Maapuolustuksen taktisten verkkojen valvonta ja hallinta

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ylemmän ammattikorkeakoulututkinnon opinnäytetyö

Teknologiaosaamisen johtaminen

Hämeenlinna 9.12.2016

Uula-Petteri Purojärvi

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

VISAMÄKI
Teknologiaosaamisen johtaminen

Tekijä Uula-Petteri Purojärvi **Vuosi** 2016

Työn nimi Maapuolustuksen taktisten verkkojen valvonta ja hallinta

TIIVISTELMÄ

Tutkimus ”Maapuolustuksen taktisten verkkojen valvonta ja hallinta” tehtiin Maavoimien esikunnalle. Aiheen valintaan vaikutti tutkijan havainto, että em. verkkojen valvontaa ja hallintaa ei ole toteutettu ITIL:n mukaisesti, vaikka ITIL on organisaatiossa valittu IT-palvelutuotannon viitekehykseksi. Tutkimuksen tarkoituksena oli tunnistaa ilmiö nimeltään maapuolustuksen taktisten verkkojen valvonta ja hallinta ja käsitteistää sitä ITIL:n viitekehyksen mukaisesti. Tutkimus tehtiin kvalitatiivisena ja induktiivisena aineistotutkimuksena. Tutkimuksen primääriaineisto kerättiin strukturoimattomilla teemahaastatteluilla. Haastattelut kohdistettiin henkilöihin, joilla on pitkä ja kattava kokemus maapuolustuksen taktisista verkoista ja sertifioitu perustietämys ITIL:stä. Sekundäärisen aineiston keräämisessä hyödynnettiin Maanpuolustuskorkeakoulun Pro Gradu- ja diplomitutkimuksia sekä julkaisusarjoja, OGC:n kehittämää ITIL – IT palvelutuotannon viitekehystä ja IETF:n standardikirjastoa. Tutkimuksen sekundäärisen aineiston valintaa ohjasi tutkimuksen julkisuusvaatimus. Siitä johtuen aineisto on kaikilta osin kerätty julkisista lähteistä. Primäärin ja sekundäärisen aineiston dialogin jälkeen havaittiin, että maapuolustuksen taktiset verkot voidaan nähdä IT-palvelutuotantona siinä missä mikä tahansa tietoverkko ja palvelut. Niiden käyttöympäristö poikkeaa merkittävästi normaalista IT-palvelutuotannosta. Poikkeavuudet liittyvät usein verkkojen tavanomaista suurempaan epävarmuuteen käytetystä teknologiasta huolimatta. Epävarmuutta aiheuttavat verkkojen tilapäinen luonne, liikkuvuus ja olosuhteet, joissa niiden toimintaa pyritään vastustajan toimesta suunnitelmallisesti haittaamaan elektromagneettisella häirinnällä tai kineettisellä vaikuttamisella. Valvontaa ja hallintaa suunniteltaessa on kiinnitettävä huomiota valvontahenkilöstön suhteessa valvottaviin laitteisiin, rajoitettuun mahdollisuuteen päästä laitteiden luokse eri tilanteissa ja laitteiden tukemiin protokolliin. Tätä tutkimusta on mahdollista julkisella tutkimuksella täydentää tutkimalla ITIL:n muutkin vaiheet kuin palvelutuotanto maapuolustuksen taktisten verkkojen kontekstissa.

Avainsanat ITIL, maapuolustus, taktinen verkko, valvonta, hallinta

Sivut 69 s. + liitteet 8 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

VISAMÄKI
Name of degree programme

Author Uula-Petteri Purojärvi **Year** 2016

Subject of Master's thesis Monitoring and control of ground defence tactical networks

ABSTRACT

This master's thesis on "Monitoring and control of ground defence tactical networks" was made for Army Command Finland. The research subject was based on the notification, that monitoring and control of ground defence tactical networks is not structured as ITIL describes them. Although the organization has chosen to use ITIL as a framework for IT service operations. In this thesis, we recognize the phenomenon of monitoring and management of ground defence tactical networks and conceptualize it according to ITIL framework. Research was conducted as a qualitative and inductive desk research. The primary source material was collected by the means of unstructured theme interviews. Interviews were aimed at persons that have long and broad experience over ground defence tactical networks and certified basic knowledge over ITIL framework. Secondary source material was gathered from a collection of The Finnish National Defence University's Master's Thesis and publications, OGC's ITIL framework publication and IETF's standardization library. Secondary source material was gathered from unclassified sources. After observing the dialog between primary and secondary source material, ground defence tactical networks were seen as IT-service networks. They have network component and services component. Their usage environment differs significantly from normal everyday IT-service operations. Differences are often related with the raised uncertainty that is not technology related. Uncertainties are caused by the temporary nature, mobility of the networks and usage environment, where the adversary with electromagnetic and kinetic force systematically hinders the network operations. The ratio between management staff and managed equipment, limited possibility to reach the managed equipment physically in various situations and the protocols supported by the equipment should be taken into consideration when planning monitoring and management of ground defence tactical networks. This master's thesis was conducted by using ITIL Service Operations in the ground defence tactical networks context. It can be complemented by studying the implementation of other stages of ITIL in ground defence tactical networks.

Keywords ITIL, ground defence, tactical network, monitoring, control

Pages 69 p. + appendices 8 p.

LYHENNELUETTELO:

ASCII	American Standard Code for Information Interchange
CCTA	Central Computer and Telecommunications Agency
COTS	Commercial off the shell
EBCDIC	Extended Binary Coded Decimal Interchange Code
eAPI	extended Application Programming Interface
FCAPS	Fault, Configuration, Accounting, Performance, Security
FTP	File Transfer Protocol
HF	High Frequency
HP IMC	Hewlett-Packard Intelligent Management Center
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Informaatioteknologia
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
LRV	Langaton runkoverkko
MANET	Mobile Ad-Hoc Network
MIB	Management information base
NVT	Network Virtual Terminal
OGC	Office of Government Commerce
OSI	Open Systems Interconnection
PDCA	Plan, Do, Check, Act –sykli
PoE	Power over Ethernet
REST	Representational state transfer
RFC	Request for comments

ROI	Return on investment
RS-232	Recommended Standard 232
SoA	Service oriented architecture
SCP	Secure Copy
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCO	Total cost of ownership
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TVM	Tiedustelu, Valvonta ja Maalittaminen
UDP	User Datagram Protocol
UHF	Ultra High Frequency
VHF	Very High Frequency
VTY	Virtual Teletype
YETTS	Yhteiskunnan Elintärkeiden Toimintojen Turvaamisen Strategia
YVI	Yhtymän viestijärjestelmä

SISÄLLYS

1 JOHDANTO

One Ring to rule them all, One Ring to find them,
One Ring to bring them all, and in the darkness
bind them (JRR Tolkien)

Yllä olevassa lainauksessa kirjasta Taru Sormusten Herrasta kuvataan yksi syy valvoa ja hallita. Maapuolustuksen taktisten verkkojen tapauksessa tuskin voidaan lähteä samoista päämääristä, vaan tarkoituksena on ennemminkin toimintaan vaikuttavien tapahtumien havaitseminen ja niiden aiheuttamien haittojen minimointi.

Suomalaisen viestiaselajin perinteet voidaan johtaa Jääkäripataljoona 27:n tiedonanto-osastossa hankittuun koulutukseen ja sotakokemukseen. Helmikuussa 1918 kotimaahan palanneiden jääkäreiden osaamisella perustettiin Jääkäripataljoona 15, jota kutsuttiin myös kenttälennätinpataljoonaksi. Pataljoonan käyttämä teknologia koostui kenttälennätinasemista ja parikaapeleista. Myöhemmin samana vuonna kalusto laajeni käsittämään venäläisiltä joukoilta haltuun otetut radioasemat Helsingissä ja Viipurissa.

Elokuussa 1918 aloitettiin ensimmäisten asevelvollisten kouluttaminen radiojärjestelmille. Tuolloin nimenä oli Sotalaitoksen radiolennätinosasto. Sotalaitoksen radiolennätinosaston nimi muutettiin 1919 aikana Kipinälennätinlaitokseksi ja koulutus avattiin myös siviileille.

Viestijoukot erotettiin omaksi aselajikseen juuri ennen talvisotaa 1939. Tuolloin käytettyinä teknologioina olivat analogiset puhelinjärjestelmät ja radiojärjestelmät. Puhelinjärjestelminä käytettiin käsivälitteisiä keskuksia sekä keskusosakeskuksia. Radiojärjestelmät täydensivät puhelinjärjestelmiä ja niitä käytettiin milloin puhelinverkon rakentaminen ei ollut mahdollista tai kannattavaa.

Automaattiset digitaaliset puhelinkeskukset, yhtymän viestijärjestelmät (YVI/YVI1M/YVI2), korvasivat myöhemmin käsivälitteiset keskukset. Täydentävinä radiojärjestelminä toimivat analogiset radiot (LV217 ja muut VHF-radiot, sekä HF-radiot). Analogisten radioiden rinnalle ja osin niitä korvaamaan ovat sittemmin tulleet digitaaliset radiojärjestelmät VHF-, HF-, ja UHF-aallonpituuksilla. Viimeisimpänä kehityksenä on ollut M18-järjestelmä, joka on toteutettu Elektrobitin TacWIN-järjestelmällä

Edellä kuvattu kehitys on johtanut siihen, että maapuolustuksen taktisten verkkojen valvonta ja hallinta on muuttunut ja kasvattanut merkitystään. Valvontaa ja hallintaa on kyettävä tekemään etänä paremman kokonaiskuvan ja järjestelmän eheyden saavuttamiseksi.

Valvonta ja hallinta eroavat piirikytkentäisten ja IP-pohjaisten tietoliikenneverkkojen välillä. Kun piirikytkentäiset verkot muodostivat puhe- ja point-to-point-yhteyksiä, IP-pohjaiset tietoliikenneverkot muodostavat loogisia kokonaisuuksia. On myös huomioitava, että piirikytkentäisissä

verkoissa käytetyt teknologiat eivät samalla tavalla mahdollistaneet valvonnan ja hallinnan avulla saatujen tietojen automaattista kognitiivista käsittelyä kuin nykyisten IP-pohjaisten tietoliikenneverkkojen teknologiat.

Tutkimuksen käynnistäneenä havaintona on, että maapuolustuksen taktisten verkkojen valvontaa ja hallintaa ei ole toteutettu ITIL:n (Information Technology Infrastructure Library) parhaiden käytäntöjen viitekehyksen mukaisesti. Taktiset verkot voidaan nähdä IT-palvelutuotannon mahdollistavana osana eli tarkoitus ei ole rakentaa tietoliikenneverkkoja, vaan tuottaa maapuolustuksen joukoille palveluita jotka edesauttavat niitä tehtävänsä suorittamisessa. IT-palvelutuotannon toteuttamiseksi on laadittu parhaiden käytäntöjen viitekehyksiä, joista maapuolustuksen käyttöön on valittu ITIL. Tutkittaville verkoille on ominaista käytettävyyden ennustettavuuden alhainen taso, vaihteleva yhteyksien laatu, mobiilius ja väliaikaisuus. Käytettävyyden ennustettavuutta laskee vastustajan pyrkimys haitata ja jopa estää tiedonsiirtoa. Yhteyksien laatu on riippuvainen verkon muodostamisen mahdollisuuksista.

Tässä tutkimustyössä tutkitaan maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttamista, huomioiden verkkojen ominaispiirteet. Tutkimuksessa pyritään tunnistamaan maapuolustuksen taktisten verkkojen ominaispiirteitä, käsitteistämään niitä ITIL-viitekehyksen mukaisesti ja selvittämään kuinka verkkoja voidaan valvoa ja hallita. Tutkimustyön tuloksena on jäsennelty käsitys maapuolustuksen taktisten verkkojen valvonnan ja hallinnan erityispiirteistä. Käsitystä voidaan käyttää valvonnan ja hallinnan prosessien, aktiviteettien ja toimijoiden roolien kuvaamiseen.

2 KÄSITEMÄÄRITTELY

Käsitteet ovat Kanasen (Kananen 2015, 105) mukaan ilmiön ymmärtämisen kannalta oleellisen tärkeitä työkaluja, joiden avulla voidaan tunnistaa alan ongelmia ja ratkaista niitä tehokkaasti. Tutkimuksessa käsitteet korvaavat arkikielen epätäsmällisiä ilmaisuja täsmällisillä ja yksiselitteisillä ilmaisuilla.

Tässä tutkimuksessa käytetyt keskeiset käsitteet ovat:

Hallinta – hallinta tarkoittaa tässä tutkimuksessa toimia, joita tehdään tietoliikenneverkon ja palveluiden tuottamiseksi, tapahtumien poistamiseksi ja ongelmien korjaamiseksi. Hallinta voi olla teknistä, jota tehdään aktiivisesti jonkin tahon toimesta, tai ylemmän vastuutahon käskemää toimintaa varsinaisen hallintatoimenpiteen suorittavalle toimijalle. Teknistä hallintaa tehdään standardoiduilla hallintaprotokollilla.

ITIL – ITIL on Iso-Britannian valtionhallinnon Office of Government Commerce:n (OGC) kehittämä ja ylläpitämä viitekehys, jossa on kuvattu IT-palvelutuotannon parhaita käytäntöjä.

Johtamisjärjestelmä – johtamisjärjestelmällä tarkoitetaan sitä teknistä järjestelmää, joka tukee johtamista tai mahdollistaa jonkin palvelun tuottamisen käyttäjälle.

Maapuolustus – maapuolustus on valtakunnan maa-alueen puolustamista ja valvontaa, sekä yhteiskunnan elintärkeiden toimintojen turvaamiseksi muille viranomaisille annetun tuen ja virka-avun antamista.

Taktinen verkko – taktinen verkko on maapuolustuksen tukemiseksi rakennettu kiinteä tai väliaikainen, staattinen tai mobiili, tietoliikenneverkko. Se mahdollistaa maapuolustuksen tarvitsemien IT-palveluiden tuottamisen käyttäjille. Taktinen verkko voi olla toteutettu sotilaskäyttöön tai kaupalliseen käyttöön (ns. COTS) suunnitelluilla laitteilla ja järjestelmillä. Taktinen verkko on osa johtamisjärjestelmää.

Valvonta – valvonta tarkoittaa tässä tutkimuksessa toimia, joita tehdään tietoliikenneverkon ja palveluiden toimintakunnon havaitsemiseksi. Toimenpiteet voivat olla aktiivisia teknisiä valvontatoimia, joita tehdään verkonvalvontaan dedikoiduilla työasemilla, passiivisia herätteisiin perustuvia toimia tai käyttäjien havaitsemia palvelutason alenemia. Teknistä valvontaa tehdään standardoiduilla valvontaprotokollilla. Valvonta voi olla myös käyttäjien ja ylläpitäjien tekemää fyysisen toimintaympäristön havainnointia.

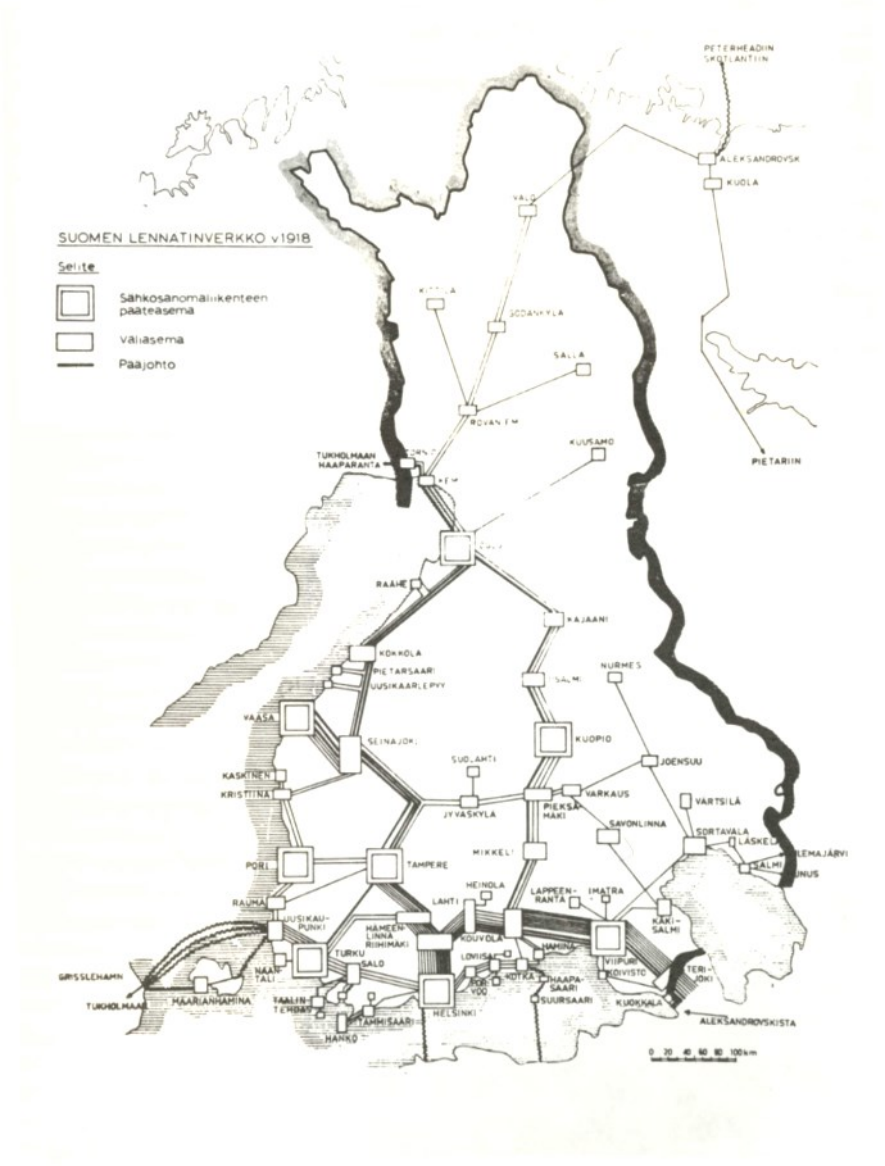
Viesti (aselaji) – viesti aselajina tarkoittaa niitä joukkoja, jotka rakentavat ja ylläpitävät taistelevien joukkojen tarvitsemia tietoliikenneverkkoja ja palveluita.

3 VIESTITOIMINNAN HISTORIAA

Maapuolustuksen taktisten verkkojen historia voidaan johtaa Suomen itsenäistymisen ajan (ja sitä aikaisemmin suuriruhtinaskunnan ajan) radio-, lennätin- ja puhelinverkkojen aikaan asti. Tuolloin ei tosin käytetty erikseen käsitettä maapuolustuksen taktiset verkot erottamaan maajoukkojen viestitoimintaa ilmassa ja merellä toimivien joukkojen viestitoiminnasta.

3.1. Suomen suuriruhtinaskunnan aika ja vapaussota

Venäjän keisarikunta oli rakentanut tuolloiseen suuriruhtinaskuntaansa lennätinverkkoa siten, että Etelä-Suomessa oli rannikkoseudun ja suurimmat liikekeskukset kattava teknisesti kehittynyt lennätinverkko. Lennätinverkko toimi myös kansainvälisen kauttakulun verkkona. Verkko ei palvellut niin hyvin keski- ja pohjoisosien tarpeita, mutta ulottui kuitenkin Hangosta Ivaloon ja sieltä Kuolan ja Aleksandrovskin kautta Peterheadiin Skotlantiin asti (kuva 1) (Mikola 1980, 14-15).



Kuva 1. Suomen lennätinverkko 1918 (Viestitoiminta Suomessa, 16)

Puhelin- ja radioverkkojen kehittämiseen ei keisarikunnalla ollut samanlaista kiinnostusta, vaan puhelinverkko oli kehittynyt yksityisten ja paikallisten intressien (esimerkiksi rautateiden) mukaisesti ja radiotoiminta oli suoranaisesti estetty, kun Venäjän sisäministeriö antoi vuonna 1902 käskyn että Suomessa kukaan ei saa käyttää ilman radiolaitteita sisäministerin lupaa. (Mikola 1980, 12-15).

Valmistauduttaessa Vapaussotaan, lennätinverkkoon rakennettiin salaisia yhteyksiä Helsingin-Viipurin ja Helsingin-Hämeenlinnan-Vaasan väleille. Lisäksi rakennettiin salaisia yhteyksiä rautateiden lennätinlinjoille siten, että Helsinkiin sijoitetut kaksi Morse-konetta kytkettiin Vaasaan ja Pietariin meneviin suoriin verkkojohtoihin. Näihin voitiin kytkeä tärkeimmät väliasemat Toijala, Tampere, Haapamäki, Seinäjoki, Kouvola ja Viipuri. Yhteyksillä liikennöitiin käyttäen salakieltä. Edelliset yhteydet oli rakennettu käyttäen suomalaisen liike-elämän yhteyksiä. Lisäksi järjestettiin lennätinkonttorien kiinni ollessa (klo 23–05 välisenä aikana) kytketty yhteys venäläisen esikunnan lennätinverkkoa käyttäen josta voitiin liikennöidä Poriin, Kristiinaan ja Vaasaan (Mikola 1980, 17).

Saksassa koulutuksessa olleella jääkäripataljoona 27:llä oli merkittävä rooli Vapaussodan aikaisen radioverkon rakentamisessa. Radiolaitteita saatiin Suomeen Saksasta mm. sukellusvene UC-57:llä ja aselaiva Equityllä vuoden 1917 lopulla. UC-57:n laitteisto sijoitettiin myöhemmin Helsingin Kulosaareen, jossa se toimi Vapaussotaa valmistelevan Sotilaskomitean vastaanottoyhteytenä Saksasta saapuville viesteille. Equityn mukana tulleet radiotarvikkeet toimitettiin Merikarvialle. (Mikola 1980, 20).

Radioyhteyksiä kehitettiin vuoden 1918 aikana siten, että Mikkeliin pystytettiin jääkärien Saksasta tuoma 1,5kW:n Telefunken-asema, sekä Tampereella ja Vaasassa vallattiin venäläiset 10kW:n asemat. Näin muodostetusta Päämajan radioverkosta voitiin muodostaa yhteyksiä Ahvenanmaalle, Härnösandiin ja Libauhun. Lisäksi saatiin Nokialta asema, joka muutettiin rautateillä liikkuvaksi ja siitä liikennöitiin Tallinnaan ja Libauhun. Saksasta saatiin jääkäreiden mukana myös neljä ilmailukenttäasemaa, kolme langatonta lennätintä ja neljä vastaanotinta. (Mikola 1980, 28)

Vapaussodan alettua maan viestiyhteyksistä suurin osa jäi punaisten haltuun. Vaikka viestiverkon operoinnista vastaavat Valtiovirkamiesyhdistykset kielsivät kapinan puhjettua kaikkia jäseniään tottelemasta punakaartien käskyjä (ja olisivat näin saattaneet koko verkon mykäksi), ylipäällikkö Mannerheim antoi ehdottoman käskyn virkamiehille jatkaa tehtäviään. Syynä tähän oli aiemmin valmisteltujen salaisten viestiyhteyksien toiminnan jatkumisen varmistaminen ja kapinallisten puhelinliikenteen kuuntelun mahdollistaminen. Kapinallisiin kuului sekä venäläisiä sotilaita, että punakaartilaisia. Venäläiset eivät osanneet kieltä ja punakaartilaiset eivät tunteneet tekniikkaa, joten kapinallisilla ei ollut mahdollisuutta valvoa viestiliikennettä. Tehokkaan ja toimivan valvonnan ja hallinnan tärkeys nousee esiin jo vuosisadan alun aikaisten puhelin- ja lennätinverkkojen ajalta. Jos kapinallisilla olisi ollut hyvä käsitys viestiyhteyksistä ja niillä välitetyistä viesteistä, olisi ylipäällikön ollut käytännössä mahdotonta saa-

da tietoja Etelä-Suomesta tai olla yhteydessä Helsinkiin jääneihin senaatin jäseniin. (Mikola 1980, 21)

3.2. Talvisota ja toinen maailmansota

Lähestyttäessä vuotta 1939 ja talvisotaa, oli Suomen puhelin- ja lennätinverkossa tapahtunut kehitystä. Koko maan kaukopuhelinpalvelu oli keskitetty valtiolle 1930-luvun puolivälissä. Pohjois- ja itäosien puhelinverkkoa oli kehitetty suhteellisesti muita enemmän, maanpuolustuksellisia näkökohtia oli otettu huomioon verkkoa kehitettäessä ja Etelä-Suomen kuormitetuimpien linjojen varmistamiseen oli varauduttu. (Mikola 1980, 123)

Radioverkkoa käytettiin täydentämään langallista verkkoa siten, että Hangosta Utöhön, Oulusta Hailuotoon ja Kotkasta Suursaareen oli käytössä kiinteät radiolinjat. Helsingin, Turun ja Maarianhaminan lentoasemilla oli ilmailuradioasemat ja kesäisin oli käytössä Tampereen, Viipurin, Vaasan, Oulun ja Kemin asemat. Näiden valtion hallinnassa olevien radioasemien lisäksi olivat 16 liikeyrityksellä ja 2 sanomalehtiyhtiöllä omat radioasemat. Radioamatöörit olivat rakentaneet koko maan kattavan radioverkon ja Yleisradiota kehitettiin. Olihan Suomessa tarkoitus järjestää olympialaiset vuonna 1940. (Mikola 1980, 124-125)

Puolustusvoimien viestitoiminta oli järjestynyt maa-, meri- ja ilmavoimiin. Maavoimien viestitoiminta keskittyi pääasiassa puhelintoimintaan ja radio nähtiin vasta vara- tai täydennysyhteysvälineenä. Kuriositeettina voi mainita, että 1930-luvun sotilasviestikoulutuksen opetusohjelmiin sisältyivät sellaiset aiheet kuin viestikyyhkys-, viestikoira-, viittoilulippu- ja vilkkukoulutus. Puolustusvoimien viestikoulutusta täydentämässä olivat Suojeluskuntajärjestön ja Lotta-Svärd-yhdistyksen jakamat koulutukset. Koulutus oli viesti- ja ilmavalvontapalvelukoulutusta. Viestikoulutuksen myötä puolustusvoimat sai käyttöönsä pätevää keskushenkilöstöä ja radisteja. (Mikola 1980, 127-128)

Saksan hyökkäys Puolaan 1.9.1939 aiheutti myös Suomessa valmiustoimenpiteiden käynnistämisen. Toimenpiteet käsittivät viestitoiminnan osalta valmisteluiden tehostamista, materiaalivarauksien kiirehtimistä ja kaukolinjojen varaamista puolustusvoimien käyttöön. Kun Neuvostoliitto esitti Suomelle poliittiset vaatimuksensa 8.10.1939, annettiin Suomessa käsky ylimääräisten kertausharjoitusten järjestämisestä. Tämä oli käytännössä yleinen liikekannallepano. Maavoimiin kuului tuolloin 9 divisioonaa. Jokaisessa divisioonassa oli 1 viesti- ja 1 linjarakennuskomppania. Muita viestiyksiköitä olivat kolmen armeijakunnan esikuntien käyttöön tarkoitetut viesti- ja linjarakennuskomppaniat, päämajan komppaniat ja ratsuväkiprikaatin viestieskadroona. Viestiyksiköitä oli siis 27 kappaletta. Lisäksi kenttätykistöpattereissa olivat viesti- ja mittausjaokset. (Mikola 1980, 130)

Sodan päättyessä viestiaselaji oli kasvanut käsittämään 12 pataljoonaa ja 14 erillistä komppaniaa. Nämä oli jaettu sotajaotukseen siten, että viestijoukkoja oli maavoimissa ja päämajassa 10.3.1940 seuraavilla yhtymillä:

- Päämaja
- Kannaksen armeija
- Haminan ryhmä
- Rannikkoryhmä
- I Armeijakunta
- II Armeijakunta
- III Armeijakunta
- IV Armeijakunta
- Ryhmä Talvela
- Pohjois-Suomen ryhmä
- Lapin ryhmä

Lisäksi viestijoukkoja oli merivoimissa, ilmapuolustuksen käytössä ja Kotijoukkojen Esikunnalla. (Mikola 1980, 165-167)

Moskovassa allekirjoitetun rauhansopimuksen jälkeen, sotatilan edelleen jatkuessa, tehtiin puolustusvoimissa johtosuhde- ja organisaatiomuutoksia. Päämaja muutti Mikkelistä Helsinkiin ja sen tiloihin Mikkelissä muutti Kannaksen armeijan esikunnasta muodostettu Maavoimien esikunta. Päämajan viestiverkko ja -laitteet päätyivät Maavoimien esikunnan haltuun. Koska sodanuhka oli vielä olemassa, sodan aikana puolustusvoimien käyttöön otetut siviiliyhteydet pidettiin puolustusvoimien hallinnassa ja maan viestiverkkoa kehitettiin huomioiden sodanajan tarpeet. (Mikola 1980, 168)

Valvontaan kuuluvaan vikapartiointiin tarvittava henkilöstö kulutti jo ennestään alimitoitettua viestivoimaa, kaluston laatu ei vastannut meikäläisiä ilmasto-olosuhteita, radioiden viritystarkkuus osoittautui puutteelliseksi ja aaltoalueet ahtaiksi, kenttäpuhelin vikapartioinnissa liian painavaksi ja 10 linjan kenttäkeskukset tykistön ja divisioonien etukomentopaikkojen käytössä liian pieniksi. Tienvarsia seuraavien linjojen ja puihin rakennettujen johtojen kestävyys vihollisen tulitoiminnan alla ei ollut riittävä. Myöskään koulutus ja kokemus kiinteiden puhelinjohtojen hyväksikäytöstä tai kunnossapidosta ei ollut puolustusvoimissa riittävällä tasolla. (Mikola 1980, 174-175)

3.3. Sotien jälkeinen aika

1950-luvun alussa ryhdyttiin muuttamaan aikaisempia divisioonaorganisaatioita prikaateiksi, joiden organisaatioon sisällytettiin viestikomppania. Prikaati sai myös viestikomentajan ja prikaatin esikunta viestitoimiston. Viestijoukkojen ja viestiyhteyksien määrän kannalta tilanne ei merkittävästi muuttunut organisaatiomuutoksen myötä. Teknologioina käytettiin vielä puhelin- ja radiojärjestelmiä, jälkimmäisten määrän ja merkityksen kasvaessa. Radiokalustoksi kehitettiin PANU radioita, joita oli kolmea erilaista taajuusalueen ja käyttötarkoituksen mukaan. Yhtymän sisäistä joh-

tamista parantavat radiohankinnat vähensivät sähkötyksen tarvetta puheella johtamisen lisääntyessä. Radioiden suunniteltu yhteismäärä oli noin 6000 kappaletta ja ne oli suunniteltu 29 prikaatin käyttöön. Niitä ei tosin koskaan saatu hankittua suunniteltua määrää, vaan lopullinen lukumäärä vastasi noin kahta viidesosaa prikaatien radiotarpeesta. Kaapelijärjestelmien suorituskyky parani muovipäällysteisten parikaapeleiden hankinnan myötä. Kirkasjohdin jäi samalla pois prikaatin sisäisten johtamisyhteyksien rakentamisesta. Prikaatien puhelinjärjestelmät kokivat myös uudistuksia ja niitä yhtenäistettiin. Radioiden määrän kasvaessa tarvittiin myös enemmän virtalähteitä. Virtalähteiden saatavuudessa oli suuria vaikeuksia ja hankaluuksia aiheutti myös joukon materiaalin siirtämiseen tarvittavan kuljetuskaluston puute. (Sirén 2015 16-24)

Vaikka prikaatien käytössä olevien radioiden määrä lisääntyi, kaapeliyhteydet muodostivat tärkeimmän viestiyhteyden. Radioiden käyttöä rajoitettiin oman toiminnan salaamiseksi varsinaiseen taistelutoimintaan. Viestitoiminta keskittyi kaapeliyhteyksien rakentamiseen jalan ja hevosvetoisilla kärryillä. Kaapeliyhteyksien suureen vikaantumistodennäköisyyteen vihollisen tulivaikutuksessa pyrittiin vastaamaan laajalla verkkokokonaisuudella ja rakentamistavalla. Radioita suositeltiin käytettäväksi harvassa puolustuksessa, eristettyjen tukikohtien ja esikunnan välillä, sekä tiedusteluosien ja väijytyspartioiden yhteydenpidossa. (Sirén 2015, 24-29)

Seuraavalle vuosikymmenelle siirryttäessä prikaatin kokoonpanoa muutettiin. Viestikomppania jaettiin kahteen viestiosastoon ja sen henkilöstömäärää supistettiin. Samalla prikaatin esikunta varauduttiin jakamaan kahteen osaan, komentoesikuntaan ja selustaesikuntaan. Viestiosasto 1 vastasi komentoesikunnan ja viestiosasto 2 selustaesikunnan perustamisesta ja viestiyhteyksistä. (Sirén 2015, 33-34)

Radiokalustoa oli hankittu aiemmin aloitetun ohjelman mukaisesti ja hankintoja jatkettiin 1960-luvun alkupuolella. Samalla niitä ryhdyttiin modifioimaan akkukäyttöisiksi transistoriradioiksi. Kaluston jatkohankinnat keskeytettiin vuosikymmenen puolessa välissä, koska saatavilla oli kehittyneempiä radiomalleja. Samalla ryhdyttiin suunnittelemaan perusyksiköiden käyttöön komppaniaradioita. Radioiden määrä ei yltänyt riittävälle tasolle (eikä komppaniaradion kehittäminen edennyt suunnittelua pidemmälle) vuosikymmenen aikana. Puhelinjärjestelmissä ei tapahtunut mainittavaa kehitystä 1960-luvulla ja virtalähteiden hankintaa vaivasivat samat ongelmat kuin edelliselläkin vuosikymmenellä. Kuljetuskaluston osalta tilanne parani polkupyörien ja traktoreiden hankinnan myötä. (Sirén 2015, 36-40)

Viestiyhteyksien painopiste alkoi siirtyä radioverkkojen suuntaan. Painopisteen muutokseen vaikutti pyrkimys nopeaan päätöksenteko- ja toimeenpanokykyyn yhtymän johdon osalta, sekä aktiiviseen ja hyökkäävään taktiikkaan taistelutoiminnan osalta. Kaapeliyhteydet olivat kuitenkin vielä merkittävässä osassa johtamisessa, ainoastaan lyhyen kantaman radioita sai käyttää ennen taisteluiden aloittamista. Radioiden käyttöön tuli ehdottomana vaatimuksena viestiliikenteen salaaminen valmisteluvaiheessa. (Sirén 2015, 40-45)

Suomen puolustuksen doktriini muuttui 1970-luvulla maanpuolustusaluejaosta sotilaslääni jaoksi. Sotilaslääni ä muodostettiin seitsemän. Sotilaslääni jaossa prikaateista muodostettiin maavoimien liikkuvien ja iskukykyisten joukkojen runko, tosin haasteena joukkojen liikkuvuudelle oli vain osittainen moottorointi. Prikaatien (ja koko maavoimien) johtamispaikkarakennetta muutettiin siten, että komentopaikkaselustaesikuntarakenteesta siirryttiin esikunta-komentopaikkarakenteeseen. Prikaatin viestikomppanian kahden viestiosaston rakenne muutettiin kolmeen viestiosastoon. (Sirén 2015, 46-49)

70-luvulla radiohankintoja suunniteltiin tehtäväksi Neuvostoliitosta. Hankaluutena oli, että hankittavaksi suunniteltu radio ei ollut eri taajuusalueen käytön vuoksi yhteensopiva olemassa olevan radiokaluston kanssa. Yhteensopivuusongelmien lisäksi laite oli teknisesti vanhentunut. Radioiden hankinta toteutettiin lisensoimalla amerikkalaisvalmisteinen radio AN PCR-77, suomalaisittain tutumpi nimi radiolle on LV-217. Laitetta valmistettiin Suomessa 1973 lähtien. Kyseistä radiota käytettiin pataljoona- ja prikaatiradiona. Puhelinjärjestelmän kehitys lähti myös liikkeelle, kun Neuvostoliitosta hankittiin TA-57 kenttäpuhelimia. Virtalähteiden, eli käytännössä paristojen ja akkujen, määrät ja latausjärjestelmät eivät olleet riittävät. Ongelmaa pahensi jatkuvasti lisääntyvä liikuteltava radiokalusto. Liikkuvuus alkoi tällä vuosikymmenellä vastata suunniteltua tehtävää, kun prikaatien moottorointi eteni. (Sirén 2015, 50-55)

Aiemmin mainittu esikunta-komentopaikkarakenne aiheutti muutoksen prikaatin johtamistoiminnassa. Uudessa rakenteessa taistelua johdettiin suoraan esikunnasta tai komentopaikoilta. Pääasiallinen johtamistapa oli nyt puheradioilla ja kaapeliyhteydet luokiteltiin varayhteyksiksi. Tosin, ennen taisteluiden aloittamista radioita ei toiminnan salaamisen vuoksi vieläkään voinut käyttää. Tähän ratkaisuna oli prikaatin rakentama itsenäinen ja varmennettu puhelinverkko, joka tukeutui kantaviestiverkkoon (armeijakunnan viestiverkko). (Sirén 2015, 55-60)

3.4. Pohdintaa menneen ajan valvonnasta ja hallinnasta

Tarkasteltaessa historian kokemuksia valvonnan ja hallinnan näkökulmasta, voidaan todeta, että aiemmin valvonta tarkoitti pääasiassa rakennettujen lankayhteyksien vikapartiointia, kytkettyjen keskusten toimivuuden ja kapasiteetin riittävyyden arviointia, sekä puheluiden kuuntelemista liikenteen selvittämiseksi. Hallinta taasen verkkojen rakentamisen suunnittelua siten, että ne kestivät vihollisen tulivaikutusta. Tähän pyrittiin rakentamistavan valinnalla, rakentamissuunnalla ja yhteyksien varmentamisella.

