Ville Rantamäki

VERKKOTOPOLOGIOIDEN MUUTOKSET PUOLUSTUKSELLISENA ELEMENTTINÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Rantamäki, Ville
Verkkotopologioiden muutokset puolustuksellisena elementtinä
Jyväskylä: Jyväskylän yliopisto, 2020, 62 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Ohjelmisto-ohjatut verkot ovat nykyaikainen, mutta vielä verrattain pienessä roolissa oleva verkkoteknologia. Modernilla taistelukentällä, jatkuvasti mukautuvan ryhmityksen ja näin ollen fyysisesti muuttuvan verkkotopologian pääasialliset haasteet on kyetty ratkaisemaan, mutta niihin kohdistuva kyberuhka on jatkuvasti kiihtymässä. Perinteiseen verkkoarkkitehtuuriin on jo vuosien ajan kehitetty jatkuvasti edistyneempiä hyökkäysmenetelmiä ja puolustuksellisissa skenaarioissa toteutettavat toimenpiteet ovat hitaita toteuttaa tai vaativat tarpeettoman paljon resursseja. Tässä tutkimuksessa tarkastellaan sitä, voisiko ohjelmisto-ohjattu verkkoteknologia tuoda muutoksen nykytilaan sujuvoittamalla äkillisiä konfiguraatiomuutoksia verkkoliikenteen rajoittamiseksi ja verkossa sijaitsevien laitteiden turvaamiseksi.

Tutkimus on toteutettu laadullisena tutkimuksena. Sen perustana on suunnittelututkimus, jossa lähtökohtatilanteen ongelmat on tunnistettu aiemmasta tutkimustiedosta ja sen jälkeen teoriaosion tarjoamia menetelmiä hyödyntäen pyritty löytämään ratkaisuja niihin. Tutkimus on rajattu siten, että se ei ota kantaa esimerkiksi taisteluosaston alueella tapahtuvaan satelliittitiedonsiirtoon ja sen tarjoamiin uhkiin ja mahdollisuuksiin, eikä myöskään ohjelmisto-ohjattujen verkkojen kyberuhkiin, vaan keskittyy esittämään mahdollisuuksia. Lähdemateriaalina on pyritty käyttämään mahdollisimman ajantasaista tutkimustietoa, koska teknologiakehitys on äärimmäisen nopeaa.

Tutkimuksen selkein tulos on se, että ohjelmisto-ohjatuilla verkoilla kyettäisiin ehdottomasti tarjoamaan joissakin käyttötapauksissa etua verrattuna konventionaalisiin verkkolaitteisiin. Häiriötilanteista aiheutuvat akuutit konfiguraatiomuutokset, joilla pystyttäisiin rajaamaan esimerkiksi hyökkäyksen leviämiseen liittyviä tapahtumia, saataisiin toimitettua huomattavan nopeasti kohteisiinsa ilman verkon täydellistä rampauttamista. Tätä puoltaa erityisesti datakerroksen ja hallintakerroksen erittely omiksi, erillisiksi verkoikseen, jotka eivät mahdollista tavanomaisiin verkkolaitteisiin suunnitellun hyökkäyksen toteuttamista. Tutkimuksen perusteella aihetta tulisi jatkotutkia käytännön testauksen avulla, jotta saavutettaisiin selkeitä, mittauskelpoisia tuloksia esitetyistä ratkaisuista.

Asiasanat: taisteluosasto, kenttäviestijärjestelmä, kyberpuolustus, SDN, ohjelmisto-ohjatut verkot

ABSTRACT

Rantamäki, Ville
Changes in Network Topologies as a Defensive Element
Jyväskylä: University of Jyväskylä, 2020, 62 p.
Computer Science, Master's Thesis
Supervisor: Lehto, Martti

Software-defined networks are a modern network technology that still holds a somewhat minor role. On the modern battlefield, the crucial challenges in the constantly shifting formation and constantly changing physical network topology have been solved, but the cyber threat directed at them is constantly accelerating. Attacks towards the traditional network architecture have been developed for years, and they are constantly evolving to be more complex. In a defensive scenario the defensive measures in such a network are either too slow or require a disproportionate amount of resources to execute. This thesis aims to consider whether software-defined network technology could bring a change to the current state by streamlining acute configuration changes required to restrict network traffic and protect the devices on the network.

The research has been executed as a qualitative study. It is based on the concept of design science, where the initial threat scenarios are based off earlier studies, and after that by applying the methods explained in the literature review are used to explore solutions to the scenarios. The research has been defined to disregard for example the opportunities or threats that satellite data transfer in a brigade combat team's area of responsibility offer, or the specific cyber threats aimed at software-defined networking. It focuses on presenting possibilities instead. The source material used is mostly as recent as available, due to the extreme speed of technological development.

The clearest conclusion of this study is that software-defined networking could definitely provide advantages over conventional networks in some use cases. Acute configuration changes caused by network incidents, that could be used to restrict the spreading of an attack could be delivered remarkably fast to their targets without entirely crippling the network. The main reason for this is the separation of a data layer and a control layer as two separate entities, which do not allow for attacks based on conventional network devices. The study shows that the subject should be researched further, especially in the form of practical empirical testing, to confirm the validity of the presented solutions by acquiring clear, measurable results.

Keywords: brigade combat team, tactical communications, cyber defence, SDN, software-defined networks

KUVIOT

TAULUKOT

SISÄLLYS

1 NYKYAIKAISEN TAISTELUKENTÄN DIGITAALINEN LUONNE

Kyberulottuvuuden merkitys sodankäynnissä on merkittävässä nousussa johtuen jatkuvasti laajenevasta tietoliikenteen merkityksestä johtamisen mahdollistajana. Kun taistelut ovat nopeita, vaaditaan myös nopeaa päätöksentekoa ja tämän mahdollistaa vain riittävän nopea tilannekuvan välittäminen sekä kyky käskeä joukkoja välittömästi tilanteiden muuttuessa. Samanaikaisesti Suomessa korostetaan johtoportaiden välistä kommunikaatiota vähentävän tehtävätaktiikan merkitystä Puolustusvoimien keskeisenä johtamismenetelmänä (Kostiainen, 2020), mutta johtamisjärjestelmä koetaan samanaikaisesti niin kriittiseksi, että sen sisällölle tulisi suorittaa jonkinlaista kybervalvontaa (Ojala, 2020).

Taisteluosastojen alueella ja välillä toimivat verkot ovat usein hyvin dynaamisia niin fyysiseltä kuin loogiselta rakenteeltaan. Viestiasemat ja niiden mukana kulkevat verkkolaitteet vaihtavat jatkuvasti paikkaa, ja verkon käyttäjät muuttuvat alueella toimivien joukkojen mukaisesti siten, että mikä tahansa päätelaite saattaa toimia eri osissa verkkoa lyhyidenkin aikojen sisällä. Koska konventionaalisissa tietoverkoissa jokainen verkkolaite vaatii erillisiä konfiguraatiomuutoksia verkon rakenteen muuttuessa, sen käyttö on hidasta, työlästä ja niin taloudellisia kuin henkilöstön resursseja kuluttavaa (Kim & Feamster, 2013; Kreutz ym., 2014). Tähän on pyritty vastaamaan siviiliorganisaatioissa ja etenkin kiinteissä verkoissa ohjelmisto-ohjatun verkon (SDN) avulla. Ohjelmisto-ohjatuissa verkoissa konventionaalisen tietoverkon laitteiden vaatimat konfiguraatiomuutokset on pystytty tekemään joustavammiksi ja nopeammiksi hyödyntämällä verkon jakamista hallinta- ja datatasoille, joita käsitellään erillään toisistaan (Nadeau & Gray, 2013).

Tämän tutkimuksen tarkoituksena on tarkastella taisteluosastojen kenttäviestijärjestelmiin kohdistuvia kyberuhkia ja sitä, kuinka ohjelmisto-ohjatun verkon menetelmillä kyettäisiin vastaamaan niihin nykytilaa paremmin. Jos tämä teknologia tarjoaa jotain selkeää etua verrattuna konventionaalisiin verkkolaitteisiin, on tarpeen tunnistaa tämä etu ja mahdollistaa jatkotutkimukset aiheen piiristä. Näiden kahden aihepiirin yhteyksiä on tutkittu julkisesti vähän tai ei lainkaan, jolloin on ollut haastavaa koostaa yhtenäistä käsitystä niiden

soveltuvuudesta täydentää toisiaan. Tutkimuksessa pyritään vastaamaan päällimmäisenä pääkysymykseen:

- Mikä on ohjelmisto-ohjattujen verkkojen kyky toimia puolustuksellisena elementtinä kenttäviestijärjestelmän teknisessä ympäristössä?

Lisäksi vastataan seuraavaan kolmeen alakysymykseen:

- Minkälaiset verkkotopologiat tai niiden muutokset tarjoavat suojaa potentiaalista hyökkääjää vastaan?
- Kuinka ohjelmisto-ohjattuja verkkoja voitaisiin hyödyntää kenttäviestijärjestelmän osana?
- Minkälaisia kyberpuolustuksellisia elementtejä ohjelmisto-ohjatut verkot tarjoavat?

Tutkimus on rakennettu vastaamaan näihin kysymyksiin siten, että pääluvussa 2 esitellään tutkimuksessa käytettävä taisteluosaston kenttäviestijärjestelmä ja sen käyttöön liittyen erilaiset verkkotopologiat. Pääluvussa 3 esitellään ohjelmisto-ohjattujen verkkojen perusperiaate ja niiden yhteys verkkotopologioihin. Pääluvussa 4 esitellään tutkimuksessa käytetyt menetelmät niin aineistonkeruun kuin analyysin osalta. Pääluku 5 on omistettu aiemmassa pro gradu – tutkielmassa tunnistamieni uhkaskenaarioiden esittelyille ja tarkennuksille tätä tutkimusta varten. Pääluvussa 6 tarkastellaan näitä skenaarioita ja sitä, kuinka ohjelmisto-ohjatut verkot kykenisivät mahdollisesti vastaamaan näissä esitettyihin uhkiin. Viimeisenä on pääluku 7, ja sen yhteydessä esitellään tutkimuksen aikana saavutetut johtopäätökset, esitetään aiheet jatkotutkimukselle ja arvioidaan tutkimuksen luotettavuutta.

2 KENTTÄVIESTIJÄRJESTELMÄT JA NIIDEN VERKKOTOPOLOGIA

Nykyaikaisella taistelukentällä on tapahtunut merkittävä muutos historialliseen sodankäyntiin verraten. Kun ennen tiedonsiirto olisi hidasta, vaivalloista ja harvojen etuoikeus, nykyisin pyritään liittämään erilaisten verkkojen avulla yhteiseen johtamisjärjestelmään niin paljon joukkoja, kuin vain kyetään. Tämä tarjoaa entistä paremman kyvyn johtaa pieniäkin joukon osia yksityiskohtaisesti, nopeasti ja pitkienkin välimatkojen päästä. Samalla kuitenkin tarjoutuu vastustajan käyttöön uusi hyökkäysrajapinta, kun tiedonsiirto on siirtynyt pääasiallisesti ip-pohjaiseen liikenteeseen niin langallisissa kuin langattomissa verkoissa.

Koska kenttäviestijärjestelmä on terminä hyvin moniulotteinen ja kattaa alleen käytännössä minkä tahansa erilaisista tiedonsiirtovälineistä muodostuvan, taistelukentälle sijoitettavan järjestelmän, on tarpeen tukeutua jonkinlaiseen olemassa olevaan malliin. Tässä tutkimuksessa tukeudutaan valmiisiin malleihin johtuen siitä, että niiden avulla saadaan lukijalle luotua jonkinlainen kuva modernista kenttäviestijärjestelmästä. Tutkimuksen empiirinen osuus keskittyy geneerisempien konseptien tasolle laite- tai verkkotyypeittäin, koska vaatisi huomattavan määrän aikaa ja konkreettisia testaustilanteita empiirisen datan tuottamiseksi tarkkaan määritellyistä laitteista ja ohjelmistoista. Rajauksella saadaan aikaan kohtalaisen suuripiirteistä tietoa laajasta määrästä tekniikoita.

2.1 Kenttäviestijärjestelmät

Kuten edellä mainittiin, olisi koko kenttäviestijärjestelmän käsitteen analysoiminen aivan liian laaja kokonaisuus yhteen tutkielmaan. Siksi tässä tutkielmassa tullaan käyttämään pohjalla toimivana sotilasorganisaationa yhdysvaltalaista jalkaväen taisteluosastoa, IBCT:a (Infantry Brigade Combat Team). Se soveltuu hyvin tähän tapaukseen, koska siihen kuuluu suuri määrä erityyppisiä joukkoja, verrattain laaja kenttäviestijärjestelmä sekä kyberhyökkäyksien kannalta tarkas-

telukelpoinen johtamisrakenne. Lisäksi sen sisällöstä, toiminnasta ja järjestelmistä on saatavilla eniten julkisia tutkimuksia ja raportteja, joiden pohjalta pystytään luomaan realistinen uhkamalli todellista, nykyaikaista taisteluosasto-organisaatiota kohtaan ja pohtimaan sen potentiaalisia puolustusratkaisuja. (Rantamäki, 2018)

Modernille sotilasorganisaatiolle valtiosta riippumatta on tyypillistä nykypäivänä hyödyntää missä tahansa taktisen tason viestijärjestelmässä perusperiaatteena MANET-verkkoja (Mobile Ad Hoc Network). Konkreettisesti selitettynä MANET on mesh-verkko, joka kykenee mukautumaan muuttuvaan fyysiseen topologiaan, ja se muodostuu automaattisesti solmujen liittyessä verkon rakenteeseen mistä tahansa pisteestä. Tämä erottaa sen perinteisestä, staattisesta verkosta. (Peacock, 2007; Rantamäki, 2018)

Samanaikaisesti tämä luo jatkuvasti muuttuvan verkon, jossa taisteluosaston viestijärjestelmän osat voivat joko liittyä verkkoon tai poistua siitä saumattomasti, tahallisesti tai tahattomasti huomioiden taistelukentällä kyseisenä ajanhetkenä vallitsevat maasto-, sää- tai sähkömagneettisen spektrin olosuhteet. (Bowman & Zimmerman, 2010; Rantamäki, 2018). Tämä joustavuus on kriittinen ominaisuus jatkuvasti muuttuvassa taistelutilanteessa, jossa oletetaan johtamisjärjestelmän olevan jatkuvasti käytettävissä.

Koska tähän tutkielmaan on valittu tarkasteltavaksi yhdysvaltalainen IBCT, on syytä esitellä siihen kuuluvan viestijärjestelmän kriittisin laitteisto. Warfighter Information Network-Tactical (WIN-T) -järjestelmä on yleisesti Yhdysvaltojen asevoimien käytössä oleva viestijärjestelmä, joka sisältää alla esitetysti erilaisia viestiratkaisuja (Kuvio 1) (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014). Kuten kuvasta on nähtävissä, IBCT:n käytössä on jopa 87 erilaista yhteyspistettä, joiden avulla kyetään rakentamaan verkko ja tarjoamaan liityntämahdollisuuksia. Jokainen yhteyspiste pitää sisällään vaihtelevan määrän erilaisia yhteystekniikoita ja laitteita, jotka on selitetty myöhemmin.(Rantamäki, 2018)

Updated 21 March 2014	WIN-T Configuration Items by Echelon						
	Corps HQ	Division HQ	ABCT	IBCT	SBCT	Fires Bde	Aviation Bde
TCN	3	3	9	9	9	4	8
TCN-L	0	3*	0	9*	0	0	0
POP	4	4	9	9	11	4	7
SNE			45	45	51	12	8
STT HP5K	3	3	2	2	2	2	2
STT+			7	7	7	2	6
TR-T	1	1	1	1	1	1	1
VWP	3	2	14	14	14	3	9
NOSC-B			1	1	1	1	1
NOSC-L	1	1	8	8	8	3	6
NOSC-D	1	1					
MCN-B	1	1	1	1	1	1	1
IP Phone	110	110	145	145	165	75	130
Secure IP Phone	50	50	60	60	70	35	55
TCN Open Rack							
POP Open Rack							
SNE Open Rack							
NOSC-B Open rack							
NOSC-D Open Rack							

Kuvio 1: WIN-T laitteiston jako eri joukkotyypeille. (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014)

Aiemmassa tutkielmassani (Rantamäki, 2018) olen esitellyt WIN-T:n laitteiston yhteyspisteet, jotka on myös selitetty alla:

- TCN(-L): Tactical Communications Node (Lite), ajoneuvoasenteinen tietoliikenneverkon solmu, joka tarjoaa lähialueelleen langallisia ja langattomia verkkoyhteyksiä ja kykenee toteuttamaan myös satelliittiyhteyksiä paikallaan ja liikkeestä. Se tarjoaa yhteyskanavan Yhdysvaltojen asevoimien maailmanlaajuiseen verkkoon (GIG, Global Information Grid) ja sen yhteydessä toimivat TR-T, VWP, STT+/HP ja NOSC. Ne ryhmitetään prikaatin ja sen alajohtoportaiden komentopaikoille. L- eli Lite-versio on pienemmälle ajoneuvoalustalle ja hinattavalle lavetille pohjautuva vastaaviin kyvykkyyksiin suunniteltu versio.(*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018)

- POP: Point of Presence tarjoaa liikkeessä tai paikallaan yhteyden taisteluosaston alueen mesh-verkkoon ja satelliitteihin kompaktimmassa koossa ja paremmalla liikkuvuudella kuin TCN. Se tarjoaa mahdollisuudet esimerkiksi komentajan johtamistoimintaan dataterminaalia tai VoIP-puhelinta käyttäen, ja sen langallisten yhteyksien kyky tarjoaa mahdollisuuden pikaiseen komentopaikkatoimintaan pysähdyksissä. Ne ovat komentajien käytössä, ja tarjoavat näin ollen johtamiskyvyn myös komentopaikkojen ulkopuolella.(*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018)

- SNE: Soldier Network Extension on taisteluosaston lähinnä etulinjaa oleva linkki WIN-T -verkkoon, ja sen kautta jalkautuneet taistelevat joukot saavat yhteyden tähän verkkoon omien radioidensa avulla (*Warfighter In-*

formation Network - Tactical Commander's Handbook Version 2.0, 2016). SNE:n tiedonsiirto perustuu satelliittitiedonsiirtoon liikkeestä ja paikallaan, ja tällöin kaistanleveys rajoittaa jonkin verran käyttöön saatavia tietojärjestelmiä esimerkiksi komppanian päälliköiden päätöksenteon tueksi (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014). SNE:ien avulla voidaan myös laajentaa taisteluosaston verkkoa alueellisesti tai tarjota lisää liityntämahdollisuuksia raskaasti liikennöidyille alueille (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018).

- VWP: Vehicle Wireless Package on ajoneuvoasenteinen järjestelmä, jolla kyetään laajentamaan TCN:n tarjoamat yhteydet suuremmalle alueelle. Niillä on kyky liittyä mihin tahansa kantamalla olevaan TCN:een. Niiden tarkoituksena on mahdollistaa jatkuvien reaaliaikaisten päivitysten saaminen taistelunjohtojärjestelmiin joukkojen ollessa liikkeellä ja mahdollistaa riittävät johtamisyhteydet liikkuville joukoille kun TCN:t toimivat staattisesti.(*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018)

Näistä osista muodostuu laaja, monin eri tekniikoin varmennettu viestijärjestelmä prikaatin taisteluosaston alueelle, ja se tarjoaa myös yhteysmahdollisuuden ylempiin johtoportaisiin (Kuvio 2). Kuvassa on esitetty myös edellisessä taulukossa mainitsematta jääneet komponentit:

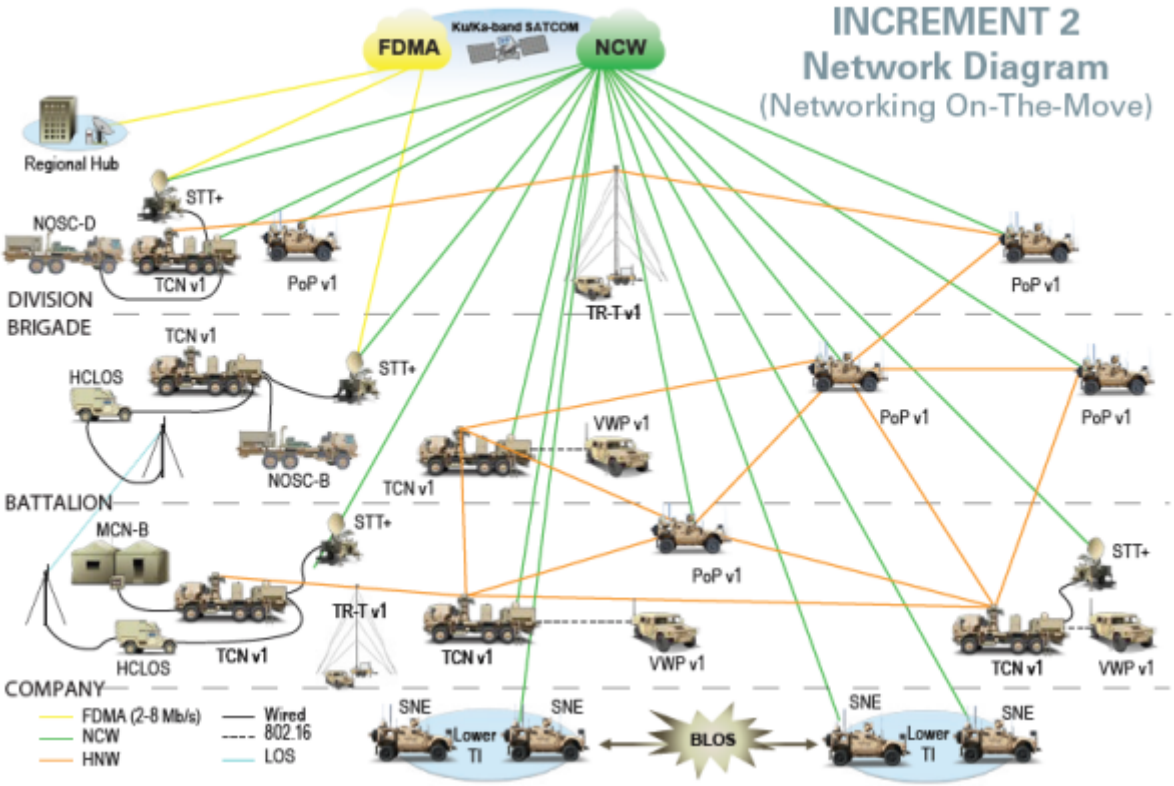
- HCLOS: High Capacity Line of Sight, joka on tiedonsiirtokanava kahden JNN:n (Joint Network Node) välillä. (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018)

- JNN: Joint Network Node, joka on kuvassa luokiteltu tekstin HCLOS yhteyteen. JNN tarjoaa käyttäjille nopeaa näköyhteyteen perustuvaa tiedonsiirtokanavaa tai satelliittiyhteyksiä hyödyntäen yhteensä 560 data/äänikanavaa, sekä videoneuvotteluteknologian. Lisäksi se sisältää informaatioturvallisuuteen liittyvän laitteiston. Niitä on BCT:n käytössä kaksi, ja ne tulevat sekä pää- että taktiselle komentopaikalle. (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018)

- MCN-B: Modular Communications Node – Basic, joka sisältää sekä analogisen gatewayn että ethernet-kytkimen, joilla on tarkoitus laajentaa taisteluosaston lähiverkkoa tarjoten lisää portteja pelkkään TCN:een verrattuna. Näitä taisteluosastolla on käytössään yksi, ja se sijaitsee useimmiten pääkomentopaikalla mutta on käytössä koko taisteluosaston yhteisenä tarvittaessa. (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018)

- NOSC: Network Operations and Security Center, joita löytyy erilaisella varustuksella eri tasoille (D = divisioona, B = prikaati). NOSC on tarkoitettu verkon hallintaan ja -valvontaan, kuten myös kryptoavainten hallintaan ja jakeluun niitä tarvitsevissa laitteissa. Se sisältää merkittävän määrän erilaisia ohjelmistoja reitittimien, kytkinten ja muiden verkkolaitteiden hallintaan, sekä esimerkiksi tulevien operaatioiden verkkosuunnitteluun. (*Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T)*, 2014; Rantamäki, 2018)

Taisteluosastolle on hyvin tyypillistä, että joukkojen ja johtamisjärjestelmien määrän takia sen alueella tapahtuu massiivinen määrä tiedonsiirtoa jatkuvasti. Koska kyseessä on laaja, suurta varmuutta vaativa verkko, vaatii jo pelkästään sen valvontaan ja hallintaan liittyvä data merkittävän määrän kaistanleveyttä etenkin valvontaan osallistuvien solmujen alueella. Erilaiset tilannekuvan esittämiseen tarkoitetut järjestelmät, puhepalvelut ja muut taistelun johtamiseen tarvittavat palvelut aiheuttavat suuret vaatimukset tiedonsiirtokapasiteetille reaaliaikaisuuden sekä palveluiden saatavuuden takaamiseksi. Koska sotilasjohtaminen pohjautuu monesti muodollisille käskyille ja niiden jakamiseen tarvitsijoille, voisi myös olettaa, että jonkinlainen tiedostopalvelin huolehtisi näiden varastoinnista erillisten työasemien kovalevyjen sijaan. (Asman ym., 2011; Rantamäki, 2018)



Kuvio 2: WIN-T -verkko prikaatin taisteluosaston alueella. (General Dynamics, 2016)

MANET-ratkaisujen suosio on aiheuttanut myös sen, että suomalainen Bittium on valmistanut oman versionsa kenttäviestijärjestelmän laitteistosta. Bittiumin TAC WIN on useasta erityyppisestä (point-to-point, point-to-multipoint tai ympärisäteilevä) laitteesta muodostuva kokonaisuus, joka kootaan yhteen valmistajan omilla tähän käyttötarkoitukseen valmistetuilla taktisilla reitittimillä. Perusrakenteeltaan järjestelmästä tulee hyvin samankaltainen kuin WIN-T:sta, mutta se ei sisällä satelliittiyhteyksiä niiden vähäisen tarpeen vuoksi kotimaisissa käyttötapauksissa. Liikennöinti taktisen verkon sisällä tapahtuu OLSR-reitityksen (Optimized Link State Routing) avulla, ja siitä lähtevät tai siihen saapuvat ulkoiset yhteydet on toteutettu OSPF/BGP-reitityksen (Open Shortest Path First / Border Gateway Protocol) avulla. VLAN:ien käyttö verkossa on myös mahdollistettu, ja järjestelmä sisältää jonkinlaisen palomuuriratkaisun itsessään. (*Bittium Tactical Wireless IP Network TAC WIN*, 2017; Rantamäki, 2018)

MANET-verkoista on muodostunut miltei standardi nykyaikaiselle taistelukentälle riippumatta valmistajasta tai käyttäjästä sen monipuolisuudesta johtuen. Erilaisten yksiköiden tai taistelijoiden tulee kyetä liittymään verkkoon missä ja milloin tahansa, niin kauan kuin toiminta tapahtuu jonkin viestijärjestelmän osan alueella. Koska laitteiden fyysinen topologia on jatkuvasti vaihtuva, muodostuu looginen topologia usein mesh-tyyppiseksi. Tätä tukevat lisäksi eri laitteiden kyvyt toimia tukiasemina ja verkon laajennuksina pois lukien yksittäisillä taistelijoilla olevat päätelaitteet, sekä monipuoliset reititysprotokollat, jotka huolehtivat verkon osien yhdistämisestä tilanteeseen sopivalla tavalla.

