MAANPUOLUSTUSKORKEAKOULU

TAISTELUOSASTOON KOHDISTUVAT KYBERUHKAT

Pro Gradu -tutkielma

Yliluutnantti
Ville Rantamäki

SM7
Maasotalinja

Huhtikuu 2018

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Sotatieteiden maisterikurssi 7	**Maasotalinja**
Tekijä **Yliluutnantti Ville Rantamäki**	
Tutkielman nimi **TAISTELUOSASTOON KOHDISTUVAT KYBERUHKAT**	
Oppiaine johon työ liittyy Sotatekniikka	Säilytyspaikka MPKK:n kurssikirjasto
Aika Huhtikuu 2018	Tekstisivuja 76 Liitesivuja 3

TIIVISTELMÄ

Nykyaikaisella taistelukentällä kyberuhkat alkavat olla osa myös taktisen tason taistelua, eivät pelkkä strateginen uhka valtionjohtoa tai kiinteitä järjestelmiä vastaan. Johtamisjärjestelmien kehityksen myötä on siirrytty tiedonsiirrossa valtavasti eteenpäin, ja taisteluosaston komentajalla ja esikunnalla on käytössään jatkuvasti enemmän välineitä johtamistoiminnan tukemiseksi. Liikenne on kaksisuuntaista, ja tiedonvaihto jatkuvaa ja aktiivista riittävän tilannetiedon takaamiseksi kaikilla toiminnan tasoilla. Tässä tutkimuksessa tarkasteltiin geneeriseen taisteluosastoon kohdistuvia mahdollisia kyberuhkia ja niiden vaarallisuutta.

Tutkimuksen teoriaosassa selvitettiin ensin mikä on taisteluosasto, ja tarkasteltiin sen historiaa, organisaatiota, johtamista ja johtamisjärjestelmää. Sen jälkeen selvitettiin erilaisten nykyaikaisten kyberuhkien ominaisuuksia vertaillen niiden ominaisuuksia ja esitellen kuuluisia esimerkkejä kustakin päätyypistä.

Tutkimuksen soveltavassa osassa esiteltiin ensin käytetty analyysimenetelmä, joka on tässä tutkimuksessa CVSS-arviointikriteeristö, jota käytetään tietoturvauhkien vaikuttavuuden arviointiin. Sen jälkeen CVSS-analyysin avulla tarkasteltiin, minkä tasoisen uhkan potentiaalinen hyökkääjä pystyisi aiheuttamaan hyökkäämällä reititintä, työasemaa tai tiedostopalvelinta vastaan todennäköisimmässä ja vaarallisimmassa tapauksessa. Analyysin perusteella vaarallisimmat uhkat kohdistuisivat reitittimiin ja tiedostopalvelimiin, koska niiden kautta leviäminen koko taisteluosaston verkkoon olisi helpohkoa toteuttaa. Kriittisimmäksi haavoittuvuudeksi taisteluosaston kannalta havaittiin saatavuuden menetys, sillä johtaminen perustuu käytettävissä olevan tiedustelutiedon hyödyntämiseen.

AVAINSANAT

kyberturvallisuus, kyberuhka, taisteluosastot, johtamisjärjestelmät

TAISTELUOSASTOON KOHDISTUVAT KYBERUHKAT

TAISTELUOSASTOON KOHDISTUVAT KYBERUHKAT

1. JOHDANTO

1.1. Aihealueen esittely

Tämän tutkimuksen aiheena on nykyaikaisen taisteluosaston kyberturvallisuuden ja siihen kohdistuvien uhkien analysointi. Aihealue on hyvin voimakkaasti sidoksissa kybersodankäynnin ja informaatiosodankäynnin kokonaisuuksiin. Kybersodankäynti käsitetään usein vain strategisen tason toimintana, jolla pyritään vaikuttamaan valtion elintärkeisiin toimintoihin ja poliittiseen päätöksentekoon, mutta tässä tutkimuksessa keskitytään perusyhtymätason taistelua uhkaavaan kyberuhkaan.