Valvonnan ja hallinnan onnistumiseksi on tunnettava tiedonsiirtojärjestelmien tekniikka ja ominaisuudet. Lisäksi on tunnistettava järjestelmillä välitettävä liikenne, jotta voidaan havaita asiaankuulumaton liikennöinti. Myös kaluston ja henkilöstön on vastattava käytön vaatimuksia. Väärän tyyppinen tai alimitoitettu järjestelmä ei kykene tuottamaan sitä suorituskykyä jota tarvitaan. Jalan ja hevosvetoisesti tapahtuneesta yhteyksien rakentamisesta on viime vuosisadan aikana siirrytty moottoroitujen vies-

tiasemien käyttämiseen, mikä on omalta osaltaan lisännyt järjestelmien liikkuvuutta. Lisääntynyt liikkuvuus aiheuttaa mahdollisuuksien lisäksi myös epävarmuustekijöitä verkon muodostamiselle. Tiedonsiirtojärjestelmien rakentamiseen ja ylläpitämiseen tarvittavan henkilöstön riittävyys tulee ennalta arvioida riittävän suureksi, on helpompi vähentää henkilöstöä kuin pikaisesti lisätä sitä.

Järjestelmien käyttämät siirtomediat ovat siirtyneet kohti radiotaajuuksia langallisten yhteyksien kustannuksella. Radiotaajuuksien käytön enenemisen myötä tiedonsiirtojärjestelmien liikkuvuus on kasvanut, mikä mahdollistaa joustavamman suunnittelun ja rakentamisen, mutta myös lisää epävarmuustekijöitä.

4 ITIL – IT-PALVELUTUOTANNON VIITEKEHYS

ITIL on Iso-Britannian valtiohallinnon Central Computer and Telecommunications Agency CCTA:n 1980- ja 1990-lukujen aikana kehittämä parhaiden käytäntöjen viitekehys IT-palveluiden hallintaan. CCTA on nykyisin nimeltään Office of Government Commerce, OGC. Viitekehystä on kehitetty jatkuvasti siten, että viimeisin versio ITILv3 julkaistiin vuonna 2007. ITIL:ssä tarkastellaan IT-palveluiden hallintaa palvelun elinkaaren kautta. Palvelun elinkaari on malli, jossa kuvataan tapaa jolla, palvelunhallinta on jäsennelty, elinkaaren komponentit linkitetään toisiinsa ja vaikutusta joka yhteen komponenttiin tehdyllä muutoksella on muihin komponentteihin ja koko elinkaarijärjestelmään. ITIL:ssä palvelun elinkaari on jaettu viiteen vaiheeseen. Vaiheet ovat palvelustrategia, palvelusuunnittelu, palvelutransitio, palvelutuotanto ja jatkuva palvelun parantaminen. Palvelustrategia on vaihe jonka mukaan muut vaiheet asettuvat. Jatkuva palvelun parantaminen vaikuttaa kaikkiin muihin vaiheisiin, myös palvelustrategiaan. (ITILv3 taskukirja 2009, 13, 19-20)

Kuva 2. ITILv3 palvelun elinkaari (ITILv3 taskukirja 2009, 20)

ITIL on jaettu vaiheittain viiteen kirjaan: Palvelustrategia, Palvelusuunnittelu, Palvelutransitio, Palvelutuotanto ja Jatkuva palvelun parantaminen. Kukin kirja kuvaa yksityiskohtaisesti vaiheen prosessit ja funktiot, sekä linkitykset muihin vaiheisiin. Kuva 2 esittää ITIL:n palvelun elinkaaren kehää, jossa on kuvattu kirjojen vaiheiden keskinäiset vaikutussuhteet. Vuonna 2011 julkaistiin päivitys, jossa kirjojen johdonmukaisuutta parannettiin (ITIL Service Operation 2011, 3-5).

Tässä tutkimuksessa tarkastellaan ITIL:n elinkaaren vaiheista Palvelutuotantoa. ITIL:n viitekehyksessä valvonta ja hallinta ovat palvelutuotannon aktiviteetti. Termien suomentamisessa on käytetty Exin:n verkkosivustolta vapaasti ladattavaa ITIL-sanastoa (AXELOS 2011).

4.1. Palvelutuotanto käytäntönä

ITIL Palvelutuotanto tarkastelee IT-palvelutuotannon parhaita käytäntöjä. Palvelutuotannon tarkoituksena on hallita ja toteuttaa prosessit ja aktiviteetit joilla tuotetaan palveluita sovitulla tavalla ja tasolla asiakkaille ja käyttäjille. Palvelutuotanto on palvelun elinkaaren kannalta kriittinen vaihe, joka mahdollistaa hyvin suunniteltujen ja toteutettujen palveluiden tuottamisen. Palvelutuotantoon osallistuvalla henkilöstöllä tulee olla käytössään asianmukaiset prosessit ja työkalut palvelutuotannon kokonaisvalvontaan ja hallintaan. Palvelutuotannon pitää nähdä tuotannon kokonaiskuva myös niissä tapauksissa, kun käytetään organisaation ulkopuolisia toimittajia. ITIL Palvelutuotanto kuvaa prosessit, aktiviteetit, organisaation ja työkalut joita tarvitaan palveluiden toimittamiseen ja tukipalveluiden järjestämiseen. Näitä ovat varsinaiset palvelut, palveluiden hallinnan pro-

sessit, tarvittava teknologia ja henkilöstö. Toimittaessa ITIL:n käytäntöjen mukaisesti, organisaatio voi saada hyötyä sekä rahallisen säästön, vähentyneen työmäärän, että kohonneen palvelutason muodossa. (ITIL Service Operation 2011, 4-5)

Palveluiden tarkoitus on tuottaa asiakkaalle haluttu lopputulos ilman palvelun tuottamisesta aiheutuvia kuluja ja riskejä. Palvelut mahdollistavat asiakkaan haluaman lopputuloksen parantamalla niiden tuottamiseen tarvittavien tehtävien suorittamista ja pienentämällä sääntelyn, rahoituksen puutteen, kapasiteetin puutteen tai teknologian aiheuttamien rajoitusten vaikutuksia. Palvelun kustannuksia tarkastellaan taloudellisin mittarein, kuten ROI ja TCO. Asiakkaalle palvelutuotannosta näkyy vain palvelun kokonaishinta, joka sisältää palveluntuottajan kulut ja riskit. (ITIL Service Operation 2011, 13)

Palvelut voidaan jaotella niiden suhteessa toisiinsa tai asiakkaaseen. Ne voidaan jakaa ydinpalveluihin, mahdollistaviin palveluihin ja lisäpalveluihin. Ydinpalvelut tuottavat haluttuja lopputuloksia yhdelle tai useammalle asiakkaalle. Ne ovat palveluita joita asiakkaat ovat ostaneet ja joista ovat valmiita maksamaan. Mahdollistavia palveluita tarvitaan ydinpalveluiden tuottamiseksi asiakkaalle. Ne voivat olla asiakkaalle näkyviä tai näkymättömiä. Lisäpalveluita tarvitaan lisäämään asiakkaan kiinnostusta palvelun hankkimiseksi. Ne eivät ole välttämättömiä ydinpalvelun tuottamiseksi, mutta voivat olla merkittävä tekijä asiakkaan valitessa palvelua tuottavaa yritystä. Yksinkertaisimmillaan palvelu mahdollistaa yksittäisen tehtävän suorittamisen, mutta useimmiten palvelut ovat monimutkaisia kokonaisuuksia jotka koostuvat laajasta kirjosta toiminnallisuuksia. Tällaisten kokonaisuuksien sisältämien palveluiden määrittäminen yksittäin on haastavaa, jolloin ne kannattaa kääriä palvelupaketiksi tai palveluratkaisuksi. Palvelupaketti tai palveluratkaisu voi sisältää kaksi tai useamman palvelun, jotka voivat olla ydinpalveluita, mahdollistavia palveluita tai lisäpalveluita. (ITIL Service Operation 2011, 14)

Palvelunhallinta on kokonaisuus organisaation kyvykkyyksiä, joilla asiakkaille tarjotaan lisäarvoa palveluiden muodossa. Kyvykkyyksien ja resurssien muuntaminen lisäarvoksi asiakkaalle on palvelunhallinnan ydintoiminto. Palvelunhallinta on kyvykkyyksien lisäksi ammattimainen tapa toimia. Ammattimainen tapa toimia koostuu korkeatasoisesta tietämyksestä, kokemuksesta ja taidoista. Palvelunhallinnalle ominaisia haasteita tuottavat lopputuloksen usein aineeton hyöty, vaatimuksien riippuvuus asiakasomaisuudesta, tuotteen välitön kuluttaminen ja asiakkaan vaatimus keskeytymättömästä palvelutuotannosta. IT-palvelun hallinta (ITSM) tarkoittaa eri asioita riippuen näkökulmasta. Suurimpana haasteena on tunnistaa kulloinenkin näkökulma ja ymmärtää kuinka IT-organisaatio nähdään osana liiketoimintaa. IT-organisaation tulisi toimia palvelutuottajana, joka käyttää palvelun hallinnan periaatteita haluttujen lopputulosten saavuttamiseksi. Palvelutuottajia on kolmea eri tyyppiä; sisäinen palvelukeskus, yhteinen palvelukeskus ja ulkoinen palvelukeskus. IT-palvelun hallinnan käsitteet määrittelevät usein toimintaympäristön siten, että käytössä on vain yksi edellä mainituista palvelutuottajatyypeistä. Todellisuudessa useimmissa organisaatioissa on käytössä kahta tai kaikkia tyyppejä. Tyy-

pillisesti sisäinen IT-organisaatio tarjoaa oman organisaation lisäksi palvelua ulkopuolisille esimerkiksi verkkopalveluiden muodossa. (ITIL Service Operation 2011, 16)

Palvelunhallinnan sidosryhmiä voivat olla sisäiset tai ulkoiset asiakkaat, käyttäjät ja toimittajat. Sisäiset asiakkaat ovat kuuluvat palvelutuottaja-organisaatioon, ulkoiset asiakkaat tyypillisesti ostavat palveluita palvelutuottajalta. Käyttäjät ovat joko sisäisen tai ulkoisen asiakkaan palveluita käyttäviä henkilöitä. Toimittajat ovat (yleensä) yrityksiä jotka tarjoavat palveluiden tuottamiseen tarvittavia tuotteita tai palveluita. (ITIL Service Operation 2011, 17)

Palvelun arvo voidaan määrittää sen mukaan kuinka hyvin se vastaa asiakkaan odotuksia. Palveluilla ei ole luontaista arvoa, vaan niiden arvo syntyy siitä mitä ne mahdollistavat niiden käyttäjille. Palvelut tuottavat organisaatiolle arvoa vain silloin, kun niiden hankkimiseen käytetty kulu on pienempi kuin niiden tuottama etuus. Palveluiden arvoa voidaan määrittää niiden tarkoituksen mukaisuudella ja käytettävyydellä. Nämä yhdessä tuottavat lopputuloksen jonka perusteella palvelun hyödyllisyyttä voidaan arvioida. Yksi palvelun arvon mittari on siitä saatu hyöty. Tarkasteltaessa mitä palvelu tekee, voidaan arvioida sen hyötyä. Jos palvelu täyttää sille asetetut tavoitteet lopputuloksen osalta tai se on tehtävään sopiva, se voidaan nähdä hyötynä. Toinen palvelun arvon mittari on takuu. Takuulla tarkoitetaan varmuutta siitä, että palvelu täyttää sille asetetut vaatimukset saatavuuden, kapasiteetin ja luotettavuuden osalta. Takuuta arvioitaessa tarkastellaan sitä, kuinka palvelu on toteutettu. Tarkastelun perusteella voidaan arvioida, sopiiko palvelu käyttötarkoitukseensa. Yhteenvetona voidaan todeta, että hyöty kertoo mitä palvelu tekee ja takuu, miten se on toteutettu. (ITIL Service Operation 2011, 17-18)

Omaisuus on mikä tahansa resurssi tai kyvykkyys jota palvelun tuottamiseen käytetään. Palvelutuottajan ja asiakkaan välinen suhde perustuu omaisuuteen ja siihen, kuinka sen rooli palvelun tuottamisessa nähdään. Omaisuus jota asiakas käyttää palvelun hyödyntämiseen tai sen toimittamiseen omille asiakkailleen, nähdään palvelutuottajan näkökulmasta asiakasomaisuutena. Asiakas näkee saman omaisuuden palveluomaisuutena. Ilman asiakasomaisuutta ei ole mahdollista määrittää palvelun arvoa, siksi asiakasomaisuuden toimivuus on palvelunhallinnan tärkein huolenaihe. Palvelutuottajilla ja asiakkailla on kahdenlaista omaisuutta, resurssit ja kyvykkyydet. Resurssit vaikuttavat suoraan palvelutuotantoon ja toteuttavat sitä. Kyvykkyydet kuvaavat organisaation kykyä koordinoida, hallita ja käyttöön ottaa resursseja. Kyvykkyydet ovat kokemusta, tietämystä ja tietoa joka organisaatiolla on sen henkilökunnalla, järjestelmissä, prosesseissa ja tekniikassa. Resurssien hankkiminen on kyvykkyyksiä helpompaa. Palvelutuottajan tuotantokyky on riippuvainen resursseista, jotka sillä on hallussaan, mutta ilman riittäviä kyvykkyyksiä resursseja ei voi hyödyntää riittävän tehokkaasti. (ITIL Service Operation 2011, 20)

Palvelunhallinnan prosessit määrittävät palvelutuotannossa käytettävät toiminnot, niiden riippuvuudet ja suoritusjärjestyksen. Prosesseille ominaista ovat mitattavuus, tunnetut lopputulokset, lopputuloksen päätyminen

asiakkaalle ja prosessin käynnistyminen tietyissä olosuhteissa. Prosessin tulee tuottaa halutun lopputuloksen lisäksi tietoa, jonka perusteella prosessin toimintaa voidaan arvioida, sekä raportteja ja ehdotuksia prosessin parantamiseksi. Prosessin lopputuloksen tulee vastata sille asetettuja ehtoja ja sen tulee olla toistettavissa. Prosessin tehokkuutta mitataan sen hallittavuudella ja siihen käytetyillä resursseilla. (ITIL Service Operation 2011, 20)

ITIL ei suoraan kerro kuinka yrityksen tulisi organisoida palvelunhallintansa. Organisoinnissa on otettava huomioon yrityksen olemassa oleva organisaatio ja palvelunhallinnan tarpeet. Huomioitavia asioita ovat toiminnot, roolit, sekä organisaatiokulttuuri ja toimintatavat. (ITIL Service Operation 2011, 23)

Toiminto on tiimi tai muu resurssi joka toteuttaa yhtä tai useampaa prosessia tai aktiviteettia. Toiminnot voi olla jaettu useamman organisaatioyksikön kesken. Jotta palvelun elinkaaren toteuttaminen onnisuu, täytyy roolien ja vastuiden olla selkeästi jaettu elinkaaren kaikissa vaiheissa. Roolit on jaettava tekijöille ja tiimien, ryhmien ja toimintojen pitää olla selkeästi perustettuja ja hallittuja. Ryhmä koostuu samanlaisia toimintoja tekevistä ihmisistä. Ryhmän jäsenten käyttämien järjestelmien ei tarvitse olla samoja, eikä ryhmä yleensä ole muodollinen organisaatio. Tiimi on muodollisempi organisaatio, jonka jäsenet työskentelevät yhteisen päämäärän eteen. Tiimejä käytetään esimerkiksi tapahtumien tai ongelmien hallintaan. Osasto on muodollinen organisaatio joka toteuttaa määrättyjä toimintoja. (ITIL Service Operation, 23)

ITIL määrittää parhaita käytäntöjä palvelupisteen, teknisen hallinnan, IT-käyttöpalvelun hallinnan ja sovellushallinnan toiminnoille. Palvelupiste on yhteyspiste, johon käyttäjät ottavat yhteyttä palvelunkeskeytystilanteissa, palvelupyyntöjen välittämiseksi tai muutoksien pyytämiseksi. Tekninen hallinta tarjoaa teknistä osaamista ja resursseja tuotannossa olevien palveluiden tarvitsemalla tavalla. IT-käyttöpalvelun hallinta suorittaa palveluiden hallinnan tarvitsemia päivittäisiä toimenpiteitä. Sovellushallinta vastaa sovelluksista niiden elinkaaren ajan. Sovellushallinta vastaa ja ylläpitää tuotannossa olevat sovellukset. Rooli muodostuu vastuista, toiminnoista ja käyttöoikeuksista, jotka myönnetään henkilölle tai tiimille. Rooleja voi yhdistellä yrityksen mukaan. Organisaatiokulttuuri tarkoittaa yhteisiä arvoja ja normeja jotka määrittävät palvelutuottajan yhteistoimintaa sidosryhmien kanssa. Organisaation arvot ovat toimintatapoja, jotka vaikuttavat organisaatiokulttuuriin. Hyvin toimivat palvelutuottajat asettavat arvoverkkonsa tehokkuuden ja vaikuttavuuden mukaan, sekä viestittävät kulttuuristaan henkilökunnalleen arvoverkon välityksellä. Toimintaa rajoittavilla tekijöillä, kuten hallinnolla, kyvykkyyksillä, standardeilla, resursseilla, arvoilla ja etiikalla on merkittävä rooli organisaatiokulttuurin muodostumisessa. (ITIL Service Operation 2011, 23)

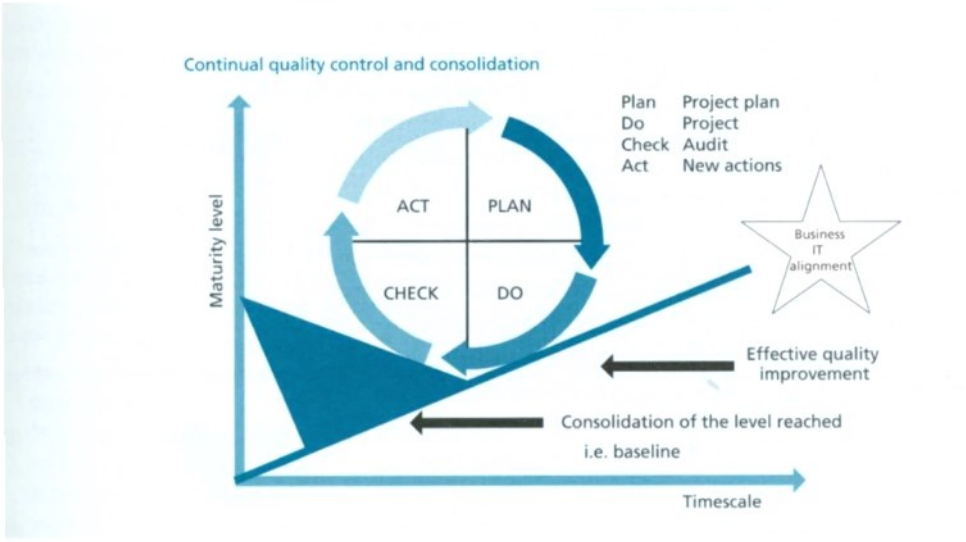
Palvelusalkku sisältää kaikki palvelutuottajan hallitsemat palvelut ja se osoittaa palvelutuottajan sitoutumisen ja sijoitukset asiakkaisiin ja markkinaan. Palvelusalkku voit sisältää muitakin kuin palvelutuottajan tuottamia palveluita. Palvelusalkussa kuvataan kaikki palvelutuottajan tuotan-

nossa olevat tai tuotantoon tulevat resurssit. Palvelusalkku voidaan jakaa kolmeen osaan: palvelukehitysputkeen, palveluluetteloon ja käytöstä poistettuihin palveluihin. Palvelukehitysputki sisältää kaikki ne palvelut joita suunnitellaan käyttöönotettavaksi tai jotka ovat kehityksessä. Palvelukehitysputkessa olevista palveluista ei yleensä kommunikoida asiakkaille. Palveluluettelo on asiakkaille näkyvä osa palvelusalkkua. Palveluluettelo määrittää kaikki palvelutuottajan tuottamat palvelut, mukaan lukien palvelut jotka ovat käyttöönotettavissa. Palveluluettelosta käy ilmi käytössä olevat palvelut, niiden käyttötapaukset, liiketoimintaprosessit jotka ne mahdollistavat, sekä palvelutason ja palvelun laadun jota asiakas voi palvelulta odottaa. Palveluluettelosta käy myös ilmi tukipalvelut, joita palvelutuottaja tarvitsee voidakseen toteuttaa asiakkaalle näkyvän palvelun. Käytöstä poistetut palvelut eivät ole saatavilla uusille käyttäjille ilman erillistä sopimusta palvelun tuottamisesta. (ITIL Service Operation 2011, 24)

Laadukas tietämyksen ja tiedon hallinta mahdollistaa prosessien toteuttamisen ja tukee tiedon vaihtoa palvelun elinkaaren eri vaiheiden ja prosessien välillä. Palvelutietämyksen hallintajärjestelmä (SKMS) mahdollistaa tehokkaan päätöksenteon tuen ja pienentää puuttuvien mekanismien aiheuttamia riskejä. Hallintajärjestelmän perustaminen voi olla suuri investointi ja jokainen organisaatio lähtee eri lähtökohdista. Lähtökohtaisesti käytössä olevan datan, tiedon ja tietämyksen tulee olla toisiinsa liittyviä läpi organisaation. Palvelutietämyksen hallintajärjestelmän perustamisen voi aloittaa perustamalla dokumenttien hallintajärjestelmän ja/tai konfiguraation hallintajärjestelmän. Palvelutietämyksen hallintajärjestelmän tulee sisältää esityskerros, tietämyksen käsittelykerros, tiedon yhdistämiskerros ja datakerros. Esityskerros mahdollistaa haut, selaamisen, noutamisen, tilaamisen ja kollaboraation. Näkymien tulee olla suojattu siten, että vain sallitut käyttäjät voivat nähdä tai muokata järjestelmään sijoitettua tietämystä, tietoa tai dataa. Tietämyksen käsittelykerroksella tieto muutetaan käyttökelpoiseksi tietämykseksi. Tiedon yhdistämiskerros mahdollistaa datan yhdistelemisen useista lähteistä. Datakerroksella sijaitsevat työkalut joilla dataa haetaan ja kerätään, sekä varsinainen data jäsentämättömässä ja jäsennetyssä muodossa. Hallintajärjestelmän tärkein komponentti on palvelusalkku. (ITIL Service Operation 2011, 24-25)

Hallintatapa sitoo IT-palvelutuotannon liiketoimintaan. Palvelut ovat yksi tapa varmistaa, että organisaatio kykenee toteuttamaan hallintatapaa. Hallintatapa määrittää yleiset ohjeet, menettelytavat ja säännöt, joita IT-palvelutuotanto ja liiketoiminta noudattavat. Hallintatapa varmistaa, että politiikoita ja liiketoimintastrategiaa noudatetaan ja että vaadittavia prosesseja toteutetaan. Hallintajärjestelmä on menettelytapojen, prosessien, toimintojen, standardien, ohjeiden ja työkalujen muodostama viitekehys, joka varmistaa, että organisaatio voi saavuttaa tavoitteensa. Organisaation hallintajärjestelmä voi koostua myös useista järjestelmästandardeista, kuten laatujärjestelmä (ISO 9001), ympäristöjärjestelmä (ISO 14000), palvelunhallintajärjestelmä (ISO/IEC 20000), tietoturvallisuuden hallintajärjestelmä (ISO/IEC 27001) tai ohjelmisto-omaisuuden hallintajärjestelmä (ISO/IEC 19770). Edellä mainitut hallintajärjestelmät käyttävät PDCA-

sykliä (kuva 3) ongelmanratkaisumallina ja kehittämismenetelmänä. (ITIL Service Operation 2011, 27)



Kuva 3. PDCA-sykli (ITIL Service Operation 2011, 27)

Palvelut ja prosessit määrittävät kuinka muutokset tapahtuvat, kun taas rakenne määrittää kuinka ne liittyvät toisiinsa. Rakenne määrittää kuinka prosessit, ihmiset, teknologia ja yhteistyökumppanit kytkeytyvät toisiinsa. Rakenne on elintärkeä tiedon lajittelussa. Palvelun elinkaaren rakenne on organisoiva viitekehys, jota tukevat organisaation rakenne, palvelusalkku ja organisaation sisäiset palvelumallit. Rakenne voi vaikuttaa tai määrittää organisaation tai siinä toimivien ihmisten käyttäytymistä. Organisaation tulee lähestyä yhteistyöhön perustuvalla tavalla käyttöomaisuutta, jolla asiakkaille tuotettavia palveluita tuotetaan ja tuetaan. Erikoistuminen ja toiminnan koordinointi ovat elinkaariajattelun ytimessä. Erikoistuminen mahdollistaa asiantuntijoiden keskittymisen palvelua tuottaviin osakokonaisuuksiin, mutta palvelun osakokonaisuuksien tulee toimia yhteen lisäarvon saavuttamiseksi. Koko elinkaaren kestävä koordinaatio luo ympäristön, joka on keskittynyt liiketoimintaan ja asiakkaan saavuttamaan hyötyyn IT:n tavoitteiden ja projektien sijaan. Koordinointi on tärkeää myös toiminnallisten ryhmien, koko arvoverkon, sekä prosessien ja teknologian välillä. Palvelutuotanto on tehokkaampaa, kun ihmisillä on selkeä käsitys prosessien keskinäisestä vuorovaikutuksesta koko palvelun elinkaaren ajan organisaation sisällä ja ulkoisten toimijoiden kanssa. Palvelunhallintaprosessien yhteensovittaminen riippuu saatavilla olevasta tiedosta yli prosessien ja organisaation sisäisten rajojen. Tiedon liikkuvuus omalta osaltaan riippuu tukevien teknologioiden ja tiedonhallintajärjestelmien käyttöönottamisesta koko organisaation laajuisesti. Toisaalta, jos palvelunhallintaprosesseja otetaan käyttöön, noudatetaan tai muutetaan ilman yhteistyötä organisaation muiden osien kanssa, niistä voi muodostua byrokraattinen painolasti joka ei tuota lisäarvoa. Elinkaaren eri vaiheiden tulee toimia yhdessä tukien palvelunhallinnan tavoitetta arvon tuottamiseksi liiketoiminnalle. Aiemmin kuvattu palvelutietämyksen hallintajärjestelmä mahdollistaa elinkaaren eri vaiheiden yhteensovittamisen ja tarjoaa turvallisen ja hallitun pääsyn tietämykseen, tietoon ja dataan joita tarvitaan palveluiden hallinnassa ja toimittamisessa asiakkaille. Palvelutuotanto on se elinkaaren

vaihe, joka toteuttaa sovittujen palveluiden tuottamiseksi vaadittuja toimintoja ja prosesseja. Palvelutuotantovaiheessa palvelustrategiassa määritetty palvelun arvo toteutuu. (ITIL Service Operation 2011, 30)

4.2. Palvelutuotannon periaatteet

Palvelutuotanto on päivittäisten toimintojen lisäksi vastuussa palveluiden elinkaaren hallintaan ja teknologian hallintaan liittyvistä prosesseista. Elinkaaren hallintaan liittyen palvelutuotannon tehtävänä on optimoida palveluiden kustannusta ja laatua. Teknologian hallintaan liittyen palvelutuotanto varmistaa palveluita tukevien komponenttien toiminnan ja suorittaa niiden kontrollointiin liittyviä toimintoja. Kokonaisuudessaan palvelutuotannon vastuulla on palveluiden tuottaminen tehokkaasti ja hyväksyttävällä kustannuksella määritettyjen palvelutasojen mukaisesti ja asiakasta tyydyttävällä tavalla. Palvelutuotanto on se palveluiden elinkaaren vaihe, jossa ulosmitataan IT-investointeihin käytetty varallisuus. (ITIL Service Operation 2011, 35)

Palvelutuotannon optimointia voidaan tehdä pitkän tähtäimen parantamisena tai lyhyen tähtäimen muutoksina. Pitkän tähtäimen parantaminen tarkoittaa palvelutuotannon prosessien, teknologioiden, toimintojen ja prosessien tuotosten tarkastelua pidemmällä aikavälillä ja mahdollisesti palveluiden parantamista palvelusuunnittelun ja palvelutransition kautta. Lyhyen tähtäimen parantaminen tapahtuu palvelutuotannon sisällä ja on enemmän hienosäätöä kuin koko palvelun muuttamista. (ITIL Service Operation 2011, 35)

Palvelutuotannon prosesseja ovat herätteidenhallinta, tapahtumanhallinta, palvelupyyntöprosessi, ongelmanhallinta ja pääsynhallinta. Herätteidenhallinnan tarkoitus on havaita ja ymmärtää herätteitä ja päättää oikeista toimenpiteistä. Tapahtumanhallinnan tarkoituksena on palauttaa keskeytynyt palvelu ja minimoida sen vaikutukset palvelutuotantoon. Palvelupyyntöprosessi käsittelee käyttäjien palvelupyyntöjä ja muutosehdotuksia. Ongelmanhallinta pyrkii löytämään tapahtumia aiheuttavia juurisyitä, toimii ennakoivasti tapahtumien estämiseksi ja dokumentoi tunnettuja virheitä palvelun palauttamisen nopeuttamiseksi. Pääsynhallinnan tarkoituksena on mahdollistaa järjestelmien toimintatapojen mukainen käyttö ja hallita pääsyoikeuksia. (ITIL Service Operation 2011, 36-37) Palvelutuotannon prosesseja käsitellään myöhemmin omissa kappaleissaan.

Palvelutuotannon toimintoja ovat palvelupiste, tekninen hallinta, IT-käyttöpalvelun hallinta ja sovellushallinta. Palvelupiste on paikka joka vastaanottaa käyttäjien ilmoituksia palvelupoikkeamista, palvelupyyntöjä ja muutosehdotuksia. Tekninen hallinta tarjoaa osaamista ja resursseja tuotannossa olevien palveluiden tukemiseksi ja käytössä olevan infrastruktuurin hallitsemiseksi. IT-käyttöpalvelun hallinnan toimenpiteisiin kuuluu päivittäinen palveluiden hallinta ja IT-infrastruktuurin tuki. IT-käyttöpalvelu jakaantuu palveluiden toimintaa valvovaan ja IT-laitteistojen toimintaa valvovaan osaan. Sovellushallinnan vastuulla on sovellusten hallinta koko niiden elinkaaren ajan. Sovellushallinta osallistuu sovellusten käytön suunnitteluun, testaamiseen ja parantamiseen. (ITIL

Service Operation 2011, 38) Palvelutuotannon toimintoja käsitellään myöhemmin omissa kappaleissaan.