Syy sille, miksi tässä tutkielmassa on valikoitu vain yksi esiteltävä, laajahko kokonaisjärjestelmä on siinä, että sen yksityiskohtaisella laitteistokokoonpanolla ei ole merkitystä uhkakuvia tarkasteltaessa. Jotta usean järjestelmän vertailulla saavutettaisiin merkittävää hyötyä, täytyisi myös uhkien tarkastelun olla hyvin teknologiakeskittynyttä, ja sen täytyisi ottaa kantaa niin ohjelmistoihin, protokolliin kuin käytettyihin siirtoteihin. Tärkeämpää tämän tutkielman kannalta on kuitenkin se, minkälainen verkon rakenne on, ja minkälaisia laitteita siihen kuuluu periaatetasolla. Koska uhkakuvat eivät ota kantaa siihen, kohdistuuko hyökkäys esimerkiksi nimenomaan Ciscon vai HP:n laitteistoon, ja toimiiko kohdejärjestelmän päätelaite Windows- vai Linux-käyttöjärjestelmällä, olisi tarpeetonta esittää laajaa valikoimaa erilaisia johtamisjärjestelmiä ympäri maailman.

2.2 Verkkotopologiat ja reititysprotokollat

Kun tarkastellaan verkkotopologioita, tarkastellaan verkon muotoa joko fyysisellä tai loogisella tasolla. Fyysinen topologia kertoo sen, missä verkon laitteet fyysisesti ovat, ja miten ne ovat kytkeytyneet toisiinsa kaapelein tai langattomasti. Loogisella tasolla taas tarkastellaan sitä, kuinka tieto liikkuu verkon sisällä. Tarkasteltavasta tasosta huolimatta topologia kertoo siis käytännössä sen, missä verkon solmut ja niiden väliset yhteydet sijaitsevat, ja missä väleissä tiedonsiirto tapahtuu. Koska tietoverkot eivät ole enää luonteeltaan pelkästään

laitteiden välisiä fyysisiä yhteyksiä, fyysinen ja looginen topologia eivät välttämättä kulje käsi kädessä. (Groth, 2005)

2.2.1 Verkkotopologiat

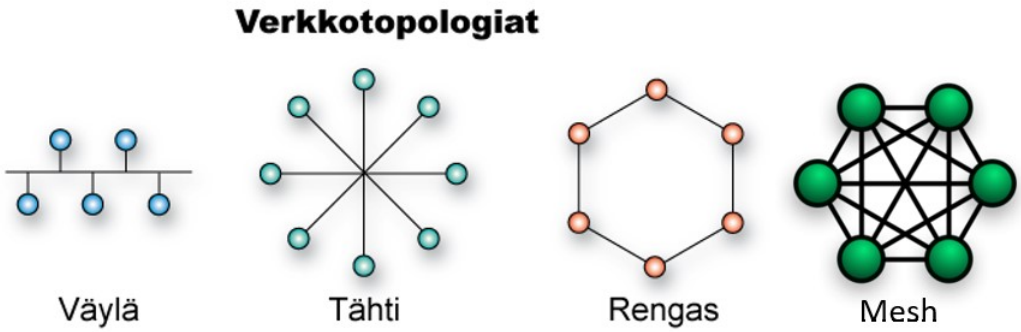
Yleisimmät fyysiset topologiat ovat väylä-, tähti-, rengas- ja mesh-topologia. Näistä varsinkin väylätopologia on jo pitkälti vanhentunut ominaisuuksiltaan, sillä siinä kaikki laitteet on kytketty yhteen linjaan, jolloin pienetkin viat runkolinjassa saattavat kaataa koko verkon yhtäaikaisesti, ja vikojen paikallistaminen saattaa olla todella työlästä. Sen haaste, etenkin langallisten yhteyksien tapauksessa on sen vaikeus mukautua liikkeeseen ja laajentumiseen, eikä se näin ollen ole kovinkaan realistinen topologia taistelukentän jatkuvasti muuttuvissa tilanteissa ja olosuhteissa.(Groth, 2005) Tämän topologian analyysiin ei ole järkevää panostaa tämänkaltaisessa tutkimuksessa, sillä sen tarjoamat skenaariot eivät ole realistisesti sovellettavissa tosielämän esimerkkeihin ja laitteistoihin.

Tähtitopologia on yleinen vielä nykypäivänäkin, ja siinä verkon eri laitteet liikennöivät jonkin yhden, keskeisen laitteen kautta (Groth, 2005). Tähden keskimmäinen laite pääsääntöisesti käsittelee signaalin, suorittaa virheenkorjausta ja lähettää sen edelleen. Yksittäiset sakarat voivat toimia erimerkiksi toisen tähtitopologian keskuslaitteena, joka mahdollistaa verkon laajentamisen yksittäisten tähtien kokoelmaksi. (Sosinsky, 2009) Yksi esimerkki voisi olla kotiverkko, jossa olohuoneen eri älylaitteet kytkeytyvät yhteen reitittimeen tai kytkimeen, joka hallinnoi langallisesti tai langattomasti yksittäisten laitteiden yhteyksiä. Jos keskimmäinen laite rikkoutuu, koko verkko lakkaa toimimasta, mutta yksittäisten laitteiden tai yhteyksien viat eivät vaikuta muihin verkon osiin.

Rengastopologiassa verkkolaitteet ovat kiinnittyneet kahteen muuhun laitteeseen ketjussa, jonka ensimmäinen ja viimeinen laite ovat toisiinsa kytkeytyneenä. Rengastopologia on mahdollista toteuttaa joko yksi- tai kaksisuuntaisella liikenteellä, mutta suurilla liikennemäärillä se alkaa herkästi kärsiä suurista siirtoviiveistä, ja lisäksi sen laajennettavuus on melko kyseenalainen fyysisissä topologioissa. (Meador, 2008) Fyysinen rengastopologia on melko harvinainen ja hankalakäyttöinen ilman langatonta tiedonsiirtoa, sillä yhdenkin laitteen poistaminen katkaisee liikenteen yksisuuntaisesta verkosta kokonaan, samoin kuin uusien laitteiden lisääminen renkaaseen. Sen sijaan loogista rengastopologiaa voidaan hyödyntää fyysisen tähtitopologian päällä, kuten Token Ring -teknologiassa, jossa keskellä sijaitseva laite käsittelee tiedonsiirtoa rengasmaisesti laitteelta toiselle. (Groth, 2005)

Mesh-topologia on luonteeltaan hieman erilainen, kuin muut aiemmin mainitut, koska kaksisuuntaisen rengastopologian lisäksi se on ainut, jossa kahden eri verkkolaitteen välillä voi olla useampia reittejä. Tämä mahdollistaa merkittävästi paremman kestävyyden erilaisia ongelmatilanteita vastaan, ja mahdollistaa suurtenkin tietomäärien siirron yksittäisten reittien ruuhkautuessa. (Meador, 2008) Koska verkon eri osiin voi kulkea useita eri reittejä, tarvitaan verkkolaitteilta älykkäitä reititysprotokollia. Näin pystytään minimoimaan kuljettu matka, tai tarvittaessa väistämään ruuhkautuneita tai vikaantuneita sol-

muja verkossa. Joissain tapauksissa kaikki verkkolaitteet ovat kytkeytyneitä toisiinsa, mutta useimmiten jokainen on kytkeytynyt muutamaan lähimpään solmuun. (Sosinsky, 2009) Eri verkkojen periaatekuvat on esitetty alla (Kuvio 3).



Kuvio 3: Verkkotopologiat. (”Verkkotopologia”, 2015)

Suurin osa verkoista, etenkin laajemmista verkoista on jossain määrin hybridiverkkoja, jotka sisältävät piirteitä useista edellä mainituista topologioista. Tällaisia voivat olla esimerkiksi väylän avulla toisiinsa liitetyt tai hierarkkisesti järjestyneet tähtitopologiat, rengas-tähtitopologiat tai hybridi-mesh, jossa yksittäiset verkon solmut saattavat muodostaa alueellaan jotain toista topologiaa noudattavan verkon osan. Etenkin hybridi-meshin avulla voidaan saavuttaa merkittävää joustavuutta ja virheensietoa erilaisissa tilanteissa. (Sosinsky, 2009)

Eri topologioiden jalkauttaminen erityisesti langatonta tiedonsiirtoa painottavissa kenttäviestijärjestelmissä on monesti toteutettava tilanteen edellyttämällä tavalla, ja muutokset olosuhteissa tai joukon liikkeet saattavat pakottaa odottamattomiinkin muutoksiin. Tässä mielessä esimerkiksi mesh- tai hybridiverkko tarjoaa selkeän edun muihin vaihtoehtoihin verrattuna. Vaikka yksi tai useampi solmu poistuisi verkosta suunnitellusti tai suunnittelemattomasti, voidaan tiedonsiirtoa jatkaa edelleen mahdollisimman moneen muuhun verkossa olevaan solmuun.

2.2.2 Reititys

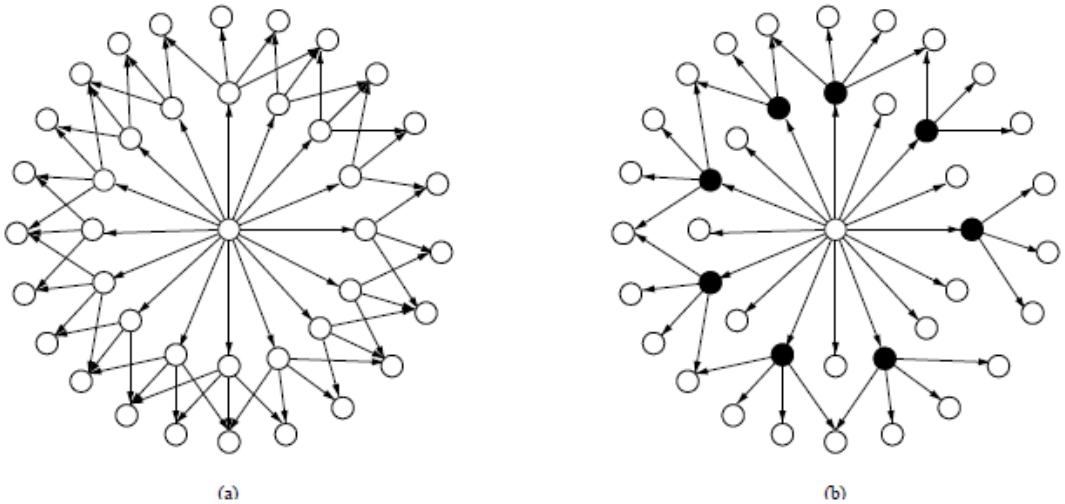
Mitä monimutkaisemmaksi verkko kasvaa, sen tehokkaampia ja älykkäämpiä reititysprotokollia sen laitteilta vaaditaan, jotta liikenne verkossa on sujuvaa ja viiveetöntä. Reititystapoja on olemassa kahdenlaisia – staattisia ja dynaamisia. Molemmat tarjoavat sekä etuja että haittoja niin käytettävyyteen, skaalautuvuuteen sekä turvallisuuteen.

Näistä staattinen on nimensä mukaisesti kiinteistä reiteistä muodostuva kokonaisuus, joka on tallennettu reititystauluun. Tässä tapauksessa reititystaulussa olevat reitit on syötetty manuaalisesti tiettyjen pisteiden välille. Reitin varrella olevilta reitittimiltä täytyy löytyä riittävästi tietoa siitä, mihin paketti tulee välittää, mikäli kohdeosoite ei löydy omasta aliverkosta, vaan se tulee jakaa eteenpäin kohti oikeaa verkon osaa. Tämä vaatii jatkuvaa reititystaulujen

ylläpitoa, eikä mahdollista verkon laajentumista ilman konfiguraatiomuutoksia kaikkiin verkon laitteisiin. (Doyle, 1998)

Dynaamiset reititysprotokollat edellyttävät verkkolaitteilta kykyä kommunikoida toistensa kanssa siten, että ne vaihtavat jatkuvasti tietoa verkon tilasta ja siinä tapahtuneista muutoksista. Tällöin vältytään tilanteelta, jossa verkon ylläpitäjän täytyy manuaalisesti ylläpitää reititystauluja kaikissa verkon laitteissa, vaan laitteet kykenevät keskenään kertomaan toisilleen niin itsestään kuin verkkonaapureistaan. Yksinkertaisimmat protokollat kuten RIP (Routing Information Protocol) saattavat laskea optimaalisia reittejä vain matkalle kertyvien verkkovälien (hop) lukumäärän minimoimalla (Doyle, 1998), mutta uudemmat kuten OSPF (Open Shortest Path First) mahdollistavat reiteille annettavan erilaisia ”hintoja” (cost) suhteutettuna niiden viiveisiin, ruuhkaisuuteen tai muihin metriikoihin (Höylä, 2012).

Yksi esimerkki tällaisesta dynaamisesta reititysprotokollasta on kenttäviestijärjestelmienkin yhteydessä mainittu OLSR (Optimal Link State Routing), jota käytetään muun muassa Bittiumin valmistamissa taktisissa reitittimissä reititinten väliseen sisäiseen liikenteeseen. (*Bittium Tactical Wireless IP Network TAC WIN*, 2017) OLSR toimii proaktiivisesti, ja välittää jatkuvasti tietoa verkon tilasta kaikille verkon reitittimille, ja olettaa kaikkien verkossa olevien reitittimien olevan luotettavia. (Adjih ym., 2003) OLSR:n hallinta voidaan toteuttaa joko kaikilta 2 verkkovälin päässä olevien laitteiden välillä, tai hyödyntäen dedikoituja releasemia (Multipoint Relay, MPR), ja nämä eri mallit ohjaavat verkon hallintaliikennettä hieman eri tavoin (Kuvio 4).



Kuvio 4: OLSR-hallintaviestien kulku, a) kaikille 2 verkkovälin päässä oleville laitteille, b) MPR:n kautta valikoidusti. (Adjih ym., 2003)

Toinen, myös Bittiumin taktisista reitittimistä löytyvä esimerkki dynaamisesta reititysprotokollasta on aiemmin mainittu OSPF. OSPF mahdollistaa verkon siirtoteiden arvottamisen niiden ominaisuuksien mukaan, sekä useampaa reittiä samaan kohteeseen tapahtuvan tietoliikenteen. Näin kyetään tasaamaan kuor-

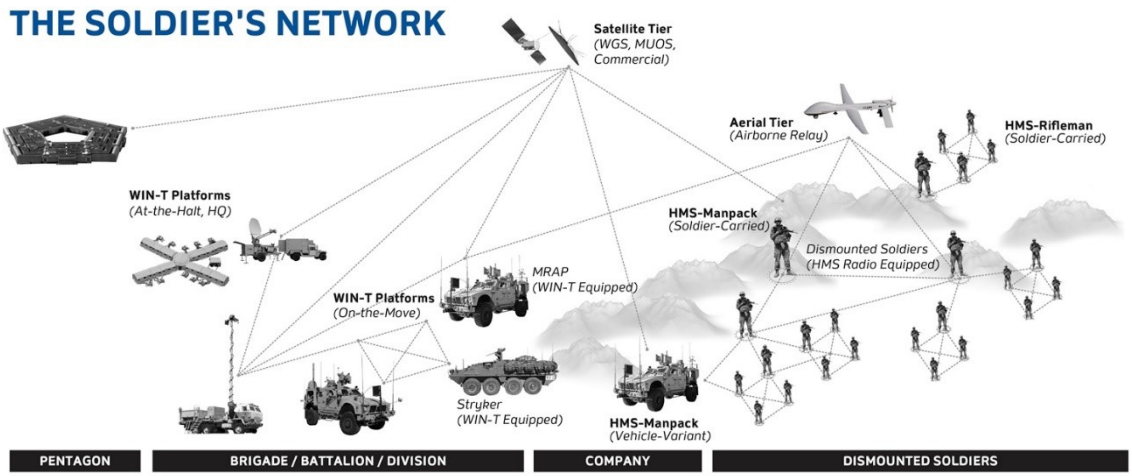
maa verkon eri osa-alueilla yksittäisten siirtoteiden tukkeutumisen välttämiseksi, sekä varmentamaan yhteysvälejä mahdollisilta virheiltä. (Höylä, 2012) Tärkein ero OLSR:n ja OSPF:n toiminnan välillä on se, että OLSR rajoittuu yleensä mahdollisen MANET-verkon sisällä toimimiseen, kun taas OSPF huolehtii verkosta sisään tai ulos suuntautuvasta liikenteestä. OSPF kykenee paremmin toimimaan yhteistyössä vanhempaa teknologiaa käyttävien verkkojen ja laitteiden kanssa, kun OLSR taas toimii käytännössä vain uudempien protokollien kanssa. (Fang ym., 2010)

2.3 Potentiaaliset topologiat ja reititys kenttäviestijärjestelmissä

On selvää, että suurin osa kenttäviestijärjestelmissä käytettävistä verkkotopologioista tulee olemaan jonkinlaisia hybridejä edellä mainituista. Yksittäiset topologiat sellaisenaan eivät tarjoa kovinkaan taistelunkestävää ratkaisua pois lukien mesh, jota hyödyntäen pystytään tekemään tarvittaessa nopeitakin muutoksia verkon rakenteeseen vaikuttamatta sen toimintaan haitallisesti. Koska kyseessä on kuitenkin monen eri verkon muodostama kokonaisuus, ei voida lukkiutua mihinkään tiettyyn topologiaan, vaan niiden liittyminen toisiinsa muodostaa jonkinlaisen hybridin.

Kuten aiemmin, kuvassa 2 esitetyssä esimerkissä prikaatin taisteluosaston kenttäviestijärjestelmästä on nähtävissä, sen eri osat toimivat erityyppisin topologioin. TCN-, PoP- ja TR-asemat muodostavat keskenään mesh-verkon, jolloin kentällä oleva liityntäverkko on ainakin jossain määrin varmennettu ja kestää kuormitusta paremmin, kuin yksittäinen suora linja pisteestä pisteeseen. Nämä kaikki ovat jonkin verkon osan kautta kytkeytyneenä satelliittiverkkoon, joka on kuvattu pilvenä, kuvitteellisena tähtitopologian keskipisteenä, joka kuitenkin muodostunee useammasta eri satelliitista. Maan pinnalla käytössä on HNW (Highband Networking Waveform), tehokasta siirtokaistaa tarjoava langaton tiedonsiirtoratkaisu, kun taas satelliitteihin päin käytössä on NCW (Net Centric Waveform), jonka käyttöperiaate on sama kuin HNW:n, mutta tarkoitettu maa-asemien ja satelliittien väliseen liikenteeseen. (*Warfighter Information Network - Tactical Commander's Handbook Version 2.0*, 2016)

Jotta tätä kokonaisuutta voitaisiin tarkastella vielä hieman yksinkertaistetummin, mutta huomioiden vielä enemmän verkon eri tasoja, voidaan katsoa General Dynamicsin tuottamaa havainnekuvaa verkon karkeasta rakenteesta ilman tekniikoiden erittelyä (Kuvio 5).



Kuvio 5: WIN-T -järjestelmän verkkotasojen havainnekuva. (*Warfighter Information Network-Tactical (WIN-T) - General Dynamics Mission Systems*, 2019)

Kun kuvasta on karsittu pois eri värit ja useat samantasoiset laitteet, verkon rakenne alkaa hahmottua paremmin. Ajoneuvot WIN-T -kalustoineen näyttävät muodostavan omia, sisäisiä mesh-verkkojaan, mutta niin tekevät myös yksittäiset taistelijat HMS-radioillaan (Handheld, Manpack and Small Form Fit). Samanaikaisesti niin satelliitit, ilma-alukset tai erityyppiset maa-asemat toimivat tähtitopologian keskipisteinä suuremmassa mittakaavassa, ja etenkin satelliittien tapauksessa yhdistävät kaikki eri tasoiset verkot toisiinsa niiden kalustosta ja verkkolaitteista riippumatta. Kokonaisuus vaikuttaa siis olevan jonkinlainen yhdistelmä tähti- ja mesh-topologioita aina Pentagonista yksittäiselle taistelijalle saakka, riippumatta maantieteellisestä sijainnista. Tämä kuitenkin kertoo vain verkon fyysisestä topologiasta, eikä ota kantaa sen sisällä vallitsevan loogisen topologian rakenteeseen.