Aihe on äärimmäisen ajankohtainen, koska kyberuhkien määrä ja vaikuttavuus ovat lisääntyneet entistä verkottuneemmassa yhteiskunnassa[75]. Sotilaalliset joukot ovat nykyisin monesti tiedonsiirroltaan riippuvaisia olemassa olevasta teleoperaattorien infrastruktuurista ja sen tarjoamista ip-verkon palveluista, tai ne rakentavat itse käyttöön tarvitsemansa verkon toiminta-alueellaan. Ei voida enää suorittaa tiedonsiirtoteknologian hankintoja perinteisinä puolustushankintoina vuosien prosessin päätteeksi, koska tällöin laite voi olla jo käyttöarvoltaan täysin vanhentunut ja soveltumaton muuttuneessa uhkatilanteessa[5]. Siksi täytyy hahmottaa myös taisteluosaston kokonaisuudessa, minkälaisia uhkia vastaan se joutuu toimimaan.

Nykyaikaisella taistelukentällä ollaan siirtymässä taisteluosastojen aikakauteen entisten pataljoona-, prikaati- tai divisioonakokonaisuuksien sijaan. Taisteluosastot ovat uudenlaisia, modulaarisia kokonaisuuksia, jotka rakentuvat näiden aiempien joukkorakenteiden pohjalle, ja niiden käyttöönoton yhteydessä on usein tarve modernille tiedonsiirtoteknologialle. Uudet tekniikat vaativat aina käyttöönoton yhteydessä valtavan määrän testaustoimintaa, jotta niiden tekninen turvallisuus, tietoturvallisuus ja osaaminen saadaan riittävälle tasolle niiden hyväksymiseksi sotavarusteiksi. Koska verkon rajapintoja tulee uusien laitteistojen mukana jatkuvasti lisää, tulee sen mukana myös jatkuvasti uusia hyökkäysvektoreita potentiaalisille kyberhyökkäyksille. Etenkin langattomien verkkojen tuominen osaksi kokonaisjärjestelmää tarjoaa uuden, hyvin merkittävän hyökkäysrajapinnan potentiaaliselle vastustajalle.

Jotta erilaisilla teknisillä ratkaisuilla ja menettelytavoilla kyetään tuottamaan riittävä suoja potentiaalisia uhkia vastaan, täytyy tunnistaa oman organisaation sisällä olevat riskit, analysoida niiden todennäköisyyksiä ja vaikuttavuuksia ja toteuttaa analyysissa havaittujen uhkien edellyttämiä vastatoimenpiteitä. Koska lähtökohtaisesti kyberoperaatioissa hyökkääjällä on aina etulyöntiasema, täytyy puolustajan toimenpiteillä pyrkiä eliminoimaan kaikki tunnetut haavoittuvuudet, ja mahdollisuuksien mukaan ennustaa myös tulevaisuuden trendien tuottamia uusia uhkakuvia.

1.2. Tutkimustehtävä ja rajaukset

Tässä tutkimuksessa selvitetään, minkälainen kyberuhka maasodankäyntiin tarkoitettua taisteluosastoa vastaan muodostuu. Tehtävänä on arvioida, minkälaisen riskin erilaiset hyökkäykset aiheuttavat taistelua ajatellen suorittamalla vaikuttavuusvertailua eri laitetyypeissä, sekä sitä, miten se saattaisi vaikuttaa taisteluosaston taisteluun laajemmassa mittakaavassa.

Tutkimuksen pääkysymys on:

- Minkälaisia kyberuhkia taisteluosastoa vastaan voi kohdistua?

Tästä voidaan johtaa tutkimuksen alakysymykset, jotka ovat:

- Mitä hyökkäysrajapintoja on käytössä?
- Kuinka suuren riskin eri hyökkäykset muodostavat?

Tässä tutkimuksessa kyberuhkan tarkastelu rajataan taisteluosastoa potentiaalisesti uhkaaviin hyökkäyksiin. Tutkimuksessa ei tulla ottamaan kantaa tarvittaviin organisaatio- tai doktriinitason muutoksiin, vaan tarkastellaan puhtaasti kyberturvallisuuden teknistä aspektia. Tämän osalta otetaan kantaa erityisesti laitteistojen erilaisten teknisten ratkaisujen ja käytössä olevien sovellusten ja konfiguraatioiden tuomia hyökkäysmahdollisuuksia taisteluosaston johtamisjärjestelmää vastaan. Vaikka olisi äärimmäisen hedelmällistä tarkastella myös puolustukseen käytössä olevia vaihtoehtoja, ne eivät mahdu tutkielmaan sen tarjoamassa laajuudessa, vaan tarvitsisivat oman, yhtä laajan tutkimuksensa.