Muuttuva toimintaympäristö aiheuttaa palvelutuotannolle haasteen palvelun jatkuvuuden turvaamisen ja muutoksiin sopeutumisen välillä. Tasapaino on pyrittävä löytämään järjestelmien teknisen ja asiakasorientoituneen näkökulman, vakauden ja vastaanottokyvyn, palvelun laadun ja kustannusten, sekä reaktiivisen ja ennakoivan toimintatavan välillä. Teknisesti orientoitunut palvelutuotanto on vaarassa tuottaa järjestelmiä jotka eivät tuota riittävästi lisäarvoa, kun taas liiallisesti asiakasorientoitunut ei välttämättä pysty tuottamaan palveluita sovitulla tasolla. IT-infrastruktuurin tulee olla vakaa, mutta pystyä takaamaan palveluiden saatavuus. Palvelun laatua tulee parantaa jatkuvasti, mutta samaan aikaan kustannuksia ei voi kasvattaa samassa tahdissa. Pelkästään reagoimalla ei pysty ylläpitämään kilpailukykyä, mutta liiallinen ennakointi voi nostaa kustannuksia kannattamattomalle tasolle. (ITIL Service Operation 2011, 39-46)

Palvelutuotannon henkilöstön tulee ymmärtää toimivansa palvelutehtävässä. Heidän tulee toimia viipeettömästi, ammattimaisesti ja käyttäytyä kohteliaasti, jotta liiketoiminta voi keskittyä omiin tehtäviinsä. Henkilökuntaa tulee kouluttaa niin palveluiden tuottamiseen ja tukemiseen, kuin tapaan jolla palveluita tuotetaan. Onnistuneella rekrytöinnillä ja henkilöstön kouluttamisella on suuri merkitys palveluiden tuottamisen onnistumisessa. (ITIL Service Operation 2011, 46)

Palvelutuotannon henkilöstö osallistuu varsinaisen palvelutuotannon lisäksi palveluiden elinkaaren muihin vaiheisiin. He tuovat palvelustrategian luomiseen tietoa olemassa olevasta suorituskyvystä ja työkuormasta. Muita palvelutuotannon keräämiä tietoja ovat tuotannon kustannukset, strategian vaikutukset tuotannossa oleviin palveluihin, tuotannon rajoitukset jotka voivat vaikuttaa strategian luomiseen ja suunnitellun strategian palvelutuotannolle aiheuttamien riskien tunnistaminen. Palvelusuunnittelu tuottaa palvelutuotannolle määrityksiä palveluiden tavoitteista ja suorituskykyvaatimuksista, kuinka palvelut linkittyvät IT-infrastruktuuriin, palvelutuotannon suorituskykyvaatimuksista, palveluiden ja teknologian yhteensovittamisesta, kyvyn mallintaa teknologian ja liiketoiminnan muutoksien vaikutuksia ja kustannustietoisuutta ROI:n määrittämiseksi ja kustannussäästöjen löytämiseksi. Palvelutransitio antaa mahdollistaa palvelutuotannon henkilöstölle tilaisuuden kouluttautua uusien palveluiden tuottamiseen, osallistua tuotantoon hyväksyntään, tunnistaa uusien palveluiden käyttöönoton vaikutuksia tuotannossa oleviin palveluihin, valmistautua uusien tai muuttuneiden palveluiden käyttöönottoon ja osallistua uusien tai muuttuneiden palveluiden laadunvarmistukseen. (ITIL Service Operation 2011, 48)

Toimiva kommunikointi palveluiden elinkaareen osallistuvien tiimien ja osastojen, käyttäjien ja sisäisten asiakkaiden ja palvelutuotannon tiimien ja osastojen välillä on ensiarvoisen tärkeää. Toimiva kommunikointi voi ennaltaehkäistä ongelmien syntymistä ja vähentää niiden vaikutusta palvelutuotantoon. Kaikella kommunikoinnilla tulee olla tarkoitus ja haluttu lopputulos. Tiedolla tulee olla selkeä kohde, jolla on jaetulle tiedolle käyttö-

tarve. Tiedon tarpeellisuutta vastaanottajille tulee ajoittain arvioida, jotta voidaan varmistua, että tieto on vastaanottajalle tarpeellista. Tiedonvaihtokanava tulee olla ennalta määrätty, jotta vastaanottaja osaa ottaa sen huomioon omassa toiminnassaan. Tiedonvaihtokanavana voivat toimia erilaiset sähköposti- ja pikaviestiohjelmat, sosiaalinen media tai mikroblogi-palvelut, puhelinkokoukset, videoneuvottelut, dokumenttien jakelujärjestelmät tai perinteiset kokoukset. (ITIL Service Operation 2011, 49-52)

IT-käyttöpalvelun hallinta, sekä tekninen hallinta ja sovellushallinta tiimit ja osastot osallistuvat dokumentointiin. Dokumentointi taltioidaan dokumenttien hallintajärjestelmään tai palvelutietämyksen hallintajärjestelmään. Dokumentointitehtäviä ovat prosessikäsikirjojen laatiminen ja päivittäminen, teknisten piirrosten laatiminen ja päivittäminen, suunnitelmadokumenttien laatiminen ja päivittäminen, palvelusalkun laatiminen ja päivittäminen, sekä palveluhallintatyökalujen ohjeiden laatiminen ja päivittäminen. (ITIL Service Operation 2011, 52)

4.3. Palvelutuotannon prosessit

Kuten jo aiemmin mainittiin, palvelutuotannon prosesseja ovat herätteidenhallinta, tapahtumanhallinta, palvelupyyntöprosessi, ongelmanhallinta ja pääsynhallinta. Seuraavissa kappaleissa kuvataan nämä prosessit tarkemmin.

4.3.1. Herätteidenhallinta

Heräte on konfiguraation rakenneosan tai IT-palvelun tilassa tapahtunut muutos. Herätteet havaitaan IT-palvelun, konfiguraation rakenneosan tai valvontatyökalun luomista ilmoituksista. Herätteiden havaitsemiseen on kaksi tapaa: aktiivinen ja passiivinen havainnointi. Aktiivinen havainnointi tarkoittaa valvontatyökalun tekemää ajoittaista konfiguraation rakenneosien tarkkailua muutosten havaitsemiseksi. Passiivisessa havainnoinnissa valvontatyökalu vastaanottaa IT-palveluiden tai konfiguraation rakenneosien luomia ilmoituksia poikkeamista. Herätteidenhallinta tunnistaa ja tulkitsee ilmoitukset, sekä päättää jatkotoimenpiteistä. Riippuen herätteiden sisältämästä tiedosta, herätteidenhallinta voidaan automatisoida. Herätteidenhallintaprosessia voidaan käyttää konfiguraation rakenneosien, ympäristötekijöiden, ohjelmistojen lisenssitietojen, turvajärjestelmien ja normaalin toiminnan hallintaan sekä automatisointiin. Herätteidenhallinta ei ole sama asia kuin valvonta. Herätteidenhallinta keskittyy IT-infrastruktuurin ja palveluiden toiminnan kannalta merkityksellisten ilmoitusten havaitsemiseen, kun taas valvonta tarkkaillee ympäristöä laajemmin. Herätteidenhallinta mahdollistaa tapahtumien havaitsemisen ennen kuin ne aiheuttavat keskeytyksiä palvelutuotannolle ja luo pohjaa tuotannon automatisoinnille. (ITIL Service Operation 2011, 58-59)

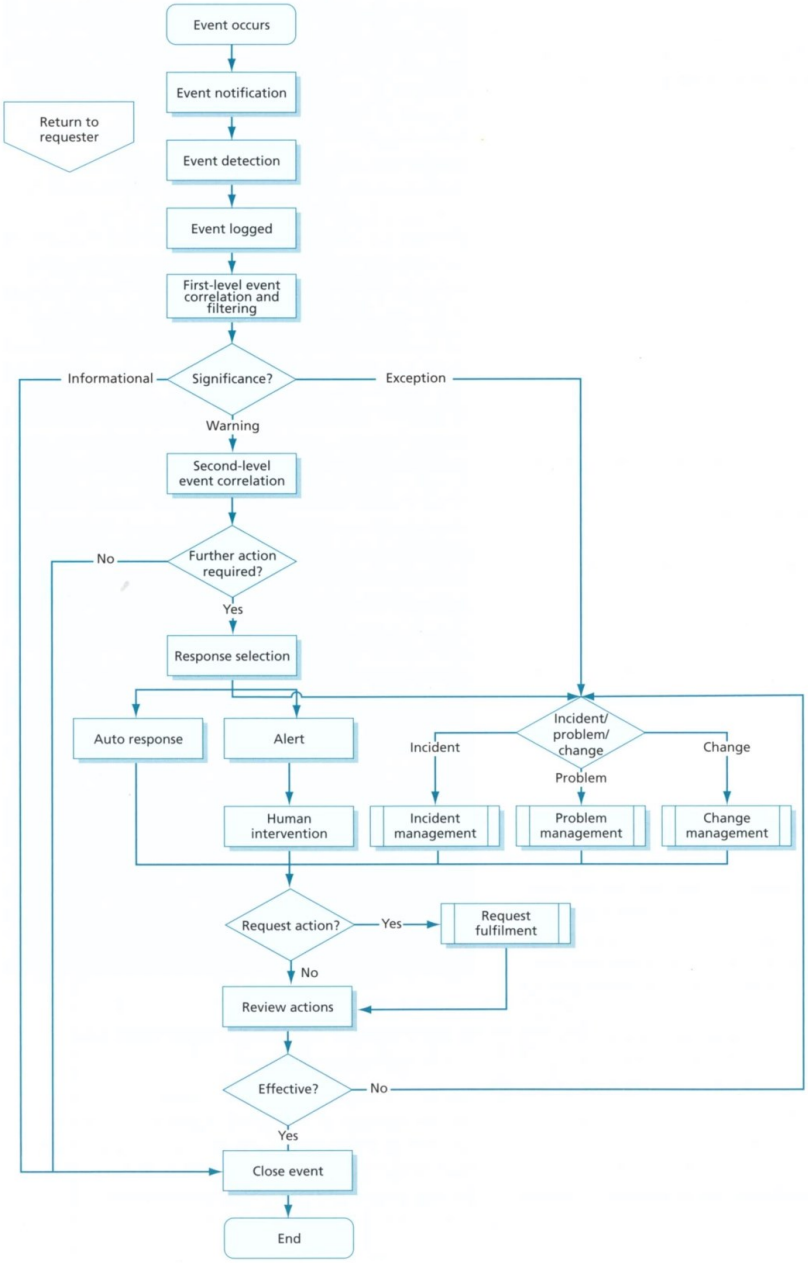
Herätteidenhallinnan toimintatapa tulisi laatia siten, että ilmoitukset välitetään vain niiden käsittelystä vastuussa oleville osastoille, ryhmille tai henkilöille. Herätteidenhallinta ja tuki tulisi mahdollisuuksien mukaan keskittää, jotta herätteiden aiheuttamien toimenpiteiden luomat ilmoitukset voi-

daan hallitusti käsitellä. Kaikkien sovellusten tulisi käyttää standardeja ilmoituksia ja protokollia herätteiden luomiseen. Herätteidenhallinta tulisi olla automatisoitu inhimillisten virheiden välttämiseksi ja niiden käsittelyyn tarvittavan henkilöstön minimoimiseksi. (ITIL Service Operation 2011, 60)

Herätteet voidaan luokitella normaalia toimintaa ilmaiseviin, epänormaalia toimintaa ilmaiseviin ja epätavallista mutta ei poikkeuksellista toimintaa ilmaiseviin herätteisiin. Normaalia toimintaa on esimerkiksi sähköpostin perillemeno ilmoitus tai ajastetun toiminnan valmistuminen. Epänormaalia toimintaa voi olla työaseman skannauksessa paljastunut luvaton ohjelmisto tai käyttäjän yritys kirjautua sovellukseen väärällä salasanalla. Epätavallista mutta ei poikkeuksellista toimintaa saattaa olla esimerkiksi toimenpiteen valmistumisajan normaalia pidempi kesto. Herätteiden luokittelun lisäksi on tärkeää luoda sopivat suodattimet merkityksellisten herätteiden havaitsemisen helpottamiseksi. (ITIL Service Operation 2011, 60-61)

Tehokkaan herätteidenhallinnan toteuttamiseksi ei riitä palvelun tuotantokäyttöön ottaminen. Herätteidenhallinta tulee suunnitella jo palvelusuunnittelussa, sekä kokeilla ja arvioida palvelutransitiossa. Palvelutuotannon toimijat osallistuvat näihin vaiheisiin ja tuovat suunnitteluun osaamisensa konfiguraation rakenneosien ja palveluiden valvonnasta ja hallinnasta, virheilmoitusten luomisesta, herätteiden havaitsemisesta ja hälytysmekanismeista. (ITIL Service Operation 2011, 61-63)

Herätteidenhallinnan vaiheet on hyvä kuvata prosessikaavioksi. Vaiheita ovat herätteen luomisen aiheuttanut syy, kuinka heräte luodaan, havaitaan ja kirjataan. Prosessin tulee myös tehdä herätteille korrelaatioita ja suodatuksia sellaisten herätteiden kohdalla jotka eivät aiheuta palvelutuotantoon häiriöitä. Herätteiden merkityksellisyyden luokittelu tavallisiin, epätavallisiin ja tavallisiin mutta poikkeuksellisiin nopeuttaa prosessin kulkua. Kaikkiin heräteluokkiin ei tarvitse välittömästi reagoida, vaan esimerkiksi tavalliset herätteet voidaan kirjata ja jättää normaalissa palvelutuotannossa huomiotta. Epätavallisia herätteitä tulee tarkastella tarkemmin ja arvioida niiden vaikutuksia palvelutuotantoon. Arvioinnin perusteella päätetään jatkotoimenpiteistä, joita voivat olla esimerkiksi tapahtuman luominen tapahtumanhallintaprosessiin, ylläpitohenkilöstön hälyttäminen, käyttäjän pääsyn rajoittaminen resursseihin tai herätteen kirjaaminen ja prosessin lopettaminen sen kohdalla. Kuvassa 4 on esimerkki herätteidenhallinnan prosessikaaviosta. (ITIL Service Operation 2011, 58-68)



Kuva 4. Esimerkki herätteidenhallinnan prosessista (ITIL Service Operation 2011, 64)

Herätteidenhallinnan esimerkkiprosessi sisältää liipaisimia, syötteitä, prosessin lopputuotteita ja kytköksiä muihin palvelun elinkaaren prosesseihin. Herätteenhallinnan voi liipaista mikä tahansa muutos konfiguraation rakenneosassa, automaattisissa toimenpiteissä tai prosesseissa, ajastetussa tehtävässä (esimerkiksi tehtävän valmistuminen), käyttäjän kirjautuminen järjestelmään tai määritetyn käyttöasteen kynnysarvon ylittyminen. Syötteenä prosessille toimivat esimerkiksi palvelutason vaatimukset; hälytykset, varoitukset ja kynnysarvot; herätteiden korrelaatiotaulut, säännöt, herätekoodit ja automaattiset vasteet; roolit ja vastuut herätteiden havaitsemisesta ja niiden välittämisestä vastuutahoille; tuotannolliset toimenpiteet herätteiden tunnistamiseksi, kirjaamiseksi, siirtämiseksi seuraavan tason asiantuntijoille tai tiedottamiseksi. Prosessin tuotteina voi olla tapahtumailmoitus, ongelmailmoitus, muutospyyntö, heräteilmoitus, automaattinen toimenpide tai hälytys ja palveluhenkilön hälyttäminen. Herätteiden-

hallinta voi kytkeytyä palvelun elinkaaren vaiheista palvelusuunnitteluun tai palvelutransitioon. Se voi myös käynnistää palvelutuotannon tapahtuman-, ongelman-, tai pääsynhallinnan prosesseja. (ITIL Service Operation 2011, 69-71)

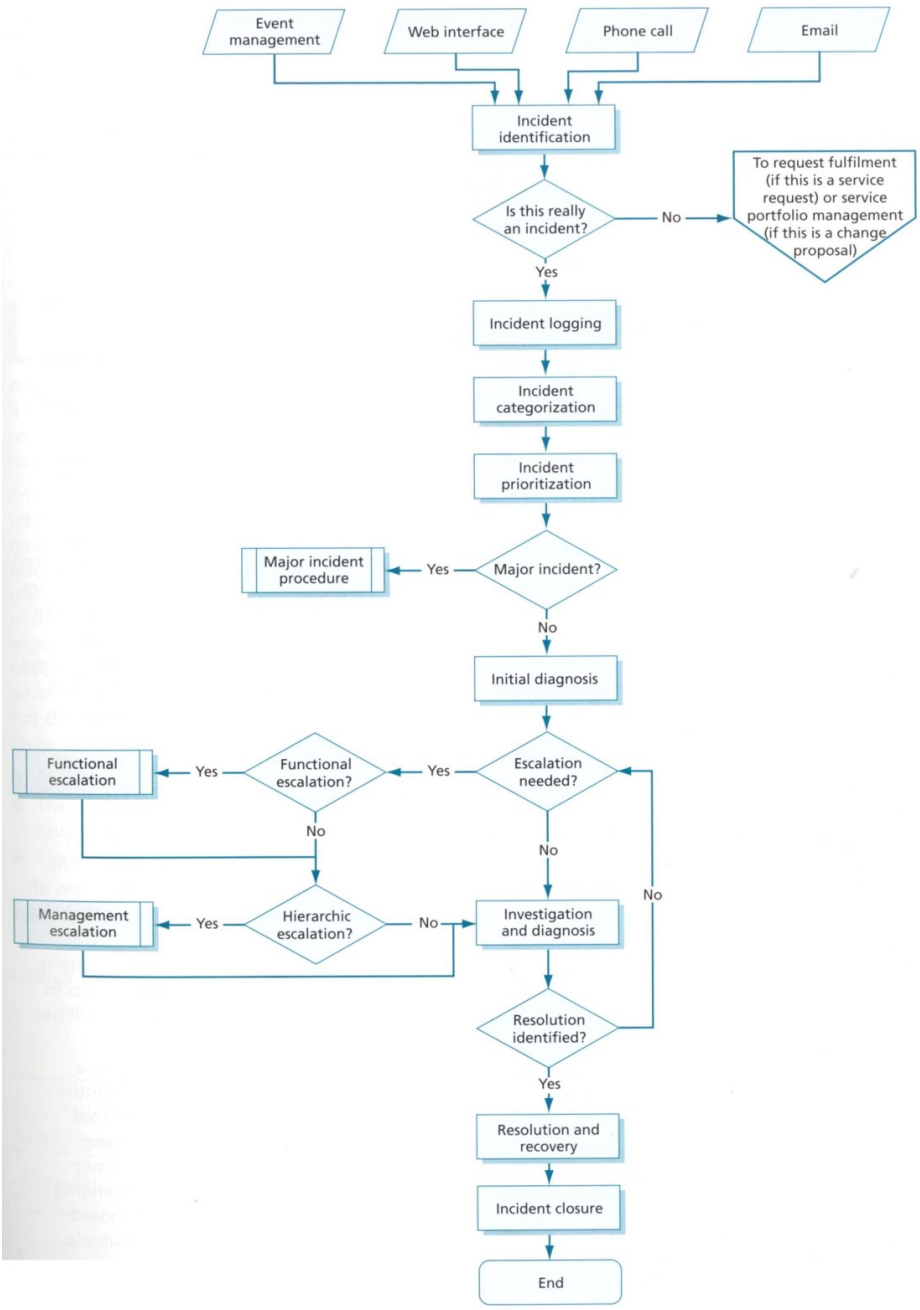
4.3.2. Tapahtumanhallinta

Tapahtuma tarkoittaa suunnittelematonta palvelutuotannon keskeytystä tai palvelutuotannon tason laskua. Tapahtuma voi olla myös konfiguraation rakenneosan häiriö, jolla ei ole suoranaista vaikutusta palvelutuotantoon. Tapahtumia hallitaan tapahtumanhallintaprosessilla. Tapahtumanhallinnan tarkoituksena on palauttaa palvelun normaalitila mahdollisimman pian ja minimoida tapahtuman vaikutus palvelutuotantoon. Normaalitila on tuotannon tila, jossa palvelut ja konfiguraation rakenneosat toimivat sovitulla tavalla ja tasolla. Tapahtumanhallinta käsittelee kaikki tapahtumat jotka aiheuttavat tai saattavat aiheuttaa keskeytyksiä palvelutuotantoon. Näitä voivat olla käyttäjiltä tulleet kysymykset ja kyselyt, tapahtumanhallinnan havaitsemat toimintahäiriöt tai teknisen henkilöstön raportoimat toimintahäiriöt. Käyttäjien yhteydenotot eivät ole aina tapahtumia, vaan ne voivat olla myös palvelupyyntöjä. Vaikka molemmat käsitellään palvelupisteellä, palvelupyyntöjä ei kirjata tapahtumina, koska ne eivät tarkoita, että palvelussa olisi häiriö. Tapahtumat eivät myöskään koskaan muutu ongelmiksi, vaikka niiden perusteella voidaankin muodostaa ongelma ongelmanhallintaprosessin käsiteltäväksi. Tapahtumanhallinta on näkyvä osa palvelutuotantoa ja se onkin yleensä ensimmäisenä käyttöönotettu prosessi. (ITIL Service Operation 2011, 72-73)

Hyvä palvelutuotannon toimintatapa on viipeetön tiedottaminen tapahtumista ja niiden tilasta niille käyttäjille tai asiakkaille, joiden palveluihin tapahtumalla on vaikutusta ja niille jotka selvittävät tapahtumia. Tapahtumat tulee ratkaista sallituissa aikarajoissa. Tieto tapahtumista tulee tallettaa tapahtumanhallintajärjestelmään, jolloin tapahtumista raportointi ja niiden tutkiminen ovat helpompaa. Tapahtumakirjauksien määräaikaisella tarkastelulla varmistutaan niiden oikeasta kirjauksesta ja kategorisoinnista. Tapahtumat tulee kirjata määrämuotoisina. Tapahtumien priorisointi ja eskaloinnin perusteet on määritettävä, jotta päätöksenteko tapahtumien käsittelystä ei ole yksittäisen tukihenkilön harteilla. (ITIL Service Operation 2011, 74)

Tapahtumanhallintaa suunniteltaessa on otettava huomioon tapahtumille asetettavat aikarajat, tapahtumamallit, laajavaikutteisten tapahtumien tunnistaminen ja tapahtumien tilan seuraaminen. Tapahtumille asetettavat aikarajat ovat sovittu asiakkaan kanssa palvelua käyttöönotettaessa. Tapahtumamalli kuvaa tapahtuman käsittelemiseen tarvittavat vaiheet. Vaiheiden määrittäminen mahdollistaa tietynlaisten tapahtumien ohjaamisen suoraan niiden käsittelystä vastaaville tahoille. Laajavaikutteisilla tapahtumilla on lyhyemmät ratkaisun aikarajat ja korkeampi tärkeys kuin tavallisilla tapahtumilla. Laajavaikutteisen tapahtuman vaikutus käyttäjiin on normaalia suurempi. Tapahtumien tila voi olla esimerkiksi avoin, työn alla, ratkaistu tai suljettu. Avoin tapahtuma on vastaanotettu, mutta sitä ei ole ohjattu tukiorganisaatiolle. Työn alla olevaa tapahtumaa tutkitaan parhail-

laan. Ratkaistu tapahtuma tarkoittaa sitä, että tapahtuma on käsitelty, mutta käyttäjä tai asiakas ei ole vielä vahvistanut tapahtuman poistumista. Jos tapahtuma on suljettu, on asiakas tai käyttäjä vahvistanut, että palvelu toimii jälleen normaalisti. Kuvassa 5 on esimerkki tapahtumanhallinnan prosessikaaviosta. (ITIL Service Operation 2011, 75-77)



Kuva 5. Esimerkki tapahtumanhallinnan prosessista (ITIL Service Operation 2011, 77)

Tapahtumien tunnistaminen pitäisi tapahtua ensisijaisesti herätteidenhallinnan prosessin tuotoksena siten, että tapahtumasta ei ole vielä aiheutunut haittaa käyttäjille ja se voidaan ratkaista ennen haitan aiheutumista. Herätteidenhallinnasta huolimatta, tapahtuma voidaan havaita vasta käyttäjän ilmoituksen perusteella. Käyttäjän ilmoitus voi olla tapahtuma tai palvelupyyntö. Palvelupyynnöt voidaan ohjata palvelupyyntöprosessin hoidetta-

vaksi ja varsinaiset tapahtumat kirjataan, luokitellaan ja priorisoidaan. Tapahtuman kirjaukseen tulee laittaa kaikki siitä saatavilla oleva tieto jatkokäsittelyn nopeuttamiseksi. Tapahtuman luokittelulla tapahtumalle määritetään tyyppi, tila, vaikutus ja kiireellisyys. Priorisoinnin tarkoituksena on määrittää tapahtuman vaikuttavuus. Vaikuttavuus voi olla hengenvaara, vaikutus useiden palveluiden toimintaan, taloudelliset tappiot, maineen menetys tai määräysten (tai lain) vastainen toiminta. Vaikuttavuuden perusteella voidaan asettaa tapahtumien ratkaisujärjestys sekä määrittää onko tapahtuma normaali- vai laajavaikutteinen tapahtuma. (ITIL Service Operation 2011, 79-80)

Jos priorisoinnin perusteella tapahtuma ei ole laajavaikutteinen tapahtuma vaan se käsitellään palvelupisteen toimesta, palvelupiste tekee tapahtumasta alustavan arvion. Alustavan arvion perusteella tapahtuma tutkitaan, diagnosoidaan ja ratkaistaan palvelupisteellä. Jos palvelupiste ei pysty ratkaisemaan tapahtumaa, se siirtää tapahtuman selvittämisen, eli eskaloi, seuraavan tason asiantuntijoille toimijoille ratkaistavaksi. Siirtäminen voi olla toiminnallinen tai hierarkkinen. Toiminnallinen eskalointi tarkoittaa tapahtuman normaalia siirtämistä asiantuntijoille joilla on palvelupistettä parempi osaaminen tai enemmän aikaa tapahtumien ratkaisemiseen. Jos tapahtuma katsotaan riittävän merkittäväksi, sen ratkaisu voidaan siirtää hierarkkisesti suoraan esimiesportaan käsiteltäväksi ja johdettavaksi. Kaikissa tapauksissa tapahtuman seuraaminen ja valvonta on palvelupisteen tehtävä. Kun tapahtuma on tutkittu ja diagnosoitu, sekä ratkaisu on löydetty ja palvelu on palautettu, tapahtuma suljetaan. Tapahtuman sulkee palvelupiste sen jälkeen, kun se on varmistunut siitä, että tapahtuma on ratkaistu ja käyttäjä tai asiakas jonka palveluun tapahtuma vaikutti, on tyytyväinen lopputulokseen. Kertaalleen suljettuja tapahtumia ei tulisi avata uudelleen, vaan mieluummin tehdä uusi tapahtuma ilmoitus ja linkittää aikaisempi tapahtuma siihen. (ITIL Service Operation 2011, 82-83)

Tapahtumanhallinnan prosessi voi käynnistyä käyttäjän soitosta palvelupisteelle, käyttäjän laatimasta ilmoituksesta tapahtumailmoitus-palveluun, herätteidenhallinnan-työkalujen tuottamasta tiedosta tai teknisen henkilöstön havainnoista. Jotkin tapahtumat voivat esimerkiksi syntyä laite- tai sovellustoimittajien haavoittuvuusilmoituksista. Prosessin syötteinä voivat olla esimerkiksi konfiguraation rakenneosien statustiedot, tunnettujen virheiden ja niiden väliaikaisten korjausten tiedot, herätteidenhallinnan tuottamat tiedot tai tapahtumanhallinnan onnistumisesta saatu asiakaspalaute. Prosessin tuotteina voi olla tapahtumanhallinnan raportteja, muutospyyntöjä, väliaikaisratkaisuja, ongelmaraportteja, palvelutasoraportteja tai palvelupyyntöjä. Tapahtumanhallinta voi kytkeytyä palvelun elinkaarenhallinnan vaiheista palvelusuunnitteluun tai palvelutransitioon. Se voi myös käynnistää palvelutuotannon ongelmanhallinnan tai pääsynhallinnan prosesseja. (ITIL Service Operation 2011, 83-84)

4.3.3. Palvelupyyntöprosessi

Palvelupyyntö on yleisnimitys erilaisille pyynnöille, joita käyttäjät esittävät. Monet niistä ovat pieniriskisiä, useasti toistuvia, kustannuksiltaan vähäisiä, sovelluksen asennuspyyntöjä, työpisteen muutospyyntöjä tai tieto-

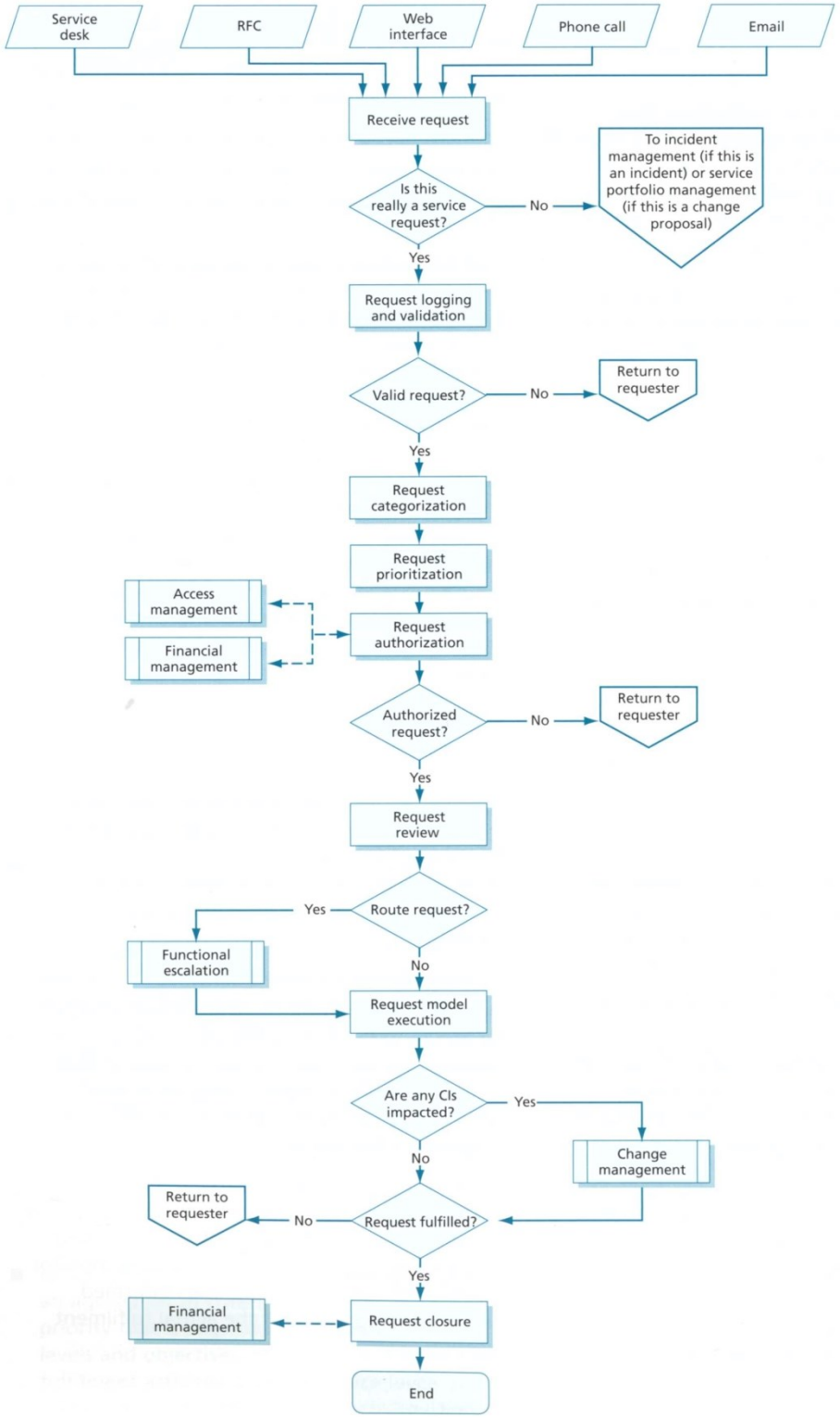
pyyntöjä. Näiden ominaisuuksien vuoksi ne kannattaa toteuttaa omana prosessinaan. Palvelupyyntöprosessilla on suuri merkitys käyttäjätyytyväisyyteen. Palvelupyyntöprosessin tarkoituksena on ylläpitää käyttäjä- ja asiakastyytyväisyyttä käsittelemällä palvelupyynnöt tehokkaasti, tarjota asiakkaille kanava pyyntöjen esittämiseen ja peruspalveluiden saamiseen, tarjota käyttäjille ja asiakkaille tietoa palveluiden saatavuuden tilasta, toimittaa peruspalveluita kuten sovellusten asennus työasemalle ja käsitellä asiakkaiden valituksia. Palvelupyyntö eroaa tapahtumasta siinä, että palvelupyyntöjen vastaanottaminen käyttäjiltä ja asiakkailta on suunniteltu palvelu, kun taas tapahtumat ovat etukäteen suunnittelemattomia poikkeamia. Palvelupyyntöprosessi mahdollistaa nopean ja tehokkaan tavan tuottaa peruspalveluita asiakkaille, sekä vähentää byrokratiaa. Lisäksi keskitetty palvelupiste parantaa palvelupyyntöjen hallittavuutta. Palvelupyyntöprosessin kautta toteutetut toiminnon on mallinnettava. Mallinnuksessa on kuvattava pyynnön toteuttamiseksi tarvittavat vaiheet, toteuttamiseen osallistuvat henkilöt tai ryhmät, tavoiteajat ja asiantuntijat joille palvelupyyntöjä voi siirtää suoritettavaksi. Palvelupiste valvoo palvelupyyntöjen toteutumista, vaikka ne eskaloitaisiin muiden toteutettavaksi. Konfiguraation rakenneosiin kohdistuvat palvelupyynnöt toteutetaan standardimuutoksina, jolloin muutoksenhallinta pystyy pitämään kirjaa muutoksista. Kaikki pyynnöt kannattaa kirjata samaan järjestelmään, jolloin niiden toteutumisen seuranta on luotettavampaa. Toteutettavien palvelupyyntöjen tulee olla hyväksyttyjä pääsynhallinta- ja tietoturvakäytännöissä. Palvelupyyntöjen esittämiseksi tai niiden toimituksen tilan tiedustelemiseksi pitää asiakkaalla tai käyttäjällä olla tiedossa palvelupisteen yhteystiedot. (ITIL Service Operation 2011, 86-88)