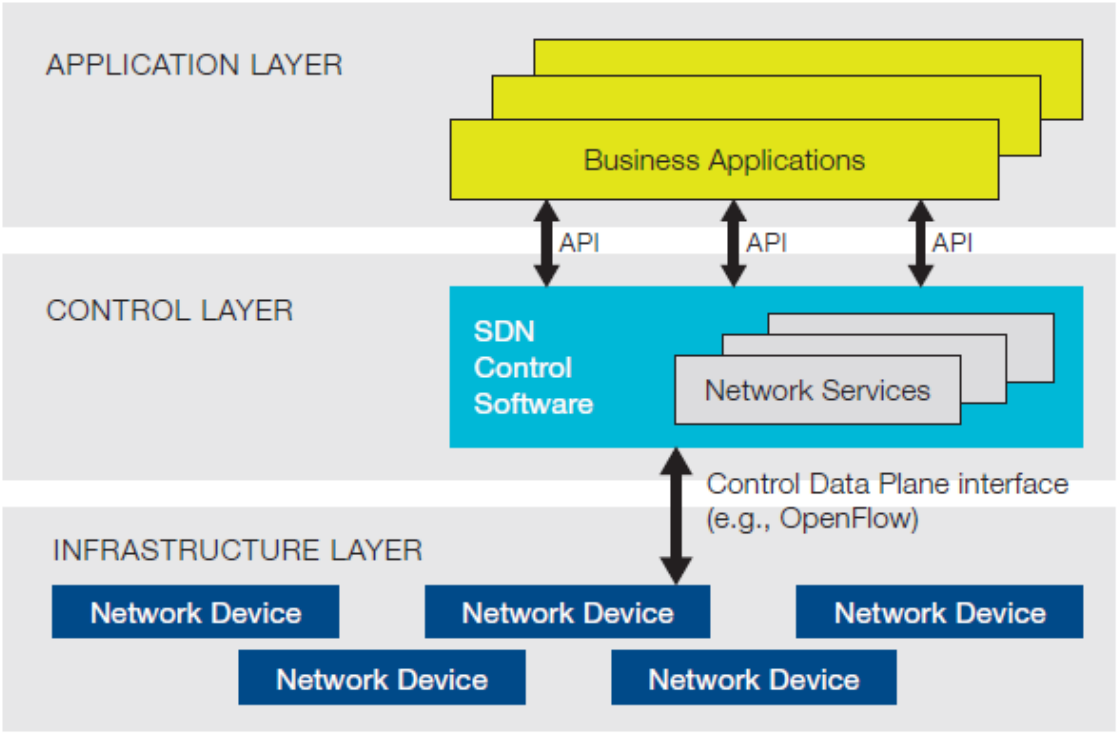
Kuten suomalaisen Bittiumin laitteistosta otetussa esimerkissä reititysprotokollista, voidaan olettaa myös yhdysvaltalaisen kaluston toimivan ainakin pääperiaatteiltaan samankaltaisesti. Dynaamiset reititysprotokollat tarjoavat mahdollisuuden muokata verkkoa taistelutilanteiden edellyttämällä tavalla, mutta ne toimivat käytännössä automatisoidusti omissa verkoissaan. Kontrolloidut loogisen topologian muutokset vaativat tuekseen esimerkiksi ohjelmisto-ohjatun verkkorakenteen, joka esitellään seuraavassa pääluvussa.

3 OHJELMISTO-OHJATUT VERKOT

Perinteisesti tietotekniikassa laskenta, varastointi ja verkkoresurssit on pyritty pitämään erillään toisistaan loogisesti ja fyysisesti, ja niiden käyttöön pyrkiviltä sovelluksilta on vaadittu paljon erilaisia käyttöoikeuksia turvallisuuden varmistamiseksi. Nykyisin tilanne on kuitenkin jokseenkin muuttunut, kun virtualisointi on vienyt kokonaiset tietokoneet bittimuotoon ja ohjelmistojen käsiteltäväksi. Samaan aikaan mahdollistettiin fyysisen laitteiston keskittäminen datakeskuksiin, ja niissä operoitavien järjestelmien saumaton siirto fyysiseltä laitteelta toiselle yksinkertaisesti kopioimalla koko järjestelmän sisältävä tiedosto paikasta toiseen. (Nadeau & Gray, 2013)

Kun virtualisaatio yleistyi, samaan aikaan mahdollistettiin muutos verkkolaitteiden toimintaperiaatteessa. Normaalisti reititys on jaettu verkkolaitteessa kahteen eri kerrokseen: tiedonvälityskerrokseen, joka yhdistää verkkolaitteen eri portit toisiinsa ja hallintakerrokseen, joka käytännössä vastaa hallinnasta ja ohjauksesta. Keskitetyssä hallinnassa kuitenkin rakentuisi vain yksi looginen hallintakerros, jonka avulla kyettäisiin hallinnoimaan kaikkia verkon laitteita, ja pakottamaan niitä muuttamaan oman fyysisen verkko-osansa toimintaa. Näistä ideoista alkoi rakentua ohjelmisto-ohjattujen verkkojen (Software Defined Network, SDN) ajatus. (Monsanto ym., 2013; Nadeau & Gray, 2013)

Yksinkertaisuudessaan SDN tarkoittaa fyysisten verkkolaitteiden täyden hallinnan luovuttamista niitä ohjaavalle ohjelmistolle. Kun aiemmin verkkolaitetta pystyi ohjailemaan monilta osin, mutta sisäinen toiminta oli silti käyttäjälle melko läpinäkymätöntä ja lukuisiin protokolliin ja standardeihin perustuvaa, tarjoaa SDN parhaimmillaan laitteen täyden hallinnan – kunhan laite kykenee vastaanottamaan ja tulkitsemaan hallintakerrokselta saapuvat komennot. Koko hallinta on keskitetty hallintakerroksen ohjattavaksi, mikä saa kokonaisen verkon näyttäytymään sovelluskerrokselle ja sen rajapinnoille yksittäisenä loogisena kytkimenä. Näin verkkoa kyetään hallitsemaan yhdestä pisteestä selkeästi sovelluskerroksella toimivien verkon toimintaan liittyvien sovellusten avulla. Alla on esitettynä yksinkertainen malli SDN-verkosta (Kuvio 6). (ONF White Paper, 2012)



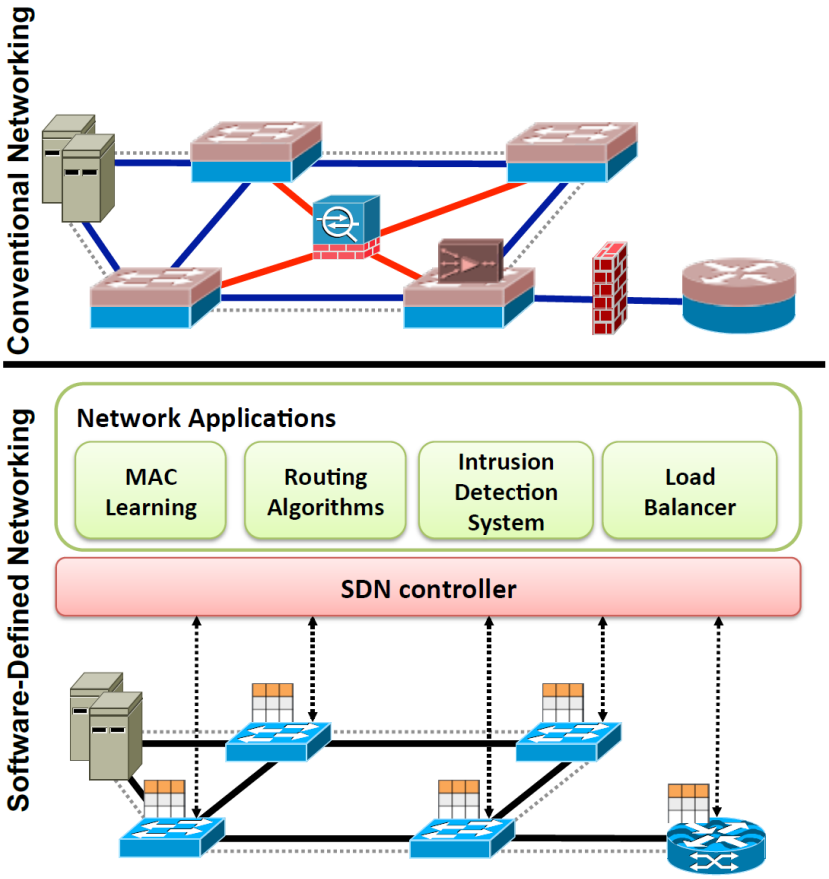
Kuvio 6: SDN-verkon perusrakenne. (ONF White Paper, 2012)

Yksi kriittisimmistä ominaisuuksista tällaisessa monipuolisen hallinnan mahdollistavassa arkkitehtuurissa on se, että verkon ohjaukseen käytettävät ohjelmistot on mahdollista tuottaa itse juuri sellaisiksi, kuin omassa käytössä oleva verkko vaatii. Normaalissa verkossa voi vain esittää toiveensa valmistajalle, mutta SDN:n avulla pääkäyttäjät kykenevät itse muokkaamaan alustan juuri haluamakseen. Arkkitehtuuri mahdollistaa monet perinteisten verkkolaitteiden tuottamat palvelut ja ominaisuudet hyödyntäen useaa avointa API:a (Application Programming Interface). (ONF White Paper, 2012) Vaikka koko toiminta perustuu avoimen lähdekoodin toimintaan, ovat suuretkin yritykset, kuten Cisco mukana kehittämässä tätä paljon mahdollistavaa uutta teknologiaa. (Cisco, 2013) Monet valmistajat ovat myös mahdollistaneet omissa laitteissaan yleisimmin käytössä olevan hallintaprotokollan, OpenFlow'n käytön. (Feamster ym., 2014)

Nykyaikaisissa konventionaalisissa verkoissa vaaditaan valtava määrä erilaisia laitteita normaalien, verkossa tapahtuvien muiden kuin reititystoiminnallisuuksien toteuttamiseen. Tällaisiksi laitteiksi voidaan lukea esimerkiksi palomuurit, tunkeutumisen havaitsemisjärjestelmät (IDS, Intrusion Detection System), tai muut, esimerkiksi pakettien sisältöä liikenteestä analysoivat järjestelmät (Kreutz ym., 2014). Erään tutkimuksen mukaan vuonna 2011 niitä oli verkossa jo yhtä paljon, kuin reitittimiä (Sherry & Ratnasamy, 2012). Tämä kasvattaa verkkoon liittyen niin kustannuksia ja kompleksisuutta, ja näin ollen tekee ylläpidosta verkon haltijalle jatkuvasti haastavampaa.

SDN:iin pohjautuvassa verkossa nämä toiminnallisuudet kyetään tuottamaan verkkotasolla toimivilla sovelluksilla tai palveluilla, jotka ovat käytettä-

vissä hallintasovelluksen välityksellä tarvittaessa koko verkon alueella (Kuvio 7) (Kreutz ym., 2014). Tässä esimerkissä mm. kytkinten MAC-oppiminen, reititysalgoritmit, IDS-toiminnallisuus sekä kuormantasaus on kaikki toteutettu sovellustasolla SDN:n ohjaamana. Näin kyetään hallinnoimaan selkeästi suurempaa kokonaisuutta kerralla sen sijaan, että jokaista yksittäistä laitetta jouduttaisiin konfiguroimaan uudelleen jokaisen muutoksen myötä. Laajoja verkkoja hallinnoivissa organisaatioissa tai yrityksissä yksittäisten virtuaalikoneiden lisääminen yksin voi tuottaa tuntien tai vuorokausien työn, kun kaikki verkkolaitteiden sisältämät pääsynhallintalistat täytyy päivittää vastamaan uutta kokoonpanoa (ONF White Paper, 2012).



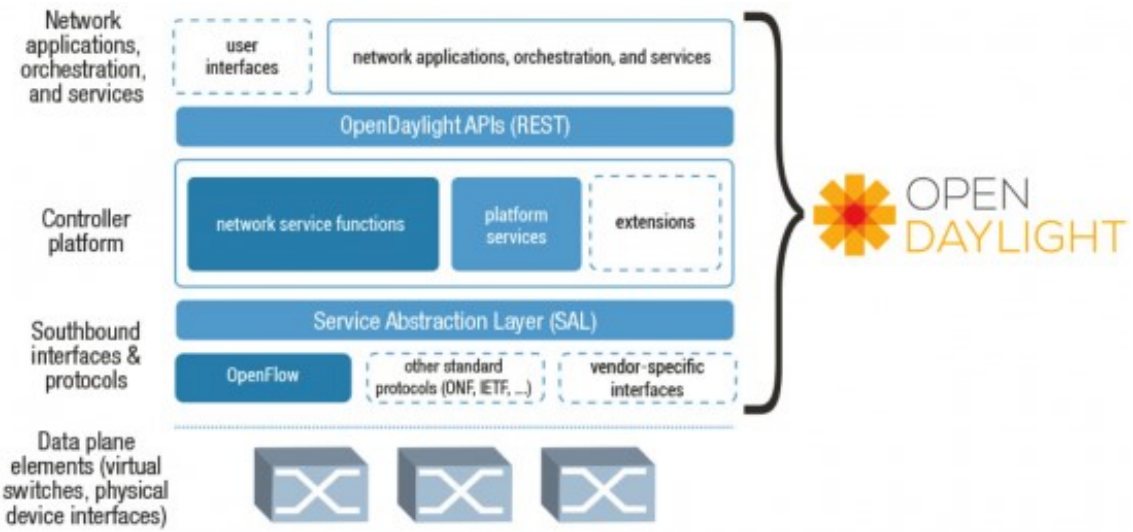
Kuvio 7: Konventionaalinen verkko vs. SDN-verkko. (Kreutz ym., 2014)

3.1 Ohjelmisto ja rajapinnat

OpenFlow-protokolla on ensimmäinen standardoitu rajapinta hallintakerroksen ja tiedonvälityskerroksen välillä. Sen avulla on mahdollista päästä suoraan käsiksi niin fyysisiin kuin virtuaalisiin verkkolaitteisiin. OpenFlow mahdollistaa erilaisten reitityssääntöjen ja -menetelmien luomisen tiedonvälityskerrokselle, sekä niiden muokkaamisen dynaamisesti sovellus-, käyttäjä- tai istuntomäärien mukaisesti aina tarpeeseen vastaten. Se sisältää myös aiempaan reitityksen hal-

lintaan verrattuna merkittävän muutoksen, kun siirrettävissä paketeissa on mahdollista käyttää 13 eri tunnistetta liikenteen ohjaamiseen sen sijaan, kun ennen kaikki ohjaus tapahtui käyttämällä vain kohteen ip-osoitetta. Vaikka OpenFlow itsessään ei kykene toteuttamaan kaikkia näitä toimenpiteitä, sen kyky toimia eri ohjelmistojen hallinnassa rajapintojensa kautta mahdollistaa sille erittäin tehokkaan kyvyn kaikkiin verkkotoimintoihin. (Feamster ym., 2014; ONF White Paper, 2012)

Kontrollerien toiminta perustuu pääasiallisesti siihen, että niiden Southbound API:na käytetään standardinomaisesti OpenFlow'ta, mutta Northbound API on pitkälti muokattavissa ja sovellettavissa eri sovelluskehittäjien omien tarpeiden ja halujen mukaan. Tämä johtuu monilta osin siitä, että olemassaolevilla sovelluksilla on tiettyjä tarpeita omille rajapinnoilleen, eikä SDN:lle ole vielä kyetty määrittelemään yhtenäistä standardia sovellusten kanssa kommunikoimiselle. (Nadeau & Gray, 2013) Yksi esimerkki avoimen lähdekoodin SDN-kontrollerista on OpenDaylight, joka hyödyntää useita Southbound-rajapintoja erilaisten verkkolaitteiden kanssa kommunikointiin (Kuvio 8**Virhe. Viitteen lähdettä ei löytynyt.**). OpenDaylight kykenee kommunikoimaan tiedonvälityskerroksen elementeille hyödyntäen niin OpenFlow'ta, muita standardisoituja protokollia, ja jopa valmistajakohtaisia rajapintoja. Sovelluskerroksen kanssa se kommunikoi hyödyntäen REST-rajapintaa. (*OpenDaylight*, 2013)



Kuvio 8: OpenDaylight-kontrollerin toimintaperiaate. (*OpenDaylight*, 2013)

Perinteisissä verkkolaitteissa kommunikaatio käyttöliittymän kautta on usein hidasta, staattista ja vaatii paljon esikonfiguroituja malleja. Yleisimpiä rajapintoja ovat esimerkiksi valmistajakohtaiset komentorivit (CLI), SNMP, CORBA ja NETCONF. Nämä ovat usein rakennettu suoraan verkkolaitteen firmwareen sekä hallintaohjelmistoon. SDN-kontrollerien osalta tilanne on sen sijaan erilainen, koska esimerkiksi OpenDaylightin Northbound API:na toimii useimmiten jonkinlainen REST-pohjainen (Representational State Transfer) API, joka mah-

dollistaa tiedonvaihdon esimerkiksi JSON-sanomilla, jotka voidaan selkeästi määrittää XML:n avulla. (Nadeau & Gray, 2013)

Tällä suoralla northbound-southbound -mallilla kyetään määrittelemään yhden kontrollerin ohjaama kokonaisuus, joka voisi toimia taisteluosastoa ajatellen esimerkiksi kiinteässä kohteessa tai taisteluosaston sisäisen verkon toiminnassa. Tämän skaalaaminen laajemmalle olisi todennäköisesti liian haastavaa, mutta verkon hallintakerrokselle on mahdollista asettaa useampia kontrollereita toimimaan yhteistyössä. Tällöin niiden välinen kommunikaatio voidaan toteuttaa east-west -protokollilla, jotka hallinnoivat sitä, miten saman tasoiset laitteet kommunikoivat verkossa. Näin jokainen erillinen kontrolleri pystyisi runkoverkosta irtautuessaankin toimimaan viimeisimpien saamiensa parametrien mukaisesti, ja sitä kyettäisiin ylläpitämään paikallisesti mahdollisuuksien mukaan. (Jammal ym., 2014)

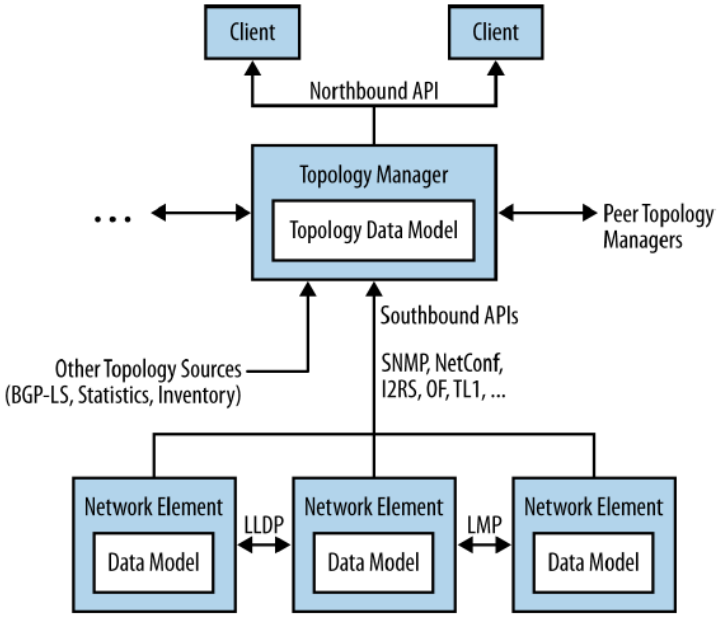
3.2 Verkkotopologiat ja SDN

Koska SDN on täysin ohjelmisto-ohjattu verkkoarkkitehtuuri, ja kaikki verkkolaitteet voivat olla käytännössä virtualisoituja, täytyy olla jokin keino rakentaa sille verkkotopologia ilman olemassa olevaa fyysistä topologiaa. Yksi vaihtoehto tämän saavuttamiseksi on rakentaa jonkinlainen topologiakontrolleri SDN-kontrollerin osaksi tai toiminteeksi. Tällöin tarvitaan ensin jonkinlainen kyky kerätä tietoa verkon vallitsevasta topologiasta, joko suoraan reititysprotokollilta tai manuaalisesti. (Nadeau & Gray, 2013)

Eräs potentiaalinen ehdokas hoitamaan tätä kartoitustehtävää on I2RS-pohjainen (Interface to the Routing System) topologiamanageri. I2RS:n keskeisimpiä ominaisuuksia on muun muassa topologiadatan kerääminen useista lähteistä, mukaan lukien verkkolaitteet, reititysprotokollat ja tilastojenkeruu. Vaikka itse I2RS:lle tämä data ei tarjoa muuta kuin tavan luoda selkeä kartta verkon topologiasta, voidaan sen avulla tarjota sovelluskerrokselle kykyä valita paremmin haluamansa liikennöintitavat verkossa. (Nadeau & Gray, 2013) I2RS-pohjaisen topologiamanagerin havainnekuva on esitetty alla (Kuvio 9).

Suunniteltaessa muutoksia verkon topologiaan tai sen hyödyntämiseen entistä tehokkaammin, on tärkeää saada kartoitettua verkosta myös ne laitteet tai niiden osat, jotka eivät ole aktiivisessa käytössä. Tämä on mahdotonta pelkästään reititysprotokollien tietoihin pohjautuvassa tiedonkeruussa, sillä ne tunnistavat vain aktiiviset laitteet verkossa. Kaikki sillä hetkellä verkosta irrotetut tai inaktiiviset portit ja laitteet näyttävät siltä, kuin niitä ei olisi olemassakaan. Laitteet itsessään sen sijaan ylläpitävät tilatietoja omasta konfiguraatiostaan ja liitynnöistään, jolloin niiden kautta pystytään keräämään tarvittavat tiedot käytössä olevista resursseista. I2RS:aa hyödyntävän topologiamanagerin tapauksessa verkkoelementit vaihtavat tietoa keskenään käyttäen LLDP:ia (Link Layer Discovery Protocol) tai LMP:ia (Link Management Protocol), jonka jälkeen ne voivat välittää tietonsa kontrollerille hyödyntäen mitä vain sen käytössä olevaa Southbound API:a. I2RS:n merkittävin ero esimerkiksi OpenFlow'n

keskitettyyn hallintamalliin kaikessa pakettien liikennöinnissä on kyky jalkauttaa käyttöön perinteisiä reititysprotokollia. (Nadeau & Gray, 2013)

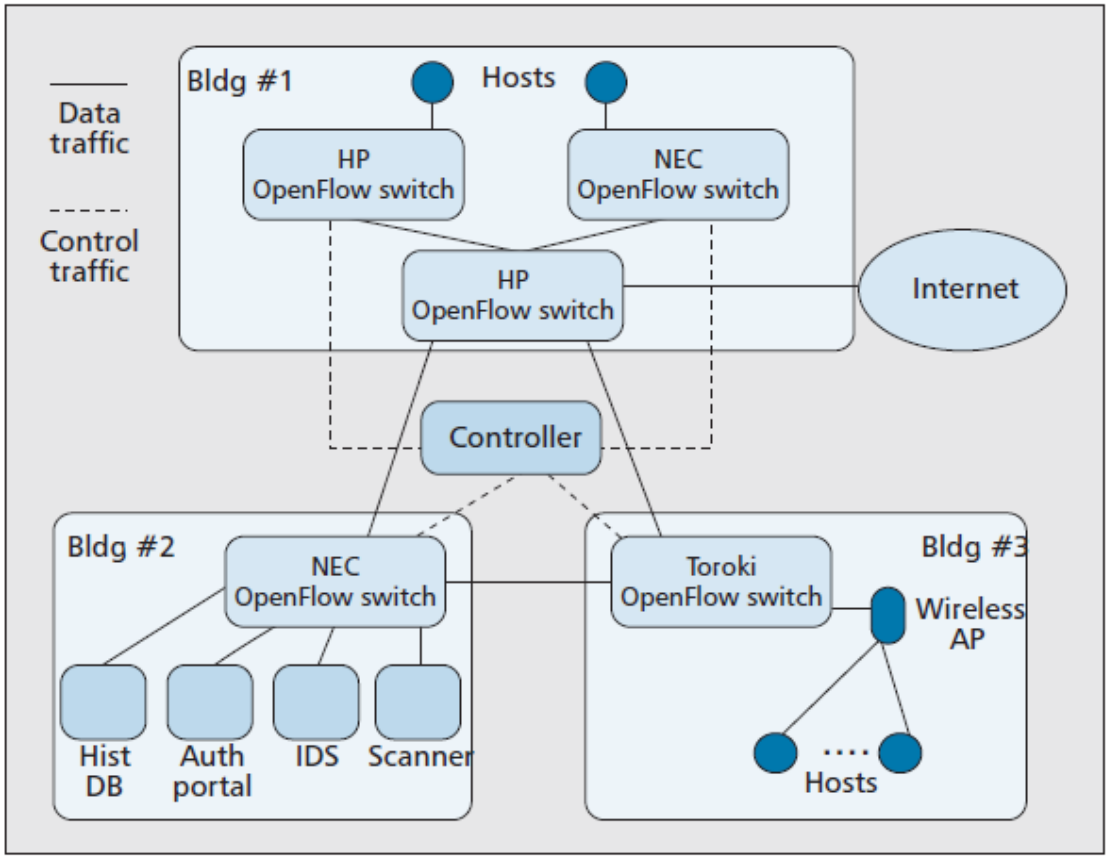


Kuvio 9: I2RS-topologiamanagerin toimintaperiaate. (Nadeau & Gray, 2013)

Yksi esimerkki jatkuvasti muuttuvasta topologiasta on esitetty Georgia Techin kampuksella toteutetusta, OpenFlow:n toimintaan pohjautuvasta verkon perusrakenteesta Kimin ja Feamsterin artikkelissa IEEE Communications Magazinessa (Kim & Feamster, 2013). Kyseisessä mallissa (Kuvio 10) nähdään kolmen rakennuksen välille rakennettu useita käyttäjiä palveleva, intra- ja internetpalveluita tarjoava verkko. Sen datakerroksen liikenne tapahtuu kytkimien välityksellä siten, että keskeisenä elementtinä pääsyä ulos sisäverkosta ohjaa yksittäinen HP:n valmistama OpenFlow-kytkin. Hallintaliikenne tapahtuu samassa fyysisessä verkossa, mutta loogisesti hallitaan kaikkia muita, paitsi internetiin yhdistettyä kytkintä. Käyttäjiä otetaan verkkoon niin rakennuksissa 1 kuin 3 sijaitsevien OpenFlow-kytkimien ja langattoman yhteyspisteen kautta, ja lähtötilanteessa ne ovat autentikoimattomassa tilassa, vailla vapaata pääsyä verkkoon. Loppukäyttäjän laitteet jaetaan kahteen virtuaaliseen lähiverkkoon (VLAN) niiden tunnistautumisstatuksen perusteella, ja ne kykenevät liikennöimään täysin eri tavalla statuksestaan riippuen. Laitteiden vaihtaminen näiden kahden eri VLAN:in välillä tapahtuu automatisoidusti, riippuen skannerin ja autentikaatiopalvelun tilasta. (Kim & Feamster, 2013)

Yhdistämisen jälkeen tarkastetaan autentikointi käyttäjätunnus-salasanaparia käyttäen, ja sen jälkeen laitteet siirtyvät ”scanning”-tilaan, jossa ne kykenevät kommunikoimaan vain rakennuksessa 2 sijaitsevan haavoittuvuusskannerin kanssa. Mikäli haavoittuvuuksia ei havaita, siirtyy laite autentikoituun tilaan ja kykenee liikennöimään niin intra- kuin internetissä normaalisti. Jos laitteessa havaitaan haavoittuvuus skannausvaiheessa, tai myöhemmin verkossa ollessaan, se voidaan siirtää limited-tilaan, jolloin sillä ei

ole enää pääsyä verkkoon. Myöskin viisi tuntia kestävä käyttämättömyys palauttaa laitteen autentikoimattomaan tilaan, ja prosessi on aloitettava alusta. (Kim & Feamster, 2013)



Kuvio 10: Georgia Techin SDN-verkko kolmen rakennuksen välillä. (Kim & Feamster, 2013)

Tällainen malli mahdollistaa periaatteessa minkälaisen verkon topologian tahansa, ja ennen kaikkea erinomaisen nopean päätelaitteiden vaihtelun loogisesti eroteltujen verkkojen välillä. Tämä tarjoaa sekä nopeutta että taloudellisuutta, kun järjestelmä ei vaadi fyysistä käyttäjää ja valvojaa, eikä kaikkia verkkolaitteita tarvitse jokaisen käyttäjän tilatiedon muuttuessa päivittää.

