta näkökulmastaan katsoen.

6.1 Diskussio

Opinnäytetyön tutkimusongelmana oli se, että valtiohallinnon häiriöhallintaryhmän harjoitustoimintaa tai harjoitustoiminnan luomisprosessia ei ollut vakiinnutettu. Tästä johdettiin opinnäytetyön pääasiallinen tavoite: luoda häiriöhallintaryhmälle harjoitusmalli, jonka avulla ryhmälle saataisi luotua kevyitä harjoituksia tehokkaasti ja helppokäyttöisesti. Peilaamalla tutkimuksesta saatuja tuloksia tavoitteisiin, voidaan todeta että tavoitteiseen päästiin työn aikana.

Tutkimusongelman ratkaisuun päästiin pitkän kehittämisprosessin avulla, missä hyödynnettiin tiedonkeruumenetelmien tuottama tieto sekä aikaisemmat harjoituskokemukset ja minkä tuloksena syntyi ratkaisuksi visioitu harjoitusmalli. Harjoitusmalli koettiin myös asiantuntijoiden näkökulmasta houkuttelevana tukivälineenä harjoitusten järjestämiseen.

Tutkimuksen tarkoituksena on tuottaa uutta tieteellistä tietoa tai tuottaa ratkaisuja käytännön ongelmiin (Ojasalo ym. 2014, 19). Tämän tutkimuksen kohdalla uuden tiedon tuottamisen näkökulmasta asiaa voidaan tarkastella siitä näkökulmasta, onko vastaavia harjoitusmalleja ennen ollut käytössä tai onko aiheesta tehty aikaisempaa tieteellistä tutkimusta. Tässä tapauksessa tietoperustan kasvattaminen kirjallisuuden kautta osoittautui haastavaksi eikä aikaisempaa merkittävää tutkimustietoa löytynyt suomenkielisistä tai kansainvälisistäkään lähteistä. Näin ollen tässä tutkimuksessa käytettyjen tiedonkeruumenetelmien tuottama tieto voidaan nähdä uutena tieteellisenä tietona, kun taas menetelmien tuottaman tiedon tuloksena syntynyt harjoitusmalli on enemmän Ojasalon ym. kuvaama ratkaisu tiettyn käytännön ongelmaan (2014, 19).

Tiedonkeruumenetelmien tuottaman tiedon analysoinnin jälkeen merkittävimpinä nostoina tutkimuksesta voidaan pitää suunnittelun tärkeyden korostamista harjoituksen järjestysprosessissa. Suunnittelu tässä tapauksessa ei kata pelkästään harjoituksen käsikirjoituksen huolellista kirjoittamista, vaan harjoitukseen syötettävien asioiden kokonaisvaltaista ja iteratiivista tarkastelua. Tämä tieto nousi esille niin havainnoinnin kuin haastatteluidenkin kautta.

Harjoituksen luomisprosessin aikana on erittäin helppo innostua keksimään paljon uusia ja omasta mielestä mielenkiintoisia skenaarioita ja keskustelunaiheita, mutta harjoituksen onnistumisen kannalta kaikkien harjoituksen osa-alueiden tulisi tähdätä harjoituksessa asetettuihin tavoitteisiin ja tutkimusongelman ratkaisemiseen. Prosessin aikana löydetty uusi tieto myös siirrettiin oleelliseksi osaksi lopullista harjoitusmallia.

Jo opinnäytetyöprosessin aikana huomattiin harjoitusmallin potentiaalin hyödyntäminen muualla valtiohallinnossa, mistä syystä mallin esitystapaa suunnattiin lievästi geneerisempään ja käyttäjäystävällisempään suuntaan. Aikaisemmin esitetyistä tuloksista voidaan myös huomata, että malli on jo herättänyt kiinnostusta useissa toimijoissa. Harjoitusmallin mahdollinen siirtäminen valtiohallinnon tietoturvallisuuden työkalupakkiin alleviivaisi työn onnistumista ja opinnäytteen validiutta.

Tärkeänä näkökulmana työn onnistumisen mittamisessa voidaan pitää luonnollisesti sitä, kuinka onnistuneena työn tilaaja piti lopputuloksena syntynyttä mallia. Alustavan esittelyn myötä tilaajan mielipide työn onnistuvuudesta oli positiivinen. Tilaajan näkökulmasta mallia voitaisiin hyödyntää laajastikin valtiohallinnossa sekä mahdollisesti myös yritysmaailmassa erityisesti suurissa konserneissa.