Palvelupyyntöprosessia suunniteltaessa on huomioitava erilaisten palvelupyyntömallien käyttäminen, valikko-pohjainen itsepalvelu, palvelupyynnön tilan seuraamisen mahdollistaminen, palvelupyyntöjen priorisointi, pyyntöjen siirtäminen seuraavan tason asiantuntijalle, palvelupyynnön toteuttamisesta aiheutuvat kustannukset ja niiden hyväksyttäminen ennen palvelupyynnön toteuttamista, muut mahdolliset hyväksynnät joita palvelupyynnön toteuttamiseksi tarvitaan, palvelupyynnön toteuttamisen tarvitsemat toiminnot ja palvelupyynnön sulkemisen edellytykset. Kuvassa 6 on esimerkki palvelupyyntöprosessista. (ITIL Service Operation 2011, 88-91)

Palvelupyyntöprosessi alkaa käyttäjän yhteydenotosta. Yhteydenotto voidaan ottaa vastaan palvelupisteeltä, muutospyyntönä, sähköpostilla, webpalvelun kautta tai puhelinsoittona. Yhteydenottoa käsiteltäessä on tunnistettava, onko se palvelupyyntö, tapahtumailmoitus vai pyyntö ominaisuuden lisäämisestä palveluun. Palvelupyynnöt käsitellään palvelupyyntöprosessissa, tapahtumailmoitukset tapahtumanhallintaprosessissa ja uusien ominaisuuksien lisääminen palvelun elinkaaren vaiheen palvelustrategia prosesseissa. Kaikissa tapauksissa yhteydenotto kirjataan käsittelyä varten lokiin. Yhteydenotosta on kirjattava kaikki saatavilla oleva tieto. Samalla varmistutaan siitä, että yhteydenotto koskee IT-palvelutuotannon tarjoamia palveluita. Lokiin kirjattu palvelupyyntö kategorisoidaan jatkokäsittelyä varten. Kategorisointi voi tapahtua esimerkiksi palveluittain, toimenpiteittäin, pyyntölajeittain, toiminnallisuuksittain tai sen mukaan mihin konfiguraation rakenneosiin pyynnöllä on vaikutusta. Palvelupyynnöt

priorisoidaan pyyntöjen käsittelyjärjestyksen määrittämiseksi. Ennen kuin palvelupyyntöä aletaan toteuttaa, sen toteuttamiselle tulee olla valtuutus. Valtuutus voi olla etukäteen pyyntölajeittain sovittu, palvelupisteen päätökseen perustuva tai vaatia tapauskohtaisen käsittelyn. Jos palvelupyynnön toteuttamiselle on perusteltua, seuraavaksi sitä on tarkasteltava toteuttajan määräämiseksi. Toteutus voi tapahtua palvelupisteen toimesta tai palvelupiste voi siirtää sen seuraavan tason asiantuntijoiden toteutettavaksi. Tapahtuipa palvelupyynnön toteuttaminen palvelupisteen tai asiantuntijoiden toimesta, tulee toteuttamisen noudattaa standardoitua toteutusmallia. Standardoitu toteutusmalli vähentää viiveitä ja pienentää virheiden mahdollisuutta. Kaikki palvelupyynnöt joilla on vaikutusta tuotannossa oleviin konfiguraation rakenneosiin, tulee käsitellä muutoshallinnan prosessissa. Kuten tapahtumanhallinnan prosessissa tapahtumien osalta, palvelupyyntöjen seuraaminen ja valvonta on palvelupisteen tehtävä. Kertaalleen suljettujen palvelupyyntöjen uudelleenavaaminen voi olla järkevää rajoittaa esimerkiksi siten, että jos tarve ilmenee seuraavan vuorokauden aikana, suljettu palvelupyyntö avataan uudelleen käsittelyyn. Muissa tapauksissa luodaan uusi palvelupyyntö. (ITIL Service Operation 2011, 91-94)

Palvelupyyntöprosessin syötteinä voivat olla esimerkiksi palvelupyynnöt, muutospyynnöt tai tietopyynnöt. Prosessin tuotteita ovat toteutetut palvelupyynnöt, tapahtumat tapahtumanhallinta prosessiin, standardimuutokset muutoksenhallinta prosessiin tai peruutetut palvelupyynnöt. Palvelupyyntöprosessi voi kytkeytyä palvelun elinkaaren vaiheista palvelustrategiaan, palvelusuunnitteluun, palvelutransitioon. Palvelutuotannon prosesseista se kytkeytyy tapahtuman- ja ongelmanhallinta prosesseihin ja pääsynhallinta prosessiin. (ITIL Service Operation 2011, 94-95)



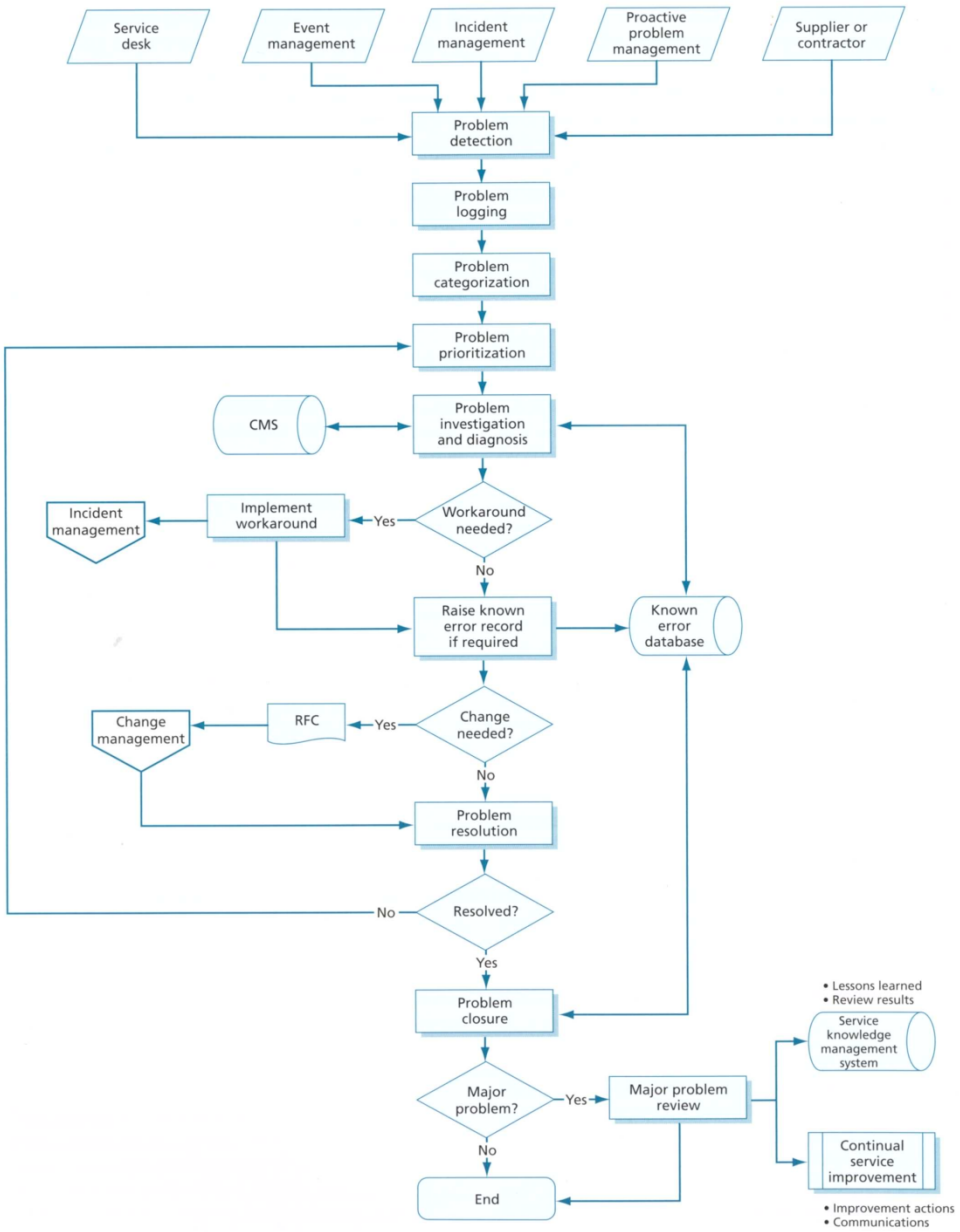
Kuva 6. Esimerkki palvelupyyntöprosessista (ITIL Service Operation 2011, 90)

4.3.4. Ongelmanhallinta

Ongelma tarkoittaa yhden tai useamman tapahtuman ilmenemiseen johtanutta syytä. Ongelmanhallintaprosessi hoitaa kaikkien ongelmien elinkaaren niiden havaitsemisesta lopulliseen selvittämiseen asti. Ongelmanhallinta pyrkii minimoimaan tapahtumien ja ongelmien liiketoiminnalle aiheuttamia haittoja selvittämällä IT-infrastruktuurissa ilmeneviä virheitä. Ongelmanhallinta etsii tapahtumien juurisyitä, dokumentoi ja tiedottaa tunnetuista virheistä ja käynnistää toimenpiteitä tilanteen korjaamiseksi. Ongelmanhallinnan prosessin tarkoituksena on estää ongelmia ja niistä johtuvia tapahtumia, poistaa toistuvia tapahtumia ja minimoida niiden tapahtumien vaikutusta joita ei voi estää. Ongelmanhallinta ja tapahtumanhallinta ovat erillisiä palvelutuotannon prosesseja, mutta niillä on hyvin läheinen suhde ja niitä tehdään usein samoilla työkaluilla, niissä käytetään samaa kategorisointia, sekä vaikuttavuus ja prioriteetti luokittelua. Ongelmanhallinta prosessi jakautuu reagoivaan ja ennaltaehkäisevään toimintaan. Reagoiva ongelmanhallinta ratkoo ongelmia tapahtumien perusteella, kun taas ennaltaehkäisevä ongelmanhallinta pyrkii korjaamaan tunnetut virheet jo ennen tapahtumien ilmenemistä. (ITIL Service Operation 2011, 97)

Ongelmanhallinta tukee liiketoimintaa lyhentämällä tapahtumien kestoaikaa ja pienentämällä niiden määrää, vähentämällä tapahtumista johtuvaa suunnittelematonta työtä, vähentämällä väliaikaisten korjausten tarvetta ja poistamalla toistuvia tapahtumia. Ongelmien ja tapahtumien käsittelyä ei tule yhdistää. Ongelmien hallinnan pitää pystyä toimimaan myös ennakoivasti, kun tapahtumien hallinta on enimmäkseen reagoivaa. Kaikki ongelmat pitää kirjata samaan järjestelmään, jossa ne luokitellaan suunnitellulla tavalla. Luokittelu mahdollistaa ongelmanratkaisumallien käyttämisen ongelmien käsittelemiseen. Tapahtumat voivat joissain tilanteissa luoda ongelmakirjauksen. Tällaisia tilanteita voi syntyä, jos tapahtumanhallinta ei pysty yhdistämään syntynyttä tapahtumaa olemassa olevaan ongelmaan tai jos tapahtumien trendi-analyysi paljastaa mahdollisen ongelman. Laajavaikutteinen häiriö saattaa käynnistää ongelmanhallinta prosessin juurisyyn löytämiseksi. Ongelmanhallintaa voidaan tarvita myös, jos palvelupiste ei pysty määrittämään tapahtumalle yksiselitteistä syytä, vaikka tapahtuma olisikin poistunut, tukiryhmä havaitsee mahdollisen piilossa olevan ongelman tai laite- tai sovellusvalmistaja julkaisee haavoittuvuusilmoituksen. (ITIL Service Operation 2011, 98-99) Esimerkki ongelmanhallinnan prosessista on esitetty kuvassa 7.

Ongelmanhallintaan on kehitetty useita tekniikoita ongelman löytämiseksi monimutkaisestakin järjestelmästä. Käytettävät tekniikat voivat olla esimerkiksi kronologinen analyysi, kipuarvoanalyysi, Kepner ja Tregoe-analyysi, aivoriihi, 5 kertaa miksi, virheen eristäminen, affiniteetti kaavio, hypoteesin testaaminen, jatkuva tarkkailu, Ishikawa kaaviot tai Pareto analyysi. (ITIL Service Operation 2011, 99-101)



Kuva 7. Esimerkki ongelmanhallintaprosessista (2011, ITIL Service Operation 2011, 102)

Ongelmanhallintaprosessi voi käynnistyä reagoivasti tai ennakoivasti. Reaktiivisia liipaisimia ovat yksi tai useampi tapahtuma joka palvelupisteen käsittelyssä on muodostanut ongelman, teknisen tuen tekemän analyysi tapahtumasta, automaattisten järjestelmien havaitsemat tapahtumat joista tarvitsee muodostaa ongelma tai laite- tai sovellustoimittajan haavoittuvuusilmoitus. Ennakoivia liipaisimia ovat tapahtuma-analyysin tuloksena havaitut piilossa olevat ongelmat, tapahtumahistorian perusteella havaittu tai havaitut piilossa oleva ongelma tai palvelun laadun parantamisen myötä havaittu ongelma. Kaikki ongelmat on kirjattava lokiin riittävillä tiedoilla, sekä kategorisoitava ja priorisoitava samaan tapaan kuin tapahtumat. Priorisoinnissa on otettava huomioon ongelmaan liittyvien tapahtumien esiintymistiheys, ongelman vakavuus asiakkaan tai käyttäjän näkökulmasta ja ongelman vaikuttavuus IT-infrastruktuuriin. (ITIL Service Operation 2011, 103-104)

Ongelmien diagnosoinnin tarkoituksena on löytää ongelman juurisyy. Ongelman selvittämisen tekniikoista on kerrottu aiemmin tässä kappaleessa. Selvitystyössä on käytettävä konfiguraatio tietokantaa ongelman vaikuttavuuden arviointiin ja vikakohdan tunnistamiseksi, sekä tunnettujen virheiden tietokantaa ongelman esiintyvyystiheyden ja mahdollisen tiedossa olevan ratkaisumallin käyttämiseksi. Joissain tapauksissa ongelmalle on olemassa väliaikainen ratkaisu. Jos ongelman ratkaisemiseen on käytetty väliaikaista ratkaisua, ongelmaa ei saa sulkea vaan se kirjataan tunnettujen virheiden tietokantaan juurisyyn kanssa. Kun ongelmaan on löytynyt juurisyy ja ratkaisu, ratkaisu otetaan käyttöön. Ratkaisun käyttöönottaminen voi vaatia toiminnallisuuksien muuttamista, jolloin asiasta pitää luoda muutospyyntö. Ratkaisun käyttöön ottaminen voi olla liiketoiminnalle kriittistä, jolloin siitä voidaan tehdä hätämuutospyyntö, joka käsitellään nopeammin. Joissain tapauksissa ongelman ratkaisu ei ole rahallisesti perusteltavissa, jolloin lopputuloksena voi olla tunnettujen virheiden tietokantaan kirjattu ongelma. Kun ongelma on saatu lopullisesti ratkaistua, se suljetaan. Samalla suljetaan kaikki ongelmaan liittyvät tapahtumat ja tunnettujen virheiden tietokantaan päivitetään tieto ratkaistusta ongelmasta. (ITIL Service Operation 2011, 104-105)

Laajavaikutteisten ongelmien ratkaisemisen jälkeen on hyvä käydä ongelman ratkaisu henkilöstön kanssa läpi. Tämän tarkoituksena on kerryttää tietämystä ongelmien ratkaisemisesta tarkastelemalla, mitkä asiat tehtiin oikein, mitkä asiat tehtiin väärin, mitä tulevaisuudessa voidaan tehdä paremmin ja oliko mukana ratkaisuun vaikuttavia ulkopuolisia tahoja tai tarvitseeko tehdä jatkotoimenpiteitä tulevaisuuden varalle. Esiin nousseet asiat tulee kirjata työohjeisiin, tunnettujen virheiden tietokantaan ja käyttää niitä henkilökunnan kouluttamisessa. Tarkastelusta saatu tietämys tulee myös ottaa esiin asiakkaan kanssa käytävissä keskusteluissa. (ITIL Service Operation 2011, 105)

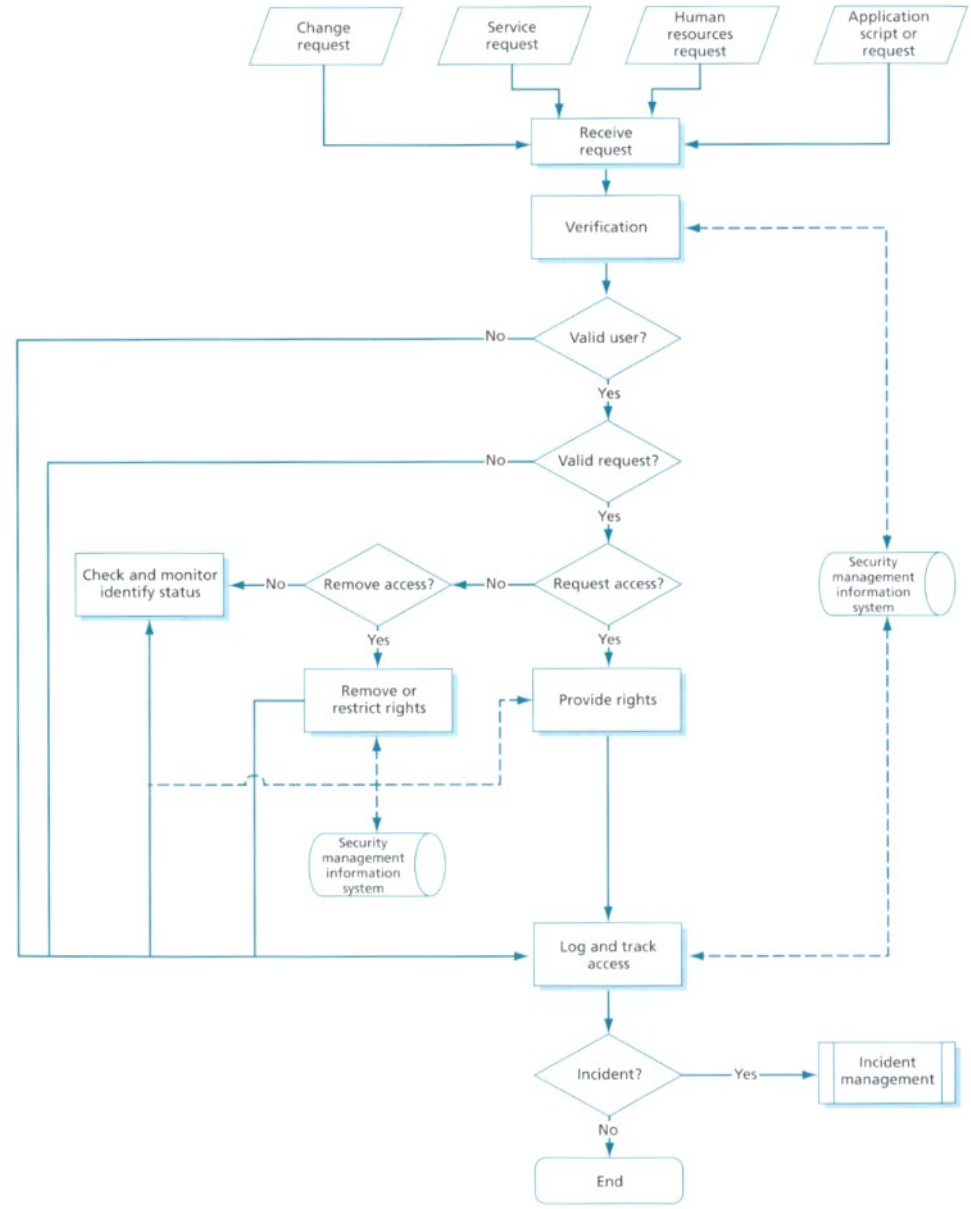
Ongelmanhallinnan syötteinä voivat toimia tapahtumakirjaukset jotka ovat käynnistäneen ongelmanhallinnan toimenpiteitä, tapahtumaraportit ja tapahtumahistoria jota on käytetty ennakoivan ongelmanhallinnan tukena, konfiguraation rakenneosien tiedot, tapahtumien ilmenemisestä saatu tieto, tieto muutospyynnöistä ja käyttöönotetuista julkaisuista, herätteiden hallinnasta saadut tiedot, asiakaspalaute, ongelmien priorisoinnin ja eskaloinnin kriteeristö tai riskienhallinnan ja arvioinnin toimenpiteet. Prosessin tuotteita ovat ongelmien ratkaisut ja ratkaisuun tarvittavat toimenpiteet, väliaikaiset ratkaisut ja niiden vaatimat toimenpiteet, tunnettujen virheiden tietokannan päivitykset, muutospyynnöt ongelmien poistamiseksi, ongelmanhallinnan raportit tai laajavaikutteisten ongelmien tarkastelussa ilmi tullut palaute ja parannusehdotukset. Ongelmanhallinta liittyy palvelun elinkaaren vaiheista palvelustrategiaan, palvelusuunnitteluun ja palvelutransitioon. (ITIL Service Operation 2011, 106-107)

4.3.5. Pääsynhallinta

Pääsynhallinta myöntää käyttöoikeuksia luvallisille käyttäjille ja estää luvattomien käyttäjien pääsyn palveluihin. Pääsynhallinta on tietoturvalli-

suuden hallinnan toimintatapojen ja toimien toteuttamista. Pääsynhallinta on osa organisaation omistaman tiedon ja immateriaaliomaisuuden luottamuksellisuuden, saatavuuden ja eheyden hallintaa. Pääsynhallinta varmistaa, että käyttäjillä on tarvittavat käyttöoikeudet palveluihin. Se ei varmista sitä, että palvelu on aina käytettävissä. Pääsynhallinta ei ole erillinen toiminnallisuus, vaan sitä toteuttavat kaikki tekninen hallinta - ja sovellushallintafunktiot. Pääsynhallintaa toteutetaan palvelusuunnittelussa laadittujen tietoturvallisuuden toimintatapojen mukaan. Pääsynhallinnan tulee kirjata ylös ja valvoa palveluihin kirjautumisia ja varmistaa että käyttäjille on myönnetty oikeat käyttöoikeudet. Pääsynhallinta ylläpitää käyttäjien oikeuksia ja tarvittaessa muuttaa niitä henkilöstön tehtävissä tapahtuvien muutosten mukaan. Pääsynhallinnan lokitietoja voidaan käyttää hyväksi tietoturvatapahtumien ja tietomurtojen selvittämisessä. Tietoturvatapahtumien toimintamallien tulee olla selkeästi määritelty, dokumentoitu ja linjassa tietoturvan toimintatapojen kanssa. (ITIL Service Operation 2011, 110-111)

Pääsynhallinnan prosessi käynnistyy pyynnöstä. Pyyntö voi olla standardipyyntö henkilöstöhallinnosta, muutospyyntö, palvelupyyntöprosessin kautta jätetty muutospyyntö tai sallitun skriptin suorittaminen. Pääsynhallinta varmistaa pyynnön oikeellisuuden tunnistamalla pyytäjän ja että pyytäjällä on perusteltu syy käyttää palvelua. Henkilön tunnistaminen voi perustua esimerkiksi käyttäjätunnus - / salasana – yhdistelmään, biometrisiin tunnisteisiin tai sähköiseen avaimeen. Tarpeellisuuden määrää esimerkiksi henkilöstöhallinnon ilmoitus käyttäjän muuttuneesta tehtävästä tai uuden henkilön palkkaamisesta. Pääsynhallinta toteuttaa pääsyoikeudet toimintatapojen ja määräysten mukaisesti, mutta ei päätä käyttöoikeuksista. Pyyntöjen käsittelyn lisäksi pääsynhallinta varmistaa, että käyttöoikeuksia käytetään tarkoituksenmukaisesti. Tarkoituksenmukaisuuden valvominen mahdollistetaan ulottamalla pääsynvalvonta ja – hallinta kaikkiin teknisen ja sovellushallinnan toimintoihin, sekä palvelutuotannon prosesseihin. Pääsyoikeuksien toteuttamisen lisäksi pääsynhallinta tekee pääsyoikeuksien rajoittamisia ja poistamisia. Pääsynhallinnan syötteinä voivat toimia muutospyynnöt, palvelupyynnöt tai henkilöstöhallinnon pyynnöt. Prosessin tuotteita ovat pääsyoikeuksien toteuttaminen, pääsynhallinnan raportit ja toteutettujen oikeuksien lokimerkinnät, sekä käyttöoikeuksien väärinkäytön raportointi. Pääsynhallinta liittyy palvelun elinkaaren vaiheista palvelustrategiaan, palvelusuunnitteluun ja palvelutransitioon. Palvelutuotannon prosesseista se liittyy palvelupyyntöprosessiin. (ITIL Service Operation 2011, 111-116) Esimerkki pääsynhallinnan prosessista on esitetty kuvassa 8.



Kuva 8. Esimerkki pääsynhallintaprosessista (ITIL Service Operation 2011, 112)

4.4. Valvonta ja hallinta

Palveluiden valvonta ja hallinta tarkoittavat valvontaa ja raportointia, sekä niiden perusteella tehtyjä hallintatoimenpiteitä. Valvonta tarkoittaa järjestelmissä tapahtuvien muutosten havainnointia. Palvelutuotannossa muutosten havainnointi tarkoittaa konfiguraation rakenneosien monitorointia, halutun kaltaisen toiminnan varmistamista ja hälytyksen tekemistä poikkeamatilanteissa, laitteiden suorituskyvyn ja käyttöasteen tarkkailua, epänormaalin toiminnan havainnointia, hyväksymättömien muutosten havainnointia, toimintatapojen valvontaa, sekä laatu- ja suorituskykyvaatimusten toteutumisen tarkkailua. Raportointi kokoaa valvonnan tuottamia tietoja tulkittavaan muotoon. Raportoinnilla varmistetaan, että päätöksentekijöillä on käytettävissään tarvittavat tiedot. Hallinta tarkoittaa laitteelle, järjestelmälle tai palvelulle tehtyjä toimenpiteitä jotka vaikuttavat sen toimin-

taan. Hallintatoimenpiteiden tulee vastata määritettyjä standardeja tai normeja. Lisäksi hallintatoimenpiteisiin johtavan syyn tulee olla määritetty, ymmärretty ja varmistettu, sekä tehtävät toimenpiteet tulee olla määritetty, hyväksytty ja tilanteeseen sopivia. Näin ollen hallinta tässä tapauksessa tarkoittaa normaalien ja epänormaalien toimenpiteiden määrittämistä; laitteiden, järjestelmien tai palveluiden toiminnan sääntelyä; sekä korjaavien toimenpiteiden suorittamista automaattisesti tai manuaalisesti. (ITIL Service Operation 2011, 123)

Valvonta ja hallinta voidaan mallintaa silmukaksi, jossa toimintaa havainnoidaan, sitä vertaillaan määritettyyn normaalitilaan ja tarvittaessa tehdään hallintatoimenpiteitä. Silmukka voi olla avoin tai suljettu. Avoimessa silmukassa määritetty hallintatoimenpide tehdään riippumatta toimintaympäristön tilasta. Suljetussa silmukassa toimenpiteet käynnistetään, kun toimintaympäristö täyttää määritetyt ehdot. Palvelunhallinnan silmukka voi myös ilmentyä monimutkaisena hallinta silmukkana, jossa edellisen silmukan lopputulos toimii seuraavan silmukan käynnistäjänä ja valvottavana kohteena on palvelua tuottava laite tai sen osa. Valvottavien kohteiden määrittäminen tulisi perustua siihen, mitä prosessilla, laitteella tai järjestelmällä halutaan saada aikaiseksi. (ITIL Service Operation 2011, 123-127)

Valvonta ja hallinta voidaan jakaa sisäiseksi ja ulkoiseksi. Sisäinen valvonta ja hallinta kohdistuvat laitteisiin ja toimintoihin jotka ovat tiimin tai osaston suoranaisessa valvonnassa ja hallinnassa ja vaikuttaa tiimin tai osaston omaan toimintaan. Ulkoinen valvonta ja hallinta kohdistuvat myös tiimin tai osaston suorassa valvonnassa ja hallinnassa oleviin laitteisiin tai toimintoihin, mutta niihin tehtävät toimenpiteet vaikuttavat jonkun toisen tiimin tai osaston vastuulla oleviin laitteisiin tai toimintoihin. (ITIL Service Operation 2011, 127-128)

Suunniteltaessa valvontaa, tulee määrittää mitkä laitteet vaikuttavat eniten palveluiden tuottamiseen. Vaikuttavuuden mittareina voivat olla palvelun toimivuuden mittarointi, tärkeimpien konfiguraation rakenneosien, niiden konfiguraation, suorituskyvyn ja saavutettavuuden, määrittely, konfiguraation rakenneosien rajoitukset tai palveluiden toiminnan rakentaminen siten että ne tuottavat merkityksellisiä herätteitä. Valvonnan ja hallinnan onnistumisen kannalta avainasemassa ovat kuitenkin sidosryhmät, jotka osallistuvat palveluiden tuottamiseen tai käyttämiseen. (ITIL Service Operation 2011, 128)

Valvonta voi olla aktiivista ja reagoivaa, passiivista ja reagoivaa, aktiivista ja ennakoivaa tai passiivista ja ennakoivaa. Aktiivinen ja reagoiva valvonta tekee laitteille tai järjestelmille kyselyitä, päättelee vastausten perusteella niiden tilaa ja tarvittavat toimenpiteet. Tämän tyyppinen valvonta tulisi kohdistaa vain tärkeimpiin konfiguraation rakenneosiin ja vianselvityksen käyttöön. Passiivinen ja reagoiva valvonta havaitsee ja tekee korrelaatiota herätteiden perusteella ja päättää sopivista toimenpiteistä niiden perusteella. Aktiivista ja ennakoivaa valvontaa käytetään laitteen, järjestelmän tai palvelun reaaliaikaiseen valvontaan. Tämän tyyppistä valvontaa tulisi käyttää kriittisten komponenttien valvontaan, tai vikaantuneen laitteen

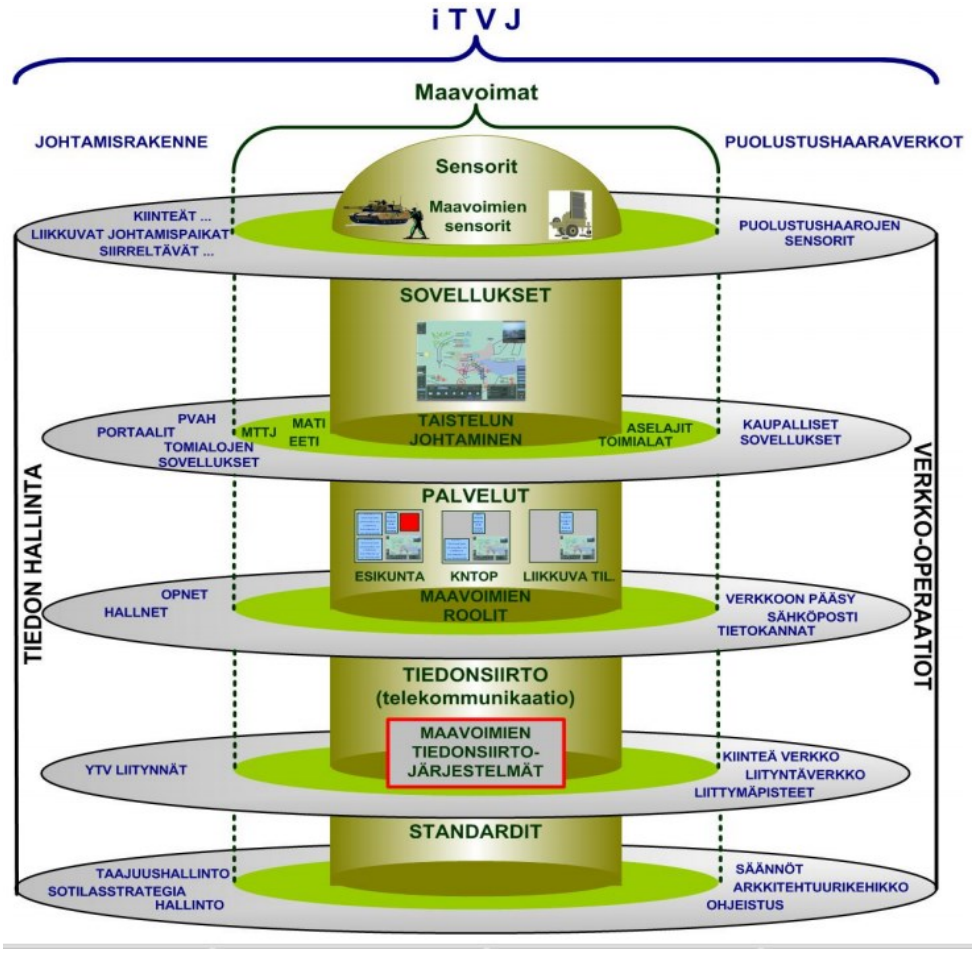
korjauksen jälkeiseen varmistumiseen vian poistumisesta. Passiivinen ja ennakoiva valvonta tekee korrelaatioita herätteistä pidemmällä aikavälillä trendien havaitsemiseksi. Trendejä käytetään ennakoivan ongelmanhallinnan prosessissa. Valvonta voi olla myös jatkuvaa tai perustua poikkeamiin. Jatkuva valvonta ei ole sama asia kuin aktiivinen valvonta, vaikka sitä tulisi kohdistaa aktiivisen valvonnan tapaan vain kaikkein tärkeimpiin laitteisiin. Jatkuva valvonta perustuu yleensä määritetyin väliajoin tapahtuvaan näytteenottoon ja niistä luotuun tilastolliseen analyysiin. Poikkeamiin perustuva valvonta ei havainnoi palveluita tai järjestelmiä reaaliaikaisesti, vaan tunnistaa ja raportoi poikkeamia. Tällaista valvontaa käytetään vähemmän kriittisten järjestelmien valvontaan tai silloin kun valvontatyökalut eivät pysty määrittämään palvelun tilaa tai laatua. (ITIL Service Operation 2011, 130)

Valvontaan ja hallintaan kiinteästi liittyvä raportointi tulee olla suunniteltu ja toteutettu siten, että raportoinnin tuloksien perusteella voidaan ennalta määrätyllä tavalla toteuttaa toimenpiteitä. Sama pätee valvontaan, valvonnan tarkoituksena pitää olla palvelun toteutuminen ja palvelutuotannon onnistuminen. Lisäksi, valvonta ilman hallintaa on merkityksetöntä ja tehotonta. (ITIL Service Operation 2011, 131)

5 MAAPUOLUSTUKSEN TAKTISET JÄRJESTELMÄT

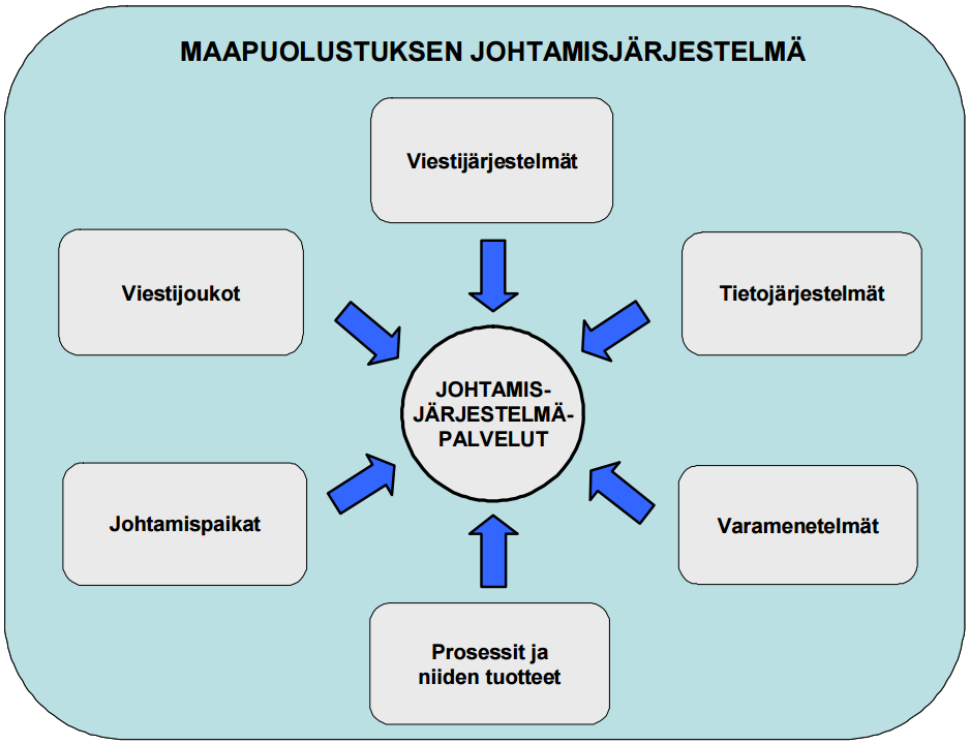
Maapuolustuksen taktisten järjestelmien arkkitehtuuri on kuvattu Jarkko Karsikkaan yleisesikuntaupseerikurssin diplomityössä (Karsikas 2007). Arkkitehtuurin mukaan maapuolustuksen taktiset järjestelmät tarkoittavat erityisesti kenttäkäyttöön tarkoitettuja johtamisjärjestelmiä. Taktinen järjestelmä koostuu tiedonsiirtojärjestelmistä, palveluista, sovelluksista ja sensoreista (kuva 9).