4 TUTKIMUKSEN TOTEUTUS JA SEN MENETELMÄT

Tässä pääluvussa on tarkoitus selventää tutkimuksessa käytettyjä tutkimusmenetelmiä, sekä perustella tutkimuksen toteutuksessa käytettyjä tarkennuksia ja rajauksia. Tämän tutkimuksen menetelmävalinta on pohjautunut niin sillä saavutettavaan tutkimukselliseen hyötyyn, kuin myös käytössä oleviin resursseihin. Taustalla ovat vaikuttaneet myös tutkijan aikaisemmat kokemukset eri tutkimusmenetelmistä, sekä eri menetelmien mahdollisuus tuottaa laadukkaita vastauksia johdannossa esitettyihin tutkimuskysymyksiin.

Tutkimus on toteutettu laadullisena tutkimuksena. Tätä lähestymistapaa puoltavat niin aiemman, sotilaskontekstissa käsiteltävien ohjelmisto-ohjattujen verkkojen aiemman tutkimuksen puute, kuin tutkijan käytössä olevat resurssit ja mahdollisuudet toteuttaa teknisiä testauksia erilaisia järjestelmiä käyttäen. Tällä lähestymistavalla mahdollistetaan kartoittava tutkimus, joka tunnistaa erilaisia merkitseviä muuttujia tietyissä skenaarioissa, ja jonka tuloksia voidaan hyödyntää suunniteltaessa saman aihepiirin määrällisiä tutkimuksia tulevaisuudessa (Kaplan & Maxwell, 2005).

4.1 Tutkimusongelma

Tämän tutkimuksen kohteena ovat ohjelmisto-ohjatun verkon sovellutukset verkon hallinnassa ja valvonnassa. Tutkimuksen tarkoitus on arvioida sitä, kuinka ohjelmisto-ohjattu verkko pystyy tuottamaan suojaominaisuuksia perinteisiin verkkoihin kohdistuvia uhkia vastaan taisteluosaston jatkuvasti liikkuvassa ja muuttuvassa verkkoarkkitehtuurissa. Omassa sotatieteiden pro gradu -tutkielmassani (Rantamäki, 2018) tutkin taisteluosastoon kohdistuvia kyberuhkia, mutta niiden minimointiin johtavia toimenpiteitä ei ole vielä analysoitu riittävästi. Kuten johdannossa todettiin, tässä tutkimuksessa vastataan seuraavaan pääkysymykseen:

- Mikä on ohjelmisto-ohjattujen verkkojen kyky toimia puolustuksellisena elementtinä kenttäviestijärjestelmän teknisessä ympäristössä?

Lisäksi vastataan seuraavaan kolmeen alakysymykseen:

- Minkälaiset verkkotopologiat tai niiden muutokset tarjoavat suojaa potentiaalista hyökkääjää vastaan?
- Kuinka ohjelmisto-ohjattuja verkkoja voitaisiin hyödyntää kenttäviestijärjestelmän osana?
- Minkälaisia kyberpuolustuksellisia elementtejä ohjelmisto-ohjatut verkot tarjoavat?

Tämä on ajankohtainen ongelma siinä mielessä, että kyberuhkien jatkuvasti yleistyessä ja niiden merkityksen kasvaessa niiden torjunnan merkitys kasvaa samassa suhteessa. Samalla taistelevien joukkojen kenttäviestijärjestelmiltä vaaditaan yhä korkeampaa suorituskykyä, kun informaatio siirtyy analogisesta puheesta ja karttaan piirretyistä kuvioista ip-pohjaiseksi puheeksi ja karttatiedostoiksi.

4.2 Aineistonkeruumenetelmä

Tämän tutkimuksen aineistonkeruu tapahtuu perinteisen kirjallisuustutkimuksen keinoin. Teoriaosio rakentuu olemassa olevan kirjallisuuden ja monista eri lähteistä yhdistellyn kuvan päälle, ja sillä pyritään tuottamaan lukijalle riittävä käsitys empiirisen osion tuottamille vastauksille ja niiden syntyyn vaikuttaville lähtökohdille ja ilmiöille (Lappalainen & Jormakka, 2004). Kirjallisuusosion avulla on tarkoitus hahmottaa lukijalle taisteluosaston käytössä olevan kenttäviestijärjestelmän, verkkotopologioiden ja ohjelmisto-ohjattujen verkkojen perusteita sekä niiden välisiä suhteita, jotta niitä yhdistelemällä voidaan saavuttaa vertailukelpoisia, tieteellisiä tuloksia.

Taisteluosaston kenttäviestijärjestelmää käsittävässä luvussa on hyödynnetty vuonna 2018 valmistunutta pro gradu -tutkielmaani ”Taisteluosastoon kohdistuvat kyberuhkat”, mutta aihepiiriä on laajennettu lisäämällä käsittelyyn myös verkkotopologiat ja niiden mahdollisuudet ja vaikutukset tässä asiayhteydessä (Rantamäki, 2018). Ohjelmisto-ohjattujen verkkojen osiossa on yritetty löytää useita eri näkökulmia verkkojen perusrakenteen muodostumiseen niin avointen lähteiden yhteisön kuin tutkijoiden julkaisuista viimeisen 10 vuoden ajalta. Oppikirjatyyppinen materiaali on jätetty tarkoituksenmukaisesti pois aineistosta, sillä tutkimustuloksia tarkastelemalla on helpompi seurata niin ohjelmisto-ohjattujen verkkojen kehitystä ajallisesti, sekä sen haasteita ja mahdollisuuksia.

4.3 Analyysimenetelmä

Tutkimuksen analyysimenetelmänä käytetään aineistolähtöistä sisällönanalyysia. Tavoitteena on mahdollisimman kompaktisti, mutta riittävän kattavasti yhdistellä aiemmista tutkimuksista saavutettuja tuloksia vallitsevien teorioiden kanssa, ja pyrkiä saavuttamaan näiden pohjalta potentiaalisia uusia tutkimustuloksia. Tutkimuksen päälähestymistapa on suunnittelututkimus, jossa on tunnistettu ongelma, ja siihen pyritään tuottamaan jonkinlainen ratkaisuehdotus. Monesti suunnittelututkimuksissa pyritään tuottamaan jonkinlainen konkreettinen lopputuote, joka ratkaisee tämän ongelman, mutta se ei aina ole vaatimus tälle tutkimustyypille. Tämän tutkimuksen puitteissa ennemminkin tarjotaan erilaisia metodologisia vaihtoehtoja tälle ratkaisulle, mutta sen tekniset yksityiskohdat jätetään tutkimuksen luonteen takia huomiotta. (Peffers ym., 2007)

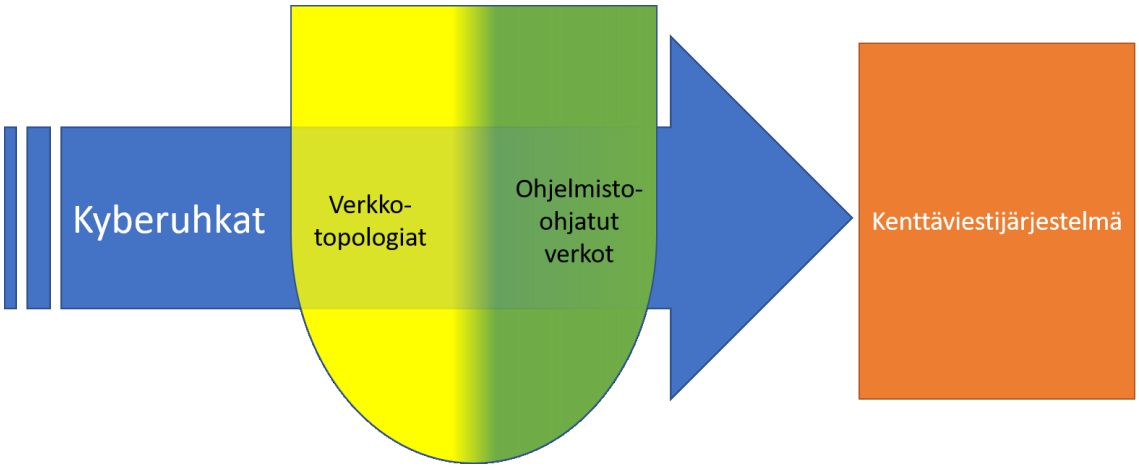
Peffersin (2007) tutkimuksessa on tutkittu seitsemää suunnittelututkimusta määrittelevää aiempaa teosta, ja niistä on tunnistettu yhteisiä elementtejä. Suunnittelututkimusta tehtäessä työskentely jakautuu niiden mukaan käytännössä kuuteen vaiheeseen. Ne ovat:

1. **Ongelman tunnistaminen ja tutkimuksen tarve**: Määritellään tutkimusongelma ja perustellaan se, miksi siihen kehitetyllä ratkaisulla on arvoa. Tämän tarkoitus on motivoida niin tutkija kuin lukijat hyväksymään ja ymmärtämään ongelma ja mahdolliset ratkaisut.
2. **Ratkaisun tavoitteiden määrittäminen:** Ongelman määrittelyn ja ratkaisujen realistisuuden hahmottamisella voidaan tuottaa tavoitteita ratkaisulle. Tämä tarjoaa mahdollisuuden tuottaa joko määrällisin mittarein laskettavia parannuksia, tai laadullisesti tarkasteltuna uuden ratkaisun tuottamaa ratkaisua ongelmaan.
3. **Suunnittelu ja kehitys:** Luodaan tuote. Tuote voi olla joko malli, menetelmä, joukko ominaisuuksia tai jonkinlainen konkreettinen väline ongelman ratkaisemiseksi. Periaatteessa mikä tahansa voi olla tämän määritelmän mukaan tuote, kunhan se tuottaa jonkinlaisen tutkimuksellisen kontribuution. Tässä vaiheessa määritellään ensin tuotteen haluttu toiminnallisuus ja rakenne, ja lopuksi toteutetaan se.
4. **Demonstraatio:** Demonstroidaan tuotteen kykyä ratkaista yksi tai useampi ongelman ilmentymä. Tämä voidaan toteuttaa joko kokeellisesti, simuloituna, tapaustutkimuksena tai millä tahansa muulla soveltuvalla menetelmällä.
5. **Arviointi:** Arvioidaan tuotteen tarjoamia ratkaisuja ongelmaan. Tässä vaiheessa on mahdollista esimerkiksi verrata tavoitteita demonstraatiossa saavutettuihin tuloksiin. Tässäkin tapauksessa arviointi voi perustua empiirisiin tuloksiin tai loogisiin todistuksiin. Lopuksi tutkijalla on mahdollisuus joko palata vaiheeseen 3 korjatakseen tuotettaan, tai jättää potentiaaliset haasteet jatkotutkimuksille riippuen tutkimuksen luonteesta.

6. **Kommunikointi:** Kun mahdollista, kommunikoi ongelmasta ja sen tärkeydestä, tuotteesta, sen käytettävyydestä ja uutuudesta, sen suunnittelun laadukkuudesta ja vaikuttavuudesta niin muille tutkijoille kuin kiinnostuneelle yleisölle. (Peffers ym., 2007)

Nämä kuusi ovat nimellisesti aikajärjestyksessä, mutta mikään ei suoranaisesti pakota tutkijaa noudattamaan tätä tiukasti. Riippuen siitä, syntyykö tarve tutkimukselle esimerkiksi aikaisemman tutkimuksen esityksistä jatkotutkimusaiheiksi, itse tunnistetusta tarpeesta jonkin tuotteen kehittämiselle, tai olemassa olevan ratkaisun hyödyntämättömyydestä ongelman kontekstissa, voi tutkija hyvinkin aloittaa prosessin vastaavasti askeleista 1, 2 tai 3 ja edetä siitä niin eteen- kuin taaksepäin tarpeen mukaan. (Peffers ym., 2007)

Näillä tutkimusmenetelmillä ja tutkimukseen kriittisimmin kuuluvien termien avulla muodostuu tutkimuksen teoreettinen viitekehys, joka on esitetty alla (Kuvio 11). Sen tarkoitus on kuvata tutkimusasetelmaa, jossa taustalla todettuun haasteeseen taisteluosastoon kohdistuvista kyberuhkista pyritään vastaamaan tuottamalla niin verkkotopologioihin kuin ohjelmisto-ohjattuihin verkkoihin perustuvia puolustusmenetelmiä.

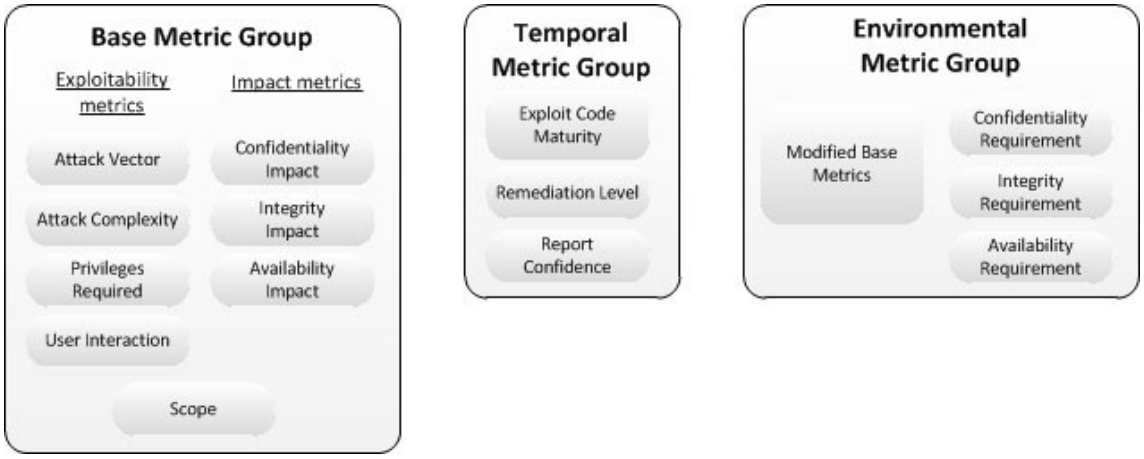


Kuvio 11: Tutkimuksen teoreettinen viitekehys.

5 TAISTELUOSASTON KONVENTIONAALISEN VERKKOARKKITEHTUURIN UHKASKENAARIOT

Tietoverkoissa toimivia laitteita ja niihin kohdistuvia hyökkäyksiä arvioitaessa on mahdollista tarkastella asiaa lähes mistä näkökulmasta tahansa, tarpeeseen perustuen. Koska tämän tutkielman puitteissa ei ole tarkoituksenmukaista suorittaa laajamittaista uhka-analyysia koko taisteluosaston verkolle, vaan keskittyä sen uhkien vastatoimiin, otetaan käsittelyyn valmiiksi analysoidut uhkat. Nämä uhkat on tunnistettu ja arvioitu aiemmin omassa pro gradu -tutkielmassani (Rantamäki, 2018) CVSS (Common Vulnerability Scoring System) v3.0 -arviointikriteeristön avulla, ja tässä luvussa esitellään lyhyesti sekä kriteeristön pääkohdat että tunnistetut uhkat.

CVSS on FIRST:n (Forum of Incident Response and Security Teams) julkaisema, informaatioturvallisuuden CIA-malliin perustuva arviointikriteeristö. Se rakentuu kolmeen ryhmään jaetuista kriteereistä: perus-, ajalliset ja ympäristömuuttujat. Näistä perusmuuttujat on vielä periaatteessa eritelty haavoittuvuuksien hyödynnettävyyteen ja niiden vaikutukseen. Tämä perusrakenne on esitelty alla (Kuvio 12). Vuonna 2019 on julkaistu myös uudempi versio, 3.1, mutta tämän perusmuuttujat ovat edelleen samat kuin aiemmassa mallissa, eivätkä näin ollen vaikuta ratkaisevasti vuotta aiemmin tunnistettujen uhkien luokitteluun. Kaikkeen laskentaan on FIRST:n internetsivustolla tarjolla laskuri, mutta myös manuaaliseen laskentaan on tarjolla kokoelma kaavoja eri muuttujien vaikutuksien huomioimiseksi. (*Common Vulnerability Scoring System v3.0: Specification Document*, 2015)



Kuvio 12: CVSS v3.0 –arviointikriteeristön muuttujien jako. (*Common Vulnerability Scoring System v3.0: Specification Document*, 2015)

Lyhyesti kuvailtuna yllä mainitut muuttujat määritellään seuraavalla tavalla:

1. Attack Vector: Kuinka kaukaa verkon yli hyökkääjä kykenee vaikuttamaan kohdejärjestelmään? Ulkoverkosta, sisäverkosta, laitteen tiedostoista vai fyysisesti?
2. Attack Complexity: Onko sellaisia olosuhteita, joihin hyökkääjä ei voi vaikuttaa, mutta joiden täytyy toteutua hyökkäyksen onnistumiseksi?
3. Privileges Required: Mitä käyttöoikeuksia hyökkääjältä vaaditaan hyökkäyksen onnistumiseksi?
4. User Interaction: Vaaditaanko hyökkäyksen onnistumiseksi jonkun muun käyttäjän, kuin hyökkääjän toimintaa?
5. Scope: Voiko haavoittuvan osan avulla hyödyntää mahdollisuutta edetä järjestelmän sisällä ohi pääsynhallinnan (escalation of privileges)?
6. Confidentiality Impact: Hyökkäyksen vaikuttavuus tiedon luottamuksellisuutta kohtaan.
7. Integrity Impact: Hyökkäyksen vaikuttavuus tiedon luotettavuuteen.
8. Availability Impact: Hyökkäyksen vaikuttavuus kohdepalvelun tai -tiedon saatavuuteen.
9. Exploit Code Maturity: Hyökkäyksessä käytettävän koodin kypsyys ja todennäköisyys sille, että sitä käytetään juuri kyseiseen haavoittuvuuteen (proof-of-conceptista täysin autonomiseen koodiin)
10. Remediation Level: Haavoittuvuuteen saatavilla olevien korjausmenetelmien taso.
11. Report Confidence: Kuinka luotettavia ja yksityiskohtaisia haavoittuvuudesta julkaistut tiedot ovat?
12. Confidentiality Requirement: Haavoittuvuutta koskettavan järjestelmän luottamuksellisuuden vaatimustaso.

13. Integrity Requirement: Haavoittuvuutta koskettavan järjestelmän luotettavuuden vaatimustaso.
14. Availability Requirement: Haavoittuvuutta koskettavan järjestelmän saatavuuden vaatimustaso. (*Common Vulnerability Scoring System v3.0: Specification Document*, 2015; Rantamäki, 2018)

Näitä kriteereitä vertailemalla CVSS-laskin (*Common Vulnerability Scoring System Version 3.0 Calculator*, 2020) tuottaa 3 erillistä, vertailukelpoista pistemäärää jokaiselle uhkalle. Ensin lasketaan suoraan kahdeksan ensimmäisen kohdan perusteella Base Score, joka perustuu käytännössä pelkästään teknisistä yksityiskohdista ja kohteen ominaisuuksista muodostuvaan uhkakuvaan. Tämän jälkeen saatuun pistemäärään yhdistetään kertoimet sen mukaan, kuinka muuttujat 9–11 vaikuttavat uhkan ajalliseen ulottuvuuteen, ja näin saadaan uhkalle Temporal Score. Lopullisen arvosanan, jota tässä arviossa on käytetty vertailuun – Environmental Scoren – saamiseen yhdistetään vielä edelliseen mukaan ympäristölliset tekijät, eli muuttujat 12–14. Kun uhkan perustiedot, ajalliset tekijät sekä haavoittuvan ympäristön tekijät yhdistetään, saadaan mahdollisimman kattava ja vertailukelpoinen tilanne eri uhkaskenaarioiden välille. (*Common Vulnerability Scoring System v3.0: Specification Document*, 2015; Rantamäki, 2018)

Uhkat ovat luonteeltaan verrattain geneerisiä, koska spesifit yksityiskohdat vaatisivat tarkkojen laitemallien ja niissä käytettyjen teknologioiden tuntemusta. Näin ollen niiden osalta ei voida tehdä suoria esityksiä potentiaalisiksi vastatoimiksi, vaan tarjota vaihtoehtoja erilaisiin uhkaskenaarioihin eri laitetyyppeihin kohdistuvissa hyökkäyksissä. Aiemmin tunnistettuihin uhkiin kuitenkin liitetään tarkentavia määreitä esimerkiksi fyysisestä sijainnista taisteluosaston verkossa, mikäli ne tarjoavat jonkinlaisen muutoksen verrattuna siihen, että ne olisivat missä tahansa vastaavassa laitteessa. Jokaisesta uhkasta on myös tunnistettu sekä todennäköinen että vaarallinen vaihtoehto, joista pyritään käsittelemään todennäköistä vaihtoehtoa, vaikka se vaatisi pieniä muutoksia.

5.1 Hyökkäys reitittimeen

Yleisesti ottaen hahmoteltaessa konventionaalisen verkon niin loogista kuin fyysistä laiterakennetta, ovat reitittimet verkon kriittisin osa. Niiden välille muodostuu käytännössä koko verkon runko, ja jokaisen runkoa muodostavan reitittimen alueella toimii todennäköisesti oma, pienempi aliverkkonsa. Näissä toimivat laitteet voivat liikennöidä omassa verkossaan joutumatta huomioimaan runkoreitittimen muita liikennöintisuuntia, mutta kaikki aliverkosta ulospäin lähtevä liikenne kulkee tämän yhden, kriittisen reitittimen kautta. Todennäköiseksi hyökkäykseksi on tunnistettu haittaohjelman toimittaminen ja asentaminen reitittimeen, ja sen analysoidut CVSS-arvot on esitetty alla (Taulukko 1) (Rantamäki, 2018).