Mallin mahdollinen jatkokehittäminen ja uusien kokemusten mukaan jalostaminen olisi kirjoittajan näkökulmasta hyödyllistä alati muuttuvan toimintaympäristön vuoksi. Kybertoimintaympäristö asettaa etenkin valtiohallinnolle paljon haasteita, mistä syystä poikkihallinnollisen tiedonjaon ja harjoittelun rooli tulee todennäköisesti korostumaan myös jatkossa. Vastaavia harjoitusmalleja voisi tehdä esimerkiksi laajempiin harjoituksiin tai eri harjoitustyyppeihin liittyen.

Jatkotutkimuksen aiheeksi kirjoittaja ehdottaa esimerkiksi työssä esitellyn harjoitusmallin jalkauttamisen toteuttamista johonkin valtiohallinnon virastoon, missä yhdessä harjoittelun tarve on tunnistettu. Samoin myös työn tilaajan mainitsema yritysten ja etenkin suurien konsernien kiinnostus yhdessä harjoitteluun ja harjoitusmalliin voisi olla yksi jatkotutkimuksen aihe. Konsernit voisivat olla kiinnostuneita harjoitusmallin hyödyntämisestä siksi, että yhden pöydän ääreen saataisiin konsernin alle kuuluvia pienempiä toimijoita ja simuloitua koko konsernia koskevia uhkia ja ennakoida niiden vaikutuksia monen eri toimijan näkökulmasta.

6.2 Reliabiliteetti

Tutkimuksessa käytetyt tiedonkeruumenetelmät olivat löydetyn tiedon perusteella perusteltuja. Tutkimus täyttää myös laadullisen tutkimuksen tunnusmerkit. Tutkimusmenetelmien käytöstä olisi kuitenkin voinut mahdollisesti saada vieläkin tarkempaa ja validimpaa tietoa. Erityisesti palautekyselyn toteuttaminen olisi voinut onnistua paremmin, sillä kysely lähetettiin sähköisenä harjoitukseen osallistuneille muutama viikko harjoituksen jälkeen. Jälkikäteen ajateltuna paras tapa toteuttaa kysely olisi ollut heti harjoituksen jälkeen paperisena versiona. Saadun tiedon analysoinnissa olisi saattanut kestää tällä metodilla hieman kauemmin, mutta vastaukset olisivat kattaneet kaikki harjoitukseen osallistuneet asiantuntijat. Vastaukset olisivat myös kuvastaneet vastaajien mielipidettä heti harjoituksen jälkeen, kun harjoitus olisi ollut vielä tuoreena vastaajien mielessä.

Teemahaastattelut olivat kokonaisuutena onnistuneita ja haastateltavien valinnat osuivat kohdalleen. Lisähaastatteluitakin olisi voinut suorittaa, mutta haastatteluista saadun tiedon kattavuuden ja ajan rajallisuuden vuoksi tästä kuitenkin pidättäydyttiin. Havainnoinnin puolesta merkittävin tiedonkeruu tapahtui harjoitusten aikana, mutta julkisuussyistä tuon tiedon julkaiseminen ei olisi ollut mielekästä eikä siitä olisi ollut työn kehityksen kannalta loppujen lopuksi edes hyötyä. Havainnoinnin tulokset jäivät näin ollen hieman pintapuoleisiksi, mutta havainnoinnin valitseminen metodiksi hyödynsi myös harjoituksessa toimivan havainnoijan roolin määrittämistä.

Hyvän tutkimuksen luonteeseen kuuluu sen tulosten toistettavuus (Hirsjärvi ym. 2013, 231). Tämän tutkimuksen kannalta toistettavuuden todistaminen on hankalaa ottaen huomioon alati muuttuvan tutkimusmenetelmien kohdejoukon. Samaten esimerkiksi palautekyselyn tulokset ovat riippuvaisia pääasiassa harjoituksen laadusta, joka muuttuu joka kerta kun uusi harjoitus tehdään. Itse harjoitusmallin sisältö voisi tutkijasta riippuen muuttua paljonkin, sillä kukin voi käsittää termin ”harjoitusmalli” monin eri tavoin. Tämän tutkimuksen tuotoksena syntynyt harjoitusmalli sisältää jokatapauksessa hyödyllisiä ja perusteltuja elementtejä hyvän harjoituksen järjestämisen edistämiseksi.