Maapuolustuksen taktiset järjestelmät ovat tarkoitettu käytettäväksi normaaliolojen harjoituksissa, poliittisen painostuksen aikana voimannäyttöön, YETTS-uhkatilanteiden aikana, kansainvälisessä toiminnassa sekä maa-alueiden valtaukseen tähtäävän hyökkäyksen torjunnassa. Järjestelmien suunnittelu perustuu suorituskykyvaatimuksiin, jotka muodostuvat tutkimustoiminnan tuloksista, sotilaallisista suunnitelmista ja suorituskyvyn arvioinnista. Kun vaatimukset on saatu näin määriteltyä, järjestelmät rakennetaan ja niitä käytetään. Käytöstä saatujen kokemusten perusteella järjestelmiä joko jatkokehitetään tai niiden suorituskykyä ylläpidetään. (Karsikas 2007, 126 ja liite 3)



Kuva 9. Maapuolustuksen taktinen järjestelmä kokonaisuuden osana (Karsikas 2007, 118)

Maapuolustuksen taktiset järjestelmät kuuluvat maapuolustuksen johtamisjärjestelmäkokonaisuuteen, joka sisältää viestijoukot, viesti- ja tietojärjestelmät, johtamispaikat, johtamisjärjestelmän prosessit ja niiden tuotteet sekä johtamisen varamenetelmät. Johtamisjärjestelmän tarkoituksena on valmiuden kohottamisen; perustettavien johtoportaiden; tiedustelun, valvonnan ja maalittamisen (TVM-toiminta), tilannekuvan kokoamisen, yhteistyön sotilaallisten toimijoiden, muiden viranomaisten ja yhteistyökumppaneiden, sekä tulen keskitetyn johtamisen ja vaikutuksen koordinoinnin mahdollistaminen. Johtamisjärjestelmän suunnittelu, rakentaminen ja ylläpito kuuluvat sitä käyttävän joukon tehtäviin. (Virtanen & Jokinen 2014, 144-145) Kuvassa 10 on kuvattu maapuolustuksen johtamisjärjestelmän kokonaisuus.



Kuva 10. Maapuolustuksen johtamisjärjestelmä (Virtanen & Jokinen, 145)

5.1. Tiedonsiirtojärjestelmät

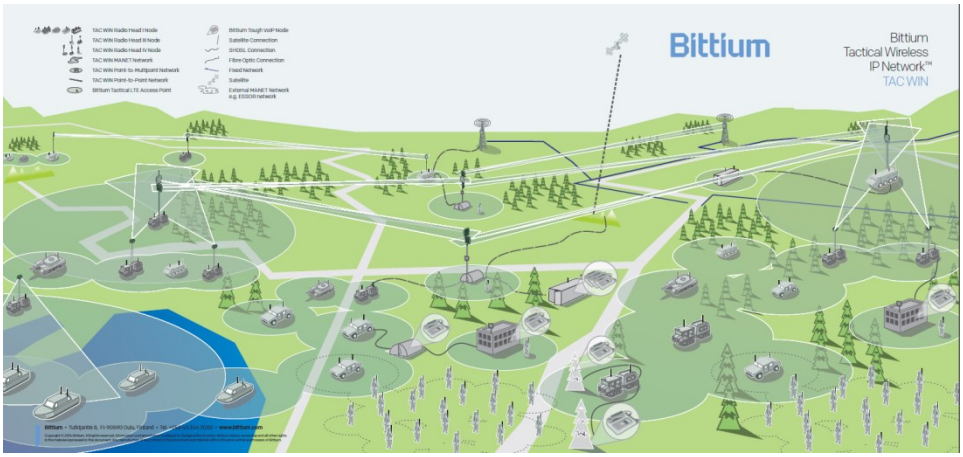
Maapuolustuksen tiedonsiirtojärjestelmästä (viestijärjestelmästä) käytetään nimeä MAAVNET. MAAVNET koostuu maapuolustuksen liityntäverkosta, sekä maavoimien ja rajavartiolaitoksen joukkojen viestijärjestelmistä. Järjestelmän yhteydet toteutetaan sekä langattomia, että langallisia teknologioita käyttäen. MAAVNET:n tarkoituksena on varmistaa keskeisten taktisten palveluiden toimivuus ja yhteensopivuus maavoimien kohdearkkitehtuurin sekä muiden puolustushaarojen kanssa. Järjestelmä on kiinteä osa puolustusvoimien verkostorakennetta. MAAVNET muodostuu kiinteistä ja liikkuvista järjestelmistä (kuva 11). (Virtanen & Jokinen 2014, 146)

Kuva 11. Maapuolustuksen viestijärjestelmä (Virtanen & Jokinen 2014, 146)

Vanhempaa tiedonsiirtotekniikkaa edustavat yhtymän viestijärjestelmät ovat M80, YVI 1m ja YVI2. M80 tarjoaa jalkaväkiprikaatin joukoille niiden tarvitsemat tiedonsiirtopalvelut. Verkko koostuu henkilövälitteisistä puhelinkeskuksista, kenttäparikaapelilla tai kenttälinkeillä muodostetuista keskusten välisistä yhteyksistä, sanomalaitejärjestelmästä ja sen päätelaitteista sekä VHF- ja HF -taajuusalueen radioverkoista. M80-järjestelmä edustaa analogista tiedonsiirtotekniikkaa. YVI1 on tarkoitettu armeijakunnan tai sotilasläänin johtamien jääkäriprikaatien kenttäviestiverkoksi. Verkko koostuu automaattisista puhelinkeskuksista, valokaapeli- ja radiolinkkiyhteyksistä, sanomalaitejärjestelmästä ja sen päätelaitteista sekä VHF-, HF- ja UHF -taajuusalueen radioverkoista. YVI 1m on modifioitu versio YVI1-viestijärjestelmästä. YVI1 ja YVI 1m käyttävät digitaalista tiedonsiirtotekniikkaa. Modifioinnissa YVI 1m:ksi kehitettiin radiolinkkijärjestelmää, parannettiin järjestelmän verkonvalvontakykyä ja siihen lisättiin langaton puhelinjärjestelmä. YVI2 on käytössä Länsi-Suomen ja Itä-Suomen valmiusyhtymillä. Verkko muodostuu tukiasemista joihin käyttäjät liittyvät, automaattisista puhelinkeskuksista, valokaapeli- ja radiolinkkiyhteyksistä, sanomalaitejärjestelmästä ja sen päätelaitteista, sekä VHF-, HF- ja UHF -taajuusalueen radioverkoista. Radiotilaajat voivat liittyä YVI2-järjestelmään digitaalisesti tai analogisesti. Järjestelmä kykenee myös auttavasti datan siirtoon. (Laitila 2009, 10-15)

Maapuolustuksen uusin viestijärjestelmä on Kainuun prikaatissa käytössä oleva M18 (mil.fi 2016). M18 on langaton laajakaistaverkko, joka mahdollistaa MANET-, linkki- ja liityntäverkkojen muodostamisen. Verkko käyttää tiedonsiirtoon IP-protokollaa. Järjestelmään kuuluu ohjelmistoradioteknologiaan perustuva taktinen reititin ja kolme eri taajuusalueilla toimivaa radiopäätä. Tiedonsiirtoyhteyksien todellinen nopeus radioverkossa riippuu olosuhteista ja etäisyyksistä, valmistajan lupaamat maksiminopeudet eri radiopäillä ovat 12-50Mbps. Valokuituyhteydellä maksimi-

nopeus on 1Gbps. (Bittium LRV-järjestelmä, 2016) Kuvassa 12 on kuvattu järjestelmän toiminnallinen kokonaisuus valmistajan näkökulmasta.



Kuva 12. Bittium LRV-järjestelmä (Bittium LRV-järjestelmä, 2016)

M18-järjestelmän viestiasemat ovat liikkuvia ja käyttötarkoituksen mukaan A-, C- tai E-tyypin asemia. A-asemia käytetään yhtymien ja taisteluosastojen rungon muodostamiseen ja alajohtoportaiden liittämiseen järjestelmään. C-asemilla laajennetaan taisteluosaston viestijärjestelmän runkoa, liitetään alajohtoportaita järjestelmään ja liitytään ylempään verkkoon. E-asemia käytetään komppanian johtamisjärjestelmäpalveluiden tuottamiseen. E-asemilla liitytään taisteluosaston runko- tai liityntäverkkoon. (Virtanen & Jokinen 2014, 146-147)

Arkkitehtuurin mukaan (Karsikas 2007) maavoimien taktiset järjestelmät liitetään suurikapasiteettisin radiojärjestelmin ja valokuituyhteyksin muodostettuun runkoverkkoon. Runkoverkko mahdollistaa taktista verkkoa suuremman tiedonsiirtokapasiteetin esikuntien ja johtamispaikkojen välille. Runkoverkko on taktista verkkoa täydentävä ja kapasiteettia tarjoava verkko, mutta taktisen järjestelmän on kyettävä toimimaan myös ilman yhteyttä siihen. YVI-järjestelmien tyyppiset alueelliset taktiset järjestelmät tulevat poistumaan seuraavan sukupolven järjestelmän (M18) yleistyessä.

5.2. Palvelut

Arkkitehtuurissa tiedonsiirtojärjestelmä toimii maapuolustuksen taktisten järjestelmien viitekehyksessä datansiirtopalvelua tuottavana osana. Datansiirtopalvelua tuotetaan järjestelmän palveluille, sovelluksille sekä sensoreille. Datansiirtopalvelun tuottamisen toimijat on jaoteltu tiedonsiirtojärjestelmän johtoon ja tekniseen johtoon. Tiedonsiirtojärjestelmän johto johtaa käyttö- ja ylläpitohenkilöstöä, tekninen johto valvonnan ja hallinnan henkilöstöä. Tiedonsiirtojärjestelmän johto vastaa suunnittelusta ja valmistelusta, tekninen johto vastaa teknisestä toteutuksesta ja toimintakunnon valvonnasta. (Karsikas 2007, 127)

Karsikkaan mukaan maavoimien joukoista käytetään nimitystä roolit. Roolit kuuluvat palvelukehykseen. (kuva 9.) Joukot jaetaan (Virtanen & Jokinen 2014, 140-147) käyttöperiaatteen mukaan operatiivisiin, alueelli-

siin ja paikallisjoukkoihin. Operatiiviset joukot on tarkoitettu sotilaallisen voiman ennaltaehkäisyyn, yllättävien tilanteiden hallintaan ja ratkaisutaisteluissa painopisteen muodostamiseen sekä hyökkääjän lyömiseen. Alueellisilla joukoilla suojataan puolustusvalmisteluita ja strategisesti tärkeitä alueita, mahdollistetaan operatiivisten joukkojen toiminta ja kulutetaan sen taisteluvoimaa. Paikallisjoukot toimivat joukkojen perustajina, kohteiden ja henkilöiden suojaamistehtävissä ja antavat virka-apua muille viranomaisille. Kuten aiemmin tässä kappaleessa on mainittu, joukot vastaavat käyttämiensä järjestelmien rakentamisesta. Järjestelmien tuottamia palveluita ovat puhe- sanoma- ja tietojärjestelmäpalvelut. Puhe- ja sanomapalvelut ulottuvat läpi koko organisaation aina liikkuville partioille, sensoreille ja aselaveteille asti.

Järjestelmien (ja samalla palveluiden) tekninen valvonta ja hallinta on porrastettu järjestelmävastuiden mukaisesti. Porrastus on tehty siten, että Maapuolustuksen taktisten järjestelmien kokonaisvalvontavastuu on Maavoimien operatiivisella järjestelmäkeskuksella. Maavoimien operatiivinen järjestelmäkeskus toimii valtakunnallisena järjestelmätukiorganisaationa. (Virtanen & Jokinen 2014, 145-146)

5.3. Sovellukset

Sovelluksista mainitaan (Virtanen & Jokinen 2014, 147) Maavoimien tietojärjestelmä MATI, joka on ohjelmisto-, sovellus-, verkko- ja päätelaiteperhe. MATI on palvelu, jolla tuetaan maaoperaatioiden johtamista, yhteisten suorituskykyjen käyttöä ja mahdollistetaan yhteistoiminta muiden sotilastoimijoiden ja yhteistyökumppaneiden kanssa. Tietojärjestelmä palvelee suunnitelmien ja tehtävien toimeenpanossa, tilannekuvan muodostamisessa ja taisteluiden johtamisessa. MATI:n käyttö painottuu taisteluosasto ja ylemmille -tasoille, alempien tasojen johtamiseen käytettävä sovellus on nimeltään Taistelunjohtojärjestelmä (TSTJJ).

MATI:n sisältämiä sovelluksia ovat tykistön ammunnan hallinta ja johtamisohjelma AHJO, viestinvälitys sovellus EETI, yleisjohtamisen ja tilannekuvan sovellus Johla08 (karttajärjestelmä), aselajisuunnittelusovellukset joista mainitaan Pionjohla ja asianhallintajärjestelmä Susinet. (Pikkarainen 2013, 46)

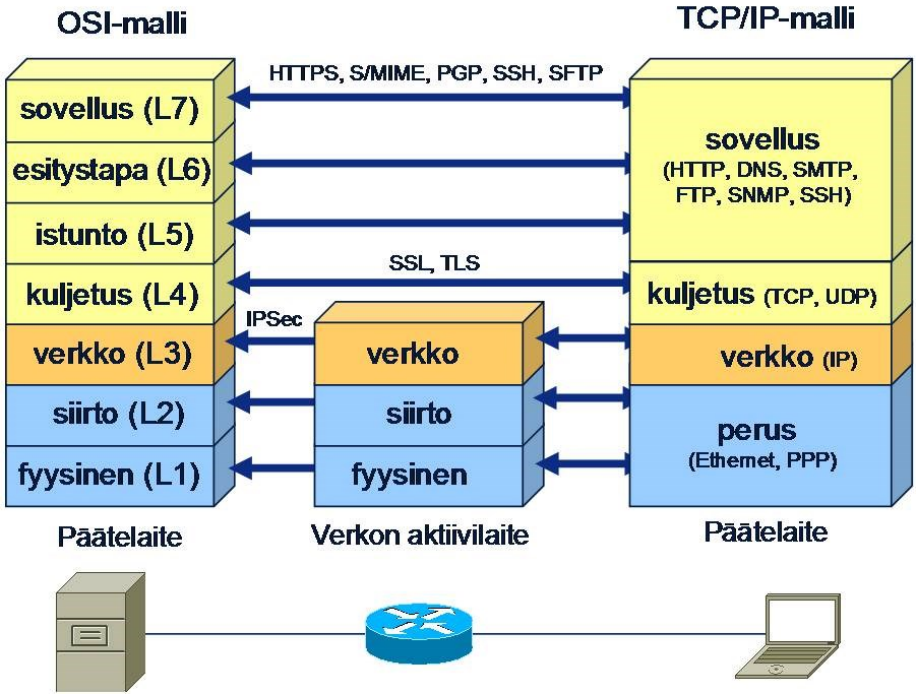
5.4. Sensorit

Sensoreina maapuolustuksen taktisissa järjestelmissä toimivat ihmiset ja tekniset sensorit (Karsikas 2007, 122). Ihmiset voidaan käsittää taistelevina joukkoina, jotka käyttävät järjestelmiä ja tekevät havaintoja ympäristöstään. Tekniset sensorit voivat tarkoittaa lennokkijärjestelmiä ja maasensoreita. Sensoreiden tuottamaa tietoa kutsutaan tiedustelutiedoksi. Sotilastiedusteluun kuuluvat partio-, signaali-, elektroninen-, lento-, kuvaus-, henkilö-, geo- ja vastatiedustelu. (Virtanen & Jokinen 2014, 140). Kärsämän mukaan (Kärsämä 2010, 14-15) maasensorijärjestelmät ovat laitteita, jotka voidaan viedä maastoon jossa ne havaitsevat kohteita, sekä pyrkivät määrittelemään kohteen laadun ja päättelemään sen kulkusuunnan. Lisäksi

ne välittävät havainnot valvontakeskukseen. Maastosensorit käyttävät havainnointiin akustisia-, seismisiä-, magneettisia- sekä infrapuna-sensoreita. Lennokkijärjestelmät ovat kiinteäsiipisiä, pyöriväsiipisiä tai aerostaattisia. Tyypin ratkaisee laitteen tapa pysytellä ilmassa.

6 VALVONNAN JA HALLINNAN TEKNOLOGIAT

Laajojen IP-verkkojen tehokas tuottaminen ei ole mahdollista ilman huolellisesti suunniteltua ja toteutettua verkonvalvontaa ja -hallintaa. Verkonvalvonnan ja -hallinnan tulee käsittää verkon kaikki aktiivilaitteet, jotka käyttävät liikennöintiin TCP/IP-protokollaa. Kuvassa 13 on havainnollistettu OSI- ja TCP/IP-mallien keskinäistä suhdetta.



Kuva 13. OSI- ja TCP/IP-mallien välinen suhde (Vahti-ohje)

TCP/IP:tä käyttäviä verkon aktiivilaitteita ovat esimerkiksi reitittimet, kytkimet (L2 ja L3), palomuurit, salaimet, palvelimet, verkkosillat ja työasemat.

Hyvin toteutettu verkonvalvonta ja -hallinta mahdollistavat järjestelmien hallitun operoinnin ja tiedonsiirron vikatilanteiden tai häiriötilanteiden minimoimisen. Tiedonsiirron häiriötilanteita voivat olla esimerkiksi tiedonsiirron hitaus, reitittyminen ei halutulle reitille, reitittyminen kalliille reitille edullisemman sijaan, reitittyminen langattomalle medialle kiinteän yhteyden sijaan, verkkolaitteen vikaantuminen tai verkkolaitteen virheellinen konfiguraatio.

6.1. Valvontaprotokollat

Tässä tutkimuksessa tarkasteltavia TCP/IP-verkkojen valvontaan käytettäviä protokollia ovat SNMP ja ICMP.

6.1.1. SNMP

SNMP:tä voi käyttää verkon aktiivilaitteiden valvonnan lisäksi niiden hallintaan. Käytettäessä SNMP:tä hallintaan, pitää huomioida sen eri versioiden käyttämät autentikointi- ja salausmenetelmät. Riippuen käytettävästä tiedonsiirtotavasta ja hallinnan laajuudesta myös hallintaa voi tehdä selväkielisenä, mutta tällöin on tiedostettava salakuuntelun (tietoliikenteen tallentaminen) riski joka sisältyy TCP/IP-pakettien siirtämiseen salaamattomana verkossa.

SNMP-protokolla on määritelty IETF:n RFC-1157:ssä (RFC-1157, 1990). Sen pohjalta on laadittu IETF:n standardi STD 15 (STD 15, 1990). RFC-1157:ssä määritetystä SNMP:n versiosta käytetään nimeä SNMPv1. SNMP suunniteltiin alun perin lyhyen tähtäimen ratkaisuksi internetsolmujen hallintaan, mutta sen saavuttaman suuren suosion vuoksi siitä on tullut IAB:n suosittelema standardi protokolla ja RFC-1157:n mukaan kaikkien IP:tä ja TCP:tä käyttävien sovellutusten tulisi olla valvottavissa ja hallittavissa SNMP:llä.

SNMPv2 paransi SNMP-protokollan toimintaa mahdollistamalla laajennetut datatyypit, rivien ja sarakkeiden käsittelyn ja tapahtumanilmoituksen kuittaamisen. Se myös parantaa tehokkuutta, suorituskykyä, virheenkäsittelyä ja määrittelykieltä. (RFC-2570, 6)

SNMP:n seuraava versio SNMPv2 on kuvattu IETF:n RFC-dokumenteissa RFC-1902, RFC-1903, RFC-1904, RFC-1905, RFC-1906 ja RFC-1907. SNMPv2 ei saavuttanut IETF:n suositusta, vaan sen sai protokollan versio SNMPv2c, joka on kuvattu tammikuulle 1996 päivätyssä IETF:n RFC-dokumentissa RFC-1901 (RFC-1901).

SNMP-protokollan seuraavan kehitysversion SNMPv3 määrittelemiseksi IETF perusti vuonna 1999 SNMPv3 Working Group – työryhmän. Työryhmän tehtävänä oli laatia suositukset seuraavan sukupolven SNMP-versiosta. Tärkeimpänä yksittäisenä tavoitteena oli turvallisuuteen ja hallintaan liittyvät määrittelyt, jotka olivat aikaisemmissa versioissa olleet puutteelliset. SNMP:n versiota 3 laadittaessa käytettiin hyväksi aikaisempien versioiden määrityksiä. Kuvauskieli on sama, versio käyttää MIB-tietokantoja ja protokolla toimii samojen periaatteiden mukaisesti. Turvallisuutta ja hallintaa taasen on parannettu työryhmälle asetettujen tavoitteiden mukaisesti. Turvallisuus ja hallinta on kuvattu kuudessa RFC-dokumentissa (RFC-2570 – RFC-2575). Dokumentit kuvaavat SNMPv3:n hallinta-arkkitehtuurin, sanomien käsittely- ja lähettämisprosessin, SNMP-ohjelmat, käyttäjätunnukseen perustuvan tunnistamisen ja näkymäperustaisen hallintamallin. (RFC-2570, 7-11).

SNMPv3:n käyttäjätunnukseen perustuva tunnistaminen on kuvattu IETF:n RFC-dokumentissa RFC-2574 (RFC-2574, 1999).

6.1.2. ICMP

ICMP-sanomia käytetään tiedonsiirron tilan ilmaisemiseen. Sanomia käytetään ilmaisemaan tiedonsiirrossa tapahtuneista virheistä. Virhe voi olla esimerkiksi, että kohdeisäntä ei ole tavoitettavissa (destination unreachable). ICMP-sanomia on 11 erilaista, joista tietoliikennelaitteiden valvontaan käytetään yleisimmin tyyppejä 8 ja 0 (echo ja echo reply). Näiden sanomien avulla voidaan saada tietoa siitä, onko liikennöinti mahdollista laitteiden välillä. (RFC-792).

6.1.3. Pohdintaa valvontaprotokollista

Tietoliikennelaitteiden valvontaan käytettävien ICMP- ja SNMP-protokollien käyttäminen on nykyaikaisessa verkottuneessa ympäristössä suositeltava tapa. Käytettäessä SNMP:tä on suunniteltava ja rajattava yksiselitteisesti verkon hallinta-asemat, joiden kanssa laitteet kommunikoivat ja valittava käytettävä versio käyttötarpeen mukaan.

SNMP:n versioksi tulisi aina valita ensisijaisesti SNMPv3 sen kehittyneimmän käyttäjätunnistuksen ja kryptauksen vuoksi. Kirjoitusoikeuksia laitteille ei tulisi sallia muilla SNMP:n versioilla. Muiden versioiden käyttöä voi harkita esimerkiksi samassa lähiverkossa sijaitsevan tulostimen valvomiseen SNMP:llä, jos laite ei tue versiota 3.

ICMP:n käytön rajaaminen siten, että laite vastaa vain tietyille verkon valvonta-asemien IP-osoitteille, rajoittaa verkon luvattomasta skannaamisesta mahdollisesti aiheutuvaa uhkaa verkolle.

6.2. Hallintaprotokollat

Hallintaprotokollilla tarkoitetaan tässä tapauksessa tapoja, joilla tietoliikennelaitteisiin otetaan yhteyttä hallintapäätelaitteella. Yhteys voi muodostua joko verkon kautta, tai suoralla sähköisellä yhteydellä kuten sarjaporttiyhteydellä. Hallintaprotokollien yhteydessä käytetään usein termiä virtuaalinen terminaali yhteys VTY (RFC-782). Yhteyden muodostamisen tarkoituksena on mahdollistaa tietoliikennelaitteiden konfiguraatioiden tarkastelu, muuttaminen ja laitteen tilojen muuttaminen kuten esimerkiksi sen käynnistäminen uudelleen.

6.2.1. Konsoli-yhteys

Konsoli-yhteydellä tarkoitetaan tapaa, jolla tietoliikennelaitteen hallintaa tehdään kytkeytymällä sarjayhteydellä laitteen fyysiseen porttiin ja hallintaan käytetään terminaali emulaatio-ohjelmaa. Konsoli-yhteydet ovat valmistajakohtaisesti määritettyjä, mutta yleisimmäksi tavaksi muodostaa yhteys on vakiintunut RS-232.

Konsoliyhteyden käyttäminen tapahtuu tyypillisesti tietoliikennelaitteen välittömästä läheisyydestä ja esimerkiksi laitteiden konfiguraatioiden alustaminen aloitetaan avaamalla konsoliyhteys laitteeseen. Konsoliyhteyttä käytetään usein laitteen ohjelmiston (firmware) päivittämiseen.

6.2.2. Telnet

Telnet on määritelty IETF:n RFC-dokumentissa RFC-854. Telnet on TCP-protokollaa käyttävä kaksisuuntainen 8-bittinen protokolla. (RFC-854, 1). Telnet-tiedonsiirto on mahdollista salata. Telnet-salaus on määritetty IETF:n RFC-dokumentissa RFC-2946. Yhteyden autentikointi on määritelty IETF:n RFC-dokumentissa RFC-2941. Telnet-yhteyden well-known-portti on 23.

Telnet-yhteydelle on ominaista host (user) – host (server) – hierarkia. User on käyttäjä joka avaa yhteyden palvelimeen (server). Käyttäjän ja palvelimen välinen kommunikaatio perustuu pyyntöihin tai ilmoituksiin ja näiden kuittauksiin. Kumpi tahansa voi lähettää toiselle osapuolelle pyyntöjä tai ilmoituksia. Pyynnöt voivat olla tyypiltään DO tai DON'T. Vastauksena voi olla WILL tai WON'T sen mukaan, miten vastaaja on konfiguroitu. Ilmoituksissa termit kääntyvät toisinpäin, eli ilmoittaja lähettää DO tai DON'T sen mukaan, miten aikoo liikennöidä ja vastaanottaja ilmoittaa WILL tai WON'T sen mukaan, miten se on konfiguroitu (RFC-854, 4).

Telnet-liikenne voi olla salattua tai salaamatonta. Telnet-yhteys avataan kuitenkin selväkielisenä ja salaus aloitetaan, kun osapuolet ovat sopineet liikenteen salaamisesta (RFC-2941, 13).

6.2.3. SSHv1 ja V2

SSH on kuvattu IETF:n RFC-dokumentissa RFC-4251. Secure Shell (SSH) protokolla on protokolla joka mahdollistaa turvallisen etäistunnon ja turvalliset verkkopalvelut turvattoman (insecure) verkon ylitse. SSH protokolla koostuu kolmesta pääkomponentista: Siirtokerroksen protokolla (Transport Layer Protocol) mahdollistaa palvelimen autentikoinnin, luotettavuuden ja yhteyden eheyden. Käyttäjätunnistuksen protokolla (User Authentication Protocol) mahdollistaa käyttäjätunnistuksen palvelimella. Yhteys-protokolla (Connection Protocol) yhdistää (multiplexing) kryptatun tunnelin useiksi loogisiksi kanaviksi. SSH:ta käyttävällä palvelimella tulee olla salaukseen käytettävä salausavain (host key). Salausavain voi olla jaettu useampien laitteiden kesken. Jos palvelimella käytetään salausavaimia, tulee vähintään yhden niistä käyttää julkisen avaimen algoritmia (public key algorithm, DSS). Palvelimen avainta käytetään yhteyden avaamisen yhteydessä vaihdettaessa salausavaimia. Palvelimen salausavain voi perustua joko aiemmin jaettuun avaintietokantaan tai luotettavan kolmannen osapuolen sertifikaattiin. (RFC-4251, 3-4).

SSH-protokolla käyttää palvelin-asiakas-mallia (server-client). Yhteyden muodostamiseen käytettävä kryptaus voi olla symmetristä, asymmetristä

tai hash-tiivisteeseen perustuvaa. Yhteyden muodostamisen yhteydessä palvelin ilmoittaa myös mitä SSH:n versiota se tukee. Jos asiakas kykenee yhteystapaan, yhteyden muodostaminen jatkuu siten että palvelin lähettää julkisen avaimensa asiakkaalle identiteettinsä varmistamiseksi. Onnistuneiden julkisten avainten vaihtojen jälkeen, muodostetaan istunnon aikainen salainen avain, jolla kryptataan myöhemmin vaihdettava varsinainen data. Käytettävä avain ei ole sama jolla osapuolet autentikoivat toisensa yhteyden muodostamisen alussa. (Digital Ocean).

SSH:n käyttämät salaustavat eivät ole tämän tutkimuksen aiheena, mutta on tärkeää huomata, että SSH-yhteydet ovat salattuja koko yhteyden muodostamisen ja tiedon vaihdon ajan.

Yhteyden aloituksen onnistuttua, palvelin suorittaa käyttäjätunnistuksen yhteyttä ottaneelle osapuolelle. Käyttäjätunnistus voi perustua käyttäjätunnus/salasana-yhdistelmään tai SSH-avainpariin. (Digital Ocean).

SSH 2 on paranneltu versio SSH:sta. Siinä on korjattu SSH:ssa todettuja ja dokumentoituja virheitä, eikä se ole yhteensopiva SSH:n kanssa.