Taisteluosastoista tullaan tarkastelemaan erilaisia osa-alueita, eri valtioiden asevoimien käytössä olevista taisteluosastokokonaisuuksista. Painopiste tullaan muodostamaan taisteluosastojen kokoonpanoihin, käyttötarkoituksiin, johtamisjärjestelmiin ja johtamiseen, jotta voidaan arvioida sitä, minkälainen vaikutus potentiaalisella kyberhyökkäyksellä tällaista taisteluosastoa vastaan olisi. Johtamisjärjestelmän osalta tarkastellaan etenkin laitteistoa ja tekniikoita, samoin kuin mahdollisia verkkotopologioita ja niiden vaikutusta kyberuhkaan.

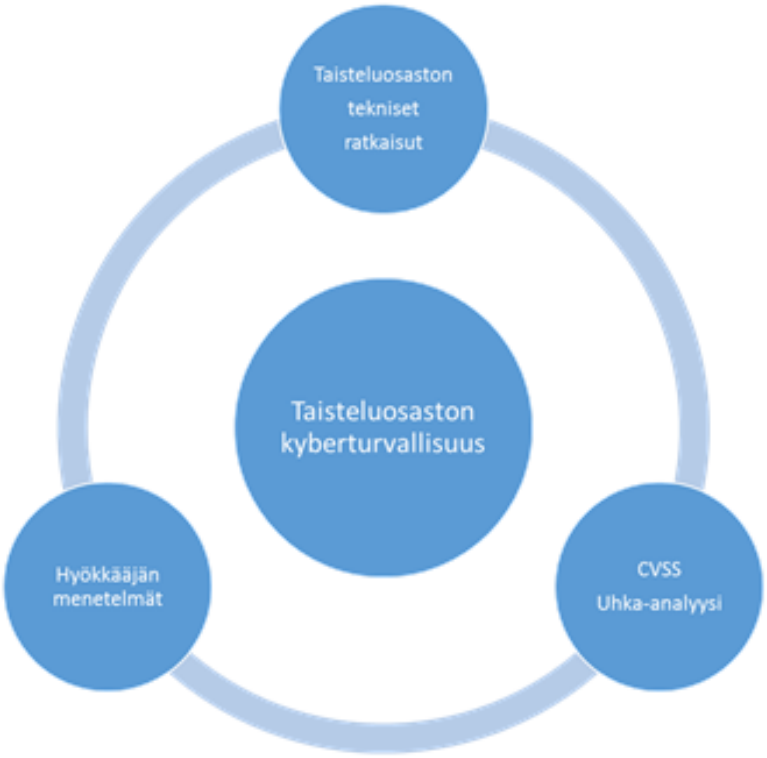
1.3. Tutkimusmenetelmät ja tutkimuksen rakenne

Tässä tutkimuksessa käytetään kirjallisuusselvitystä teoriaosuuden pohjana, ja CVSS-uhka-analyysia tukemaan johtopäätöksiä nykyaikaisista kyberuhkista. Kirjallisuustutkimuksen avulla pyritään luomaan aiempiin tutkimuksiin perustuen teoriapohja taisteluosaston kybersodankäynnin ulottuvuudesta, tarkastellen niin taisteluosaston teknologioita kuin kyberhyökkäysten trendejä nykyaikaisessa kybersodankäynnissä.

Tutkimuksen teoriaosio on toteutettu varsin perinteisenä kirjallisuustutkimuksena, jossa sisältöä on analysoitu aineistolähtöisen sisällönanalyysin metodeilla. Sen tarkoituksena on tuottaa lukijalle ymmärrys aihepiiristä ja sen sisällä vaikuttavista ilmiöistä, joiden pohjalle muu tutkimus rakentuu[58]. Laadullisen sisällönanalyysin tarkoituksena tämän tutkimuksen sisällä on saada yhdisteltyä eri lähteistä kerättyä tietoa uudeksi kokonaisuudeksi, ja tämän jälkeen suorittamalla sisällölle jatkoanalyysia tuottamalla määrällisiä tuloksia sanallisesti kuvatusta aineistosta.[74] Tämä menetelmä soveltuu hyvin tutkimuksen teoriapohjan selittämiselle ja siihen, että kyetään rakentamaan selkeä kuva kokonaisuudesta ennen analyysin toteuttamista.