6.3 Oman työn arviointi

Kirjoittajan näkökulmasta työ onnistui alustaviin odotuksiin nähden hyvin. Opinnäytetyöprosessin alkuvaiheessa ei ollut kovin hyvää selvyyttä siitä, kuinka paljon kovaa työtä prosessin läpivieminen todellisuudessa vaatiikaan. Alkuperäisestä aikataulusta poikettiin ainakin kahdesti ja työn loppuvaiheeseen kohdistui merkittävä osa koko prosessin kirjoitustyöstä. Tämä osa-alue lieneekin ollut työn suurin kompastuskivi. Jälkikäteen ajateltuna olisi myös ollut hyvä pyytää enemmän opinnäytetyön ohjausaikoja jatkuvamman seuraamisen parantamiseksi.

Lopputuloksena syntynyt harjoitusmalli on myös sellainen josta kirjoittajana voi olla tyytyväinen. Se toimii hyvänä opasteena harjoitusten luomiseen, vaikka harjoituksen järjestäjällä ei olisikaan olemassa olevaa kokemusta harjoitusten järjestämisestä, saati valmiita omia materiaaleja sellaisen toteuttamiseen. Oli myös ilahduttavaa kuulla, että mallin käyttöönottoa voitaisiin laajentaa myös muualle valtiohallintoon.

Kokonaisuutena opinnäytetyön kirjoittaminen oli raskas, mutta lopulta palkitseva kokemus. Kyberturvallisuuden tutkiminen aiheena oli myös mielenkiintoista ja opettavaa. Prosessi on antanut uusia eväitä tulevaisuuden varalle ja valtiohallinnon turvallisuuden parissa työskentely on avannut silmiä sille kuinka yhteiskuntamme pyrkii varautumaan sitä kohtaan asettuvia uhkia vastaan. Lopuksi kirjoittaja esittää sydämelliset kiitoksensa läheisille, työn tilaajalle sekä työn ohjaajalle tuesta matkan varrella.

Lähteet

Kirjallisuuslähteet

Burdett, A. & Bowen, D. 2013. BCS Glossary of Computing and ICT. 1. painos. Swindon: BCS Learning and Development Limited.

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

Gillham, B. 2005. Research interviewing: the range of techniques. Berkshire: Macgraw-hill education.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2013. Tutki ja kirjoita. 18. painos. Porvoo: Bookwell.

Metsämuuronen, J. 2001. Laadullisen tutkimuksen perusteet. 2. painos. Viro.

Mowbray, T. 2014. Cybersecurity – Managing Systems, Conducting Testing, and Investigating Intrusions. 1. painos. Indianapolis: Wiley.

Ojasalo, K., Moilanen, T. & Ritalahti J. 2014. Kehittämistyön menetelmät. 3. uudistettu painos. Helsinki: Sanoma Pro Oy.

Phelps, R. 2010. Emergency Management Exercises. 1. painos. San Francisco: Chandi Media.

Puolustusministeriö. 2010. Yhteiskunnan turvallisuusstrategia. 1. painos. Vammala: Vammalan kirjapaino.

Turvallisuuskomitean sihteeristö. 2013. Suomen kyberturvallisuusstrategia. 1. painos. Forssa: Forssa Print.

Vehkalahti, K. 2014. Kyselytutkimuksen mittarit ja menetelmät. 1. painos. Helsinki: Finn Lectura.

Vilkka, H. 2006. Tutki ja havainnoi. 1. painos. Vaajakoski: Gummerus Kirjapaino.

Sähköiset lähteet

Ahola, K. 2014. Valmiusharjoituksen onnistumiseen vaikuttavat tekijät osallistujien näkökulmasta. Viitattu 20.05.2015
http://www.doria.fi/bitstream/handle/10024/102381/SM%20858.pdf?sequence=2

FEMA. 2012. National Level Exercise 2012: Cyber Capabilities Tabletop Exercise. Viitattu 06.05.2015 https://www.fema.gov/media-library/assets/documents/26845

Hankerekisteri. 2015. Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke. Viitattu 29.04.2015 http://www.hare.vn.fi/mAsiakirjojenSelailu.asp?h_iId=19225&a_iId=227950

Laine, H. 2011. Varautumissuunnitelma Seniortek Oy:n asiakaskohteeseen. Viitattu 20.05.2015 http://urn.fi/URN:NBN:fi:amk-201105178280

Tuomikoski, P. 2014. Jatkuvuudenhallinnan kehittäminen valmistavassa teollisuudessa. Viitattu 20.05.2015 http://urn.fi/URN:NBN:fi:amk-2014082113529