6.2.4. TFTP

TFTP on kuvattu IETF:n RFC-dokumentissa RFC-1350. TFTP on yksinkertainen tiedonsiirtoprotokolla (Trivial File Transfer Protocol). TFTP käyttää tiedonsiirtoon UDP-protokollaa. Ainoat toimenpiteet mihin se kykenee, ovat tiedostojen lukeminen ja kirjoittaminen palvelimelta tai palvelimelle. Siihen ei sisälly tiedostojärjestelmän listausta tai käyttäjän autentikointia. TFTP tukee kolmea erilaista siirtotapaa: netascii, oktetti ja mail. TFTP-tiedonsiirto alkaa pyynnöllä lukea tai kirjoittaa tiedosto. Pyyntö toimii myös pyyntönä avata yhteys. Jos palvelin hyväksyy pyynnön, avataan yhteys ja tiedosto siirretään 512 bitin lohkoissa. Jokainen paketti sisältää yhden datalohkon, joka pitää kuitata kuittauspaketilla ennen seuraavan lohkon siirron aloittamista. 512 bittiä pienempi datalohko ilmaisee tiedonsiirron päättymisen. Jos lähetettävä paketti ei saavu perille, vastaanottajan laskuri aiheuttaa aikakatkon (timeout) ja se lähettää edellisen paketin uudelleen. Paketti voi olla datalohko tai kuittauspaketti. Kadonneen paketin lähettäjä lähettää näin uudelleen kadonneen paketin. Useimmat virhetilanteet aiheuttavat yhteyden katkaisemisen. Virhetilanteesta ilmaistaan lähettämällä virheen ilmaiseva paketti. Virheestä ilmaisevista paketeista ei lähetetä kuittaussanomia. Virhetilanteita tunnistetaan kolme: palvelin ei pysty täyttämään pyyntöä, vastaanotettaessa paketti joka on väärin muodostettu ja pääsy tarvittavaan resurssiin on estynyt. Kaikissa edellä mainituissa tilanteissa muodostetaan virheestä ilmaiseva paketti ja yhteys katkaistaan. (RFC-1350, 2-3)

6.2.5. FTP

FTP on kuvattu IETF:n RFC-dokumentissa RFC-959. FTP on tiedonsiirtoprotokolla, jonka tarkoituksena on tarjota mahdollisuus tiedostojen siirtämiseen, mahdollistaa tietokoneiden etäkäyttö, tarjota yhtenäinen rajapin-

ta erilaisten tiedostojärjestelmien käyttämiseen ja tarjota mahdollisuus siirtää dataa luotettavasti ja tehokkaasti. FTP mahdollistaa terminaaliyhteydet, mutta on pääsääntöisesti tarkoitettu mahdollistamaan tiedostojen siirto ohjelmien välillä. FTP käyttää tiedonsiirtoon TCP-protokollaa. FTP käyttää tiedonsiirtoon kahta yhteyttä: kontrolliyhteys, jota käytetään FTP-komentojen ja vastausten välittämiseen ja datayhteys, jota käytetään tiedostojen siirtämiseen. Kontrolliyhteys voidaan muodostaa asiakkaan ja palvelimen tai kahden palvelimen välille. Muodostettaessa kontrolliyhteys palvelimen ja asiakkaan välille, asiakas tekee pyyntöjä palvelimelle ja kuuntelee TCP-porttia, jota halutaan käyttää tiedoston siirtämiseen (datayhteyden muodostamiseen). Palvelin, jolle pyyntöjä esitetään, muodostaa datayhteyden asiakkaaseen päin. Muodostettaessa yhteys kahden palvelimen välille, kontrolliyhteys muodostetaan molempiin palvelimiin ja data siirretään datayhteyttä käyttäen suoraan palvelimelta palvelimelle. Kontrolliyhteys muodostetaan käyttäen Telnet-protokollaa ja sen on oltava auki koko datan siirron ajan. Siirrettävä data voi olla ASCII, image (binääri), EBCDIC tai local muotoista. ASCII muotoa käytetään siirrettäessä tekstimuotoisia tiedostoja. Lähettäjä muuntaa datan käyttämästään merkkiesitysmuodosta 8-bittiseen NVT-ASCII esitysmuotoon ja lähettää sen vastaanottajalle. Vastaanottaja muuntaa datan käyttämäänsä merkkiesitysmuotoon. Image (binääri) -muotoa käytetään kuvien siirtämiseen. Image-muotoinen data muutetaan 8-bittisiksi siirtotavuiksi ja tallennetaan vastaanottavassa päässä jatkuvana bittivirtana. EBCDIC-muoto on tarkoitettu käytettäväksi silloin kun molemmat tiedonsiirtoon osallistuvat osapuolet käyttävät sitä merkkiesitysmuotonaan. Local -datamuotoa käytetään, kun käsiteltävien tiedostojen tallennusmuoto on jotain muuta kuin 8-bittiä. FTP:n tiedonsiirto voi olla aktiivista tai passiivista. Aktiivisessa tiedonsiirrossa asiakas avaa yhteyden palvelimelle FTP kontrollikanavalla porttiin 21 ja ilmoittaa TCP-portin numeron, jota se kuuntelee datayhteyden muodostamiseksi. Palvelin lähettää ACK-sanoman asiakkaan lähdeporttiin ja avaa datayhteyden asiakkaan ilmoittamaan TCP-porttiin käyttäen lähdeporttina porttia 20. Asiakas lähettää ACK-sanomat palvelimelle porttiin 20. Passiivisessa tiedonsiirtotavassa, asiakas avaa yhteyden palvelimelle FTP kontrollikanavalla porttiin 21 ja ilmoittaa tiedonsiirtomuodoksi PASV. Palvelin lähettää asiakkaan lähdeporttiin sanoman, jossa se ilmoittaa tiedonsiirtoon käytettävän TCP-portin numeron. Asiakas avaa datayhteyden palvelimen ilmoittamaan TCP-porttiin ja palvelin aloittaa tiedonsiirron asiakkaan lähdeporttiin. Palvelin lähettää lähdeporttiin siirrettävän datan ja ACK-sanomat. FTP käyttää käyttäjätunnistukseen Telnet:n käyttäjätunnus/salasana-yhdistelmää. (RFC-959, 1-26)

6.2.6. SFTP

SFTP tarkoittaa tässä yhteydessä SSH File Transfer Protocol eikä Simple File Transfer Protocol. SFTP on kuvattu IETF:n luonnoksessa draft-ietf-secsh-filexfer-13 (SFTP-draft). Protokolla on kuvattu SSH2-protokollan yhteydessä, mutta se on tarkoitettu käytettäväksi myös muiden sovellutusten kanssa. (SFTP-draft, 4).

SFTP tarjoaa mahdollisuuden turvalliseen tiedostojen siirtoon, yleisemmin mahdollistamaan pääsy tiedostojärjestelmään. Protokolla olettaa, että sitä

käytetään turvallisen yhteyden ylitse, että palvelin on autentikoinut käyttäjän ja että protokollalla on tieto käyttäjän identiteetistä. (Everything explained).

6.2.7. SCP

SCP:stä ei ole laadittu IETF:n RFC-dokumentaatiota (Secure Copy, Wikipedia). SCP perustuu BSD:n RCP-protokollaan. SCP tukee tiedostojen siirtoa verkkolaitteiden välillä. SCP käyttää SSH:ta siirtomekanismina. Se siis tukee SSH:n tavoin autentikointia tiedonsiirron aitouden ja luotettavuuden varmistamiseksi. SCP on SSH:n tavoin tyypiltään client-server – tiedonsiirtotapa. Asiakas voi ladata tiedostoja palvelimelle tai palvelimelta. SCP:n TCP-portti on 22, mutta se on vaihdettavissa. Käytettäessä SCP:tä, asiakas avaa SSH-etäyhteyden ja pyytää palvelinta aloittamaan SCP-prosessin. SCP-prosessi voi toimia joko lähdetilassa (Source mode) tai vastaanottotilassa. Lähdetilassa tiedosto luetaan palvelimelta ja lähetetään asiakkaalle. Vastaanottotilassa (Sink mode) tiedosto vastaanotetaan asiakkaalta ja kirjoitetaan palvelimen levyjärjestelmään. SCP:llä ei voida siirtää tiedostoja palvelimelta palvelimelle FTP:n tyyliin, jossa avataan kontrolliyhteys molemmille palvelimille ja siirrettävä data kulkee erillistä datayhteyttä myöden. SCP:llä voidaan kuitenkin reitittää siirrettävä data kulkemaan molempiin palvelimiin, yhteyden avanneen asiakkaan kautta. (Secure Copy, Wikipedia).

6.2.8. Pohdintaa hallintaprotokollista

Hallintaprotokollat voidaan jakaa karkeasti kahteen tyyppiin: terminaaliyhteysprotokolliin ja tiedonsiirtoprotokolliin. Molemmissa tyypeissä korostuu uudempien protokollien kyvykkyys tiedonsiirron salaamisessa ja yhteyden muodostavien tahojen aitouden varmistamisessa.

Pääsääntöisesti voidaan sanoa, että siirrettäessä tietoa tai avattaessa yhteyksiä sellaisten yhteyksien yli, jotka eivät ole luotettavia tai joiden turvallisuutta koko yhteyden matkalla ei voida taata, tulisi käyttää vahvan kryptauksen mahdollistavia protokollia kuten SCP, SFTP ja SSH:n eri versiot. Niidenkin turvallisuus perustuu kuitenkin riittävän vahvoihin salasanoihin ja sertifikaatteihin, sekä käytettävien salausalgoritmien hyvyyteen.

Konsoliyhteyksiä käytettäessä korostuu laitteen käyttöympäristön fyysinen turvallisuus. Koska yhteyden käyttämiseen vaaditaan pääsyä laitteen välittömään läheisyyteen, sen luvattoman hyödyntämisen estäminen perustuu siihen, ettei välittömässä läheisyydessä ole kuuntelulaitteistoja, laitetilan lukitukseen ja kulkuoikeuden rajaamiseen.

6.3. Valvonta- ja hallintasovellukset

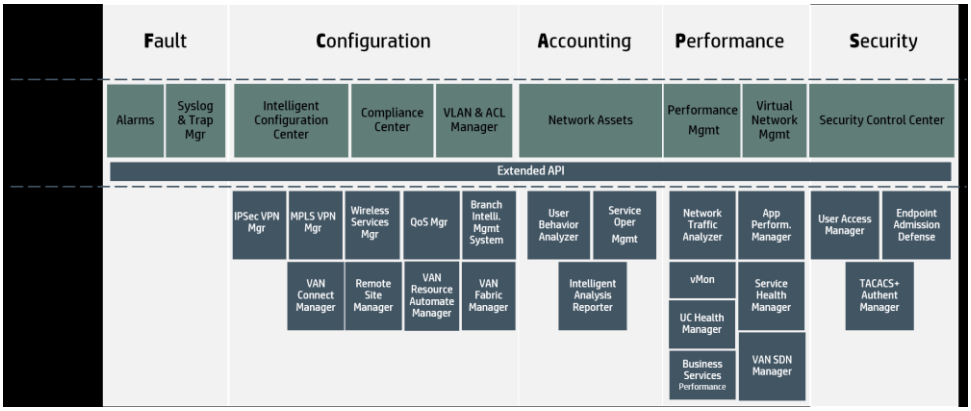
Valvonta- ja hallintasovelluksilla keskitetään verkkolaitteiden operointia. Niiden tarkoituksena on mahdollistaa ja yksinkertaistaa monimutkaisten tietoliikenneverkkojen laitteiden, ohjelmistojen ja konfiguraatioiden hallinta.

Niiden tarkoituksena on toimia verkon hallinta-asemana, laitteiden tuottamia hälytyksiä ja ilmoituksia vastaanottavina laitteina, raporttien laatimisen mahdollistavina tietolähteinä tai tietokantoina, visualisoida verkon tapahtumia ja ilmiöitä, tehdä näkyväksi mahdolliset verkkoon tai sen palveluihin kohdistuvat tunkeutumisyritykset ja haitanteot, sekä tehdä näkyväksi verkon toiminnan aiheuttamat epätoivotut palvelutason alentumat. Parhaassa tapauksessa nämä sovellukset toimivat myös tietovarantoina konfiguraatioiden ja ohjelmistojen hallitsemiksi, jolloin ne nopeuttavat palautumista häiriötilanteista.

Tässä tutkimustyössä tarkastellaan kahta tähän käyttöön tarkoitettua sovellusta, HP IMC:tä ja MG-Soft NetInspectoria. Niiden ominaisuudet ovat toisistaan poikkeavia, NetInspectorin käytettävyyden rajoittuessa enemmän reaaliaikaiseen valvontaan ja HP IMC:n pyrkiessä kokonaisvaltaisempaan ratkaisuun.

6.3.1. HP IMC

HP IMC on kokonaisvaltainen hallintajärjestelmä, joka tukee FCAPS-mallia (Fault, Configuration, Accounting, Performance, Security) (kuva 14). Se tarjoaa ominaisuuksia ja toiminnallisuuksia, jotka on suunniteltu verkkoinfrastruktuurin kokonaisvaltaiseen hallintaan (HP IMC)



Kuva 14. FCAPS-malli (HP IMC)

IMC:n ohjelmistoversio on kirjoitushetkellä v7.2 (E0403) ja siitä on tarjolla kolmea eri versiota: Basic, Standard ja Enterprise. (HP IMC)

Basic on suunnattu pienille ja keskisuurille yrityksille ja kuluttajille pieniin verkkoympäristöihin. Se sisältää häiriöiden hallinnan, verkkoelementtien konfiguroinnin ja verkonvalvonnan ominaisuuksia ja tuen muillekin kuin HP:n valmistamille laitteille. Basic lisenssi mahdollistaa 50. laitteen hallinnan. (HP IMC)

Standard on suunnattu yrityskäyttöön. Se sisältää samat ominaisuudet kuin Basic, mutta niiden lisäksi RESTful eAPI-ohjelmakirjaston johon voidaan integroida kolmannen osapuolen ohjelmistoja lisäominaisuuksien saavuttamiseksi. Standard lisenssi mahdollistaa 50 laitteen hallinnan, mutta sii-

hen on ostettavissa lisälisenssejä suuremman laitekannan hallitsemiseksi. (HP IMC)

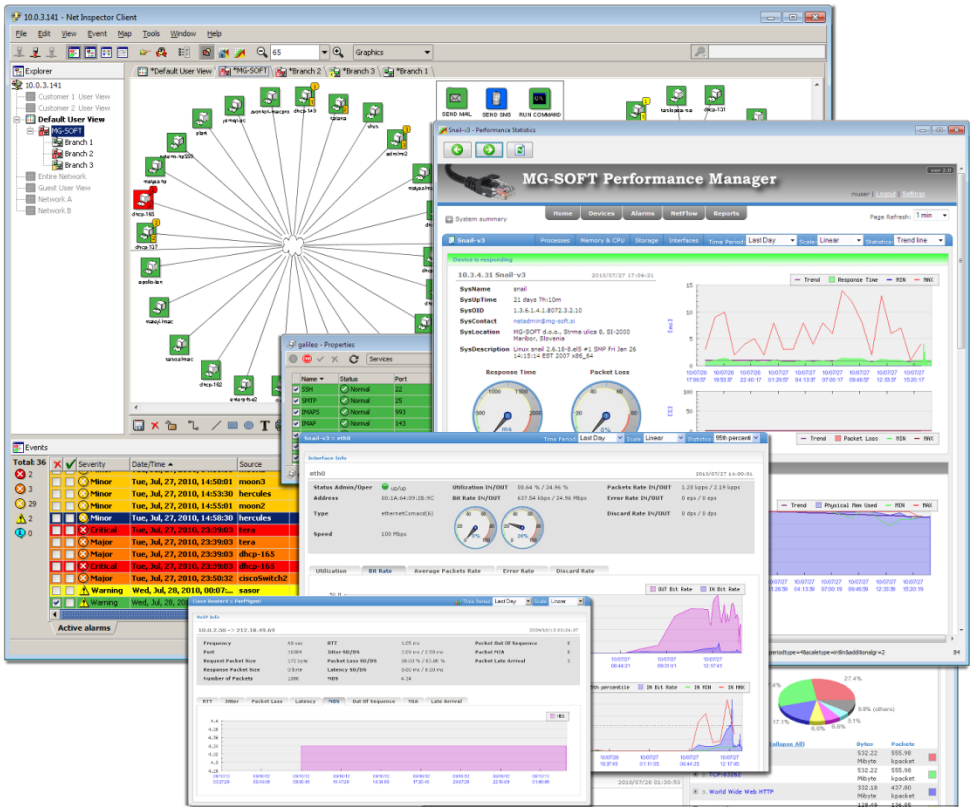
HP IMC on suunniteltu tukemaan ITIL-viitekehyksen mukaisia IT-käytäntöjä. Se käyttää yhden näytön hallinta – mallia ja mahdollistaa IT-palveluiden kokonaisvaltaisen hallinnan, skaalautuu erityylisille järjestelmäarkkitehtuureille, käyttää SoA-mallia, mahdollistaa erillisten hallintatyökalujen integroinnin ja antaa mahdollisuuden laajentaa infrastruktuurin hallintaa uusien skaalautuvuutensa ja uusien tekniikoiden käyttöönoton myötä. (HP IMC)

HP IMC koostuu perusalustasta ja palvelukomponenteista. Palvelukomponentit lisäävät toiminnallisuuksia. Perusalusta tarjoaa ylläpitäjille ja operaattoreille HP IMC:n hallintaan ja HP IMC:llä hallittavien laitteiden hallintaan tarvittavat toiminnallisuudet. HP IMC perusalusta tarjoaa hallintatyökalut IMC:n hallintaan ja käyttämiseen. Näihin kuuluvat myös IMC:n ominaisuuksien käyttöoikeuksien myöntäminen tai rajoittaminen operaattoritunnuksille tai operaattoriryhmille. Perusalusta sisältää myös ominaisuuksia järjestelmänlaajuiseen laitetietojen keruun hallintaan ja tiedon jakoon kaikkien IMC:n moduulien välillä kuten laite, käyttäjä ja palvelu ryhmien luominen ja ylläpito; laitevalmistajien, laitesarjojen ja laitemallien tietojen hallitseminen; SNMP MIB hallinta ja muut järjestelmänlaajuiset asetukset ja toiminnot. (HP IMC)

HP IMC:ssä on laaja ominaisuuksien kirjo verkkolaitteiden hallintaan, kuten laitteiden konfiguraatioiden hallinta SNMP:llä, Telnet:llä ja SSH:lla, spanning treen konfigurointi ja kytkimien PoE:n hallinta. IMC:llä voidaan tehdä konfiguraatioihin ja ohjelmistoihin kohdistuvia toimintoja joko yksittäisille laitteille tai laiteryhmille. (HP IMC)

6.3.2. NetInspector

MG-Softin NetInspector on virhe- ja suorituskykyhallinta ohjelma, joka on suunniteltu verkkolaitteiden tilan ja suorituskyvyn valvontaan ja valvottavien IPv4 ja IPv6 verkkolaitteisiin liittyvien herätteiden hallintaan. (MG-Soft) (kuva 15)



Kuva 15. NetInspector (MG-Soft)

NetInspector on client-server ohjelma, jossa palvelin tarkkailee jatkuvasti verkon palveluita ja tärkeitä SNMP parametreja verkon laitteissa. Se käynnistää hälytyksiä virhetilanteissa (esim. laite tai palvelu ei vastaa kyselyyn, tai jos SNMP muuttuja ylittää kynnysarvon). Ohjelmassa on sisäänrakennettu tuki useiden verkkopalveluiden valvontaan. Aktiivisen laitteiden valvonnan lisäksi NetInspector voi ottaa vastaan SNMP-protokollan herätteitä. Ohjelmisto kääntää vastaanotetut SNMP-herätteet ITU X.733-yhteensopiviksi hälytyksiksi, tallettaa ne tietokantaan ja lähettää ilmoitukset herätteistä liittyneille asiakkaille. (MG-Soft)

Palvelin on suunniteltu skaalautuvaksi. Käytettäessä ohjelmistoa pienemmissä verkoissa, palvelin toimii yhdessä palvelimessa. Suuremmissa verkoissa voidaan käyttää kahta tai useampaa kyselyitä tekevää palvelinta (engines) tehokkaan verkon valvonnan mahdollistamiseksi. (MG-Soft)

6.3.3. Pohdintaa verkonvalvonta- ja hallintasovelluksista

Tässä esitellyt kaksi verkon valvonta- ja hallintasovellusta eroavat ideologialtaan siten, että siinä missä HP IMC on suunniteltu kokonaisvaltaiseen IT-palveluiden hallintaan, NetInspector keskittyy laitteiden toiminnan valvontaan. Molemmat mahdollistavat herätteiden hallinnan SNMP-protokollaa käyttäen ja valvonnan ICMP-sanomilla.

7 TUTKIMUSASETELMA

Maapuolustuksen taktisten verkkojen kehittyminen, sekä tiedonsiirtokapasiteetin, että käytettävien verkkoteknologioiden osalta, ovat aiheuttaneet tarpeen valvonnan ja hallinnan kehittämiselle. Nykyaikaisten IP-verkkojen valvontaa ja hallintaa ei ole mahdollista toteuttaa samalla tavalla kuin perinteisten analogisten, tai edes digitaalisten, puhelinverkkojen. Muuttuneet vaatimukset aiheuttavat tarpeen tutkia uusilla teknologioilla toteutettujen verkkojen valvontaan ja hallintaan kehitettyjen tapojen ja protokollien käyttöä maapuolustuksen taktisten verkkojen valvonnassa ja hallinnassa.

Tutkittaville verkoille on ominaista käytettävyyden ennustettavuuden alhainen taso, vaihteleva yhteyksien laatu, liikkuvuus ja väliaikaisuus. Käytettävyyden ennustettavuutta laskee vastustajan pyrkimys haitata, ja jopa estää, tiedonsiirtoa. Yhteyksien laatu on riippuvainen verkon muodostamisen mahdollisuuksista. Kaikissa tapauksissa ei ole mahdollista rakentaa verkkoa teknologian kannalta parhaita maantieteellisiä sijainteja tai radiotaajuuksia käyttäen. Liikkuvuus ja väliaikaisuus ovat ominaisuuksia, joiden vuoksi on haasteellista varmistua siitä, pitäisikö jonkin verkon osan olla toiminnassa tiettynä ajan hetkenä vai onko siinä sellainen ongelma (tekninen tai tilanteen aiheuttama), joka estää verkon muodostamisen.

Taktiset verkot voidaan nähdä IT-palvelutuotannon mahdollistavana osana. Tarkoitus ei ole rakentaa tietoliikenneverkkoja, vaan tuottaa maapuolustuksen joukoille palveluita, jotka edesauttavat niitä tehtävänsä suorittamisessa. IT-palvelutuotannon toteuttamiseksi on laadittu parhaiden käytäntöjen viitekehyksiä, joista maapuolustuksen käyttöön on valittu ITIL - Information Technology Infrastructure Library. Tutkija on havainnut, että valittua viitekehystä ei käytetä yksiselitteisesti maapuolustuksen taktisten verkkojen valvonnassa ja hallinnassa. Tämä ennakko-oletus suuntaa tutkimaan maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttamista ITIL:n mukaisesti.

7.1. Tutkimusongelma

Tutkimusongelmana tunnistetaan, että maapuolustuksen taktisten verkkojen valvontaa ja hallintaa ei ole yksiselitteisesti toteutettu ITIL:n parhaiden käytäntöjen viitekehyksen mukaisesti.

Tutkimusongelmasta johdettu tutkimuskysymys on:

- Voiko maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttaa ITIL:n käytäntöjen mukaisesti?

Tutkimuskysymykseen pyritään vastaamaan selvittämällä seuraavat alakysymykset:

- Millainen on ITIL:n valvonnan ja hallinnan viitekehys?
- Mitä ovat maapuolustuksen taktiset verkot ja mikä niille on ominaista?
- Mitä teknologioita valvonnan ja hallinnan toteuttamiseksi on käytettävissä?

Tutkimus rajataan koskemaan maapuolustuksen taktisia verkkoja. Verkkoja käsitellään yleisesti käytössä olevien tietoliikennetekniikoiden ja protokollien kautta. Tutkimuksessa ei kuvata verkkoja tai niitä käyttäviä joukkoja yksityiskohtaisesti, eikä siihen sisällytetä viestitaktiikkaa. Tutkimus ei myöskään ota kantaa kyber-ulottuvuuteen. IT-palvelutuotannon viitekehyksistä tutkimus rajataan koskemaan ITIL:iä. Tutkimuskysymysten vastauksena voidaan käsitteistää maapuolustuksen taktisten verkkojen valvonta ja hallinta ITIL:n mukaisesti. Tutkimuksessa ei testata teoriaa käytännössä.

7.2. Tutkimusote

Tutkimusote on laadullinen eli kvalitatiivinen. Laadullinen tutkimus voidaan valita, kun ilmiöstä tiedetään vähän. Perusteita kvalitatiivisen tutkimuksen valinnalle voi olla esimerkiksi:

- Ilmiöstä ei ole tietoa, teorioita, tutkimusta (ilmiötä ei tunneta)
- Ilmiöstä halutaan saada syvällinen näkemys
- Käytetään triangulaatiota eli ns. mixed-tutkimusstrageiaa
- Ilmiöstä halutaan saada hyvä kuvaus

(Kananen 2015, 71).

Edellä mainituista perusteista tutkimusotteen valintaa tukevia ovat ainakin tarve saada tietoa, teorioita tai tutkimusta ja halu saada ilmiöstä hyvä kuvaus.

Maapuolustuksen taktisten verkkojen valvonta ja hallinta nähdään tutkimustyössä prosesseina, jotka saavat syötteitä järjestelmien valvonnan ja hallinnan tekniikoilta. Syötteet aiheuttavat prosessin toteuttamistarpeita, joiden onnistuminen voidaan todentaa palvelun jatkuvuutena tai palautumisena.

Tutkittaessa käytännöstä liikkeelle lähtevää ilmiötä, tutkimus on induktiivinen eli tutkimus perustuu yksittäistapauksiin, joista pyritään saamaan ymmärrys ilmiöstä (Kananen 2015, 67). Maapuolustuksen taktisten verkkojen valvonta ja hallinta voidaan nähdä tähän käyttötapaukseen liittyvänä ilmiönä, jota ei sellaisenaan voida yleistää koskemaan kaikkia tietoliikenneverkkoja. Tämän vuoksi tämä tutkimus voidaan nähdä induktiivisena tutkimuksena, jonka tarkoitus on ymmärryksen saaminen yksittäisestä ilmiöstä.

7.3. Aineiston keruu- ja analyysimenetelmät

Kvalitatiivisen tutkimuksen aineistonkeruumenetelmät jaotellaan primääriaineistoihin ja sekundääriaineistoihin. Primääriaineistoja ovat haastattelut, havainnointi ja kyselyt. Sekundääriaineistoja ovat dokumentit. (Kananen 2015, 131)

Primääriaineiston keräämiseen käytettiin valikoituihin henkilöihin kohdistettuja teemahaastatteluita. Teemahaastatteluiden valintaa tutkimusmeto-

diksi puoltaa vähäinen ennakkotieto ilmiöstä, jolloin tarkkojen kysymysten esittäminen on haasteellista. Haastateltaviksi valittiin maapuolustuksen taktisista verkoista riittävän kokemuksen omaavia henkilöitä, jotka tuntevat ITIL:n viitekehyksen. ITIL:n tuntemus mahdollistaa maapuolustuksen taktisten verkkojen ilmiöiden sitomisen viitekehykseen ja ohjaa haastattelua oikean tiedon suuntaan.

Sekundääriaineistona käytettiin tiedeyliopistojen ja ammattikorkeakoulujen opinnäytetöitä, tutkimuksia ja julkaisuja, telekommunikaatioalan standardeja, sekä ITIL:n IT-palvelutuotannon viitekehykseen liittyvää kirjallisuutta. Tiedeyliopistojen ja ammattikorkeakoulujen opinnäytetöiksi valittiin vähintään Pro Gradu- tai Master's -tasoisia töitä. Jos opinnäytetyön aihe osui suoraan tämän tutkimuksen aihepiiriin, voitiin varauksella käyttää myös alemman tason töitä. Yleisesti tiedeyliopistojen ja ammattikorkeakoulujen tuottama aineisto nähtiin tiedeyhteisön hyväksymänä ja luotettavana tietona tutkimuksen tekemiseksi. Yleensä tietoliikennejärjestelmät on rakennettu telekommunikaatioalan standardien mukaan. Standardit määrittävät ja yhdenmukaistavat reaalielämän ilmiöitä. ITIL on viitekehys, joka on valittu käytettäväksi maapuolustuksen IT-palvelutuotannossa. Tätä premissiä ei ollut mahdollista tämän tutkimuksen piirissä muuttaa.

Haastattelut nauhoitettiin ja litteroitiin yleiskieliseksi. Yleiskielinen yhteismitallistaminen on riittävää, koska tutkimuksen tarkoitus on tunnistaa ilmiön ja viitekehyksen välisiä suhteita, eikä niinkään haastateltavien tuntemuksia tai tunnetiloja. Aineiston sisältöanalyysi tehtiin aineistolähtöisesti. Aineistolähtöinen tulkinta sovittaa olemassa olevien teorioiden käsitteitä aineistoon, eli pyrkii löytämään aineistosta teorian olettamia tekijöitä tai käsitteitä (Kananen 2015, 171).

7.4. Luotettavuuden arviointi

Kanasen mukaan (Kananen 2015, 344) laadullisen tutkimuksen luotettavuuskriteerejä ovat luotettavuus, siirrettävyys, riippuvuus ja vahvistettavuus. Luotettavuus tarkoittaa sitä, että esitetty tulkinta vastaa todellisuutta. Siirrettävyys tarkoittaa tulkinnan käytettävyyttä toisessa tilanteessa, riippuvuus tulkinnan oikeellisuutta ja vahvistettavuus tulkinnan tarkastuttamista tulkinnan kohteelta. Edellisten lisäksi, luotettavuutta voidaan arvioida tarkkailemalla aineiston saturaatiota.

Tämän tutkimuksen kohdalla, edellisten mukaan, tulkinnan luotettavuuden ja siirrettävyyden arviointi voi ilmiön julkisuusrajoitusten takia olla haasteellista. Niiltä osin, jotka tutkimuksessa koskevat viitekehyksen ja maapuolustuksen taktisten järjestelmien valvonnan ja hallinnan perusperiaatteita, julkisuusrajoitukset eivät ole este luotettavuuden tai siirrettävyyden arvioinnille. Riippuvuus varmistettiin työnantajan ohjaajan avulla. Aineiston vahvistettavuus varmistettiin luetuttamalla haastatteluista tehdyt johtopäätökset haastatteluiden kohteilla ja vertailemalla niitä sekundääriseen aineistoon. Saturaation saavuttaminen on mahdollista pienelläkin haastattelumäärällä, jos haastatteluiden esivaatimukset kohteiden kokemuksesta ja osaamisesta täyttyvät ja haastateltavat onnistutaan saamaan haastateltavaksi. Haastateltavien määrä jäi pieneksi, koska haastateltavien kriteerit

oli määrätty korkeaksi. Alhainen määrä aiheuttaa tutkimuksen luotettavuudelle epävarmuustekijöitä, joita pyrittiin poistamaan sekundäärisellä aineistolla.

7.5. Tutkimuskohde

Maavoimien taktisten verkkojen valvonta ja hallinta on muuttunut tiedonsiirtojärjestelmien kehittymisen ja tiedonsiirtoon osallistuvien laitteiden määrän lisääntymisen myötä kompleksisempaan suuntaan. Kompleksisuus ja määrän kasvu pakottavat verkkoja rakentavat ja ylläpitävät tahot vielä aiempaakin suunnitelmallisempaan toimintaan ja prosessien käyttämiseen eri toimijoiden välillä. Tietoliikenteen ja tietotekniikan kehityksen myötä on myös laadittu viitekehyksiä, joihin on mahdollista tukeutua parhaiden käytäntöjen käyttämiseksi. Näiden viitekehyksien käyttämisellä ja käytännön tutkimuksella on mahdollista luoda malleja, joita käyttämällä verkot pystyvät suoriutumaan tehtävästään IT-palvelutuotannossa paremmin. Mallit mahdollistavat myös verkkoja rakentaville ja ylläpitäville organisaatioille resurssien säästöä.

Tehokas ja yksiselitteinen valvonta ja hallinta ovat integraalinen osa nykyaikaisia tiedonsiirtoverkkoja. Tehokkuus perustuu parhaiden käytäntöjen käyttämiseen ja niiden kattavaan implementointiin. Yksiselitteisyys perustuu kattavuuteen koko verkon osalta. Mukaan luetaan laitteistojen ominaisuuksien ja asetusten, sekä henkilöstön toimintatapojen laatiminen siten, että ne mahdollistavat valitut käytännöt.

Tutkimuskohteena oleva maapuolustuksen taktisten verkkojen valvonta ja hallinta valikoitui tutkimuskohteeksi tutkijan työn kautta. Kohteena ovat sekä järjestelmät, että järjestelmiä rakentavat ja ylläpitävät organisaatiot. Tutkittavasta kohteesta pyritään löytämään ne osat ja toiminnallisuudet, jotka voi liittää ITIL:n viitekehykseen ja mallintamaan niitä sen mukaan.

Tutkimuksen toteuttamiseksi laadittiin maavoimien esikunnalle tutkimuslupahakemus (Liite 1). Hakemuksen vastauksena saatiin tutkimuslupa (Liite 2), jossa tutkimukselle asetettiin julkisuusvaatimus ja haastateltaville henkilöille annettiin osallistumiseen vapaaehtoisuus mahdollisuus.

8 TUTKIMUSTULOKSET

8.1. Haastattelut

Haastattelut tehtiin strukturoimattomina eli teemahaastatteluina. Haastattelut kohdistuivat tarkoilla kriteereillä valikoituihin henkilöihin ja ne suoritettiin teemahaastatteluina. Haastateltavien valinnan kriteereinä olivat pitkä kokemus maapuolustuksen taktisista verkoista ja ITIL:n tuntemus. Kokemusta haluttiin olevan koko järjestelmän laajuisesti, vähintään kompaniatasolta puolustushaaraesikuntaan asti. Tämän valinnan rajoittavuus tiedostettiin etukäteen, mutta luotettiin että tällä valinnalla haastateltavien määrä voidaan pitää hallituissa rajoissa. Valinnalla haluttiin myös varmis-

taa se, että haastatteluilla saatu tieto on koko järjestelmän kattavaa. ITIL:n tuntemiseksi riitti haastateltavan perustason sertifiointi. Teemahaastatteluita varten laadittiin haastattelusuunnitelma, joka perustuu Kanasen (Kananen 2015, 154) haastattelun suunnittelumalliin. Haastattelusuunnitelma on liitteenä 3.

Haastattelut olivat yksilöhaastatteluita. Haastatteluita ei rajattu kysymyspatteriin, vaan niiden annettiin edetä vapaasti. Keskustelu aloitettiin teemalla ja keskustelua kuljetettiin haastattelun aikana esiin nousseiden kysymysten mukaan. Teemahaastattelun runko on liitteenä 4.

Haastattelut tallennettiin digitaalisella tallentimella ja litteroitiin yleiskielisiksi. Litteroidut haastattelut ja digitaaliset tallenteet ovat tutkijan hallussa. Litteroituja haastatteluita analysoitiin lukemalla ja vertaamalla sekundääriseen aineistoon. Analyysin työkaluna käytettiin yksinkertaista Excel-taulukkoa. Analyysin tarkoituksena oli tunnistaa haastateltavien kertomuksista sekundäärisen aineiston määritelmiä ja kokonaisuuksia. Tunnistetuista määritelmistä ja kokonaisuuksista tutkimuksen kannalta merkittävimmät kirjattiin ylös ja ne on käsitelty myöhemmin haastatteluiden tuloksia analysoivassa kappaleessa.