Taulukko 1: Reitittimen todennäköisen uhkakuvan CVSS-arvio. (Rantamäki, 2018)

Kriteeri	**Lyhenne**	**Arvo**				
Attack Vector	AV	Network (N)	**Adjacent (A)**	Local (L)	Physical (P)	
Attack Complexity	AC	Low (L)	**High (H)**			
Privileges required	PR	None (N)	Low (L)	**High (H)**		
User Interaction	UI	**None (N)**	Required (R)			
Scope	S	**Unchanged (U)**	Changed (C)			
Confidentiality	C	**None (N)**	Low (L)	High (H)		
Integrity	I	None (N)	**Low (L)**	High (H)		
Availability	A	None (N)	Low (L)	**High (H)**		
Exploit Code Maturity	E	Not Defined (X)	Unproven (U)	Proof-of-Concept (P)	**Functional (F)**	High (H)
Remediation Level	RL	Not Defined (X)	Official Fix (O)	Temporary Fix (T)	**Workaround (W)**	Unavailable (U)
Report Confidence	RC	Not Defined (X)	Unknown (U)	**Reasonable (R)**	Confirmed (C)	
Confidentiality Req.	CR	Not Defined (X)	**Low (L)**	Medium (M)	High (H)	
Integrity Req.	IR	Not Defined (X)	Low (L)	**Medium (M)**	High (H)	
Availability Req.	AR	Not Defined (X)	Low (L)	Medium (M)	**High (H)**	

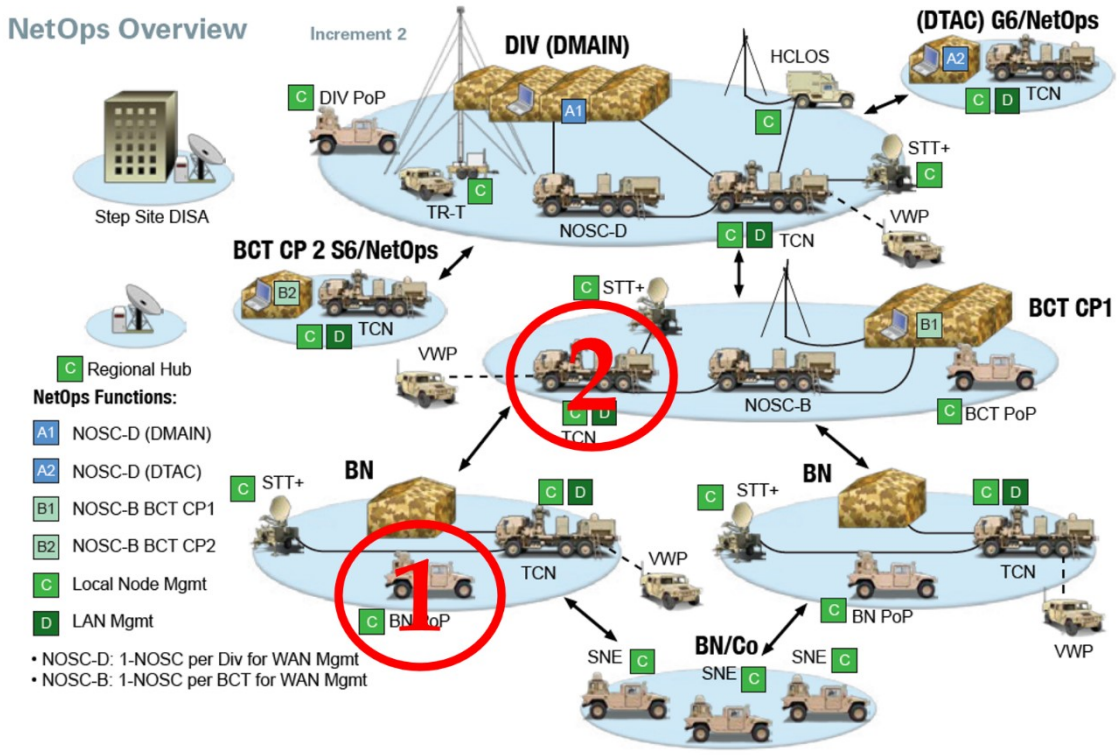
Esimerkkitapauksessa haittaohjelma kyetään toimittamaan reitittimeen verkon yli, mutta kuitenkin vain siten, että hyökkääjä on valmiiksi samassa fyysisessä tai loogisessa verkossa kohdelaitteen kanssa, koska runkoverkon tietoturvan oletetaan olevan korkealla tasolla. Tämän lisäksi hyökkäyksen katsotaan olevan hienostunut, sillä sen täytyisi kyetä valikoimaan kohdelaitteensa riittävällä tarkkuudella ilman suorituksen aikaista ohjausta. Käyttöoikeuksien osalta vaaditaan erilliset järjestelmänvalvojan oikeudet, joita ilman ei pääse muuttamaan kriittisiä ominaisuuksia reitittimessä. (Rantamäki, 2018)

Koska reititin on myös luonteeltaan verrattain staattinen verkkolaite, on epätodennäköistä odottaa, että sitä operoitaisiin jatkuvasti. Näin ollen käyttäjän toimenpiteitä ei edellytetä myöskään hyökkäykseltä. Hyökkäyksen ei myöskään uskota laajentuvan samassa verkossa toimiviin muihin laitetyyppeihin, vaan pyrkivän vaikuttamaan nimenomaan reitittimeen liikennettävä haittaavalla tavalla. Aiemmin todettiin, että hyökkäys ei kykene kulkemaan sisään runkoverkon reititinhyppyjen kautta, ja tästä syystä oletetaan, että hyökkäys ei myöskään kykene siirtämään tietoja ulos haluamaansa kohteeseen käytännössä lainkaan. Tämä pitää tietojen luottamuksellisuuteen kohdistuvan uhkan mität-

tömänä. Eheyteen sen sijaan pyritään varmasti vaikuttamaan muokkaamalla reitittimen sisältämiä tietosisältöjä. Olivat kyseessä sitten peruskonfiguraatiot tai reititintaulut, niiden tiedot pyritään muuttamaan, mutta tämä on havaittaessa kohtalaisen helposti korjattavissa, jolloin eheyteen kohdistunut uhka on matala. Reitittimen tapauksessa ehdottomasti kriittisin uhka kohdistuu lähes poikkeuksetta saatavuuteen, ellei sen tietoturva ole täysin olematon. Pahimmillaan tällainen yksittäisen reitittimen lamauttaminen saattaisi sulkea suuren joukon tietoliikenneyhteyksien osalta oman onnensa nojaan, tai pakottaisi ainakin turvautumaan vaihtoehtoisiin menettelyihin täyden kapasiteetin sijaan. Base Score tällaisella uhkalla on 4,8 (Medium), eli ei puhuta sinänsä vielä kovinkaan tuhoisasta uhkasta. (Rantamäki, 2018)

Kun siirrytään tarkastelemaan ajallisen ulottuvuuden muuttujia, nousee esiin se, että hyökkäyksiä ei ole välttämättä ehditty valmistella täysin piiloutuviksi, hienostuneiksi ja tuhovoimaisiksi, mutta se ei välttämättä ole tarpeen nopeatempoisessa taistelutilanteessa. Oletuksena hyökkääjällä on kuitenkin hallussaan toimivaa, testattua haittaohjelmakoodia jota ei tarvitse luoda täysin tyhjästä, mutta sen tarkka räätälöinti saattaa olla vielä tekemättä. Samasta syystä myös puolustuskeinoja oletetaan löytyvän ainakin workaround-tasolla – jos haittaohjelma ei leviä aggressiivisesti, reitittimen ohjelmisto kyetään todennäköisesti uudelleenasentamaan jonkinlaiseen peruskonfiguraatioon siedettävässä ajassa ja reititysprotokollat huolehtivat reititystaulujen uudelleen kokoamisesta sen jälkeen. Kun hyökkäys todennäköisimmin kohdistuu saatavuuteen, eikä sitä ole ehditty viimeistellä täysin, se saadaan myös kohtalaisen suurella todennäköisyydellä paikannettua ja analysoitua luotettavasti. Käyttöperiaatteissa havaitaan todennäköisesti viitteitä vastaavanlaisista hyökkäyksistä muita yrityksiä tai valtioita vastaan, jolloin muista lähteistä voidaan saada omaa analyysia tukevia tietoja. Temporal Score on näin ollen vain 4,4 – jopa alhaisempi kuin Base Score – koska olosuhteet tukevat puolustajaa. (Rantamäki, 2018)

Reitittimen toiminnassa on syytä huomioida erityisen tarkasti kriittiset, verkon toiminnan kannalta ratkaisevat vaatimukset. Luotettavuuden osalta ei ole tarpeen vaatia tällaisessa hyökkäyksessä korkeaa tasoa, koska hyökkääjä on todennäköisesti saanut tiedustelun avulla tarvitsemansa tiedon reitittimestä ennen hyötykuorman toimittamista kohteeseen, eikä sieltä ole aiemman arvion mukaan mahdollisuutta toimittaa tietoa ulospäin kovinkaan tehokkaasti. Eheys on hieman merkittävämpi, johtuen etenkin konfiguraatiotiedostojen muokkaamisesta aiheutuvista seurannaisvaikutuksista. Saatavuuden vaatimus on tässä tapauksessa ehdottomasti korkea, koska muutoin pääosa liikenteestä sekä runkoverkon muodostamien asemien välillä pysähtyy, ja potentiaalisesti myös suuri osa viestiaseman/vastaavan alueella toimivasta alueellisen verkon liikenteestä. Kun nämä muuttujat huomioidaan pisteytyksessä, on reitittimeen kohdistuvan uhkan Environmental Score 5,7 (Medium), joka on ehdottomasti huomioitava verkkopuolustusta suunniteltaessa. (Rantamäki, 2018)



Kuvio 13: BCT:n verkon rakenne ja uhkaskenaariot; 1) Pataljoonan verkon laajennussolmu, 2) Prikaatin keskeinen tietoliikennesolmu. (*Warfighter Information Network - Tactical Commander's Handbook Version 2.0*, 2016)

Yllä (**Virhe. Viitteen lähdettä ei löytynyt.**) on esitetty kaksi potentiaalista tilannetta, joissa taisteluosaston verkossa kohdistuisi hyökkäys reitittimeen. Ensimmäisessä tapauksessa – myöhemmin skenaario 1 – hyökkäys kohdistuu pataljoona- tai komppaniatasolla toimivaan viestiasemaan, jonka päätarkoitus on liittää alueella toimivat joukot taisteluosaston verkkoon, ja hallinnoida verkkoaan vain paikallisesti. Toisessa tapauksessa – myöhemmin skenaario 2 – hyökkäys kohdistuu taisteluosaston keskeiseen viestiasemaan, johon on kiinnittyneenä niin satelliittiyhteys, taisteluosaston verkon hallinta- ja valvonta-asema sekä epäsuorasti komentopaikka. Tässä skenaariossa reitittimen sijainnissa on mahdollista hallita niin paikallista verkkoa kuin koko taisteluosaston alueella toimivaa lähiverkkoa. *(Warfighter Information Network - Tactical Commander's Handbook Version 2.0, 2016)*

Skenaario 1 on vaikutuksiltaan todennäköisesti merkittävästi pienempi näistä kahdesta. Sen alueella toimii vain jokin osa suuremmasta taistelevasta joukosta, ja sen kautta kulkeva tietoliikenne on määrältään pienempi ja verkon fyysisen rakenteen kannalta vähemmän merkitsevä. Jos sijaintia ajatellaan fyysisen topologian kautta, kyseinen kohde on joko tähden yksittäinen sakara tai mesh-verkon reunapiste, jonka ei pitäisi olla, ainakaan suunnittelun niin mahdollistaessa, kriittinen solmu muun verkon osalta. Loogista topologiaa ajatellen sen kannattaa olla kutakuinkin vastaavassa roolissa, koska sillä ei ole laajaa kattavuutta yhteyksien osalta, eikä myöskään merkittävää kykyä verkon operointiin. Mikäli hyökkäys kykenisi vaikuttamaan reitittimeen, se sulkisi tällöin lä-

hinnä alueellisen joukon pois taisteluosaston johtamisjärjestelmästä, ja ongelmaa kyettäisiin ratkomaan niin paikallisesti kuin taisteluosaston yhteiseltä verkon valvonta- ja hallinta-asemalta.

Skenaario 2 olisi merkittävästi vaarallisempi taisteluosaston näkökulmasta. Se kohdistuu verkkotopologian kannalta ratkaisevaan pisteeseen, puhuttiin sitten loogisesta tai fyysisestä topologiasta. Jos puhutaan taisteluosaston lähiverkosta, se olisi tähtitopologian keskipiste tai mesh-verkossa keskeinen solmu. On kuitenkin tärkeä muistaa, että tämän aseman kautta tapahtuu myös liikennöinti ylempään johtoportaaseen, kuten kuviossa 13 esitettyyn divisioonaan. Näin ollen se on runkoyhteyksiä ajatellen ainut liityntä kahden erillisen verkon välillä, jolloin hyökkäyksen toteutuessa ainoaksi yhteysmenetelmäksi johtoportaiden välillä jäisi pataljoonaan mahdollisesti saatava suora satelliittiyhteys. Tilanteen korjaaminen voisi olla haastavaa etäyhteyksin, mutta suora kaapeliyhteys verkon valvonta- ja hallinta-asemaan tarkoittanee kohtuullisen nopeasti saavutettavaa lähitukea.

5.2 Hyökkäys työasemaan

Tässä tutkimuksessa tarkastellaan työasemaa lähtökohtaisesti geneerisenä loppukäyttäjätyöasemana taisteluosastossa. Tämä rajaa pois alkutilanteesta esimerkiksi verkon valvonta- ja hallintatyöasemat sekä järjestelmänvalvojan työasemat, jotka täytyisi arvioida täysin omana kategorianaan käyttöoikeuksiensa vuoksi. Tällöin voidaan olettaa, että työasema sisältää sotilaalliseen suunnitteluun tarvittavat perusohjelmistot: kuvankäsittely, tekstinkäsittely, tallentamiseen tarkoitettu päätelaitteen oma levyasema tai mahdollinen verkkolevy ja joukkotyypin käytössä olevat spesifit johtamis- ja tietojärjestelmät. Koska aiemmin (Rantamäki, 2018) tunnistetuissa uhkissa työasemaan kohdistuva todennäköinen uhka sai vain pistemäärän 2,8 ja oli näin ollen erittäin matala, tarkastellaan tässä tutkimuksessa vaarallisinta vaihtoehtoa. Työasemaan kohdistuvan vaarallisimman uhkan CVSS-arvio on esitetty alla (Taulukko 2).

Taulukko 2: Työaseman vaarallisimman uhkakuvan CVSS-arvio. (Rantamäki, 2018)

Kriteeri	**Lyhenne**	**Arvo**				
Attack Vector	AV	**Network (N)**	Adjacent (A)	Local (L)	Physical (P)	
Attack Complexity	AC	Low (L)	**High (H)**			
Privileges required	PR	None (N)	Low (L)	**High (H)**		
User Interaction	UI	**None (N)**	Required (R)			
Scope	S	Unchanged (U)	**Changed (C)**			
Confidentiality	C	None (N)	Low (L)	**High (H)**		
Integrity	I	None (N)	Low (L)	**High (H)**		
Availability	A	None (N)	Low (L)	**High (H)**		
Exploit Code Maturity	E	Not Defined (X)	Unproven (U)	Proof-of-Concept (P)	Functional (F)	**High (H)**
Remediation Level	RL	Not Defined (X)	Official Fix (O)	Temporary Fix (T)	Workaround (W)	**Unavailable (U)**
Report Confidence	RC	Not Defined (X)	**Unknown (U)**	Reasonable (R)	Confirmed (C)	
Confidentiality Req.	CR	Not Defined (X)	Low (L)	**Medium (M)**	High (H)	
Integrity Req.	IR	Not Defined (X)	Low (L)	**Medium (M)**	High (H)	
Availability Req.	AR	Not Defined (X)	**Low (L)**	Medium (M)	High (H)	

Esimerkkitapauksessa hyökkäys on kyettävä toteuttamaan kohdelaitteeseen selkeästi verkon yli, jopa useamman kuin yhden verkkohypyn yli saavuttaakseen riittävän yllätyksellisyyden. Tällöin uhka saavuttaisi kohteen joko kaukaa reititinverkon yli tai esimerkiksi vastustajan langattomien laitteiden kautta yksittäiseen taisteluosaston viestiasemaan. Joka tapauksessa maantieteellinen paikantaminen ja attribuutio olisi haastavaa tai mahdotonta. Hyökkäykseen liittyvät tiedustelu- ja valmistelutoimeenpanot olisivat mittavat sotilasorganisaation luonteesta johtuen, ja hyökkäyksen toistettavuus saattaisi silti olla vajavainen. Koska kyseessä on loppukäyttäjän työasema, voidaan olettaa, että peruskäyttäjällä ei ole täysiä käyttöoikeuksia. Hyökkäyksen vaikuttavuus kuitenkin edellyttää selkeästi korkeampia käyttöoikeuksia, jolloin se todennäköisesti pyrkisi korottamaan käyttöoikeutensa jonkin haavoittuvuuden kautta. (Rantamäki, 2018)

Hienostuneelta hyökkäykseltä ei oleteta vaadittavan käyttäjän toimintaa toimiakseen. Hyökkäyksen ei myöskään kannata olettaa rajoittuvan pelkästään työasemaan vaarallisessa tapauksessa. Sen sijaan työaseman voi nähdä hyvänä

alustana verkon tiedustelulle ja mahdollisesti muihin verkkolaitteisiin siirtymiselle, koska työasemaohjelmistoissa on suurempi todennäköisyys löytää sisäänpääsyn mahdollistava haavoittuvuus, kuin spesifeissä laitteissa. Kun hyökkäys on oletettavasti päässyt järjestelmään joko reitittimien välityksellä tai jonkin langattoman tukiaseman kautta, sillä voidaan olettaa olevan kyky myös siirtää tietoa ulos samaa reittiä. Näin ollen kaikki tieto, johon työasemalla on pääsy, on oletettavasti vastustajan hallussa ja luottamus täysin menetetty. Jos hyökkäyksellä on pääsy työasemaan, sillä on oletettavasti myös pääsy muokkaamaan sen sisältämää informaatiota hallitusti tai hallitsemattomasti. Eheys on joka tapauksessa menetetty tässäkin tapauksessa, eikä mihinkään työaseman käsittelemään dataan voi suhtautua varauksetta. Saatavuuteen kohdistuu myös täydellisen menetyksen uhka, sillä riittävillä oikeuksilla hyökkääjä voisi sulkea tietoliikenteen molempiin suuntiin työasemalta, ja tarvittaessa tuhota tai esimerkiksi kryptata sen sisältämää dataa. Näistä muodostettu Base Score on 8,0 (High). (Rantamäki, 2018)

Hyökkäyksen kypsyys on saavuttanut korkean tason, ja hyökkäys pyrkii leviämään verkossa ainakin muihin kohdetta vastaaviin päätelaitteisiin, ja tarvittaessa keräämänsä tiedon perusteella muihin verkon laitteisiin. Hyökkäyksen toiminnassa on täysin uusia piirteitä, ja se kykenee mahdollisesti mukauttamaan omaa toimintaansa havaitessaan vastatoimenpiteitä. Näin ollen suoria vastatoimenpiteitä ei kyetä toteuttamaan, mutta joitain yksittäisiä ominaisuuksia kyetään ajallisesti tai paikallisesti rajoittamaan. Koska kyseessä oli vaarallisin uhkakuva, on myös syytä olettaa, että kyseisestä hyökkäyksestä ei ole saatavilla minkäänlaista luotettavaa tietoa ulkoisista lähteistä, ja sisäinen analyysi tulee viemään merkittävästi aikaa. Aikamuuttujien jälkeen saavutettu Temporal Score on 7,4 (High) johtuen Report Confidence -kriteerin hieman erikoisesta luonteesta, jossa ”Unknown” on matalin arvo, vaikka se tarkoittaa, ettei uhkasta ole saatavilla paljoa tai ollenkaan uskottavaa, varmistettua tietoa. (Rantamäki, 2018)

Ympäristömuuttujat eivät riipu niinkään kohteeseen kohdistuvasta uhkasta, vaan itse kohteen luonteesta, ja ne on johdettu todennäköisen uhkan yhteydessä. Yleisenä oletuksena on käytetty sitä, että itse työasemalla ei ole kovinkaan paljon uhkaa aiheuttavia tekijöitä. Tiedostojen sijainti tullee olemaan valmiilla tuotteilla jollain yhteiskäyttöisellä palvelimella tai vastaavalla, mutta niiden muuttaminen saattaisi toteutuessaan silti aiheuttaa suuren riskin. Saatavuus sen sijaan on hyvinkin kierrettävissä, tai työasema korvattavissa uudella hyökkäyksen toteutuessa. Näin ollen uhkan tietoturvavaatimukset ovat kohtalaisen keskitasoisia ja Environmental Score on 7,4 (High). (Rantamäki, 2018)

Työasemaan kohdistuvasta uhkasta on turhaa muodostaa useampaa eri skenaariota, koska alussa todettiin kyseessä olevan geneerinen työasema, jonka tarkoitus on toimia taisteluosaston loppukäyttäjien suunnittelutyökaluna. Työasemaan kohdistuva hyökkäys on näin ollen skenaario 3. Oletetun hyökkäyksen luonteen takia päätelaitteen loogisella tai fyysisellä sijainnilla verkossa ei ole kovinkaan ratkaiseva merkitys muutoin kuin siltä osin, kuinka pienellä hyppymäärällä se kykenee saavuttamaan muita kriittisiä laitteita taisteluosas-

ton sisällä tai muissa verkoissa, joihin se on liittyneenä. Topologisesti päätelaite ei suoranaisesti ole verkossa muuta, kuin päätepiste mallista riippumatta, sillä se ei ohjaa verkkoliikennettä useampaan eri suuntaan. Etenemismekanismeistaan tai vaikuttamismahdollisuuksistaan johtuen voidaan kuitenkin huomioida se, että potentiaaliset korjaustoimenpiteet tai vastatoimet verkossa tapahtuvaan hyökkäykseen voidaan toteuttaa paikallisesti tai etänä sijainnista riippumatta.