Valtiovarainministeriö. 2015. JulkICT-toiminto. Viitattu 27.04.2014 http://vm.fi/julkisen-hallinnon-ict

Viestintävirasto. 2014. Viestintäviraston Kyberturvallisuuskeskus aloitti toimintansa 1.1.2014. Viitattu 29.04.2014
https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/tietoturva-artikkelit/viestintavirastonkyberturvallisuuskeskusaloittitoimintansa1.1.2014.html

Julkaisemattomat lähteet

Janhunen, K. 2015. Erityisasiantuntija, SecICT-hankkeen hankepäällikkö. Valtiovarainministeriö. Haastattelu 17.04.2015

Kiuru, A. 2015. Tilannekeskusryhmän päällikkö. Kyberturvallisuuskeskus. Haastattelu 08.05.2015

Sillanpää, A. 2015. Erikoistutkija. Turvallisuuskomitean sihteeristö. Haastattelu 04.05.2015

Valtiovarainministeriö. 2014. VIRT-toiminnan aloitustilaisuuden kokousmuistio. Aloitustilaisuus 29.10.2014

Kuviot

Liitteet

Liite 1. Palautekyselyn kysymykset

Palautekyselyn kysymykset – VIRT-harjoitus 18.12.2014
Vastausvaihtoehdot:

Täysin eri mieltä
Osittain eri mieltä
Ei samaa eikä eri mieltä
Osittain samaa mieltä
Täysin samaa mieltä

Skenaariot:

- Harjoituksessa esitettiin realistisia skenaarioita
- Harjoituksen skenaariot olivat ajankohtaisia
- Harjoituksen skenaariot voisivat koskettaa omaa organisaatiotani

Keskustelu:

- Harjoituksen aiheet herättivät kehittävää keskustelua
- Opin uusia asioita keskustelun myötä
- Keskusteluaiheet koskettivat omaa organisaatiotani
- Jokainen sai halutessaan puheenvuoron keskustelussa

Tavoitteisiin pääseminen:

- Vastuut ja tehtävät laajavaikutteisessa häiriötilanteessa selkiytyivät
- Yhteistoiminnan periaatteet häiriötilanteen sattuessa ovat selkeytynyneet

Kokonaisuus:

- Pöytäharjoitus oli kokonaisuutena onnistunut
- Pöytäharjoitus oli toteutettu teknisesti hyvin
- Pöytäharjoituksesta oli hyötyä omalle organisaatiolleni
- Pöytäharjoitus oli hyvä tapa harjoitella tällä kokoonpanolla

Harjoituksen pituus

- Pöytäharjoitus oli pituudeltaan... (liian pitkä, hieman liian pitkä...)

Avoin kysymys: toiveita tulevista skenaarioista.

Liite 2. Haastattelujen kysymykset

Kirsi Janhunen, Valtiovarainministeriö:

1. Kerro lyhyesti taustastasi ja työnkuvastasi Valtiovarainministeriössä
2. Kerro SecICT-hankkeesta, sen taustoista, tavoitteista ja nykytilanteesta.
3. VIRT-toiminta – kuinka toiminta sai alkunsa ja mitä tavoitteita sillä on?
4. Mitä asioita VIRT-harjoitustoiminnalla halutaan selvittää tai saavuttaa?
5. Harjoitusmallin aihioksi on valittu nimenomaan pöytäharjoitus. Miksi?
6. Minkälaisia toiveita ja odotuksia sinulla ja ministeriöllä on harjoitusmallin suhteen? Kuinka sen tulisi palvella VIRT-toimintaa ja/tai valtiohallintoa?
7. Näkisitkö harjoitusmallin sopeutuvan myös muualle valtiohallintoon tai yritysmaailmaan?
8. Minkälaisia kokemuksia sinulla on Suomen tieto- ja kyberturvallisuusharjoituksista?

Antti Sillanpää, Turvallisuuskomitean sihteeristö:

1. Kerro lyhyesti itsestäsi, taustastasi ja tämänhetkisestä työnkuvastasi
2. Kerro yleisesti Suomessa järjestettävien kyberharjoitusten historiasta (milloin aloitettu, kuinka usein, erot harjoitusten välillä)
3. Kuvaile harjoitusten suunnitteluprosessia (pituutta, käytössä olevia resursseja, aikajännettä...)
4. Minkä tyyppisiä asioita on harjoiteltu?
5. Millaisia tuloksia on saatu eri kyberharjoituksista? Miten osallistujat kokevat harjoitukset?
6. Mitkä ovat näkymät VIRT-toiminnasta ja sen hyödyllisyydestä? Entä yhdessä harjoittelun merkitys ryhmän kesken?
7. Mitä oppeja tai hyviä käytäntöjä Suomen muista kyberharjoituksista voisi ottaa VIRT-harjoituksiin?