Laadullisen sisällönanalyysin lisäksi uutta tietoa pyritään tuottamaan suorittamalla CVSS-arviointikriteeristön mukainen analyysi erilaisille uhkakuville. CVSS-analyysissa erilaisille uhkatekijöille on annettu tietyt painokertoimet, joiden mukaan niiden vaikuttavuutta arvioidaan kohdeympäristössä. CVSS-analyysin perusteet on esitelty tarkemmin luvussa 4. Tarkoitus on arvioida erilaisia uhkavektoreita käyttävistä hyökkäyksistä vaarallisin ja todennäköisin hyökkäysmenetelmä. Uhka-analyysi on tällaisessa tutkimuksessa hyödyllinen menetelmä, sillä sen avulla kyetään mahdollisesti hahmottamaan selkeitä trendejä potentiaalisten uhkien joukosta ja erottelemaan selkeästi kriittiset ja vähemmän vaaralliset uhkatilanteet toisistaan.

Tutkimuksen viitekehys on esitetty kuvassa 1. Tutkimuksen rakenne perustuu siihen, että keskiössä on jatkuvasti taisteluosaston kyberturvallisuus. Siihen vaikuttavina tekijöinä analysoidaan niin taisteluosaston teknisiä ratkaisuja, hyökkääjän potentiaalisia keinoja kuin puolustuksen ratkaisuja, välineenä CVSS-arviointikriteeristön mukainen uhka-analyysi.



Kuva 1: Tutkimuksen viitekehys.

Tutkielman toisessa pääluvussa esitellään esimerkki nykyaikaisen taisteluosaston organisaatiosta perustuen muiden valtioiden käytössä oleviin kokonaisuuksiin, johtamisjärjestelmälaitteisto sekä johtamiseen liittyvät kriittiset tietotekniset ja tiedonsiirrolliset tekijät. Luvun tarkoituksena on antaa käsitys siitä, minkälaisessa kyberympäristössä potentiaalinen hyökkääjä joutuisi toimimaan hyökkäystilanteessa.

Tutkielman kolmannessa pääluvussa esitellään potentiaalisia kyberhyökkäyksen välineitä nykyaikaisissa tietojärjestelmissä ja -verkoissa. Tarkoituksena on esittää erilaisia vaihtoehtoja sille, minkä tyyppisiä hyökkäyksiä taisteluosastoa vastaan olisi ylipäänsä mahdollista suorittaa, eikä niinkään sitä, mikä olisi todennäköisin hyökkäysvaihtoehto mihinkin tilanteeseen.

Tutkielman neljännessä pääluvussa esitellään tutkielman varsinainen analyysimenetelmä, CVSS-arviointikriteeristö. Tämän luvun tarkoituksena on selventää lukijalle käytetty menetelmä, ja nostaa esiin sen eri osa-alueiden esiintymistä taisteluosaston viitekehyksessä. Siinä pyritään yhdistämään toisen ja kolmannen pääluvun sisältöä konkreettiseksi, yhtenäiseksi kokonaisuudeksi.

Tutkielman viidennessä pääluvussa tarkastellaan uhka-analyysin tuloksia. Tämän tarkoituksena on esittää analyysin toteuttaminen ja sen avulla saadut tulokset, sekä selvittää lukijalle eri uhkien vaikutukset taisteluosaston toiminnalle.

Viimeisessä pääluvussa esitellään tutkielman johtopäätökset ja mahdolliset jatkotutkimusaiheet. Tämän lisäksi tarkastellaan tulosten luotettavuutta.