5.3 Hyökkäys tiedostopalvelimeen

Koska nykyaikaiseen sodankäyntiin liittyy usein hyvin voimakkaasti erilaisten suunnitelmien, tilannekuvatuotteiden tai esittelyaineistojen laadinta, vaaditaan usein taistelevan joukon käyttöön jonkinlainen tiedostonjakopalvelu. Koska yhteiseen käyttöön tarkoitettuja asiakirjoja ei ole tarkoituksenmukaista säilyttää suoraan työasemilla tai välittää päätelaitteiden välillä esimerkiksi sähköpostipalvelun avulla, on usein tarpeen toteuttaa jonkinlainen tiedostopalvelin joko taisteluosaston omalla kalustolla, tai ainakin toteuttaa jonkinlainen yhteys asevoimien hallinnoimaan, etäkäytettävään tiedostopalvelimeen. Tiedostopalvelimeen kohdistuvan todennäköisen uhkan CVSS-arvio on esitetty alla (Taulukko 3). (Rantamäki, 2018)

Taulukko 3: Tiedostopalvelimen todennäköisen uhkakuvan CVSS-arvio. (Rantamäki, 2018)

Kriteeri	**Lyhenne**	**Arvo**				
Attack Vector	AV	Network (N)	Adjacent (A)	**Local (L)**	Physical (P)	
Attack Complexity	AC	Low (L)	**High (H)**			
Privileges required	PR	None (N)	**Low (L)**	High (H)		
User Interaction	UI	**None (N)**	Required (R)			
Scope	S	**Unchanged (U)**	Changed (C)			
Confidentiality	C	**None (N)**	Low (L)	High (H)		
Integrity	I	None (N)	**Low (L)**	High (H)		
Availability	A	None (N)	Low (L)	**High (H)**		
Exploit Code Maturity	E	Not Defined (X)	Unproven (U)	Proof-of-Concept (P)	**Functional (F)**	High (H)
Remediation Level	RL	Not Defined (X)	Official Fix (O)	Temporary Fix (T)	**Workaround (W)**	Unavailable (U)
Report Confidence	RC	Not Defined (X)	**Unknown (U)**	Reasonable (R)	Confirmed (C)	
Confidentiality Req.	CR	Not Defined (X)	Low (L)	Medium (M)	**High (H)**	
Integrity Req.	IR	Not Defined (X)	Low (L)	**Medium (M)**	High (H)	
Availability Req.	AR	Not Defined (X)	Low (L)	Medium (M)	**High (H)**	

Esimerkkitapauksessa hyökkäys olisi luonteeltaan todennäköisesti jonkinlainen haittaohjelma, jonka pyrkimys olisi joko muokata, tuhota tai kryptata palvelimen sisällä olevat tiedostot tai osa niistä, jolloin taisteluosaston kyky keskitettyyn tiedostonjakoon häiriintyisi. Jos uhkan oletetaan kohdistuvan nimenomaan tällaiseen palvelimeen, se toimitettaisiin todennäköisesti suoraan laitteeseen tai sen hallintakoneelle, jotka eivät toimi hyökkäyskelpoisissa verkoissa. Haittaohjelma pyrkisi todennäköisesti tunnistamaan joko palvelimen kovalevyjen käytettyä tallennustilaa tai sinne tallennettuja tiedostotyyppejä, ja pyrkisi piiloutumaan riittävän hyvin kyetäkseen aktivoimaan hyötykuormansa useammin kuin kerran. Käyttöoikeuksien osalta tällainen hyökkäys ei luultavasti vaatisi kovinkaan korkeita käyttöoikeuksia, sillä oletettavasti jokainen peruskäyttäjä kykenee vähintään tallentamaan ja muokkaamaan tallennettuja tiedostoja, monissa tapauksissa myös poistamaan. (Rantamäki, 2018)

Vaikka yksi menetelmä haittaohjelman aktivoimiselle voisi olla esimerkiksi makron piilottaminen tekstitiedostoon, on oikean kaltaisen tiedostonimen arvaaminen hankalaa ennen taisteluosaston käytön alkua tallennettuun tiedos-

toon. Lähtökohtaisesti voidaan olettaa, että käyttäjän toimia ei tarvita aktivoitumiseen. Hyökkäys ei myöskään tässä tapauksessa oletettavasti pyri leviämään muihin laitteisiin alkuperäisestä kohteestaan, vaan se kohdistuu yksinomaan tiedostopalvelimen tietosisältöön. Joissain tapauksissa, jos haittaohjelma kuitenkin kykenee saastuttamaan tiedostoja, ja käyttäjä lataa niitä omalle kiintolevylleen, niiden voitaneen olettaa toimivan samalla periaatteella päätelaitteen tiedostojärjestelmässä. Kuten reitittimeen kohdistuvassa tapauksessa, oletetaan ettei runkoverkon tietoturva mahdollista ulkoyhteyksiä, ja näin ollen tiedon luottamuksellisuus ei vaarannu missään vaiheessa. Eheyteen vaikuttaminen on mahdollista, mutta koska komentoyhteyttä ei oleteta olevan, ovat muutokset joko hallitsemattomia tai niitä ei tapahdu. Sen sijaan tarkoista yksityiskohdista riippumatta hyökkäyksen toiminta tulee kohdistumaan tiedon saatavuuteen. Tietojen kryptaaminen tai poistaminen aiheuttaa välittömän ja täydellisen saatavuuden menettämisen, ja ilman hyvin hallittua varmuuskopiointia niitä ei välttämättä kyetä palauttamaan lainkaan. Näillä lähtökohdilla saadaan Base Score 5,3 (Medium). (Rantamäki, 2018)

Tämän kaltaisessa hyökkäyksessä sen teknisille ominaisuuksille ei ole erityisen korkeita vaatimuksia. Kuten todettua, jo pelkkä tietojen poistaminen satunnaisena ajankohtana aiheuttaa täydellisen saatavuuden menetyksen hetkeksi. Vastatoimien toteuttaminen voi olla haastavaa tapauksesta riippuen, sillä suoraan toimittajilta saaduissa tai asennetuissa toiminta perustuu usein sopimuksin ja tarkastuksin varmistettuun luottamukseen. Ensimmäisen havainnon jälkeen kuitenkin varmuuskopioiden palautus ja palvelimen puhdistus ovat helposti toteutettavissa, joskin vaativat aikaa. Tällainen haittaohjelma tulee väistämättä herättämään käyttö- ja ylläpitohenkilöstön huomion toiminnallaan ennemmin tai myöhemmin. Tiedostojen jatkuvasta muokkaamisesta kertovat aikaleimat, katoavat tiedostot tai asiakirjojen outo sisältö paljastavat jonkinlaisen ongelman, mutta tarkkoja yksityiskohtia voi olla vaikea selvittää ennen varsinaisen syyllisen löytymistä. Ajalliset muuttujat huomioiden uhkan Temporal Score on 4,6 (Medium).

Tiedon varastointiin keskittyvästä roolistaan johtuen tiedostopalvelimen luotettavuusvaatimus on ehdottomasti äärimmäisen korkea, vaikka hyökkäyksen ei oletetakaan kohdistuvan siihen. Tietojen vuotaminen vääriin käsiin olisi katastrofaalinen tapahtuma koko taisteluosastolle. Eheyden osalta tilanne riippuu paljon siitä, minkälaisesta eheyden menetyksestä on kyse. Satunnaiset muutokset tiedon sisällössä ovat vaarattomia, vaikkakin haitallisia, mutta suunnitelmallinen datan vääristely olisi – jälleen – katastrofaalista. Saatavuuden vaatimus on tässä tapauksessa myös korkea, koska menetettäessä tiedostopalvelin vaihtoehtoina on joko olla käyttämättä sitä lainkaan ja menettää samalla koko sen tarjoama suorituskyky, tai pyrkiä siirtämään tiedostoja muita reittejä ja mahdollisesti tukkimaan myös muiden palveluiden käytössä oleva kaistanleveys. Näin saadaan lopullinen Environmental Score 5,8 (Medium). (Rantamäki, 2018)

Aiemmin mainittiin kaksi erilaista tapausta, joissa tiedostopalvelin voisi mahdollisesti sijaita – taisteluosaston omalla kalustolla tai jossain etäkäytettä-

vässä toimipisteessä. Koska etäkäytettävän pisteen hallinta olisi todennäköisesti jonkin toisen tahon hallussa, sitä ei kannata käsitellä taisteluosaston puolustuksen yhteydessä. Näin ollen myös tiedostopalvelimesta muodostuu vain yksi skenaario – skenaario 4. Tässä tapauksessa palvelimen kannattaa olettaa sijaitsevan verkossa fyysisesti ja loogisesti lähellä verkon hallinta- ja valvonta-asemaa, joko sen tai sen välittömässä läheisyydessä sijaitsevan keskeisen viesti-aseman yhteydessä. Tällöin ainakin vastatoimet on merkittävästi helpompi aloittaa nopeasti täydellisen saatavuuden menettämisen yhteydessä, vaikka eteneminen kriittisiin pisteisiin kompleksisella uhkalla olisikin näin aseteltuna helpompaa.

6 OHJELMISTO-OHJATTUJEN VERKKOJEN KÄYTTÖMAHDOLLISUUDET PUOLUSTUKSESSA

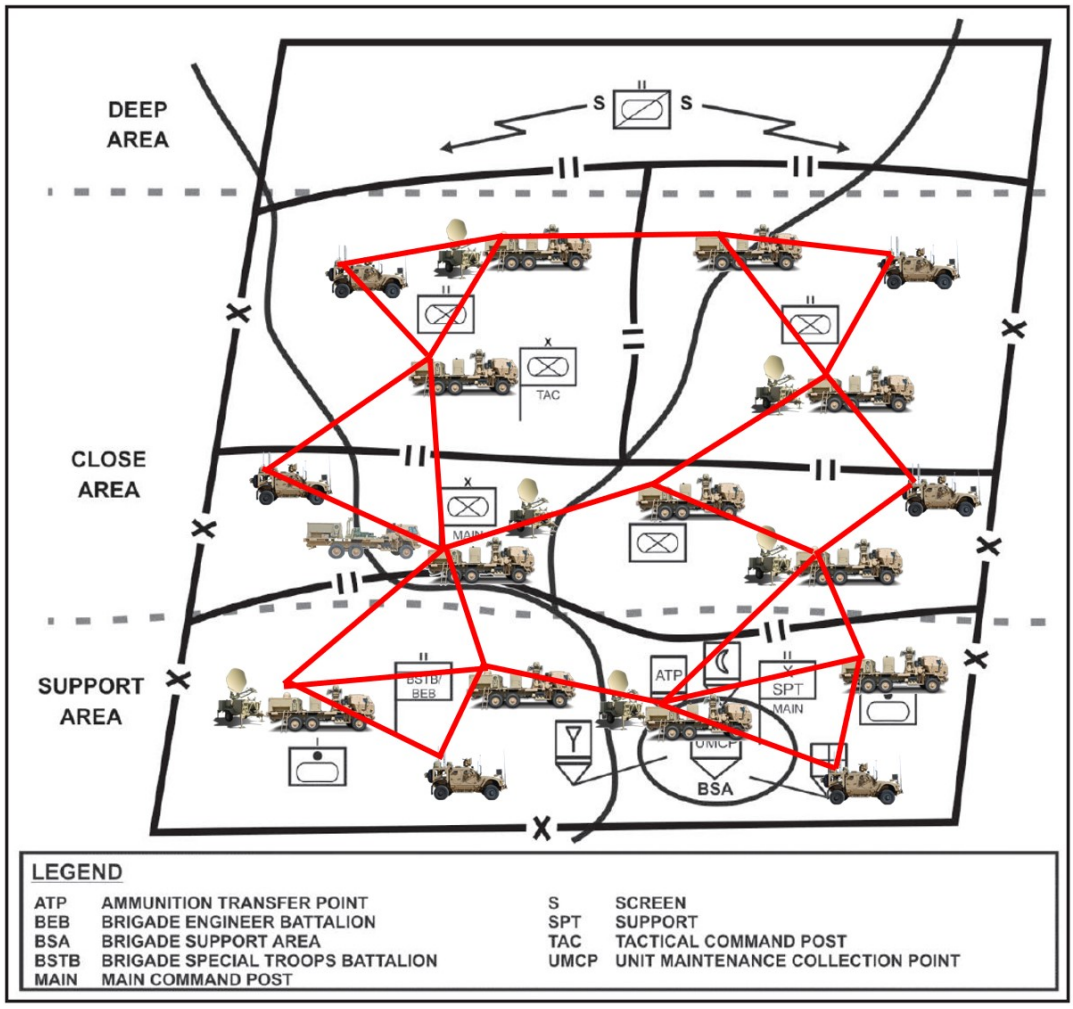
Tässä pääluvussa on tarkoitus vastata tutkimusmenetelmäluvussa esitetyn mallin mukaisesti suunnittelututkimuksen vaiheisiin 2, 3, 4 ja 5 – ratkaisun tavoitteiden määrittäminen, suunnittelu ja kehittäminen, demonstraatio ja arviointi. Ongelma on esitetty neljän eri skenaarion muodossa pääluvussa 5, ja tämä pääluku on jäsennelty vastaamaan jokaisen näistä erityispiirteisiin omassa alaluvussaan. Nämä skenaariot on muodostettu perinteiseen verkkoarkkitehtuuriin pohjautuvassa taisteluosaston kenttäviestijärjestelmässä, ja tarkoituksena on tarkastella nimenomaan sitä, voidaanko ohjelmisto-ohjatulla verkolla vastata näiden skenaarioiden tuottamiin uhkakuviin.

Tarkasteltaessa näitä neljää skenaariota pyritään saavuttamaan hyökkäykseen liittyen sellainen ratkaisu, jossa ohjelmisto-ohjattu verkko kykenee tuottamaan suojautumiskeinon uhkalta. Optimitilanteessa tämä ratkaisu kyetään toteuttamaan perinteiseen verkkoarkkitehtuuriin verrattuna pienemmin resurssein ja heikentämättä järjestelmän käytettävyyttä samassa suhteessa kuin radikaalisti kiristyvät tietoturvakontrollit. Yksi syy tälle lähestymistavalle on se, että tavanomaisiin verkkoihin suuntautuu jatkuvasti valtavia määriä hyökkäyksiä niiden yleisyyden takia, ja vaikka ohjelmisto-ohjatut verkot eivät missään tapauksessa ole sotilaskontekstiin suunniteltu sovellutus, niiden harvinaisuus julkisissa verkoissa vähentää niihin suuntautuviin hyökkäyksiin käytettäviä resursseja. Jo pelkästään vähentynyt pikkurikollisuus ja harrastuneisuus julkaistuine haavoittuvuuksineen tietyn järjestelmän osalta tarkoittaa aina sitä, että hyökkäysten kehittäminen täytyy aloittaa lähes aina hyvin alkutekijöistään ja vaatii näin ollen usein yksityiskohtaista osaamista tai paljon aikaa.

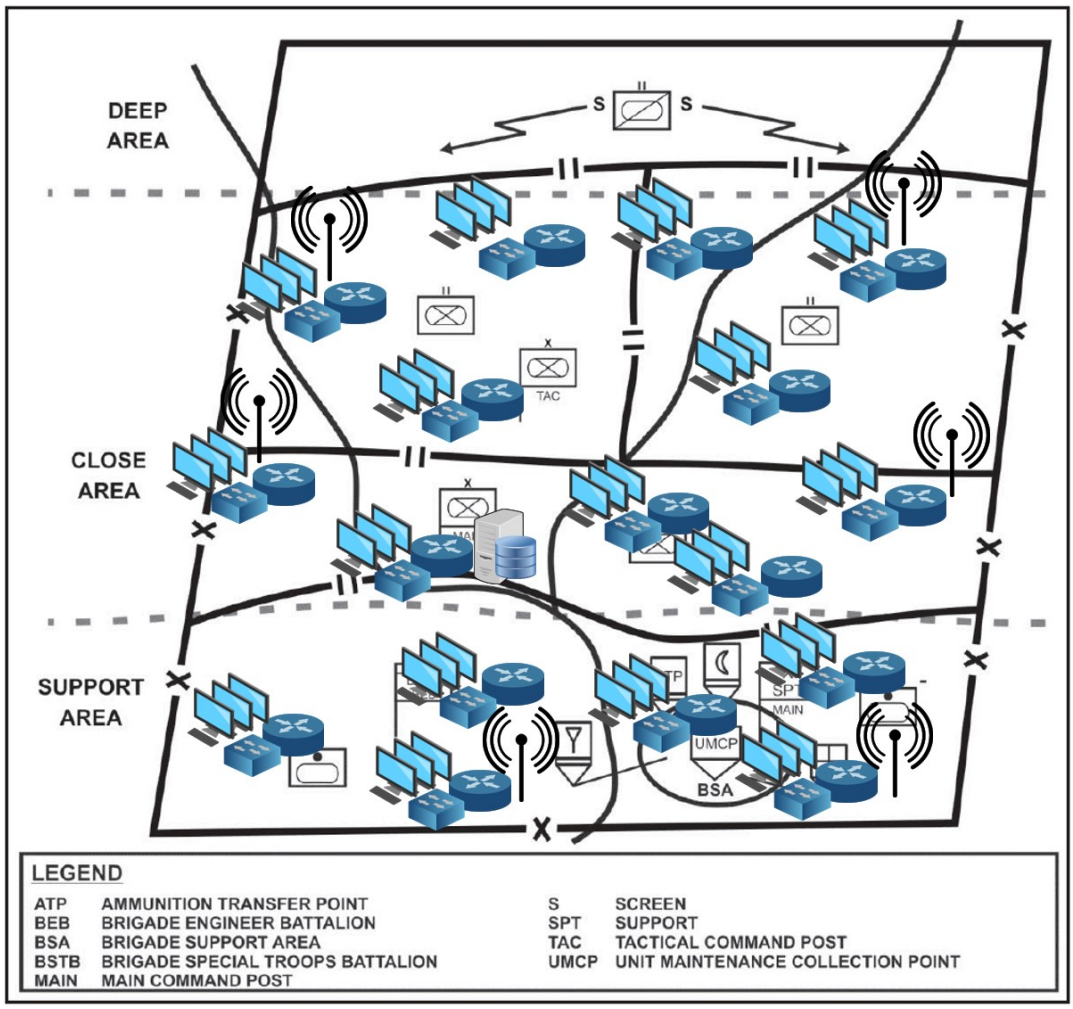
Nykyisessä mallissa haasteet liittyvät usein massiivisten konfiguraatiomuutosten tekemiseen tiukoissa aikaikkunoissa hyökkäysten leviämisen rajoittamiseksi tai vaikutuksen minimoimiseksi kohteessa, jos toimenpide vaatii mitään muuta kuin verkkokaapelin irrottamisen ja laitteen sammuttamisen. Verkkojen loogisesti tehtävät topologiamuutokset mahdollistavat myös paljon nopeamman vaikuttamisen, mikäli etäyhteydet ovat käytettävissä, kun välistä jää pois tarve tavoittaa hyökkäyksen alaisen toimipisteen henkilöstöä fyysisten toimenpiteiden suorittamiseksi. Koska ei ole yksiselitteistä, minkälainen hallintajärjestely olisi optimaalinen henkilöstöä ja riskienhallintaa ajatellen, on myös

tarpeen tarkastella kuinka matalalle tasolle hallintatasoa on mahdollista levittää. Mitä useammasta pisteestä verkkoa kyetään hallitsemaan, sen helpompi sitä on korjata tarvittaessa, mutta myös uhkavektorien määrä kasvaa samassa suhteessa.

Kaikille skenaarioille on tarpeen hahmotella yhteinen lähtökohtatilanne, jotta kaikkien ratkaisuehdotukset ovat vertailukelpoisia keskenään, silloin kun ne eivät liity yksinomaan hyökkäyksen alaiseen laitteeseen. Alla on esitetty kaksi kuvaa (Kuvio 14), (Kuvio 15), joissa on hahmoteltu taustalle luvun 2 mukaisen prikaatin taisteluosaston ryhmittyminen puolustukseen syvällä alueella. Ensimmäisessä kuvassa on havainnollistettu alueella olevia viestiasemia periaatetasolla, jättäen huomiotta satelliittiyhteydet ja aivan alimman tason langattomat laajennusasemat. Toisessa kuvassa on hahmoteltu karkeasti edellisen kuvan pohjalta se, missä sijainneissa on minkälaisia verkkolaitteita, ja korostettu etenkin laajennusasemien langatonta liityntäkykyä. Myös muut viestiasemat pystyvät tarjoamaan alueellaan langatonta liittymistä, mutta sitä ei ole tarpeen korostaa skenaarioihin liittyen.



Kuvio 14: Taisteluosaston viestiasemien ryhmitysperiaate ja yhteysvälit. (*FM 3-96: Brigade Combat Team*, 2015; *Warfighter Information Network - Tactical Commander's Handbook Version 2.0*, 2016)



Kuvio 15: Taisteluosaston verkkolaitteiden periaatekuva. (*FM 3-96: Brigade Combat Team*, 2015)

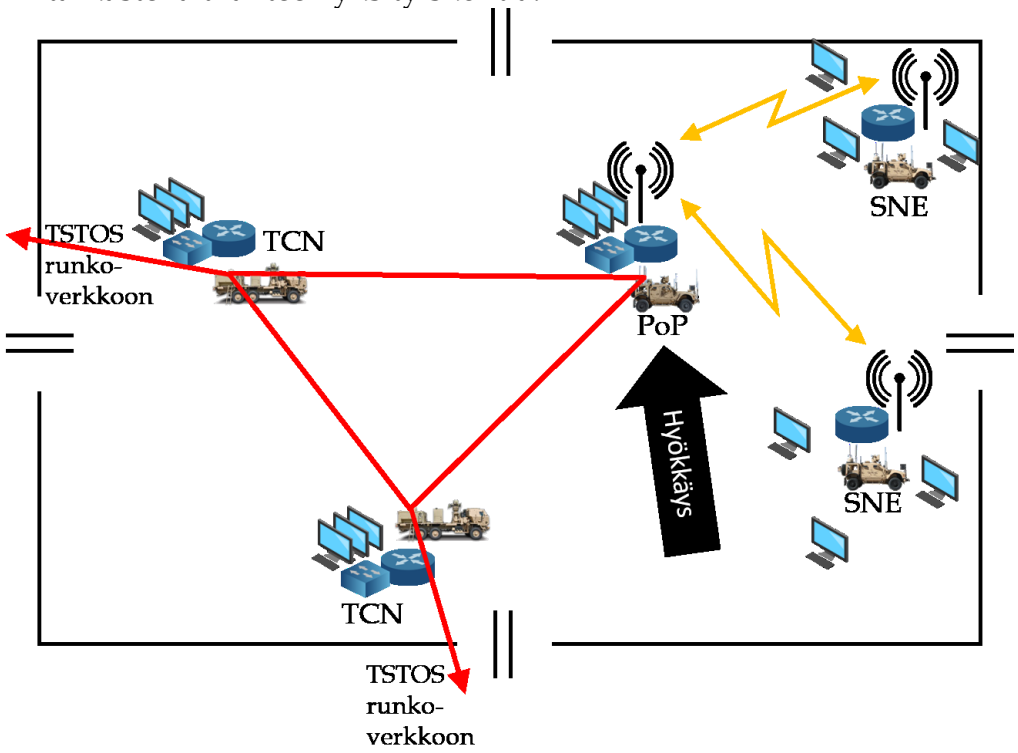
Kuviossa 14 on luotu skenaariolle verkon rakenne, jonka perusteella tässä luvussa tullaan käsittelemään aiemmin esiteltyjä uhkia. Näin voidaan nähdä esimerkiksi tilanteet, joissa yksittäisen verkkolaitteen saatavuuden menetys saattaa aiheuttaa verkkoliikenteen reititykseen vaadittavia muutoksia, kun data ei pääse enää kulkemaan oletettavasti lyhyintä reittiä. Kuvan ei ole tarkoitus antaa täydellisen kattavaa, kiistämätöntä verkon rakennetta, vaan luoda yksi realistinen rakenne verkolle. Jokaiselle pataljoonalle on tässä mallissa annettu käyttöön kaksi runkoverkon asemaa (TCN) ja yksi laajennusasema (PoP), ja näiden lisäksi prikaatin esikunnalle on annettu oma runkoverkon asema sekä verkon hallinta- ja valvonta-asema (NOSC). Jos käsitellään vielä alemmalta tasolta tullutta hyökkäystä, voidaan olettaa esimerkiksi jonkin PoP-aseman verkkoon liittyneen sen alapuolella olevia komppanian laitteita tai niiden käytössä oleva laajennusasema (SNE).

Kuviossa 15 on pyritty kuvaamaan kuvion 14 ryhmittelyä hyödyntäen karkea verkkolaitekuvaus jokaiselta toimipisteeltä. Lähtökohtainen olettamus on se, että ainakin kenttäviestijärjestelmän ei-satelliittiyhteyksillä on yksi yhteinen reititinkanta, jonka reitityssuunnitelmat rakentuvat hyödyntäen joko OSPF-

tai OLSR-menetelmiä. Jokaiselle viestiasemalle on näin ollen sijoitettu yksi reititin, joka huolehtii verkon topologian muodostamisesta ja liittymisestä, ja yksi kytkin, jonka takana ovat viestiaseman sisällä tai välittömässä läheisyydessä toimivat päätelaitteet, jotka on kuvattu tässä yhteydessä tietokoneina. PoP-laajennusasemien yhteyteen on liitetty myös erilliset langattoman tukiaseman merkit, joilla on tarkoitus ilmaista alueella toimivia, runkoverkosta yhtä tai useampaa tasoa alempana liikennöiviä joukkoja, joiden liityntä runkoverkkoon on toteutettu näiden asemien välityksellä. Kuvassa on myös esitetty tiedostopalvelin yhtenä osana prikaatin esikunnan viestiasemaa tai sen välitöntä läheisyyttä, jotta voidaan käsitellä siihen kohdistuvan hyökkäyksen vaikutuksia verkon näkökulmasta skenaariossa 4.

6.1 Skenaario 1 (Hyökkäys pataljoonan laajennussolmun reitittimeen)

Ensimmäisessä skenaariossa kuvailtiin hyökkäys taisteluosastossa toimivan pataljoonan PoP-laajennusaseman reitittimeen. Kuten kuviossa 14 on kuvattu, yksikään näistä asemista ei ole kriittinen taisteluosaston verkon muodostumiselle, eikä sen menettäminen estä tiedon kulkua muualle, kuin omalle alueelleen ja asemaan liittyneisiin alemman tason joukkoihin. Näin ollen sillä ei ole verkon topologian kannalta merkitystä, mikä näistä asemista valitaan potentiaalisen hyökkäyksen kohteeksi. Skenaarion hahmottamisen tueksi kuvioiden 14 ja 15 sisältöä on yhdistelty ja tarkennettu alla (Kuvio 16), jotta voidaan paremmin tarkastella tilanteen yksityiskohtia.



Kuvio 16: Skenaario 1:n tarkentava kuva.

Kuvasta nähdään, kuinka laajennusaseman merkitys taisteluosaston runkoverkon osalta on melko pieni, mutta häiriintyessään aiheuttaa alueellaan toimiville joukoille niiden johtamista helpottavien yhteyksien menetyksen. Tilanne riippuu paljolti siitä, minkälaiseen vaikutukseen reitittimeen kohdistunut hyökkäys pääsee – jos se muokkaa reititystauluja epäedullisesti, se voi katkaista yhteydet joko runkoverkon viestiasemiin tai langattomat yhteydet alueella toimiviin joukkoihin – pahimmassa tapauksessa molemmat. Pienimmällä vaikutuksella haittaohjelma saattaisi katkaista vain toisen suoran yhteyden runkoverkon asemiin, jolloin tilanne vaatisi vain reititysmuutokset siten, että liikenne kiertäisi aina toisen aseman kautta kohteesta riippumatta.