Antti Kiuru, Kyberturvallisuuskeskus:

1. Kerro lyhyesti itsestäsi, taustastasi ja tämänhetkisestä työnkuvastasi
2. Eri kyberharjoitukset Euroopassa ja muualla, milloin aloitettu, minkälaisia harjoituksia, miten usein...
3. Onko kokemuksia miten harjoituksia suunnitellaan, kuinka pitkään, millä resursseilla..
4. Minkä tyyppisiä asioita harjoitellaan? (Teknistä puolta vai kansainvälistä yhteistyötä)
5. Millaisia tuloksia on saatu harjoituksista?
6. Mitkä ovat näkymät VIRT-toiminnasta ja sen hyödyllisyydestä? Entä yhdessä harjoittelun merkitys ryhmän kesken?
7. Mitä oppeja tai hyviä käytäntöjä ulkomaisista kyberharjoituksista voisi ottaa VIRT-harjoituksiin?

Liite 3. Havainnointilomake

HAVAINNOINTILOMAKE - PÖYTÄHARJOITUS			
NRO	**SYÖTE**	**HAVAINTO**	**MUUT HUOMIOT**
1	**Osioon varattu aika (30 min)**		
1.1			
1.2			
1.3			
1.4			
1.5			
1.6			
1.7			
1.8			
2	**30 min**		
2.1			
2.2			
2.3			
2.4			
2.5			
2.6			
2.7			
2.8			
2.9			

Liite 4. Ohjeistus pöytäharjoituksen järjestämiseen – sisällysluettelo

Sisällysluettelo

Liite 5. Harjoituksen toteutusaikataulu

AIKATAULU PÖYTÄHARJOITUKSEN TOTEUTTAMISEEN		
Tehty	**Tehtävä**	**Huomioita**
10 viikkoa ennen harjoitusta		
x	Päivämäärän ja kellonajan valitseminen harjoitukselle	
	Tilavarauksen tekeminen	
	Kalenterikutsun lähettäminen osallistujille	
	Suunnitteluvaiheen aloittaminen	
	Tavoitteiden ja tutkimusongelman asettaminen	
8 viikkoa ennen harjoitusta		
	Käsikirjoituksen luonnoksen laatiminen	
	Skenaarioiden ideoiminen tavoitteiden pohjalta	
	Havainnointilomakkeen teko	
6 viikkoa ennen harjoitusta		
	Käsikirjoitus pääpiirteittäin valmis	
	Skenaariot pääpiireittäin valmiina	
	Keskustelukysymysten laatiminen skenaarioiden pohjalta	
	PowerPoint-esityksen teon aloittaminen	
	Suunnan tarkastaminen verrattuna asetettuihin tavoittesiin	
4 viikkoa ennen harjoitusta		
	PowerPoint-esityksen viimeistelyä	
	Kuvien, videoiden ja oheismateriaalin luomista	
	Palautekyselyn luominen	
2 viikkoa ennen harjoitusta		
	Tarjoilujen tilaaminen	
	Esitysmateriaali ja käsikirjoitus valmiina	
Viikko ennen harjoitusta		
	Muistutussähköposti harjoituksesta osallistujille, ohjelman lähettäminen	
	Mahdollisten materiaalien tilaaminen tai printtaaminen	
Päivää ennen harjoitusta		
	Kokoustilan varmistaminen	
	Etäyhteyksien ja muiden teknisten laitteiden toimivuuden testaaminen	
	PowerPoint-esityksen testaaminen	
Harjoituspäivänä		
	Harjoituksen vetäminen	
	Palautteen kerääminen harjoituksen jälkeen	
	Talleta tai tuhoa harjoitusmateriaali harjoituksen jälkeen	
Korkeintaan kaksi viikkoa harjoituksen jälkeen		
	Analysoi havainnointimuistiinpanot ja kerätty palaute	
	Kirjoita muistio harjoituksesta ja sen onnistumisesta	
	Esittele tuloksia osallistujille ja johdolle	