1.4. Tutkimustilanne

Tutkimuksen yleisiä konsepteja on tutkittu niin eri valtioiden asevoimissa kuin niiden ulkopuolella paljon etenkin viime vuosina. Taisteluosastot erilaisine kokoonpanoineen ja nykyaikaisen taistelun erityispiirteet ovat olleet erinomainen alusta tutkimuksille, ja niistä onkin tuotettu verrattain paljon tietoa. Yhdysvaltain asevoimat ovat julkaisseet paljon tietoa julkisesti, mutta muilta valtioilta tietoa on saatavilla hieman vähemmän yksityiskohtaisesti. Kyberturvallisuus on maailmanlaajuisesti hyvin tutkittu aihe, ja sitä tutkivatkin aktiivisesti niin yritykset kuin yliopistot. Tässä tutkimuksessa on selvitettävä, kuinka nämä kaksi konseptia kohtaavat toisensa nykyaikaisella taistelukentällä ja potentiaalisesti tulevaisuudessa.

Kapteeni Erno Pasanen kuvasi tutkimuksessaan keväällä 2015 tietoverkkovaikuttamisen suorituskyvyn vaatimuksista, joita voidaan hyödyntää joiltain osin tämänkin tutkimuksen lähtökohtina käsiteltäessä kyberturvallisuuden vaatimuksia. Tutkimuksen kohteena oli tuottaa DOTMLPFIi-mallin mukainen luokittelu hyökkäyksellisten tietoverkkovaikuttamisen elementtien osalta, ja siinä tarkasteltiin tietoverkkovaikuttamista hyvin kokonaisvaltaisesti. Sen päätuotteena oli tilannekuvaus Puolustusvoimien tämänhetkisestä tilanteesta tietoverkkovaikuttamisessa, ja tämän tutkimuksen kannalta sen kriittisin tuote oli etenkin doktriinitason tarpeiden ja mahdollisten toimintavaihtoehtojen erittely.[67]

Kapteeni Tommi Marttinen on tutkinut vuonna 2010 esiupseerikurssi 62:n tutkielmassaan mekanisoidun pataljoonan (2020) operatiivisia suorituskykyvaatimuksia, ja tutkimuksessa on esitelty paljon tätä tutkielmaa tukevia yleisiä aiheita. Tutkielmassa käsitellään eri valtioiden sotilasorganisaatioiden, erityisesti maavoimien kehityssuuntia, ja tarkastellaan esimerkiksi käytettävien joukkojen johdettavuutta, itsenäisyyttä, järjestelmien yhteensopivuutta, informaation hallintaa ja johtamisjärjestelmien vaatimuksia. Nämä näkemykset luovat hyvän lisäsyvyyden tarkastelulle yhteistoiminnassa muiden valtioiden näkemysten kanssa.[62]

Vasileios Gkioulos julkaisi taktisten palvelusuuntautuneiden arkkitehtuurien turvallisuutta käsittelevän väitöskirjan helmikuussa 2018 Norwegian University of Science and Technologyssa. Tässä väitöskirjassa tarkastellaan hyvin kattavasti taktisen ympäristön aiheuttamia haasteita ja vaatimuksia tietoturvallisuudelle, ja siinä tarjotaan myös hyvin kattavasti ratkaisuvaihtoehtoja erilaisiin skenaarioihin. Pääosa sisällöstä pohjautuu ”TACTICS: TACTICal Service Oriented Architecture”-kehittämisohjelmassa saatuihin havaintoihin sekä Gkioulosin ja muiden aihetta tutkineiden aiempiin tutkimuksiin. TACTICS:iin on osallistunut useita yliopistoja ja puolustusteollisuuden toimijoita, muun muassa suomalainen Patria.[30]

Erilaisten kyberhyökkäysten tutkimus on hyvin aktiivista ja avointa nykypäivänä. Etenkin uusista, useimmiten mediassakin uutisoiduista kyberhyökkäyksistä on usein saatavilla hyvin yksityiskohtaisia tutkimuksia ja analyyseja, joita tietoturvayhtiöt ja yliopistot pyrkivät tuottamaan hyvinkin nopeasti näiden esiintymisen jälkeen.