Tarkastellaan ensin kahta pienemmän vaikutuksen vaihtoehtoa – joko vain toinen runkoyhteyksistä katkeaa, tai langattomat yhteydet alemman tason laajennusasemiin katkeavat. Tässä tapauksessa perinteisin menetelmin olisi nopeaa saada ilmoitus häiriöistä verkossa esimerkiksi hallinta- ja valvonta-asemalle. Kun tieto yhteyksien katkeamisesta saavuttaisi verkon hallinnasta vastaavan tahon, hyökkäyksen kohteeksi joutunutta reititintä voitaisiin alkaa korjata etähallinnan keinoin. Yksinkertaisin ratkaisu alkuun voisi olla reititystaulun tyhjentäminen, jolloin reititysprotokolla alkaisi automaattisesti muodostaa lähellä olevista reitittimistä verkon topologiaa uudelleen. Tällöin haittaohjelma kuitenkin todennäköisesti toistaisi toimintansa, ja ongelma toistuisi yhtä usein kun sitä yritettäisiin korjata. Vaihtoehtona olisi ajaa jonkinlainen tietoturvallisuusohjelmiston tarkastus laitteistoon, mikäli sellainen on mahdollista suorittaa reitittimen käyttöjärjestelmässä. Jos haittaohjelma saadaan poistettua perinteisin keinoin, voidaan reititys palauttaa melko vaivattomasti alkuperäiseen tilanteeseensa. Tällaisessa tilanteessa ohjelmisto-ohjattu verkko ei tarjoaisi mitään huomattavaa etua verrattuna perinteiseen verkkoon, koska topologiamuutokset pystyttäisiin toteuttamaan nopeasti perinteisin menetelmin.

Haastavammassa tilanteessa, jos haittaohjelmalla kyetään katkaisemaan molemmat yhteydet taisteluosaston runkoverkon suuntaan, tilanne muuttuu merkittävästi haastavammaksi. Vaikka langattomat yhteydet laajennusasemien välillä toimisivat, niistä ei todennäköisesti löydy kykyä ongelman selvittämiseksi, ja vain viestiasemalla fyysisesti oleva henkilöstö kykenee suorittamaan toimenpiteitä reitittimelle. Jos haittaohjelma saa toimia kohteessa esteettä, ainut vaihtoehto perinteisellä verkkotekniikalla olisi tyhjentää reititin kokonaan ja asentaa se uudelleen oikealla konfiguraatiolla. Tämä on periaatteessa mahdollista, mikäli jokaisella viestiasemalla on hallussaan jollain tallennusvälineellä koko konfiguraatio, mutta tämä on aikaa vievä prosessi, jonka aikana kaikki tietoliikenne aseman läpi pysähtyy. Jos käytössä olisi ohjelmisto-ohjattu verkkolaitteisto, olisi hyökkäyksellä mahdotonta aiheuttaa ainakaan kovin hallittuja muutoksia verkkoliikenteeseen laitteiden luonteesta johtuen. Periaatteessa haittaohjelma voisi pyrkiä kuluttamaan laitteen muistiin tai laskentatehoon käytössä olevia resursseja palvelunestotoiminnallisuuden toteutumiseksi, mutta jos laitteelle ei asenneta muuta kuin paikallinen hallintakäyttöliittymä ja ohjelmisto-ohjatun verkon kyvykkyydet, ei haittaohjelmalla välttämättä ole samankaltaista kykyä toimia kuin perinteisen käyttöjärjestelmän tarjoamissa puitteissa.

Näissä tapauksissa ohjelmisto-ohjattu verkko tarjoaisi yhden helpon ja nopean ratkaisun ainakin leviämisen rajoittamiseksi – yhdensuuntaisen liikenteen. Ongelman hoitamisen ajaksi liikenne laajennusaseman ja runkoverkon asemien välillä voitaisiin asettaa hallintakerrokselta sekunneissa tai minuuteissa yhdensuuntaiseksi, jolloin tarvittavat korjaustoimenpiteet voitaisiin suorittaa ilman pelkoa ongelman leviämisestä.

Yksi vaihtoehto olisi ulottaa ohjelmisto-ohjattu verkko pelkästään runkoverkkoon liittyviin asemiin. Näin ollen jos laajennusasemalla sijaitseva, langattomien liittyjien kanssa kommunikointiin tarkoitettu reititin jostain syystä saastuisi, taattaisiin joka tapauksessa yhteydet runkoon ja näin ollen jokaiseen muuhun taisteluosaston osaan. Silloin tärkeimmät johtamisyhteydet voitaisiin ylläpitää esimerkiksi satelliittiteitse, vaikka menetettäisiinkin kyky joihinkin johtamistoimintaa merkittävästi helpottaviin palveluihin, esimerkiksi tiedostopalvelimeen. Näin voitaisiin myös melko luotettavasti todentaa se, missä potentiaalinen hyökkääjä olisi päässyt tunkeutumaan taisteluosaston verkkoon. Tämä ohjelmisto-ohjattu verkko tarjoaisi aina tarvittaessa ainakin runkoyhteyden taisteluosaston sisäisiin palveluihin, ja periaatteessa laitekytkentöjä vaihtamalla voisi mahdollistaa perinteisten reitittimien etähallinnan hallinta- ja valvonta-asemalta mahdollistamalla yksittäisten työasemien tai verkkolaitteiden suoran pääsyn tähän liittyjiltä irralliseen verkkoon.

6.2 Skenaario 2 (Hyökkäys taisteluosaston keskeiseen reitittimeen)

Toisessa skenaariossa kuvailtiin hyökkäys taisteluosaston kenttäviestijärjestelmässä keskeisellä topologisella sijainnilla sijaitsevaan reitittimeen. Tämän tilanteen pääperiaatteet selviävät kuviosta 14, jossa kohteeksi valikoitunut viestiasema ja sen reititin ovat viisisakaraisessa risteyksessä kuvion vasemmalla puoliskolla. Perustoiminnaltaan kyseessä on samanlainen hyökkäys kuin skenaariossa 1, joten myös ratkaisuvaihtoehdot tulevat mukailemaan toisiaan melko monilta osin. Keskeisimpänä erona ensimmäiseen skenaarioon on vaikutus, jonka tämän reitittimen toiminnan pysäyttäminen aiheuttaa. Ensimmäisessä skenaariossa joko rajoitettiin tai estettiin tiedonsiirtoa tiettyihin osiin joukkoja, mutta tässä skenaariossa yhteydet katkeavat pahimmassakin tapauksessa vain tältä yhdeltä asemalta ja siihen paikallisesti liittyneiltä joukoilta. Mikä tekee tästä kuitenkin kriittisemmän tilanteen on se, että paikallisesti liittyneissä joukoissa on taistelullisista päätöksistä vastaava prikaatin komentopaikka sekä taisteluosaston verkon hallinta- ja valvonta-asema.

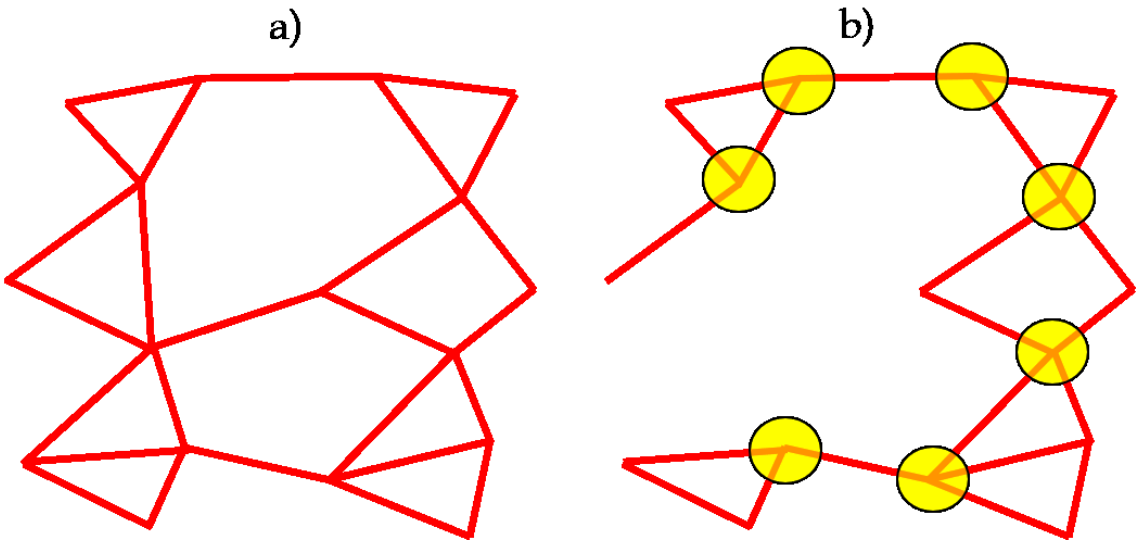
Kuten edellisessä skenaariossa jo huomattiin, myös tässä yksittäisiä yhteyksiä katkaisevaa mutta merkitykseltään melko vähäistä hyökkäystä on verrattain turha tarkastella siltä kannalta, voisivatko ohjelmisto-ohjatut verkot tarjota tähän tilanteeseen erityistä ratkaisua. Perinteiset menetelmät mahdollistavat verkon ylläpitämisen ja korjaamisen riittävän hyvin nykytilassaan.

Jos hyökkäys sen sijaan pystyisi lamauttamaan reitittimen toiminnan täysin, sulkisi se valtavan liikenteen solmukohdan taisteluosastolta. Tämä aiheuttaisi useita erilaisia ongelmia niin johtamisen kuin kenttäviestijärjestelmän osalta. Jaetaan tämä tilanne neljään pienempään osakokonaisuuteen, joista kukin aiheuttaa oman erillisen ongelmansa:

1. Verkon hallinta- ja valvonta-asema ei enää kykene havainnoimaan verkossa tapahtuvia poikkeamia eikä reagoimaan niihin ilman muilla menetelmillä toimitettuja ilmoituksia.
2. Taisteluosaston tiedostopalvelinta ei pystytä käyttämään taisteluosaston sisäiseen tiedostonjakoon.
3. Taisteluosaston komentopaikka ei pysty käyttämään pääjärjestelmäänsä johtamiseen, vaan joutuu käyttämään varamenetelmiä pienemmillä kyvykkyyksillä.
4. Taisteluosaston tietoliikenne ruuhkautuu etenkin kuvion 14 oikean reunan asemilla, koska verkko muuttuu selkeän mesh-verkon sijaan ennemmin hybridiksi väylä- ja mesh-verkoksi, ja sen sisälle muodostuu yksittäisiä pullonkauloja.

Jos asiaa ajattelee ensimmäisen ongelman näkökulmasta, tilanne on sinänsä hallittavissa niin kauan, kun verkko oletettavasti toimii ja siellä ei uskota olevan vierasta liikennettä. Valvonnan ja hallinnan merkitys kasvaa samassa suhteessa kuin verkossa esiintyvät ongelmat. Tällaisessa tapauksessa ensimmäisen skenaarion kaltainen käyttötapaus, jossa runkoverkon reitittimet korvattaisiin ohjelmisto-ohjatulla laitteistolla, kuten OpenFlow-kykyisillä kytkimillä, voitaisiin varmistua edelleen siitä, että verkon liikennöinti olisi taattu ja se olisi valvottavissa, vaikka johonkin reitittimeen päästäisiin vaikuttamaan.

Toiseen ongelmaan saataisiin samalla menetelmällä ratkaisu, kun liitettäisiin kaikki taisteluosaston yhteiset palvelut tähän samaan, ohjelmisto-ohjattuun runkoverkkoon. Tälle on myös toinen merkittävä lisäarvo, koska tiedostopalvelimen tarvitsema tietoliikennemäärä jakautuisi tasaisesti koko verkon alueelle sen sijaan, että joukot joutuisivat jakamaan tiedostoja muilla menetelmillä. Tämä edistäisi entisestään neljännen ongelman syntyä, kun normaalin tietoliikenteen lisäksi kapeisiin solmukohtiin keskittyisi merkittävästi lisääntynyttä tiedostojen siirtoon liittyvää liikennettä (Kuvio 17). Luonnollisesti toinen vaihtoehto olisi mahdollistaa useamman eri tietoliikenneyhteyden käyttö tiedostopalvelimeen liittymisessä, tai kahdentaa palvelimen sisältö useampaan paikkaan taisteluosaston sisällä, mutta nämä toisivat merkittävästi lisää tarvetta rahalliselle resurssille ja tarjoaisivat uusia uhkavektoreita tiedostopalvelimen suuntaan.



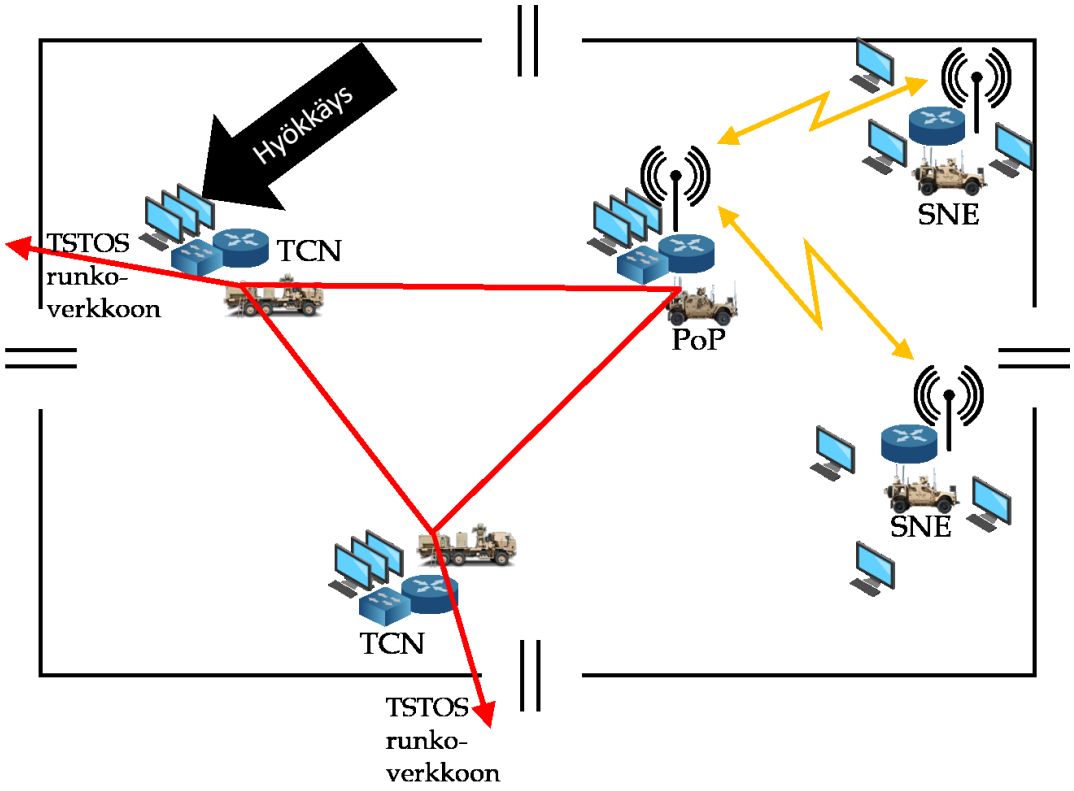
Kuvio 17: Skenaario 2:n a) alkutilanne ja b) liikenteen kapeikot hyökkäyksen toteuduttua.

Periaatteessa kaikki taisteluosaston tietoliikennesolmut olisi mahdollista toteuttaa ohjelmisto-ohjattujen verkkojen avulla, mutta tällöin olisi kriittistä suunnitella se, kuinka niiden hallinta toteutettaisiin. Jos keskimääräisen IBCT-taisteluosaston vahvuus on noin 4000 henkilöä, se tarkoittaa valtavaa määrää eri tasoisia runkoverkon asemia ja laajennusasemia eri yhteysmenetelmin. Jos yksittäisen hallinta- ja valvonta-aseman henkilöstön täytyisi samanaikaisesti kyetä valvomaan koko joukon tietoliikenne, se voisi osoittautua mahdottomaksi tehtäväksi. Jos taas hallintaverkkoa ulotettaisiin alemmille tasoille, kuten runkoverkon asemille, se voisi tarjota tarpeettoman uhkavektorin hallintaverkkoon. Tällöin olisi ehkä loogisinta pitäytyä siinä tilanteessa, että pääsääntöisesti verkkoa hallinnoisi yksi kontrolleri hallinta- ja valvonta-asemalta, ja kontrolleri olisi mahdollista siirtää toiseen toimipisteeseen tai ylläpitää muilla asemilla valmius ottaa käyttöön kontrolleri omasta pisteestään. Mikäli kaikki tietoliikennelaitteet haluttaisiin hallintaan, täytyisi kontrollereille jakaa omia vastuualueitaan kuorman tasaamiseksi.

6.3 Skenaario 3 (Hyökkäys työasemaan)

Kolmannessa skenaariossa kuvattiin vaarallinen hyökkäys taisteluosaston sisällä toimivaan, geneeriseen suunnittelutyöhön käytettävään työasemaan. Tässä skenaariossa todettiin, että työaseman fyysisellä sijainnilla ei sinänsä ollut samanlaista merkitystä kuin reitittimen tapauksessa, koska päätelaite on joka tapauksessa verkon päätepiste. Tapauksen tarkentamiseksi voitaisiin hahmotella skenaarion 1 kaltainen tilanne, jota voidaan tarkentaa lähinnä määrittelemällä hieman eroava hyökkäyksen kohde (Kuvio 18). Tässä voidaan olettaa, että kyseinen työasema on kytkeytynyt paikallisesti runkoverkon viestiaseman yhteyteen, mutta ei kuitenkaan toimi sen hallintakoneena. Voidaan myös olettaa, että

kyseinen viestiasema ei ole skenaarion 2 kaltaisessa keskeisessä roolissa taisteluosaston verkon kannalta, vaan sillä on vain kohtalaisen merkittävä rooli.

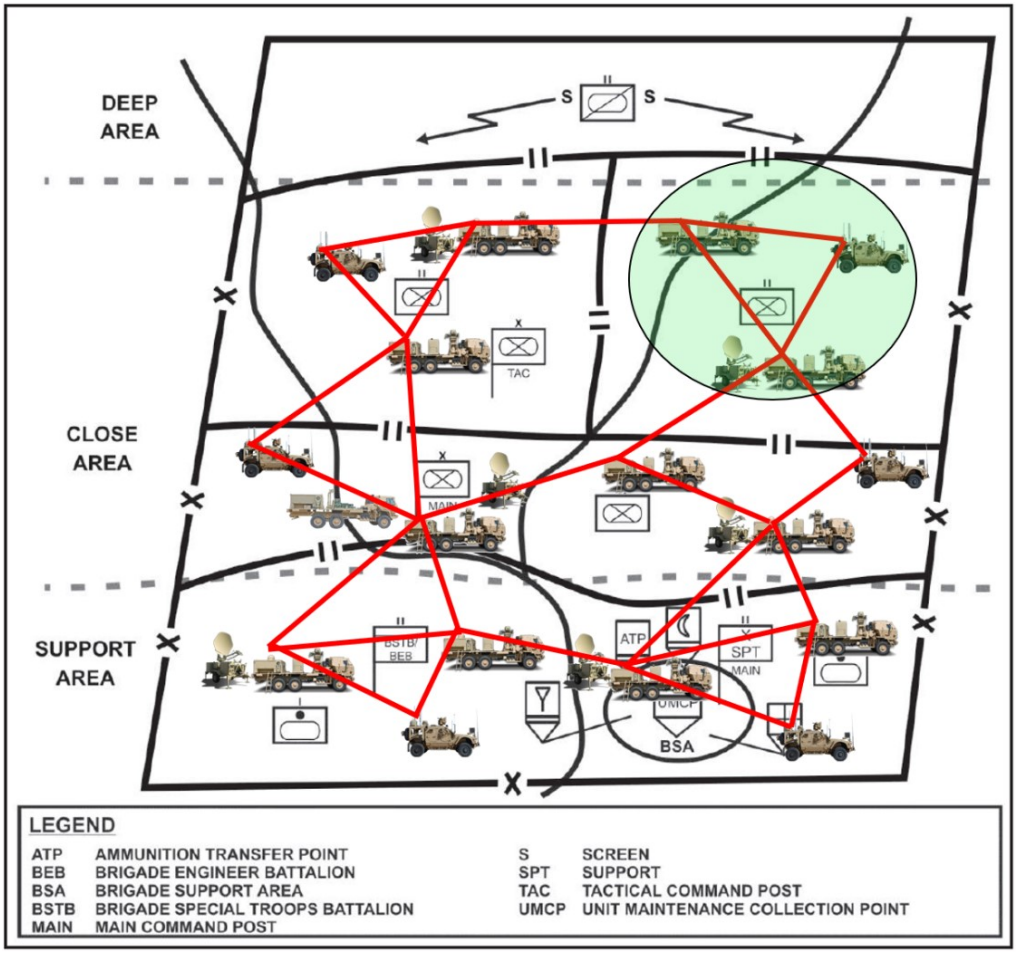


Kuvio 18: Skenaario 3:n tarkentava kuva.

Kuviossa 18 on esitetty niin hyökkäyksen kohteeksi joutunut työasema, kuin sen periaatteellinen sijainti taisteluosaston verkossa. Uhkaskenaarion erityispiirre muihin verrattuna oli se, että hyökkäys on kyetty toteuttamaan selkeästi muualta verkon alueelta, eikä hyökkääjän ole tarvinnut päästä esimerkiksi lähimmän viestiaseman reitittimen kautta samaan lähiverkkoon. Näin ollen uhka on voinut saapua työasemalle esimerkiksi joko saman pataljoonan alueella toimivien langattomien asemien kautta, mutta myös periaatteessa mistä tahansa muualta taisteluosaston alueelta tai jopa sen ulkopuolelta, riippuen siitä kuinka laajalti se on liittynyt erilaisiin verkkoihin. Hyökkääjällä oletettiin myös olevan kyky liikennöidä ulospäin taisteluosaston verkosta samaa reittiä, jota se on päässyt sisään hyödyntäen jotain hyvin tiedusteltua haavoittuvuutta.

Oletettavasti taisteluosaston sisällä toimivan työaseman laitetiedot ja konfiguraatio ovat tiedossa riittävällä tasolla siltä osin, että myös verkon suojana toimivat laitteet (palomuurit tai vast.) luottavat kyseisen työaseman toimivan hyvässä tarkoituksessa. Näin ollen ainut tapa huomata merkittävästi poikkeava liikehdintä verkossa tai päätelaitteella olisi jonkinlainen käyttäjän ilmoitus, tai selkeästi peittelemätön yhteysyritys sallitun osoiteavaruuden ulkopuolelle, josta välittyisi tieto hallinta- ja valvonta-asemalle. Mikäli hyökkääjä kykenisi kuitenkin naamioimaan liikenteensä näyttämään normaalilta, ainut selkeä havainto voisi tulla loppukäyttäjäilmoituksista, ja tällöin asian selvittäminen kestäisi

todella kauan. Oletetaan, että hyökkääjä pystyisi siirtämään haluamaansa tietoa saastutetulta työasemalta haluamaansa kohteeseen. Oletetaan myös, että hyökkäys on kyennyt leviämään esimerkiksi kuviossa 17 näkyviin työasemiin ainakin kaikilla runkoverkkoon suoraan liittyneillä asemilla, mutta ei vielä ainakaan tunnistetusti sen verkkolaitteisiin eikä muihin taisteluosaston osiin. Näin ollen voidaan tunnistaa taisteluosaston verkosta saastunut osio, ja tarkastella tähän tilanteeseen soveltuvia vaihtoehtoja (Kuvio 19).



Kuvio 19: Taisteluosaston verkon saastunut alue, kuvattuna vihreällä.