Haastattelut etenivät haastattelusuunnitelman (liite 4) mukaisesti. Ensin haastateltavien kanssa keskusteltiin aikaisemman sukupolven maapuolustuksen taktisten verkkojen (YVI-järjestelmät) hallinnasta ja valvonnasta. Tämän tarkoituksena oli orientoida keskustelua kohti maapuolustuksen taktisten verkkojen hallinnalle ja valvonnalle ominaisia piirteitä. Tämän jälkeen keskustelua ohjattiin ITIL:n ja nykyaikaisten taktisten verkkojen ilmiöiden suuntaan ja pyrittiin löytämään sieltä ne viitekehyksen mukaiset käsitteet ja määritelmät, jotka ovat ominaisia juuri niille. Viimeisenä teemana oleva valvonnan- ja hallinnan teknologiat jätettiin jälkiruoaksi. Siinä toivottiin vielä nousevan esiin asioita, jotka olivat jääneet syystä tai toisesta edellisissä teemoissa käsittelemättä. Haastateltavien ei oletettu olevan syvällisesti teknologia orientoituneita, eikä näin ollen pyritty yksityiskohtaiseen teknologioiden vertailuun.

8.2. Haastatteluiden tuloksien analysointi

Haastatteluiden ensimmäisenä teemana olivat aikaisemmat maapuolustuksen taktiset verkot ja niistä erityisesti YVI-verkot. Kuten kappaleessa 5.1, ”Tiedonsiirtojärjestelmät”, todetaan, YVI-verkot edustavat vanhempaa puhelinteknologiaa. Teeman sisällä päästiin myös nykyisiin ja tuleviin verkkoihin, jollaisia edustaa M18-järjestelmä. Teeman tulokset ovat analysoituna kappaleessa 8.2.1, ”Aikaisemmat järjestelmät, YVI-verkot ja tulevat maapuolustuksen taktiset verkot”.

Toisena teemana keskusteltu ITIL ja sen käyttäminen maapuolustuksen taktisten verkkojen valvonnan- ja hallinnan viitekehyksenä, toi esiin verkoille luonteenomaisia piirteitä. Ne asettavat tiettyjä haasteita parhaiden käytäntöjen toteuttamiselle. Teeman piirissä saadut tulokset on käsitelty kappaleessa 8.2.2, ”ITIL ja maapuolustuksen taktisten verkkojen valvonta ja hallinta”

Kolmas teema oli valvonnan- ja hallinnan teknologiat, joiden osalta keskustelu jäi lyhyemmäksi. Muutamia tärkeitä teknologioiden käyttämiseen liittyviä huomioita kuitenkin ilmeni. Teema on analysoitu kappaleessa 8.2.3, ”Valvonnan ja hallinnan teknologioista”.

8.2.1. Aikaisemmat järjestelmät, YVI-verkot ja tulevat maapuolustuksen taktiset verkot

YVI-verkkoja edeltävät järjestelmät olivat analogisia puhelinjärjestelmiä, joiden rakentamiseksi käytettiin sekä parikaapeli-, että radiolinkkijärjestelmiä. Näistä järjestelmistä käytettiin nimeä M80. Radiolinkkijärjestelmien lisäksi käytössä oli myös VHF-radioita, joilla muodostettiin puheyhteyksiä (ja myöhemmin sanomalaiteyhteyksiä) pataljoonan sisäisen johtamisen ja tulenjohtamisen mahdollistamiseksi. Radioita kuitenkin käytettiin vasta taisteluiden alettua ja varmentavina yhteyksinä, mikä käy ilmi myös kappaleesta 3.3, ”Sotien jälkeinen aika”.

YVI-verkot olivat ensimmäisiä maapuolustuksen taktisia verkkoja, joissa oli havaittavissa verkkomainen rakenne. Se ilmeni joko runkoverkkona, johon liitettiin liittyjiä tai hilamaisena rakenteena, jolloin runkoverkkoa ja liittyjiä ei voinut selkeästi erotella toisistaan. Vaikka YVI-verkot kokonaisuutena olivatkin ensimmäisiä verkko-kokonaisuuksia, niitä rakentavat joukot toimivat kuten analogisten järjestelmien aikaan, rakentaen yksittäisiä yhteyksiä. YVI-verkon käytettävyyttä parannettiin muodostamalla yhteyksiä yleiseen televerkkoon. Yhteys mahdollisti puheluiden muodostamisen yleiseen televerkkoon ja muihin YVI-verkkoihin käyttäen yleistä televerkkoa siirtotienä. (katso 5.1, ”Tiedonsiirtojärjestelmät”)

Viestijoukot rakensivat ja ylläpitivät YVI-verkkoja, valvoivat niiden muodostamia linkkiyhteyksiä, sekä sanomalaiteverkon toimintaa. YVI-verkkojen, tai niitä edeltäneiden M80-järjestelmien, tuottamia palveluita olivat puhe- ja sanomapalvelu. Niistä ei puhuttu, tai niitä ei tuotettu, kappaleessa 4.1, ”Palvelutuotanto käytäntönä” kuvatulla tavalla, jolloin olisi voitu selvästi hahmottaa palveluiden suhde toisiinsa tai asiakkaaseen.

Verkonvalvonta ja -hallinta olivat toimintoja, joiden tarkoituksena oli pitää verkko toimintakykyisenä. Näin voitiin katsoa, että puheella ja sanomilla tapahtuva viestintä oli mahdollista käyttäjien välillä. Verkon ylläpitäjinä toimivat valvontajoukkueet, sekä viestiasemien henkilöstö oman asemansa osalta. Verkon ylläpitäjillä oli mahdollisuus saada verkon viestikeskuksista ja niiden välisistä yhteyksistä tietoa verkkoon kiinteästi kuuluvalla valvontalaitteella. Verkkomainen rakenne ei näkynyt selvästi asematasolla. Asemien henkilöstö osallistui verkon ylläpitoon varmistamalla, että heidän asemallaan toimivat käsketyt yhteydet, sekä puhelinverkossa, että sanomalaiteverkossa.

Valvontaa ja hallintaa ei ollut teknisesti mahdollista organisoida suuremmiksi kokonaisuuksiksi. Valvonta ja hallinta oli rajattu sen organisaation toiminnaksi, joka verkon rakensi ja vastasi sen ylläpidosta.

2010-luvun alussa YVI-verkkoihin lisättiin IP-verkon kykyjä liittämällä asemien datakanaviin IP-reitittimiä. Reitittimet mahdollistivat datan välittämisen piirikytkentäisessä digitaalisessa puhelinverkossa. Tämän muutoksen myötä verkoissa käytettiin ensimmäistä kertaa standardoituja, tietoliikenneverkon valmistajasta riippumattomia tiedonsiirtotekniikoita. Tiedonsiirtotekniikoiden lisäksi käyttöön otettiin myös valvontasovelluksia, kuten NetInspector. Valvontasovellukset käyttivät standardoituja valvonnan ja hallinnan protokollia (katso kappale 6.3.2, ”NetInspector”). Valvontasovelluksien käyttö tapahtui valvontajoukkueen toimesta. Datan siirto rajoittui kuitenkin YVI-verkon sisälle, eikä sitä voinut tässä kehitysvaiheessa tehdä yleisen televerkon lävitse.

Tulevissa maapuolustuksen taktisissa verkoissa siirrytään käyttämään IP-tiedonsiirtotekniikkaa. Tulevia verkkoja on esimerkiksi kappaleessa 5.1, ”Tiedonsiirtojärjestelmät”, mainittu M18-järjestelmä. Aikaisemmin verkot olivat puhelinjärjestelmiä, joita käytettiin piirikytkentäisesti puheen siirtoon. Sanomaliikennettä siirrettiin samalla tavalla muodostettujen yhteyksien välityksellä. Jatkossa verkot ovat ns. all-IP-verkkoja. Tiedonsiirtoon käytetään IP-protokollaa ja verkkoja muodostetaan käyttäen MANET (Mobile Ad-hoc Network) toiminnallisuutta. Siirtyminen IP-teknologian käyttöön mahdollistaa aiempaa parempien palveluiden tuottamisen ja riippumattomuuden järjestelmän valmistajasta palveluiden tuottamiseksi.

8.2.2. ITIL ja maapuolustuksen taktisten verkkojen valvonta ja hallinta

Haastatteluiden toisena teemana käsiteltiin ITIL:iä ja sen käyttämistä maapuolustuksen taktisten verkkojen valvonnan ja hallinnan viitekehyksenä. Haastateltavien näkemyksenä oli, että ITIL ei ole sellaisenaan käytössä verkkojen valvonnassa ja hallinnassa. Syyksi tähän esitettiin, että ITIL:n prosessit ovat lähtökohtaisesti liian raskaita käytettäväksi maapuolustuksen taktisten verkkojen palvelutuotannossa. Toinen näkökulma oli, että sotilaat käyttävät asioiden kuvaamiseen omaa, aikojen saatossa muotoutunutta, ammattikieltään.

Haastatteluissa kävi ilmi, että maapuolustuksen taktisten verkkojen suunnittelussa ja palvelutuotannossa on vahvana tekijänä vuosien aikana kertynyt kokemus piirikytkentäisten puhelinverkkojen parissa. Vaikka osa taktisesta verkosta on kiinteästi rakennettua, palveluiden tuottaminen nähdään useasti verkkojen rakentamisena. Tähän näkemykseen johtaa myös se, että usein palveluita tuotetaan alueille, joilla ei ole verkkoinfrastruktuuria käytettävissä tai se ei ole riittävän helposti muunnettavissa tähän käyttöön. Tällöin palveluiden tuottamiseksi tarvittavat siirtotiet on ensin rakennettava ja ylläpidettävä palveluita tuottavan joukon toimesta. Rakentamisen mahdollistamiseksi on oltava sopivat prosessit ja toimintatavat, joilla laitteista jotka rakentavalle joukolle on suunniteltu käyttöön, voidaan rakentaa palveluita tuottava verkko.

Rakentamisen suunnittelu alkaa paljon ennen varsinaista käyttötarvetta rauhan aikana tapahtuvana tutkimuksena, kehittämisenä, kokeiluna, kouluttamisena ja harjoitteluna. Tutkimus ja kehittäminen, sekä niihin liittyvä kokeilu, tapahtuvat hankkeina joiden tietoon aselajit tuovat palvelutar-

peensa. Hankkeet tuottavat tekniset ratkaisut, joilla palvelutarpeisiin voidaan vastata. Kouluttaminen ja harjoittelu valmistavat rakentamisorganisaatioon suunniteltuja henkilöitä rakentamaan taktisia verkkoja poikkeusoloissa.

Kun verkkoinfrastruktuuri on saatu muodostettua, joukko tuottaa sen avulla itselleen palveluita. Tuotettavat palvelut, joita ovat kohdassa 5.2, ”Palvelut” mainitut puhe-, sanoma- ja tietojärjestelmäpalvelut, voidaan nähdä joukon sisäisenä palvelutuotantona. Koska maapuolustuksen taktisia verkkoja voidaan liittää yhteen ja ylemmän tason verkkoihin, voidaan palveluita tuottaa myös ulkoisesti. Niissä tapauksissa, joissa palveluita tuotetaan ulkoisesti, verkon toiminnasta vastaava joukko nähdään niiden näkökulmasta asiakkaana. Verkkoja yhdistetään tarpeen mukaan. Tarve muodostuu käynnissä olevan operaation luonteesta ja siihen liittyvistä joukoista. Verkkokokonaisuuden (ja sillä tuotettavien palveluiden) suunnittelu muodostuu hierarkkisesti siten, että ylempi taso suunnittelee kokonaisuuden toiminnan ja alemmat tasot sovittavat oman toimintansa siihen kokonaisuuteen. Määräävänä tekijänä verkkojen suunnittelussa voi olla esimerkiksi tarve saada tilannekuva taisteluosaston johtamispaikalle tai välittää tulikomento tulenjohtajalta tuliyksikköön.

Maapuolustuksen taktiset verkot olivat aiemmin liikuteltavia ja jatkossa niiden on tarkoitus olla liikkuvia (katso kappale 5.1, ”Tiedonsiirtojärjestelmät”). Liikuteltavat verkot ovat sellaisia, jotka voidaan rakentaa kohtuullisessa ajassa haluttuun maantieteelliseen sijaintiin. Ne pystyvät välittämään tietoliikennettä ollessaan liikkumattomana. Liikkuvien verkkojen on tarkoitus välittää tietoliikennettä myös liikkeestä. Tällainen verkon ominaisuus on huomioitava kohdan 4.3.3, ”Palvelupyyntöprosessi”, palvelupyyntöprosessissa, jotta verkon muutokset saadaan kirjattua tarpeellisilta osin standardimuutoksina. Esimerkkinä voidaan mainita, että jokainen komentopaikan siirto on muutos joka pitää voida käsitellä standardimuutoksena. Muutokset otetaan vastaan johtamisjärjestelmän komentopaikalla (johtamisjärjestelmän komentopaikan tehtävistä lisää myöhemmin).

Verkon suunniteltu liikkuvuus aiheuttaa jo lähtökohtaisesti epävarmuustekijöitä verkon toiminnalle. Sen lisäksi epävarmuustekijänä on myös vastustajan pyrkimys vaikuttaa verkon palvelutuotantoon, sekä kineettisesti, että elektromagneettisesti. Edellä mainitut epävarmuustekijät voivat johtaa siihen, että joukon taktinen verkko ei suunnitelmista huolimatta pysty liittymään ylempään verkkoon. Tällöin myöskään palvelut, jotka mahdollisesti tuotetaan joukon verkkokokonaisuuden ulkopuolella, eivät ole käytettävissä. Tällaisia voivat olla kappaleessa 4, ”ITIL -IT-palvelutuotannon viitekehys”, kerrottujen herätteiden, tapahtumien (häiriöiden), ongelmien, palvelupyyntöjen ja pääsynhallinnan prosesseihin liittyvien järjestelmien tuottamat palvelut, datansiirtopalvelut ja varsinaiset maapuolustuksen taktisten verkkojen palvelut. Eri prosessien toteuttamiseksi tarvittavien palveluiden (esim. tunnettujen virheiden tietokanta) on oltava käytettävissä mahdollisimman monissa tilanteissa.

Maapuolustuksen taktisten verkkojen valvonnalla ja hallinnalla tarkoitetaan maapuolustuksen organisaatioiden tekemää työtä, jonka tarkoituksena

on taata palveluiden käytettävyys. Tämä on kappaleessa 4.4, ”Valvonta ja hallinta”, tarkoitettua valvontaa ja hallintaa. Sotilasorganisaation toiminta pyrkii hierarkkisuuteen, jossa seuraavalla tasolla on edellistä tasoa enemmän alaisia ja vastuullaan olevia verkkoja. Tämä on havaittavissa ainakin kappaleessa 5.2, ”Palvelut”, kuvatusta vastuiden jakautumisesta. Maapuolustuksen taktisten verkkojen valvontaa ja hallintaa tekevät hallintajoukkueet ja -ryhmät. Työ sisältää verkkojen teknistä valvontaa, palvelupyyntöjen (eli sotilaskielessä ilmoitusten) vastaanottamista ja niiden mukaan toiminnan suuntaamista, sekä yhteydenpitoa toimintaa johtavaan organisaation osaan eli johtamisjärjestelmän komentopaikkaan. Näiden lisäksi valvontaan voidaan laskea kohdassa 5.4, ”Sensorit”, mainituista sensoreista palveluita käyttävät joukot.

Johtamisjärjestelmäpäällikkö johtaa joukon johtamisjärjestelmän suunnittelua, rakentamista ja käyttöä. Johtamisjärjestelmän komentopaikka johtaa verkkojen suunnittelua ja rakentamista johtamisjärjestelmäpäällikön tahtotilan mukaisesti. Johtamisjärjestelmän komentopaikka muodostaa valvomon, joka voidaan nähdä IT-käyttöpalveluna (katso 4.2, ”Palvelutuotannon periaatteet”). Valvomosta tehdään verkon valvontaan ja hallintaan liittyvää herätteiden hallintaa ja tapahtuman (häiriön) hallintaa (katso 4.3.1, ”Herätteiden hallinta” ja 4.3.2, ”Tapahtumanhallinta”). Valvomot toimivat hajautetusti, minkä tarkoituksena on varmentaa niiden toimintakyky useimmissa tilanteissa. Palvelupyyntöprosessin toteuttaminen kuuluu johtamisjärjestelmän komentopaikalle. Tästä huolimatta, se ei varsinaisesti perusta palvelupistettä joka palvelee loppukäyttäjää palveluiden käyttämisessä. Oletusarvona on, että joukot osaavat käyttää palveluita sillä tiedolla mitä heille on koulutettu ennen tehtävän aloittamista.

Verkon rakentamisen ja verkkorakenteen muutokset, hallintajoukkueen suunnitelman mukaisesti, tekevät viestiasemajoukkueet. Viestiasemajoukkueiden voidaan katsoa olevan osa teknistä hallintaa (katso 4.2 ”Palvelutuotannon periaatteet”). Viestiasemajoukkueiden tehtävänä on rakentamisen ja muutoksien lisäksi viestiasemien valvonta ja ylläpito.

Aikaisemmin on jo mainittu, että johtamisjärjestelmän komentopaikan tehtäviin kuuluu palvelupyyntöprosessin toteuttaminen. Valvomoiden tehtäviin kuuluvat herätteiden hallinta ja tapahtumanhallinta. Ongelmanhallintaa ei varsinaisesti tehdä tehtävässä olevan joukon toimesta. Maapuolustuksen taktinen verkko muodostetaan tarpeen ja tilanteen mukaan. Tarve ja tilanne riippuvat käytävästä taistelulajista (hyökkäys, puolustus, viivytys, hajautettu toiminta) ja vastustajan toiminnasta. Lisäksi, kuten aiemmin mainittiin, verkkoon pyritään vaikuttamaan vastustajan toimenpitein. Edellä luetellut syyt aiheuttavat sen, että verkko voi olla kaikkina ajanhetkinä erilainen ja ongelmien juurisyiden (kappaleet 4.2, ”Palvelutuotannon periaatteet” ja 4.3.4, ”Ongelmanhallinta”) löytäminen on yleensä mahdotonta. Ongelmanhallintaa voidaan toteuttaa valmistautumisaikana, jos ongelmia havaitaan koulutus- ja harjoittelutehtävissä. Tuolloin ne kuitenkin siirretään ratkaistavaksi kehitysorganisaatioille.

Maapuolustuksen taktisen verkon pääsynhallinnan toteuttamisessa on huomioitava, että verkosta ei voida taata yhteyttä ylempään verkkoon.

Tämä sulkee pois yleisimmät ja yleensä keskitetyt pääsynhallinnan järjestelmät. Lisäksi, koska verkot on suunniteltu käytettäväksi poikkeusoloissa, ei pääsynhallintaa välttämättä ole mielekästä laatia käyttäen henkilökohtaiseen tunnistamiseen perustuvia järjestelmiä (esimerkiksi biometriset tunnisteet kappaleessa 4.3.5, ”Pääsynhallinta”).

8.2.3. Valvonnan ja hallinnan teknologioista

Haastateltavat korostivat valvonnan ja hallinnan merkitystä siirryttäessä IP-verkkojen käyttämiseen. Erityisen merkitykselliseksi nähtiin etäältä tapahtuva valvonta ja hallinta, standardoitujen protokollien käyttäminen ja hajautetun valvontahierarkian muodostaminen.

Etäältä tapahtuva valvonta ja hallinta korostuvat erityisesti siksi, että laitteiden määrä tulee aikaisemmasta kasvamaan. Siinä tapauksessa useimmille laitteille ei ole mahdollista asettaa paikallista henkilöstöä. Laitteiden luokse ei myöskään välttämättä pääse vapaasti taisteluiden aikana. Pääsyä hankaloittavat vastustajan toiminta ja omien joukkojen tekemät sulutteet ja murrosteet. Standardoitujen protokollien käyttäminen on merkityksellistä, koska maapuolustuksen taktisessa verkossa käytetään yleisesti saatavilla olevia, kaupalliseen käyttöön tarkoitettuja laitteita. Yleisesti saatavilla olevien laitteiden käyttö tulee yleistymään niiden hinnan laskiessa ja sotilaskäyttöön tehtyjen laitteiden hinnan noustessa. Tämän lisäksi sotilaskäyttöön kehitettävien laitteiden toiminta perustuu entistä enemmän yleisesti käytössä oleviin standardeihin.

Valvontahierarkia on rakennettava siten, että järjestelmät toimivat myös verkon pirstaloituessa yksittäisiksi viestiverkoiksi. Tämä asettaa valvonnan ja hallinnan järjestelmille vaatimuksen niiden hajauttamisesta (esimerkkejä järjestelmistä kappaleessa 6.2, ”Valvonta- ja hallintasovellukset”). Verkon rakentajalla on oltava tarvittavat verkonhallintatyökalut, joilla verkko on hallittavissa useimmissa tilanteissa. Voi myös olla, että valvontaa ja hallintaa tekee verkon rakentajan lisäksi toinen taho. Suunnittelussa voidaan käyttää kappaleen 4.4, ”Valvonta ja hallinta” jakoa sisäiseen ja ulkoiseen valvontaan ja hallintaan.

Verkon valvonnan ja hallinnan lisäksi on tehtävä palveluiden valvontaa ja hallintaa. Palveluiden valvonnalla ja hallinnalla pyritään parantamaan palveluiden käyttöastetta käyttäjällä. Palvelun käyttö voi olla esimerkiksi tulikomentojen lähettämistä tulenjohtajalta tuliyksikölle. Käyttöastetta voidaan arvioida esimerkiksi sillä, kuinka usein tulikomennot välittyvät tulenjohtajalta tuliyksikölle. Maapuolustuksen taktinen verkko pyritään rakentamaan mahdollisimman hajautetusti. Hajautetulla toiminnalla pyritään minimoimaan vastustajan tulivaikutusta. Hajauttaminen voi aiheuttaa tilanteen, jossa yhteysetäisyydet kasvavat niin suuriksi, että ne vaikuttavat verkon toimivuuteen heikentävästi. Valvontaan ja hallintaan liittyvä raportointi voi oikein toteutettuna tuottaa palveluita (tai mahdollistavia palveluita eli verkkoja) rakentavalle ja ylläpitävälle joukolle tietoa, joka johtaa esimerkiksi yhteysvälien lyhentämiseen.

Aiemmin mainittu etäältä tapahtuva valvonta ja hallinta asettavat myös korotetun vaatimuksen tietoturvalle. Käytettävät protokollat (6.1, ”Valvontaprotokollat” ja 6.2, ”Hallintaprotokollat”) on valittava siten, että ne mahdollistavat liikenteen salaamisen. Salatun liikenteen tulkitseminen kaapatusta tiedonsiirrosta on hankalampaa kuin salaamattoman.

Kaikelle etäältä tapahtuvan valvonnan ja hallinnan suunnittelulle tuottaa lisähaasteen maapuolustuksen taktisen verkon käyttötapa, jossa verkon asemat saattavat olla pois verkosta oman toiminnan (siirtymiset, radiohiljaisuus, liittymisjärjestys jossa liittävä asema liittyy viimeisenä tai jopa asemalle sähköä tuottavan aggregaatin tankkaaminen) tai vastustajan toiminnan (asemien tuhoutuminen, elektroninen häirintä) vuoksi. Näitä tilanteita varten täytyy suunnitella teknisen valvonnan lisäksi toimintatapoja, joihin sisältyvät tietyt ilmoitukset. Tällainen voi olla esimerkiksi ilmoitus aseman suunnitellusta siirtymisestä.

9 POHDINTA

Tutkija ei löytänyt aikaisempia tutkimuksia maapuolustuksen taktisten verkkojen valvonnasta ja hallinnasta. Hakusanoilla ”Maapuolustuksen taktisten verkkojen valvonta ja hallinta” Kansallisarkiston ylläpitämä Doria (Doria, 2016) palautti kaksi osumaa. Tutustuttaessa näihin osumiin, toinen niistä oli tässä tutkimuksessa lähteenä käytetty Kybertaistelu 2020 ja toinen Verkostoavusteinen puolustus 2030, joka ei liittynyt tutkimuksen aihepiiriin. ITIL:iä on käytetty viitekehyksenä runsaasti erilaisten systeemien tutkimisessa. Haettaessa Kansallisarkiston Doria julkaisuarkistossa termiä ”ITIL”, palautti järjestelmä 174 osumaa. Google-haku sanoilla ”ITIL thesis” palautti 357 000 tulosta.

9.1. Tulosten yhteenveto

Tutkimuksen tutkimuskysymys oli:

Voiko maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttaa ITIL:n käytäntöjen mukaisesti?

Tutkimuskysymykseen pyrittiin vastaamaan selvittämällä seuraavat alakysymykset:

Millainen on ITIL:n valvonnan ja hallinnan viitekehys?
Mitä ovat maapuolustuksen taktiset verkot ja mikä niille on ominaista?
Mitä teknologioita valvonnan ja hallinnan toteuttamiseksi on käytettävissä?

Lyhyt vastaus tutkimuskysymykseen on kyllä. Sen lisäksi, että se on mahdollista, maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttaminen ITIL:n parhaiden käytäntöjen mukaisesti voi tarkoittaa verkkojen parempaa käyttövarmuutta ja alhaisempia hankinta- ja käyttökustannuksia. Laajemmin tutkimuskysymykseen on vastattu primäärin ja se-

kundäärisen aineiston dialogilla, jonka johtopäätökset on kuvattu seuraavissa kolmessa kappaleessa.

9.1.1. ITIL:n viitekehys

ITIL:n viitekehys on kattava teoria, jonka avulla on mahdollista käsitteistää IT-palvelutuotannon ilmiöitä. ITIL:n viitekehys kattaa koko IT-palveluiden elinkaaren ja mahdollistaa sen parhaiden käytäntöjen mukaisesti suunniteltujen ja ylläpidettyjen palveluiden tuottamisen kustannustehokkaasti ja luotettavasti. Palveluiden elinkaari koostuu viidestä vaiheesta: palvelustrategia, palvelusuunnittelu, palvelutransitio, palvelutuotanto ja jatkuva palvelun parantaminen. Suunniteltaessa palveluita ITIL:ssä kuvatut osa-alueet huomioiden, voidaan minimoida riskejä joita palveluiden tuottamiseen sisältyy. ITIL:n mukaisia palvelutuotannon prosesseja ovat herätteiden hallinta, tapahtuman hallinta, palvelupyyntöprosessi, ongelman hallinta ja pääsynhallinta. Valvonta ja hallinta ovat palvelutuotannon aktiviteetteja.

Valvonnalla pyritään havaitsemaan IT-palvelutuotannon poikkeamia ja reagoimaan niihin muodostamalla hälytyksiä. Hälytyksiä voivat aiheuttaa esimerkiksi laitteiden epänormaali toiminta, suorituskyvyn lasku tai käyttöasteen epänormaali kasvu. Laitteiden normaalitilan tarkkailun lisäksi valvonnalla pitää havaita myös niihin tehtyjen epätoivottujen muutosten tekeminen tai niiden luvaton käyttö. Valvontaan liittyvät olennaisesti myös kerätystä tiedosta laadittavat raportit. Raportit on tarkoitettu palvelutuotannosta päättävien tahojen työkaluksi. Raportoinnilla tulee olla tarkoitus, koska raportointi joka ei johda mihinkään jatkotoimenpiteisiin on turhaa.

Hallinta nähdään toimenpiteinä jotka vaikuttavat laitteen, järjestelmän tai palvelun toimintaan. Sallitut hallintatoimenpiteet on määritetty, ne ovat tilanteeseen sopivia ja niiden tekeminen on hyväksytty. Hallintatoimenpiteitä määritettäessä, on tunnistettava mitkä toimenpiteet ovat normaaleja ja mitkä ovat epänormaaleja. Hallinta ei tarkoita sitä, että se on aina ihmisen tekemää. Se voidaan myös automatisoida sellaisissa tapauksissa, joissa on pieni tai olematon riski, että automaattinen hallintatoimenpide aiheuttaa häiriöitä tai ongelmia. Tällaisia voivat olla esimerkiksi tietoliikenteen kuormantasaustilanteet.

9.1.2. Maapuolustuksen taktiset verkot ja niiden ominaispiirteet

Maapuolustuksen taktiset verkot voidaan nähdä IT-palvelutuotantona siinä missä mikä tahansa tietoverkko ja palvelut. Niiden käyttöympäristö poikkeaa merkittävästi normaalista IT-palvelutuotannosta. Poikkeavuudet liittyvät usein verkkojen tavanomaista suurempaan epävarmuuteen käytetystä teknologiasta huolimatta. Epävarmuutta aiheuttavat verkkojen tilapäinen luonne, liikkuvuus ja olosuhteet, joissa niiden toimintaa pyritään vastustajan toimesta suunnitelmallisesti haittaamaan elektromagneettisella häirinnällä tai kineettisellä vaikuttamisella.

Koska maapuolustuksen taktiset verkot ovat perimmäiseltä olemukseltaan tietoliikenneverkkoja, on niiden toteuttamiseksi mahdollista käyttää standardoituja teknologioita. Standardoitujen teknologioiden valinnalla voidaan saavuttaa valmistajakohtaisiin ratkaisuihin verrattuna säästöjä, koska niillä toteutettujen systeemien hankinnassa voidaan kilpailuttaa useampia toimittajia. Säästöt eivät aina tarkoita alhaisempaa hankintahintaa tai käyttökustannusta. Säästöt voivat maapuolustuksen taktisten verkkojen tapauksessa tarkoittaa alhaisempaa laitteen yksikköhintaa, joka mahdollistaa varmennetumman, toimintavarmemman ja käyttötarkoitukseen paremmin sopivan verkon rakentamisen.

Verkkojen ominaispiirre on pyrkimys hajautettuun toimintaan ja toiminnan jatkaminen myös niissä tilanteissa, joissa verkot ovat pirstoutuneet pienemmiksi kokonaisuuksiksi. Tämän vuoksi, kun verkkoja ja niiden rakentamiseksi tarkoitettuja laitteita ja järjestelmiä suunnitellaan, joudutaan tekemään redundantteja ratkaisuja. Näin siitä huolimatta, että niiden tekeminen nostaa palvelutuotannon kokonaiskustannusta.

Tarkasteltaessa maapuolustuksen taktisia verkkoja palvelunhallinnan näkökulmasta, havaitaan että sisäiset ja ulkoiset asiakkuudet voivat vaihdella. Myös palvelutuottaja ja asiakas -roolit vaihtelevat sen mukaan, miten verkkoja muodostetaan. Toisaalta se seikka, että verkon rakentaja vastaa sen valvonnasta, hallinnasta ja ylläpidosta, ei muutu.

Maapuolustuksen taktisten verkkojen valvontaan on käytettävissä standardoitujen protokollien ja verkon valvontaan tarkoitettujen laitteiden lisäksi myös muita sensoreita. Muita sensoreita ovat järjestelmiä käyttävät organisaatiot ja niiden osat. Jokainen taistelukentällä oleva ihminen on sensori, joka edesauttaa taktisen verkon palvelutuotantoa havainnoimalla vähintään fyysistä käyttöympäristöä.

9.1.3. Valvontaan ja hallintaan käytettävät teknologiat

Maapuolustuksen taktisten verkkojen valvontaan ja hallintaan käytettävien teknologioiden valinnassa on tunnettava em. verkkojen ominaisuudet ja rajoitukset. IT-verkkojen valvontaan on käytettävissä valvontaprotokollia, kuten SNMP ja ICMP. Suunniteltaessa maapuolustuksen taktisen verkon valvontaan ja hallintaan käytettäviä teknologioita, on huomioitava valvontahenkilöstön määrä suhteessa valvottavien laitteiden määrään, rajoitettu mahdollisuus päästä laitteen luokse eri tilanteissa ja laitteiden tukemat protokollat.

Valvontaprotokollilla saadaan erilaista tietoa verkon laitteiden tilasta ja toiminnasta. ICMP kertoo yleisesti sen, onko laite saavutettavissa verkon välityksellä. SNMP taasen mahdollistaa tarkemman tiedon saamisen laitteen toimintatiloista. Tarkempi tieto voi olla esimerkiksi tietoliikenneyhteyksien käyttöaste tai kirjautuminen laitteeseen hallintayhteydellä. SNMP:llä tehtävä valvonta voi olla aktiivista tai passiivista. Aktiivisessa valvonnassa verkon hallinta-asema (NMS) tekee kyselyitä verkkolaitteille. Passiivisessa valvonnassa, laitteissa olevat SNMP-agentit luovat TRAP-sanomia, jotka välitetään hallinta-asemalle. SNMP:stä on useita versioita,

joista SNMPv3 mahdollistaa valvontatiedon salaamisen ja valvontaa tekevän tahon luotettavan tunnistamisen. Versiota valittaessa on otettava huomioon valvottavan laitteen sijainti verkossa ja tietoliikenteen salakuuntelun riski.

Hallintaan on käytettävissä useita protokollia. Tietoturvallisuuden näkökulmasta suositeltavimpia ovat sellaiset, joiden ulottuvuus on rajoitettu (kuten konsoli-yhteys) tai liikennöinti on salattu (SSH ja sen versiot, SFTP ja SCP). Rajoitettu ulottuvuus tarkoittaa sitä, että hallintaa tehdään paikallisesti laitteen läheltä. Läheltä tapahtuvalla hallintayhteydellä salakuuntelun riski on pieni. Riskiarvio perustuu siihen, että hallintaa tekevä taho on havainnoinut fyysisen hallintaympäristön (esimerkiksi tila, kaapeli, hallintapääte) ja poistanut mahdolliset salakuuntelulaitteet. Etähallinnassa ei voida yksiselitteisesti sulkea pois mahdollisuutta, että jollain yhteysvälillä tietoliikennettä voidaan salakuunnella. Salakuuntelulla kaapatun liikenteen tulkitsemista hankaloittaa hallintaliikenteen kryptaaminen.