Jos nyt oletetaan perinteisen verkon menetelmin, että saadaan tieto jonkinlaisesta haittaohjelmaepäilystä saastuneen alueen työasemista, niin vaihtoehdot toimenpiteille ovat melko vähäiset. Jos hyökkäys on niin edistynyt, että se ei tuota herätettä virustorjunta- tai muille tietoturvaohjelmistoille, ainut vaihtoehto leviämisen estämiseksi olisi joko irrottaa kaikki työasemat verkosta ja toivoa, että verkkolaitteita ei ole saastunut, tai katkaista kaikki tietoliikenneyhteydet saastuneelle alueelle. Tällöin kokonaisen pataljoonan alue jäisi ilman tietoliikenneyhteyksiä, mutta muut taisteluosaston osat pystyisivät liikennöimään kohtalaisen normaalisti pienin poikkeamin reitityksissä. Haittapuolena on se, että saastuneiden viestiasemien reitittimiä ei pystyisi käyttämään lainkaan, koska riski niiden saastumisesta uhkaisi koko viestiverkkoa. Tämän lisäksi kaiken lait-

teiston tarkastus ennen niiden kytkemistä takaisin verkkoon olisi todennäköisesti lähes mahdoton toteuttaa taistelutilanteessa.

Jos perinteiset reitittimet korvattaisiin ohjelmisto-ohjatulla laitteistolla, tilanne olisi hieman erilainen. Nyt taisteluosaston hallinta- ja valvonta-asemalta käsin kyettäisiin jakamaan uudet säännöstöt laitteisiin siten, että ne eivät päästä lävitseen mitään sellaista liikennettä, joka on lähtöisin työasemilta viestiasemien yhteydessä. Tämä tarjoaisi välittömästi turvaa hyökkäyksen leviämistä vastaan, ja rajoittaisi mahdollista tiedonsiirtoa työasemilta hyökkääjän haltuun. Samalla voitaisiin, mikäli olisi pelko jonkinlaisesta haittaohjelman leviämisestä, rajoittaa liikennettä ulospäin saastuneilta asemilta. Näin varmistettaisiin tarvittaessa liikennöintikyky sisäänpäin saastuneelle alueelle edelleen, ja mahdollisesti jonkinlaisen varalaitteen kytkeminen edestakaista liikennettä varten. Kaikki reititystaulut kyettäisiin päivittämään nopeasti siten, että datakerroksen liikennettä ei ohjattaisi saastuneen alueen kautta edes läpikulkutarkoituksessa varmuuden vuoksi, ja vain hallintaliikenne säilyisi jatkuvana.

Vaikka haittaohjelma etsisi potentiaalisesti haavoittuvia verkkolaitteita lähiympäristöstään, ohjelmisto-ohjatun verkon tilanteessa se ei pystyisi datakerroksella toimiessaan suoraan hyökkäämään näihin. Vaikka ohjelmisto-ohjatuilla verkoilla on omat ongelmansa ja yksi kriittinen näkökulma on jonkinlainen hyökkäys kontrollikerrokselle esimerkiksi palvelunestohyökkäyksen muodossa (Oinasmaa, 2020), tässä tutkimuksessa ei ole tarkoitus ottaa kantaa suoranaisesti niihin. Näin ollen haittaohjelman oletetaan pyrkivän vain verkossa oleviin päätelaitteisiin tai mahdollisesti taisteluosaston tiedostopalvelimelle. Jos datakerroksen liikenne kyetään rajoittamaan, sillä ei ole tätä kykyä. Tässä skenaariossa voidaan selkeästi todeta se, että ohjelmisto-ohjatuilla verkoilla saavutettaisiin etua konventionaalisiin verkkolaitteisiin verrattuna, ainakin sillä oletuksella, että niitä kohtaan kohdistuisi vähemmän suoria hyökkäyksiä.

6.4 Skenaario 4 (Hyökkäys taisteluosaston tiedostopalvelimeen)

Neljännessä skenaariossa kuvattiin hyökkäys taisteluosaston tiedostopalvelinta vastaan. Luonteeltaan hyökkäys on kohtalaisen yksinkertainen, ja sen tarkoitus on vaikuttaa käytössä olevan tietovarannon eheyteen ja saatavuuteen, ei niinkään sen luottamuksellisuuteen. Fyysiseltä topologialtaan skenaariossa ei ole juurikaan suunniteltavaa, koska oletuksena tiedostopalvelin sijaitsee taisteluosaston esikunnan yhteydessä ja se on näin ollen fyysisesti kiinnittyneenä skenaarion 2 kuvaamaan keskeiseen viestiasemaan. Tämä skenaario on uhkan luonteeltaan hyvin erilainen kuin skenaario 3, mutta siihen kohdistuvat toimenpiteet ja suunnittelu ovat lähes identtiset johtuen työaseman ja tiedostopalvelimen samankaltaisesta roolista verkon kokonaisuudessa. Tiedostopalvelimia on taisteluosastossa kuitenkin oletetussa tilanteessa vain yksi, mutta leviämisen osalta on oletettu, että pääasiallisesti hyökkäys pysyisi palvelimella itsellään tai korkeintaan leviäisi tiedostoja lataamalla työasemille.

Koska kyseessä on päätelaite, ja vain yksittäinen sellainen, voisi tämän ongelman hoitaa kohtalaisen nopeasti perinteisen verkon menetelminkin sulkemalla joko kytkimestä tai reitittimestä sen portin, jonka kautta tiedostopalvelimelle liikennöidään. Kiireellisessä tilanteessa olisi helppoa jopa irrottaa verkkokaapelit laitteesta tai sammuttaa se. Suurin resurssien käyttö tällaista uhkaa vastaan muodostuisi ehdottomasti tiedon säilyttämiseen tai sen palauttamiseen, mikäli se on saatu poistettua tai muokattua epäedulliseksi, ja tässä ohjelmisto-ohjattu verkko ei tarjoa mitään etua tavanomaiseen verrattuna. Tässäkin skenaariossa, kuten edellisessä, olisi suurin riski lähinnä silloin, jos hyökkäys pyrkisi leviämään aggressiivisesti verkon muihin osiin ja laitteisiin, jolloin ohjelmisto-ohjatun verkon hallintakerroksen toimenpitein voitaisiin pyrkiä rajoittamaan sen liikettä, kuitenkaan täysin estämättä muuta liikennöintiä.

Yhteenvetona tähän skenaarioon ei saavuteta ohjelmisto-ohjatulla verkolla minkäänlaista uutta näkökulmaa verrattuna skenaarioon 3 tai muilta osin konventionaaliseen laitteistoon. Mikäli haittaohjelma pysyisi tiedostopalvelimessa tai leviäisi työasemille, voitaisiin ohjelmisto-ohjatulla verkolla ottaa käyttöön skenaarion 3 kaltaiset vastatoimenpiteet. Staattisessa tapauksessa myös konventionaalisen verkon keinoin voitaisiin sulkea tiedostopalvelin pois verkosta ja aloittaa siihen kohdistuvat puhdistustoimenpiteet. Jatkotarkastelulle ei ole tarvetta tämän tutkimuksen puitteissa.

7 JOHTOPÄÄTÖKSET JA JATKOTUTKIMUSAIHEET

Tutkimuksen tavoitteena oli selvittää ohjelmisto-ohjattujen verkkojen ja erilaisten verkkotopologioiden käyttömahdollisuuksia puolustuksellisena elementtinä, ja yhteisenä alustana tälle käytettiin yhdysvaltalaista jalkaväkiprikaatin taisteluosastoa (IBCT) WIN-T -kenttäviestijärjestelmällä varusteltuna. Tätä pohjustettiin esittelemällä ensin kenttäviestijärjestelmän rakennetta ja toimintaperiaatetta, sekä sen avulla mahdollisesti muodostettavia verkkotopologioita. Sen jälkeen tarkasteltiin ohjelmisto-ohjattujen verkkojen erityispiirteitä verrattuna konventionaalisiin verkkoihin, esiteltiin konventionaalisiin verkkoihin kohdistettuja arvioituja uhkaskenaarioita, ja lopuksi arvioitiin sitä, olisiko ohjelmisto-ohjattujen verkkojen menetelmillä mahdollista pienentää näiden uhkien aiheuttamaa riskiä. Tässä pääluvussa otetaan kantaa suunnittelututkimuksen prosessin vaiheeseen 5 – arviointi – kun tarkastellaan, onko tuloksilla jonkinlaista merkittävää annettavaa luvussa 4 esitettyihin tutkimuskysymyksiin.

Kun tarkasteltiin taisteluosaston kenttäviestijärjestelmään kohdistuvaa uhkaa neljän eri skenaarion kautta, oli mahdollista huomata joitain selkeitä tilanteita, joissa ohjelmisto-ohjattu verkko pystyisi tuottamaan jonkinlaista lisäarvoa verrattuna perinteiseen. Näistä ehkä selkeästi päällimmäisenä nousi skenaarioiden 3 ja 4 kautta esille tullut mahdollisuus siitä, että taisteluosaston sisällä toimivan runkoverkon reitittimet korvattaisiin ohjelmisto-ohjatuilla verkkolaitteilla. Tämä mahdollistaisi hallintaliikenteen ja dataliikenteen eriyttämisen muutenkin, kuin virtuaalilähiverkkoja käyttämällä, ja tarjoaisi mahdollisuuden suorittaa nopeitakin konfiguraatiomuutoksia verkossa yhdeltä tai useammalta kontrollerilta verkossa. Sen merkittävin etu tavanomaiseen verkkoon nähden olisi nimenomaan tämä kyky nopeisiin muutoksiin, sillä manuaalinen reititystaulujen muutos tai automaattisesti reititysprotokollilla syntyvä verkkotopologia ovat joko liian hitaita tai eivät kykene kunnolla reagoimaan sellaisiin tilanteisiin, joissa tiettyjä reittejä ei haluta käyttää niiden tarjoamasta taloudellisesta reitistä huolimatta.

Vaikka periaatteessa olisi loogista toteuttaa tällainen järjestely käytännössä kaikkien taisteluosaston verkkoliikenteeseen osallistuvien laitteiden osalta, siinä on myös omat haittapuolensa. Puhtaan tekninen tarkastelu ei suoranaises-

ti huomioi henkilöstöresurssiin kohdistuvaa lisärasitetta, mikäli valvonnan ja hallinnan oletetaan olevan jatkuvaa ja kohdistuvan käytännössä kaikkiin taisteluosaston verkkolaitteisiin aktiivisesti. Jos nykyisellään voidaan olettaa, että nämä toiminnot keskittyisivät ensisijaisesti valvontaan ja valvojan ja laitetta hallinnoivan viestiaseman väliseen tiedonvaihtoon, täysimittaisessa verkon hallintatapauksessa tarvittaisiin merkittävä määrä lisää asiantuntijoita toteuttamaan toimenpiteitä verkossa. Toinen tällaiseen malliin kohdistuva merkittävä uhka tulisi siitä, että hallintatason yhteydet ulottuisivat käytännössä verkon jokaiseen osaan, kasvattaen potentiaalista hyökkäyspinta-alaa merkittävästi. Esitettyjen skenaarioiden perusteella tällä ei välttämättä saavutettaisi sellaista hyötyä, joka olisi perusteltu syy muuttaa nykymallia täysin ohjelmisto-ohjattujen verkkojen suuntaan.

On vaikea ottaa kantaa siihen, onko tämän tutkimuksen puitteissa mahdollista nostaa erityisesti mitään tiettyä verkkotopologiaa puolustuksellisesti edullisemmaksi kuin muut. Mesh-topologia on monipuolisen rakenteensa takia ehdottomasti paras valinta suunniteltaessa mahdollisimman toimintavarmaa liikennöintikanavaa mistä tahansa pisteestä toiseen taisteluosaston sisällä. Skenaarioissa 2 ja 3 nähtiin esimerkit siitä, kuinka tällainen rakenne mahdollistaa liikennöinnin myös sellaisissa tilanteessa, kun osa verkosta saastuu tai jokin sen solmuista muuttuu käyttökelvottomaksi tilapäisesti. Tämä esimerkkirakenne muistuttaa osaltaan yhdistelmää mesh- ja rengastopologioista, jolloin yksittäisten solmujen poistuminen käytöstä mahdollistaa vielä liikennöinnin renkaan toista sivustaa. Tämän lisäksi käytännössä jokaisen skenaarioissa käytetyn solmun yhteyteen muodostuu vielä jonkinlainen tähtitopologia esimerkiksi langattomasti liittyville laitteille, ja parhaissa tapauksissa ne muodostavat vielä oman mesh-verkkonsa, kuten luvussa 2 on esitelty. Kattavampi runkoverkkoa tukeva mesh-verkko todennäköisesti tarjoaisi vielä tätäkin paremman häiriösietoisuuden, mutta se vaatisi lisää asemia ja näin ollen merkittävän taloudellisen panostuksen. Tällainenkin malli tarjoaa kohtalaisen häiriösietoisuuden, ja jos tämän lisäksi huomioidaan esimerkiksi satelliittiteitse toteutettavat yhteydet, voidaan nykymallin nähdä tarjoavan riittävän hyvän topologian.

Kokonaisuutena voitaneen todeta, että ohjelmisto-ohjatut verkot tarjoaisivat ehdottomasti etuja niin taisteluosaston kyberpuolustukselle kuin yleiselle ICT-toimintavarmuudelle. Niille olisi hyvin potentiaalista käyttöä taisteluosaston viestiasemien konventionaalisten verkkolaitteiden korvaajina, ilman merkittäviä tarpeita teknologiselle muutokselle muissa laitteissa. Mikäli tavallista laitteistoa olisi tarpeen käyttää johtuen yhteensopivuushaasteista esimerkiksi vanhojen teknologioiden kanssa, ne kannattaisi sijoittaa ohjelmisto-ohjatun verkon reunoille tukemaan esimerkiksi langatonta liittymistä kuitenkin siten, että ne kyettäisiin aina joko sulkemaan pois verkosta tai vähintään vaikuttaa niiden liikenteen ohjaamiseen ilman omatoimista kykyä suunnitella loogista topologiaa.

Koska tähän tutkimukseen liittyvistä irrallisista osa-alueista on kyetty tekemään paljonkin aiempaa tutkimusta liittämättä niitä kuitenkaan toisiinsa, voitaisiin tästä johtaa useampiakin jatkotutkimuksia. Yksi ehdottomasti tär-

keimmistä olisi toteuttaa empiirinen kenttäkoe jonkinlaisilla viestiasemilla, joko Puolustusvoimien kontekstissa todenmukaisella kalustolla tai vain demonstraatiotarkoituksessa kaupallisilla tuotteilla. Tässä kokeessa tulisi todentaa erilaisten skenaarioiden vaikutukset ja ohjelmisto-ohjattujen verkkojen tarjoama mahdollinen vastatoimikyky niitä vastaan. Tälle pohjalle voisi perustaa myös useampia samankaltaisia tutkimuksia, joilla arvioitaisiin esimerkiksi ohjelmisto-ohjatun verkon kontekstissa verkon suorituskykyä kuormittamalla sitä ilman haitallista toimintaa ulkopuolelta, verkon kykyä palautua siihen kohdistuneista hyökkäyksistä, tai esimerkiksi tämän tyyppisen verkon laajennettavuutta liikettä edellyttävässä ympäristössä.

7.1 Tutkimuksen luotettavuuden arviointi

Tämän tutkimuksen perimmäisenä tarkoituksena oli tarkastella ohjelmisto-ohjattujen verkkojen tarjoamia puolustuksellisia vaihtoehtoja perinteiseen verkkolaitteistoon verrattuna. Tutkimuksen teoriaosuudessa on tuotu esille selkeästi se, minkälaisessa toimintaympäristössä skenaarioita on tarkoitus tarkastella sekä se, minkälaisesta menetelmästä ohjelmisto-ohjatuissa verkoissa on kyse. Näistä on saatu rakennettua yhtenäinen pohja tutkielman loppuosioille.

Aineiston keruu on toteutettu teoriaosiossa tarkastelemalla erilaisia tutkimusjulkaisuja ohjelmisto-ohjattuihin verkkoihin liittyen, sekä julkisista lähteistä saatavilla olevia ohjesääntöjä ja oppaita taisteluosaston kokoonpanoon, kalustoon ja käyttöperiaatteisiin liittyen. Uhkien osalta olisi ollut haastavaa yrittää saada kovinkaan kattavaa lähdemateriaalia, sillä sotilaskontekstissa ja etenkin kenttäviestijärjestelmiin liittyen kyberpuolustuksesta on laadittu verrattain vähän tutkimustietoa. Uhkat pohjautuivat kuitenkin aiempaan pro gradu –tutkielmaani, jossa uhkakuvat on muodostettu miltei kahdeksaakymmentä lähdettä hyödyntäen. Siksi tässä työssä näyttää päällisin puolin olevan melko vähän lähdemateriaalia, vaikka taustalla sitä on huomioitu selkeästi enemmän. Skenaariovalinnat toteutettiin aiemmin tunnistettujen uhkien mukaisesti, mutta ne eivät tarjonneet aivan optimaalista tarkastelutilannetta. Skenaariot 1 ja 2 olivat luonteensa takia sellaisia, että käytännössä koko tilanne muuttuisi ohjelmisto-ohjatun verkon takia, ja skenaariot 3 ja 4 olivat verkon kannalta lähes identtiset. Tätä tilannetta voisi viedä tässä tapauksessa ehkä vielä syvemmälle verkkoja päätelaitteiden yksityiskohtien tasolle, koska tällöin saataisiin vielä selkeämmin esille ohjelmisto-ohjattujen verkkojen mahdolliset hyödyt tai haitat.

Menetelmävalintana suunnittelututkimus oli resurssien niukkuuden takia käytännössä ainoa realistinen valinta toteutukselle. Alkuperäinen suunnitelma oli haastatella aihepiirin parissa työskenteleviä asiantuntijoita, mutta tämän hetken maturiteetti aihepiiristä esimerkiksi Puolustusvoimissa on vielä verrattain alhainen, kun Federated Mission Networking (FMN) –kyvykkyyksiä aletaan huomioida vasta uudemmissa järjestelmissä, ja sitä on alettu testaamaan aktiivisesti vasta selkeästi tutkimuksen aloittamisen jälkeen (Ruska, 2019). Tällä menetelmävalinnalla ei saavutettu selkeitä, yksiselitteisiä, tieteenalallaan uusia

ja merkittäviä tuloksia, joita voitaisiin sellaisenaan ottaa käyttöön missään, mutta sen kautta pystyttiin nostamaan esille joitakin mahdollisia toimintamalleja ja verkkoratkaisuja, joita pystyttäisiin laajemmilla resursseilla tutkimaan ja testaamaan. Näin ollen tutkimuksen voidaan todeta yleisesti täyttävänsä sille asetetut tavoitteet.

LÄHTEET

Adjih, C., Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., & Raffo, D. (2003). *Securing the OLSR protocol*. 11.

Asman, B. C., Kim, M. H., Moschitto, R. A., Stauffer, J. C., & Huddleston, S. H. (2011). Methodology for analyzing the compromise of a deployed tactical network. *2011 IEEE Systems and Information Engineering Design Symposium*, 164–169. https://doi.org/10.1109/SIEDS.2011.5876871

Bittium Tactical Wireless IP Network TAC WIN. (2017). https://www.bittium.com/download/781/bittium_tactical_wireless_ip_network/pdf

Bowman, E. K., & Zimmerman, R. (2010). Measuring Human Performance in a Mobile Ad Hoc Network (MANET). *ITEA Journal*, *31*, 217–231.

Cisco. (2013). *Software-Defined Networking: Why We Like It and How We Are Building On It*. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/cis13090_sdn_sled_white_paper.pdf

Common Vulnerability Scoring System v3.0: Specification Document. (2015). FIRST.

Common Vulnerability Scoring System Version 3.0 Calculator. (2020). FIRST — Forum of Incident Response and Security Teams. https://www.first.org/cvss/calculator/3.0

Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T). (2014). Cyber Center of Excellence.

Doyle, J. (1998). *Routing TCP/IP*. Cisco Press. http://www.net130.com/tutorial/cisco-pdf/routingtcpipv1.pdf

Fang, J., Goff, T., & Pei, G. (2010). Comparison studies of OSPF-MDR, OLSR and Composite Routing. *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, 989–994. https://doi.org/10.1109/MILCOM.2010.5679574

Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: An intellectual history of programmable networks. *ACM SIGCOMM Computer Communication Review*, *44*(2), 87–98. https://doi.org/10.1145/2602204.2602219

FM 3-96: Brigade Combat Team. (2015). Headquarters, Department of the Army. http://data.cape.army.mil/web/character-development-project/repository/fm3-96-2015.pdf

General Dynamics. (2016). *Warfighter Information Network-Tactical Commander's Handbook*. https://gdmissionsystems.com/-/media/General-Dynamics/Ground-Systems/The-Soldiers-Network/PDF/general-dynamics-2016-win-t-commanders-handbook.ashx

Groth, D. (2005). *Network+ study guide* (4th ed). SYBEX.

Höylä, T. (2012). *OSPF-reititysprotokollan ominaisuudet* [Mikkelin Ammattikorkeakoulu]. https://www.theseus.fi/bitstream/handle/10024/51571/Opinnaytetyo_Tero_Hoyla.pdf?sequence=1&isAllowed=y

Jammal, M., Singh, T., Shami, A., Asal, R., & Li, Y. (2014). Software defined networking: State of the art and research challenges. *Computer Networks*, *72*, 74–98. https://doi.org/10.1016/j.comnet.2014.07.004

Kaplan, B., & Maxwell, J. (2005). Qualitative Research Methods for Evaluating Computer Information Systems. Teoksessa *Evaluating the Organizational Impact of Healthcare Information Systems* (ss. 30–55). https://doi.org/10.1007/0-387-30329-4_2

Kim, H., & Feamster, N. (2013). *SOFTWARE DEFINED NETWORKS Improving Network Management with Software Defined Networking*.

Kostiainen, V. (2020). *Komppanian päällikkö, sodan kitka ja tehtävätaktiikka – Poikkeusolojen jalkaväkikomppanian johtaminen*. Maanpuolustuskorkeakoulu.

Kreutz, D., Ramos, F. M. V., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-Defined Networking: A Comprehensive Survey. *ArXiv:1406.0440 [Cs]*. http://arxiv.org/abs/1406.0440

Lappalainen, E., & Jormakka, J. (2004). *Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa*. MPKK Tekniikan laitos.

Meador, B. (2008). *A Survey of Computer Network Topology and Analysis Examples*. 11.

Monsanto, C., Reich, J., Foster, N., Rexford, J., & Walker, D. (2013). *Composing Software-Defined Networks*. 13.

Nadeau, T. D., & Gray, K. (2013). *SDN: Software defined networks* (First edition). O'Reilly.

Oinasmaa, J. (2020). *Taktisen (kognitiivisen) tietoliikennejärjestelmän kyberturvallisuuden vaatimukset ja toteutusvaihtoehdot* [Maanpuolustuskorkeakoulu]. https://www.doria.fi/bitstream/handle/10024/177734/SM1539.pdf?sequence=1&isAllowed=y

Ojala, H. (2020). *Perusyhtymän johtamisjärjestelmän kybervalvonta* [Maanpuolustuskorkeakoulu]. https://www.doria.fi/bitstream/handle/10024/177735/SM1540.pdf?sequence=1&isAllowed=y

ONF White Paper. (2012). *Software-Defined Networking: The New Norm for Networks*. Open Networking Foundation.

http://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

OpenDaylight: The Start of Something Big for SDN. (2013, huhtikuuta 8). Blogs@Cisco - Cisco Blogs. https://blogs.cisco.com/datacenter/opendaylight-the-start-of-something-big-for-sdn

Peacock, B. A. (2007). *Connecting the Edge: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare:* Defense Technical Information Center. https://doi.org/10.21236/ADA497761

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Rantamäki, V. (2018). *Taisteluosastoon kohdistuvat kyberuhkat*. National Defence University.

Ruska, H. (2019, toukokuuta 9). *Bold Quest 19.1 -tapahtumassa kehitetään teknistä yhteensopivuutta kumppanimaiden kanssa*. https://ruotuvaki.fi/-/bold-quest-19-1-tapahtumassa-kehitetaan-teknista-yhteensopivuutta-kumppanimaiden-kanssa

Sherry, J., & Ratnasamy, S. (2012). *A Survey of Enterprise Middlebox Deployments* (Technical Report UCB/EECS-2012-24). University of California at Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-24.html

Sosinsky, B. (2009). *Networking Bible*. John Wiley & Sons.

Verkkotopologia. (2015). Teoksessa *Wikipedia*. https://fi.wikipedia.org/w/index.php?title=Verkkotopologia&oldid=15238973

Warfighter Information Network – Tactical Commander's Handbook Version 2.0. (2016). General Dynamics. https://gdmissionsystems.com/-/media/General-Dynamics/Ground-Systems/The-Soldiers-Network/PDF/general-dynamics-2016-win-t-commanders-handbook.ashx

Warfighter Information Network-Tactical (WIN-T) – General Dynamics Mission Systems. (2019). https://gdmissionsystems.com/en/communications/warfighter-information-network-tactical