Valvontaan ja hallintaan käytettävien sovellusten valinnassa on tunnistettava mitä halutaan saada aikaiseksi ja millainen on systeemi jossa niitä käytetään. Systeemi asettaa vaatimuksia verkon hallinta-asemien ominaisuuksille ja hallinta-asemien hajauttamiselle tai monentamiselle. Hallinta-aseman ohjelmistot voivat olla hyvin erilaisia. Ne vaihtelevat NetInspectorin tapaisista, pelkästään valvontaan käytettävistä sovelluksista, kokonaisvaltaiseen IT-palveluiden valvontaan ja hallintaan tarkoitettuihin sovelluksiin kuten HP IMC.

9.2. Luotettavuuden arviointi

Tutkimuksen luotettavuutta arvioitaessa kiinnitettiin huomiota sekundäärisen aineiston julkaisuajankohtaan ja laatuun. Julkaisuajankohdan perusteella hylättiin yleensä yli 10 vuotta vanhat lähteet, pois lukien ne jotka kuvaavat mennyttä aikaa tai ovat standardeja. Laatua arvioitiin sen mukaan, minkä tasoista tutkimustietoa lähde on. Lähteeksi hyväksyttiin vähintään Pro Gradu tai Master’s -tasoisia tutkimuksia. Historiallinen dokumentaatio ja standardit hyväksyttiin sellaisenaan.

Historiaa kuvaava Viestitoiminta Suomessa on julkaistu 1980-luvulla. Sen julkaisuajankohta ei vaikuta luotettavuuden arviointiin, koska se kuvaa selkeästi mennyttä aikaa. Se ei sinällään ole tieteellinen tutkimus, vaikka siinä onkin kattavat lähdeviittaukset ja sen kirjoittamiseen ovat osallistuneet henkilöt jotka ovat kokeneet kirjassa kuvattuja tapahtumia henkilökohtaisesti.

ITIL-viitekehystä koskevana dokumentaationa käytettiin OGC:n julkaisemaa alkuperäistä englanninkielistä kirjaa. Viitekehyksestä valittiin käytettäväksi se kirja, joka eniten kuvaa IT-järjestelmien valvontaa ja hallintaa. Tällä perusteella päädyttiin käyttämään kirjaa Service Operations, jossa on kuvattu palvelutuotanto. Tämän dokumentaation luotettavuutta ei asetettu kyseenalaiseksi, koska ITIL-viitekehys on OGC:n kehittämä ja ylläpitämä viitekehys.

IETF:n standardit ja RFC-dokumentit ovat julkaistu pääsääntöisesti yli 10 vuotta ennen tutkimuksen tekemistä, mutta standardit muuttuvat hitaasti ja tähän tutkimukseen valitut dokumentit tarkastettiin niiden voimassaolon perusteella. IETF:llä on tähän tarkoitukseen oma merkintätapansa. Merkintätavasta käy ilmi onko standardista tai RFC-dokumentista olemassa päivitetty versio. Standardeista ei käy ilmi niiden tieteellisyyttä, mutta niitä käytetään yleisesti järjestelmien kehittämisessä joten niiden laadun ei nähty aiheuttavan ongelmia tutkimuksen validiteetille.

Maanpuolustuskorkeakoulun Pro Gradu, YE-diplomityö ja julkaisusarjan dokumenteista valikoitiin käytettäväksi enintään 10 vuotta ennen tämän tutkimuksen tekemistä laadittuja viestijärjestelmiin, johtamisjärjestelmiin tai maapuolustuksen taktisiin järjestelmiin liittyviä tutkimuksia ja julkaisuja. Pro Gradu ja YE-diplomityö ovat tieteellisen toimintatavan mukaisesti tarkastettuja ja hyväksyttyjä. Julkaisusarjan dokumentaation validiteetissa luotettiin Maanpuolustuskorkeakoulun reliabiliteettiin heidän julkaisusarjojensa paikkansapitävyyden osalta. Tutkimuksen julkisuusvaatimuksen vuoksi ei kyetty täysin varmistamaan, että lähteenä käytettyjen tutkimusten tulokset kuvaavat kaikkia maapuolustuksen taktisten verkkojen ilmiöitä. Tätä epävarmuutta pyrittiin poistamaan tutkijan omalla vuosikymmenen kokemuksella tutkittavasta kohteesta.

Primääriaineiston validiteetti pyrittiin varmistamaan valikoimalla tutkimuksen kohteeksi henkilöitä, joilla on pitkä kokemus työskentelemisestä maapuolustuksen taktisten verkkojen parissa ja tuntemusta ITIL:stä. Haastateltavien löytäminen osoittautui haasteelliseksi, koska varsinkin kokeneemmilta asiantuntijoilta saattoi puuttua ITIL:n tuntemus tai kokemus verkoista oli niin kapea-alaista, ettei siitä ollut tutkimuksen kannalta merkittävää hyötyä. Haastateltavaksi löydettiin kaksi henkilöä, mikä aiheuttaa haastatteluiden saturaation puutteen vuoksi validiteetille haasteen. Tätä epävarmuutta haastatteluilla kerätyn tiedon luotettavuudesta, mikä kvalitatiivisessa tutkimuksessa on varsin mahdollista, päätettiin tutkimuksessa sietää. Epävarmuutta pyrittiin poistamaan sekundäärisen tiedon validiteetin varmistamisella, vertailemalla primääriaineistoa ja sekundääristä aineistoa kattavasti ja hyväksyttämällä haastatteluista tehdyt johtopäätökset haastateltavilla.

9.3. Tutkimuksen onnistumisesta

Tutkimuksen onnistumisesta oli tutkijalla ennakkokäsityksenä, että tietoa maapuolustuksen taktisista verkoista ei ole saatavilla julkisista lähteistä. Tämä ennakkokäsitys osoittautui vääräksi jo hyvin varhaisessa vaiheessa, koska Maanpuolustuskorkeakoulu tutkimuksineen ja julkaisusarjoineen on hyvin runsas tietolähde. Tieto, jota niistä on saatavissa, on tieteellisesti tuotettua ja pääosin myös vertaisarvioitua. Ilmiöstä maapuolustuksen taktisten verkkojen valvonta ja hallinta, oli siis saatavilla riittävästi sekundääristä aineistoa. ITIL osoittautui erinomaiseksi lähteeksi ilmiön käsitteistämisessä universaalisti ymmärrettävään muotoon. Tärkeimmäksi seikaksi osoittautuikin tutkimuksen kannalta sopiva rajaus, jossa valittiin ITIL:n vaiheista palvelutuotanto.

Kuten aiemmin mainittiin, on tietoa maapuolustuksen taktisista verkoista saatavilla julkisista lähteistä riittävästi ilmiön ymmärtämiseksi ja käsitteistämiseksi. Kaikki tutkimuksessa käytetty sekundäärinen tieto on kerätty julkisesta lähdemateriaalista. Siitä huolimatta, voi tietoa yhdistelemällä muodostua kokonaisuus, jonka suojaustaso nousee suojaustasolle IV, suojaustasolle III tai korkeammaksi (Finlex, 2010). Tällöin puhutaan tiedon keräytymisen aiheuttamasta suojaustason nousemisesta. Julkisen tiedon keräytymistäkin suuremman riskin työn julkisuudelle aiheuttaa haastattelemalla kerättävä primäärinen tutkimusaineisto. Sitä ei ole etukäteen luokiteltu, vaan tiedon suojaustason määrittäminen jää tutkijan päätettäväksi. Riskiin suojaustason nousemisesta julkista tasoa korkeammaksi vastattiin pyytämällä työnantajan asettamaa tutkimuksen ohjaajaa tarkastamaan tutkimusraportti. Tarkastuksen lausunto on liitteenä 5. Samassa lausunnossa on myös arvio työn onnistumisesta ja sen merkityksestä maapuolustuksen taktisten verkkojen valvonnan ja hallinnan kehittämisessä.

Tutkimus alkaa tarkastelemalla viestitoiminnan historiaa noin vuodesta 1918. Valinta on sopiva, kun nähdään että tutkimuksessa käsiteltyjen maapuolustuksen taktisten verkkojen viimeisin evoluutio on M18, vuoden 2018 mukaan. Näin voidaan todeta, että ensi vuonna 100 vuotta täyttävän Suomen viestitoimintaa on käsitelty sadan vuoden ajalta.

Primääriaineiston kerääminen kvalitatiivisella haastattelututkimuksella osoittautui hyvin aikaisessa vaiheessa oikeaksi ratkaisuksi, koska riittävällä tiedolla ja kokemuksella varustetuista haastattelun kohteista ei ollut runsauden pulaa.

9.4. Lopuksi

Tutkimuksen tekeminen on toiminut tutkijalle ajatusmaailmaa selkeyttävänä prosessina, niin tutkimuksen tekemisen, kuin maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttamisen osalta. Tutkija työskentelee tässä tutkimuksessa käsiteltyjen asioiden parissa ja pystyy suoraan hyödyntämään sen tuloksia maapuolustuksen taktisten verkkojen valvonnassa ja hallinnassa.

Koska tutkimus toteutettiin julkisena, siinä ei kuvattu yksityiskohtaisesti maapuolustuksen taktisten verkkojen ilmentymiä. Tutkimuksessa pyrittiin käsitteistämään ja yleistämään ilmiötä. Tästä lähtökohdasta voidaan sanoa, että tutkimus on saavuttanut sille asetetun tavoitteen. Ilmiön tutkiminen jatkuu tutkijan toimesta virkatyönä, jossa havaitut käsitteet viedään yksityiskohtaisesti maapuolustuksen taktisiin verkkoihin. Tätä tutkimusta on mahdollista julkisella tutkimuksella täydentää tutkimalla ITIL:n muutkin vaiheet kuin palvelutuotanto maapuolustuksen taktisten verkkojen kontekstissa.

Lopuksi on tarpeellista kiittää työnantajan nimittämää ohjaajaa työn tekemiseen annetusta tuesta työn julkisuuden varmistamisessa, haastateltuja henkilöitä pitkän kokemuksensa luovuttamisesta ilmiön kuvaamiseen ja lähteenä käytettyjen tutkimusten ja julkaisujen kirjoittajia ansiokkaasta

lähdemateriaalista. Ei myöskään pidä aliarvioida tutkijan läheisten tuen merkitystä työn loppuunsaattamiselle. Kiitos.

LÄHTEET

AXELOS. Pdf-tiedosto. ITIL-sanasto. https://www.exin.com/assets/exin/frameworks/108/glossaries/finnish_glossary_v1.0_201404.pdf. Viitattu 13.7.2016.

Bittium LRV-järjestelmä. Pdf-tiedosto. Bittium Tactical Wireless IP Network. http://www.bittium.com/file.php?fid=781. Viitattu 21.7.2016.

Cabinet Office. 2011. ITIL Service Operation. Iso-Britannia. ISBN 978-01-1331-3075.

Digital Ocean. Portaali. https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process. Viitattu 25.1.2016.

Doria. Portaali. http://www.doria.fi/. Viitattu 23.10.2016.

Everything explained today. Portaali. http://everything.explained.today/SSH_File_Transfer_Protocol/. Viitattu 26.1.2016.

Finlex. Portaali. http://www.finlex.fi/fi/laki/alkup/2010/20100681. Viitattu 4.11.2016.

HP IMC. Portaali. http://www8.hp.com/us/en/networking/network-management/modules.html. Viitattu 11.11.2015.

IETF. Julkaisu. STD 15: A Simple Network Management Protocol (SNMP). http://tools.ietf.org/html/std15. Viitattu 11.11.2015.

IETF. Julkaisu. RFC-782: A Virtual Terminal Management Model. https://tools.ietf.org/html/rfc782. Viitattu 24.11.2015.

IETF. Julkaisu. RFC-792: INTERNET CONTROL MESSAGE PROTOCOL. https://www.ietf.org/rfc/rfc792.txt. Viitattu 18.11.2015.

IETF. Julkaisu. RFC-854: TELNET PROTOCOL SPECIFICATION. https://www.ietf.org/rfc/rfc854.txt. Viitattu 24.11.2015.

IETF. Julkaisu. RFC-959: FILE TRANSFER PROTOCOL (FTP). https://www.ietf.org/rfc/rfc959. Viitattu 25.1.2016.

IETF. Julkaisu. RFC-1157: A Simple Network Management Protocol (SNMP). https://www.ietf.org/rfc/rfc1157.txt. Viitattu 2.7.2015.

IETF. Julkaisu. RFC-1350: THE TFTP PROTOCOL (REVISION 2). https://tools.ietf.org/html/rfc1350. Viitattu 25.1.2016.

IETF. Julkaisu. RFC-1901: Introduction to Community-based SNMPv2. https://tools.ietf.org/html/rfc1901. Viitattu 11.11.2015.

IETF. Julkaisu. RFC-2570: Introduction to Version 3 of the Internet-standard Network Management Framework. https://www.ietf.org/rfc/rfc2570.txt. Viitattu 11.11.2015.

IETF. Julkaisu. RFC-2574: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). https://www.ietf.org/rfc/rfc2574.txt. Viitattu 11.11.2015.

IETF. Julkaisu. RFC-2941: Telnet Authentication Option. https://tools.ietf.org/html/rfc2941. Viitattu 25.11.2015.

IETF. Julkaisu. RFC-2946: Telnet Data Encryption Option. https://tools.ietf.org/html/rfc2946. Viitattu 25.11.2015.

IETF. Julkaisu. RFC-4251: The Secure Shell (SSH) Protocol Architecture. https://tools.ietf.org/html/rfc4251. Viitattu 25.1.2016.

IETF. Julkaisu. SFTP-draft: SSH File Transfer Protocol draft-ietf-secsh-filexfer-13.txt. https://tools.ietf.org/html/draft-ietf-secsh-filexfer-13. Viitattu 25.1.2016.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Jyväskylä. Jyväskylän ammattikorkeakoulun julkaisuja.

Karsikas, J. 2007. Pdf-tiedosto. Maavoimien verkostokeskeisen tiedonsiirtojärjestelmän arkkitehtuuri ja sen toteuttaminen. Diplomityö. Helsinki. Maanpuolustuskorkeakoulu.
https://www.doria.fi/bitstream/handle/10024/74312/Y2471_Karsikas_Jarkko_YEK53.pdf?sequence=1

Kärsämä, M. 2011. Pdf-tiedosto. Kaupallisten tuotteiden käyttö taistelukentän valvontajärjestelmä. Esiupseerikurssin tutkielma. Helsinki. Maanpuolustuskorkeakoulu.
http://urn.fi/URN:NBN:fi-fe201201271255

Laitila, T. 2009. Pdf-tiedosto. Jalkaväkiprikaatin kenttäviestijärjestelmän tekniset ratkaisut 2010-luvulla. Kandidaatin tutkielma. Helsinki. Maanpuolustuskorkeakoulu.
http://urn.fi/URN:NBN:fi-fe201505258989

MG-Soft. Portaali. MG-Soft Net Inspector.
http://www.mg-soft.com/netinsp.html. Viitattu 11.11.2015.

Mil.fi. Portaali. Puolustusvoimien verkkosivusto. http://maavoimat.fi/kainuun-prikaati/varusmiehena-meilla. Viitattu 21.7.2016.

Sirén, J. 2015. Pdf-tiedosto. Perusyhtymän viestijoukkojen suorituskyvyn kehittyminen jatkosodasta alueelliseen puolustukseen. Pro Gradu. Helsinki. Maanpuolustuskorkeakoulu.
http://urn.fi/URN:NBN:fi-fe2015100214580

Pikkarainen, A. 2013. Pdf-tiedosto. Hajautettuun ryhmitykseen soveltuva tilannekuvajärjestelmä: näkökulmana viestihuoltokomppania. Pro Gradu. Helsinki. Maanpuolustuskorkeakoulu.
http://urn.fi/URN:NBN:fi-fe201309115717

Vahti-ohje. Valtiovarainministeriö. Portaali. https://www.vahtiohje.fi/web/guest/tietoliikennemallit. Viitattu 2.7.2015.

Van Haren Publishing. 2009. ITILv3 taskukirja. ISBN 978-90-8753-555-1.

Virtanen, J-P & Jokinen, J. 2014. Pdf-tiedosto. Kybertaistelu 2020. Maanpuolustuskorkeakoulun julkaisusarja 2, No. 1/2014. Tampere.
http://urn.fi/URN:ISBN:978-951-25-2618-5

Wikipedia. Portaali. Secure Copy. https://en.wikipedia.org/wiki/Secure_copy. Viitattu 26.1.2016.

Haastattelut

Eiste, J. Opistoupseeri, kapteeni, Maavoimien operatiivisen järjestelmäkeskuksen varapäällikkö. Haastattelu 16.9.2016.

Särmä, J. Upseeri, majuri, Maavoimien operatiivisen järjestelmäkeskuksen päällikkö. Haastattelu 16.10.2016.

Liite 1

TUTKIMUSLUPAHAKEMUS (PUROJÄRVI)

1. TYÖN TEKIJÄ, OPPILAITOS JA TUTKINTO

Tutkimustyön tekijä: INSKAPT Uula-Petteri Purojärvi, Maavoimien Esikunta / Johtamisjärjestelmäosasto p. <PUHELINNUMERO POISTETTU>

Oppilaitos: Hämeen Ammattikorkeakoulu (HAMK)

Tutkinto: Ylempi ammattikorkeakoulututkinto (YAMK), Teknologiaosaamisen johtamisen -koulutusohjelma

2. TYÖN ALUSTAVA NIMI JA VALMISTUMISAIKATAULU

Työn nimi: Maapuolustuksen taktisten verkkojen valvonta ja hallinta

Valmistumisaikataulu: 31.12.2015 mennessä.

3. TYÖN OHJAAJAT OPPILAITOKSESSA JA MAAVE:SSA

Työn ohjaaja oppilaitoksessa: Pirjo Valokorpi (HAMK), PL 230 13100 Hämeenlinna, p. <PUHELINNUMERO POISTETTU>, <OSOITE POISTETTU>

Työn ohjaaja MAAVE:ssa: KAPT Markus Tanskanen, Maavoimien Esikunta / Henkilöstöosasto, p. <PUHELINNUMERO POISTETTU>

4. TYÖN PÄÄPIIRTEINEN SISÄLTÖ

Tässä tutkimustyössä tutkitaan maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttamista huomioiden verkkojen ominaispiirteet sekä kehitetään verkkojen käytettävyyden ylläpitoon ja palauttamiseen liittyvät prosessit. Tutkimustyön tuloksella pyritään luomaan tapa jolla maapuolustuksen taktisten verkkojen valvonta ja hallinta voidaan toteuttaa siten että se antaa todellisen kuvan verkkojen tilasta ja käytettävyydestä. Todellisen tilannekuvan avulla mahdollistetaan verkkojen käytettävyyden ylläpitoon ja palauttamiseen liittyvien prosessien toteuttaminen.

Tutkimustyön tulosta on tarkoitus käyttää maapuolustuksen taktisten verkkojen ylläpitäjien ja tuotannon johtajien päivittäisessä käytössä ja saavuttaa tilanne jossa verkkojen vikatilanteet tai vikatilanteiden aiheuttamat

häiriöt on minimoitu. Tutkimussuunnitelma on liitteenä 1.

5. HAASTATTELUT JA TIEDON KERÄÄMINEN

Haastattelut toteutetaan teemahaastatteluina henkilöille jotka valvovat ja hallitsevat maapuolustuksen taktisia järjestelmiä (tai johtavat em. toimintaa).

Haastatteluiden ja aineistotutkimuksen perusteella pyritään tunnistamaan tavat, joilla voidaan luotettavasti toteuttaa valvontaan ja hallintaan liittyvät prosessit.

Aineistotutkimuksessa tutustutaan ja tulkitaan tapaukseen sopivaksi telekommunikaatioalan standardeja, Puolustusvoimien julkisia määräyksiä (mahdollinen luokiteltu materiaali julkaistaan luottamuksellisessa liitteessä) ja alan parhaita käytäntöjä valvonnan ja hallinnan prosessien luomiseksi ja toteuttamiseksi.

Tiedon keräämisen apuna käytetään myös tutkijan omaa kokemusta tietoliikenneverkkojen valvonnasta ja hallinnasta. Tutkija on työskennellyt tietoliikennetekniikan tehtävissä kymmenen vuoden ajan.

Lopuksi kuvataan prosessit joilla organisaatio kykenee toimimaan aktiivisesti ja reaktiivisesti systeemin tuottaman tiedon perusteella. Tiedon kohteena ovat ensisijaisesti Maavoimien johtamisjärjestelmiä suunnittelevat sekä valvontaa ja hallintaa toteuttavat ja johtavat toimijat. Toissijaisena tarpeena ovat tiedeyhteisön tarpeet.

6. TIEDON KERUU PUOLUSTUSVOIMIEN ULKOPUOLELTA

Puolustusvoimien ulkopuolelta kerätään tietoa tietoliikennetekniikan standardeista, IETF:n (Internet Engineering Task Force) tietokannoista, oppilaitoksen kirjastosta tai sähköisistä tietokannoista aiemmista tutkimustöistä ja julkisista internet-lähteistä. Kerättävä tieto koskee tietoliikenneteknologiaa, tiedonsiirtotekniikkaa, IT-alan tuotannon prosesseja ja MPKK:n julkaisuista saatavia tietoja taktisista verkoista. Puolustusvoimien ulkopuolisia tahoja ei haastatella.

Tutkimustyössä käytettävä merkittävin Puolustusvoimien ulkopuolisten tahojen lähdemateriaali:

- IETF:n tietokannat
- Tietoliikennelaitteiden valmistajien ohjesivustot
- Viestisäätiön julkaisu Viestitoiminta Suomessa, 1980

- Doria - Kansallisarkiston ylläpitämä julkaisuarkisto

7. SALASSA PIDETTÄVÄN AINEISTON KÄSITTELY

Tutkimustyö (opinnäytetyö) on julkinen. Jos työ sisältää toimeksiantajan eli Puolustusvoimien kannalta salassa pidettävää tietoa, tämä esitetään erillisessä liitteessä, joka jää ainoastaan Puolustusvoimien käyttöön. Tutkimustyössä haastateltavilta henkilöiltä saatava aineisto voi osoittautua luokitelluksi. Yksityiskohtainen, Maavoimien käyttöön tuleva, valvonnan- ja hallinnan yksityiskohtainen konsepti tehdään loppuun opinnäytetyön ulkopuolisena virkatyönä. Suojaustason osalta tutkimustyö tarkastetaan Maavoimien materiaalilaitoksen esikunnassa ennen julkaisua.

Tietoliikenneinsinööri
insinöörikapteeni Uula-Petteri Purojärvi

Tämä asiakirja on sähköisesti allekirjoitettu.

LIITTEET

JAKELU MAAVE
Yrjö Sairanen, Maavoimien esikunta Johtamisjärjestelmäosasto
Jari Särmä, Maavoimien esikunta Johtamisjärjestelmäosasto

TIEDOKSI

Liite 2

ML14786 TUTKIMUSLUPAHAKEMUS (PUROJÄRVI)
PUHELU JA PVAH-VIESTIT: 30.6 JA 2.7 MAJ SÄRMÄ- INSMAJ LAHTINEN
PUHELU: 3.7 EV SAIRANEN- INSMAJ LAHTINEN

PÄÄTÖS TUTKIMUSLUPA-ASIAAN (INSKAPT PUROJÄRVI)

1 Tausta

Maavoimien esikunnan Johtamisjärjestelmäosastolla työskentelevä inskapt Uula-Petteri Purojärvi on osoittanut Maavoimine esikunnalle tutkimuslupahakemuksen. Tutkimuslupahakemus liittyy inskapt Purojärven siviiliopintoihin Hämeen ammattikorkeakoulussa. Opintojen tavoitteena on ylempi ammattikorkeakoulututkinto Teknologiaosaamisen johtamisen koulutusohjelmassa.

Inskapt Purojärven tutkimuksen (opinnäytetyö) tarkoituksena on tutkia maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttamista huomioiden verkkojen ominaispiirteet. Lisäksi tarkoituksena on kehittää verkkojen käytettävyyden ylläpitoon ja palauttamiseen liittyviä prosesseja. Työn alustava nimi on Maapuolustuksen taktisten verkkojen valvonta ja hallinta. Tutkimustyön tulosta on tarkoitus hyödyntää maapuolustuksen taktisten verkkojen ylläpitäjien ja tuotannon johtajien tehtävissä.

Tutkimuksen tiedon kerääminen on ajateltu toteuttaa haastatteluin ja aineistotutkimuksen perusteella. Työn ohjaajana MAAVE:ssa toimii Kapt Markus Tanskanen.

MAAVEJOJÄOS puoltaa Inskapt Purojärven tutkimusta. Tutkimuksen nähdään tukevan maapuolustuksen tietoliikenteen valvonnan ja hallinnan toimeenpanoa ja kehittämistä.

2 Päätös lupaehtoineen

Maavoimien esikunta myöntää inskapt Purojärvelle tutkimusluvan seuraavin ehdoin:

- Lupa on henkilökohtainen ja määräaikainen. Luvan voimassaolo päättyy 31.05.2016.
- Tutkimuksesta ei saa aiheutua kustannuksia puolustusvoimille.
- Tutkimukseen liittyvät kyselyt ja haastattelut ovat siihen osallistuville henkilöstölle vapaaehtoisia. Haastateltava voi keskeyttää haastattelun ilman perusteluita. Nämä seikat on selkeästi ilmoitettava haastateltaville ennen kyselyiden aloittamista.

- Tutkimuksessa käytettävästä aineistosta ei saa syntyä henkilötietorekisteriä.
- Tutkimuksessa kerättyä aineistoa saadaan käyttää ainoastaan hakemuksessa kuvatun tutkimuksen toteuttamiseen. Aineistonkäyttöoikeutta ei voida siirtää kolmansille osapuolille.
- Tutkimusaineiston keräämisessä, käsittelyssä, säilyttämisessä ja tuhoamisessa tulee noudattaa henkilötietolakia kokonaisuudessaan sekä hyvää tutkimusetiikkaa.
- Tutkimus tehdään puolustusvoimien tietoturvamääräyksiä noudattaen.
- Tutkimustyön tulee lähtökohtaisesti olla julkinen. Mikäli työssä syntyy luottamuksellista aineistoa, ei sitä liitetä opinnäytetyön julkiseen versioon. Inskapt Purojärvi vastaa työn julkisuudesta ja tarkastuttaa työn (MAAVEJOJÄOS/ Kapt Markus Tanskanen) ja tekee siihen mahdolliset muutokset ennen työn jättämistä koululle arvioitavaksi.
- Inskapt Purojärvi toimittaa lopullisen tutkimustyön Maavoimien esikuntaan (tiedostona).
- Maavoimien esikunnalla on oikeus tallettaa työn Puolustusvoimien tutkimusrekisteriin.

Asiaa Maavoimien esikunnassa hoitaa Insmaj Pauli Lahtinen (<PUHELINNUMERO POISTETTU>).

Esikuntapäällikkö
Kenraalimajuri Jorma Ala-Sankila

Osastoinsinööri
Insinöörimajuri Pauli Lahtinen

Tämä asiakirja on sähköisesti allekirjoitettu.

LIITTEET

JAKELU

TIEDOKSI Yrjö Sairanen, Maavoimien esikunta Johtamisjärjestelmäosasto
Uula-Petteri Purojärvi, Maavoimien esikunta Johtamisjärjestelmäosasto
Markus Tanskanen, Maavoimien esikunta Henkilöstöosasto
Jari Särmä, Maavoimien esikunta Johtamisjärjestelmäosasto

Liite 3

Haastattelusuunnitelma

Tutkimuskysymys/-kysymykset:

- Voiko maapuolustuksen taktisten verkkojen valvonnan ja hallinnan toteuttaa ITIL:n käytäntöjen mukaisesti?
- Millainen on ITIL:n valvonnan ja hallinnan viitekehys?
- Mitä ovat maapuolustuksen taktiset verkot ja mikä niille on ominaista?
- Mitä teknologioita valvonnan ja hallinnan toteuttamiseksi on käytettävissä?

Tarvittava aineisto/tieto tutkimuskysymyksen ratkaisemiseksi:

Haastateltavilta tarvitaan tietoa maapuolustuksen taktisten verkkojen valvonnan aikaisemmasta toimintatavasta eli digitaalisten kenttäviestijärjestelmien ajasta. Tämä tieto palvelee maapuolustuksen taktisten verkkojen ja niille ominaisten piirteiden tunnistamisessa. Historia-teeman kautta haastattelussa edetään ITIL:n viitekehykseen ja maapuolustuksen taktisten verkkojen nykyiseen olemukseen. Tämän teeman tarkoitus on yhdistää reaalimaailma teoreettiseen viitekehykseen. Lopuksi haastattelussa keskustellaan yleisesti valvonnan ja hallinnan teknologioista.

Haastateltavat:

Haastateltavien valinnassa on käytetty perusteena pitkää työuraa viestiaselajissa ja laaja-alaista kokemusta maapuolustuksen taktisista verkoista, sekä ITIL-viitekehyksen tuntemusta. Haastateltavia tunnistettiin kaksi, joilla molemmilla on yli kolmenkymmenen vuoden kokemus maapuolustuksen taktisten verkkojen rakentamisesta, operoinnista ja johtamisesta. Haastateltavat ovat työskennelleet verkkojen parissa yksittäisistä osajärjestelmistä valtakunnalliseen kokonaisuuteen saakka. ITIL-viitekehyksen tuntemuksena asetettiin vaatimukseksi vähintään muodollinen koulutus, joka molemmilta haastateltavilta löytyy.

Haastattelun protokolla:

Haastattelun aluksi haastateltaville kerrotaan tutkimusluvan (Liite 2) ehdot. Haastateltaville kerrotaan, että tutkimuksen tarkoituksena on muodostaa ITIL-viitekehyksen mukainen ymmärrys maapuolustuksen taktisten verkkojen valvonnasta ja hallinnasta. Tutkimusluvan mukaisesti tutkimustyön tulee olla julkinen. Mahdollista luottamuksellista aineistoa joka syntyy haastattelun aikana, ei liitetä opinnäytetyön julkiseen versioon. Haastateltavilta on pyydetty lupa haastattelun tallentamiseen digitaalisella tallentimella. Tallentimen lisäksi käytetään konseptilehtiötä haastattelun aikaisten lisäkysymysten kirjaamiseksi ja jos haastattelun aikana tulee tarve kuvallisesti hahmotella haastattelussa ilmitulleita kokonaisuuksia. Nämä ovat konseptitasoisia muistiinpanoja.

Liite 4

Teemahaastattelun runko

Taustatietoja:

Tutkittava kohde on maapuolustuksen taktiset verkot, tarkemmin niiden valvonta ja hallinta. Maapuolustuksen taktiset verkot ovat maavoimien johtamisjärjestelmiä jotka on tarkoitettu sotilaskäyttöön normaali- ja poikkeusoloissa.

Haastattelijana on tutkimuksen tekijä, Uula-Petteri Purojärvi. Ensimmäisenä haastateltavana on kapteeni Jukka Eiste, joka on Maavoimien operatiivisen järjestelmäkeskuksen varapäällikkö. Toisena haastateltavana on majuri Jari Särmä, joka on Maavoimien operatiivisen järjestelmäkeskuksen päällikkö. Haastattelut kestävät enintään neljä tuntia.

Haastattelun aiheena on maapuolustuksen taktisten verkkojen valvonta ja hallinta. Haastattelun ensimmäinen teema on maapuolustuksen taktisten verkkojen historia. Teeman tarkoituksena on valottaa maapuolustuksen taktisten verkkojen valvonnan ja hallinnan aikaisempia tekniikoita ja toimintatapoja. Toisena teemana haastattelussa on ITIL-viitekehys ja sen mukaiset toimintatavat ja toimijat. Pyrkimyksenä on tunnistaa maapuolustuksen taktisten verkkojen ja ITIL-viitekehyksen yhtäläisyyksiä ja muodostaa ymmärrys niiden yhteensovittamisesta. Kolmantena teemana on yleisesti valvonnan ja hallinnan teknologiat, joita voidaan käyttää maapuolustuksen taktisten järjestelmien valvomiseksi ja hallitsemiseksi.

Liite 5

Työnantajan edustajan lausunto opinnäytetyöstä

Lähettäjä: Tanskanen Markus PV MAASK <OSOITE POISTETTU>
Päiväys: 3. marraskuuta 2016 klo 12.06
Aihe: VS: Opinnäytetyön tarkastaminen
Vastaanottaja: Uula Purojärvi <OSOITE POISTETTU>

Terve Uula,

työ on luettu ja alla on minun kommentit. Voin kirjoittaa virallisenkin arvion, jos sellaista kaivataan. Haasteenasi on ollut julkisuusvaatimus, mutta olet sen kyllä hyvin onnistunut ratkaisemaan.

Markus

Työssä on sopivan mittainen ja laajuinen tiivistelmä. Sisällysluettelo on työn laajuuteen nähden myös sopivan mittainen eikä pirstaloi itse työtä liian pieniin palasiin. Sisällysluettelossa on myös selkeä etenemismalli ja näin se asettaa työlle ns. punaisen langan. Työssä käsitellään ITIL palvelutuotantoa ja aiheeseen liittyvien protokollien standarditekstejä liiankin yksityiskohtaisesti. Näissä osuuksissa olisi toivonut tutkijan omaan pohdintaa enemmän. Tutkimusasetelma oli suoraviivainen ja käsiteltyyn aiheeseen sopiva. Tutkimustulokset ja pohdinta oli ilo lukea ja toivottavasti ihmisillä on rohkeutta tuottaa tällaista tekstiä myös laajemminkin, koska tällaiset asioiden käsittelytavat johtanevat jollain aikavälillä positiivisiin muutoksiin organisaation ohjeistuksessa ja toiminnassa kehittäen sitä. Tätä silmälläpitäen työllä on hyvät mahdollisuudet vaikuttaa käytännössä, koska tutkija jatkaa työn tekemistä virkatyönään osallistuen ja vaikuttaen tulevaisuuden ratkaisuihin. Kaiken kaikkiaan voidaan todeta, että työ täyttää hyvin oppilastyölle asetetut tavoitteet ja vaatimukset. Olen tarkastanut työn ja se voidaan sellaisenaan julkaista julkisena.

Kapt Markus Tanskanen
Korkeakouluosaston johtaja
Viestikoulu
<PUHELINNUMERO POISTETTU>
<OSOITE POISTETTU>