Muita sotilaallisen organisaation tietoliikenteeseen liittyviä hyödyllisiä tutkimuksia tämän tutkimuksen tueksi ovat myös muun muassa seuraavat:

- Asman, Brian et al.: Methodology for Analyzing the Compromise of a Deployed Tactical Network
- Peacock, Brent: Connecting the Edge: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare

1.5. Aineiston esittely ja lähdekritiikki

Tutkimuksessa käytetään pääosiltaan kahta erityyppistä kirjallista aineistoa: eri valtioiden tuottamia tutkimuksia asevoimien taisteluosastotaktiikasta ja niiden kalustosta, Yhdysvaltojen asevoimien tuottamia field manualeja, jotka ovat käyttöön hyväksyttyjä toimintatapamalleja, sekä tietoturvayhtiöiden ja yliopistojen tietoturva-aiheisia julkaisuja. Näitä kaikkia voidaan pitää hyvin luotettavina ja puolueettomina lähteinä, koska niiden tarkoituksena ei ole osoittaa minkään menetelmän ylivertaisuutta vaan tutkia niiden faktuaalisia ominaisuuksia.

Etenkin United States Army Collegen ja Naval Postgraduate Schoolin tuottamat tutkimukset ovat erinomaisia lähteitä tätä tutkielmaa ajatellen, sillä ne kuvaavat parhaiten tämänhetkisiä, voimassa olevia toimintatapamalleja, joiden avulla taisteluosaston taistelua toteutetaan todellisissa kriisitilanteissa ja miten sitä suunnitellaan toteutettavan tulevaisuuden kriiseissä. Niistä on saatavissa usein organisaatioon tai johtamisjärjestelmään liittyvää tarkkaa tietoa, joka riittää monilta osin laadukkaan uhka-analyysin tekemiseen. Laitteistoista on kuitenkin sotilasjoukkojen tietoliikennettä käsittelevien tutkimusten pohjalta mahdollista arvioida ainakin laitetasolla, sillä tarkkuudella, käytetäänkö toiminta-alueella langallisia vai langattomia verkkoja, radioyhteyksiä tai muita yhteysmenetelmiä.

Tietoturvayhtiöiden raportteja ja julkaisuja haittaohjelmiin liittyen voidaan pitää hyvin luotettavana lähteenä, sillä ne ovat rakenteeltaan hyvin analyyttisia ja tarkkoja, ja sisältävät jopa ohjelmakoodia myöten tärkeimpiä tekijöitä haittaohjelmien toiminnasta. Yleisemmät, potentiaalisia uhkatrendejä ennustavat raportit ovat myös hyvin tarkkoja ja pohjautuvat määrälliseen aineistoon, joka on usein analysoitu selkeästi.

Pääosa lähteistä on luonteeltaan teknisiä raportteja, eivätkä ne tällöin sisällä subjektiivisia näkemyksiä tai jonkinlaisiin johtopäätöksiin vievää analyysia. Ne eivät myöskään sisällä spekulaatioita mahdollisista tietoturvauhkien toimijoista tai poliittisista tai taloudellisista motivaatioista, jolloin niiden lähteiden osalta voidaan ehdottomasti olettaa, että niiden sisältöön voi luottaa. Esimerkiksi tietoturvaennusteissa sen sijaan on olemassa yritys- ja yhteisökohtaisia eroavaisuuksia, mutta tämän tutkimuksen piirissä ei ole tarkoitus tarkastella absoluuttisesti tulevaisuuden uhkien teknologisia vaikutuksia ja näin ollen sisältö on relevanttia.

Yhdysvaltojen omille joukkotyypeilleen ja materiaaleilleen suorittamissa tutkimuksissa on väistämättä jonkin asteinen asenteellisuus omia järjestelmiä kohtaan, joskus negatiivinen tai joskus positiivinen, mutta se on hieman tutkijariippuvaista. Toisaalta on äärimmäisen hankalaa löytää täysin neutraalin tutkijan toteuttamaa tutkimusta, jossa käsiteltäisiin asevoimien materiaalia tai toimintaa yksityiskohtaisesti.

Suurin osa aineistosta on hyvin tuoretta, 2000-luvulla tuotettua, pois lukien tutkimusmenetelmiin, taisteluosaston historiaan tai tietoturvallisuuden perusteisiin käytetyt teokset, joiden sisältö on säilynyt pitkälti muuttumattomana.

2. TAISTELUOSASTON KOKOONPANO JA ERITYISPIIRTEET

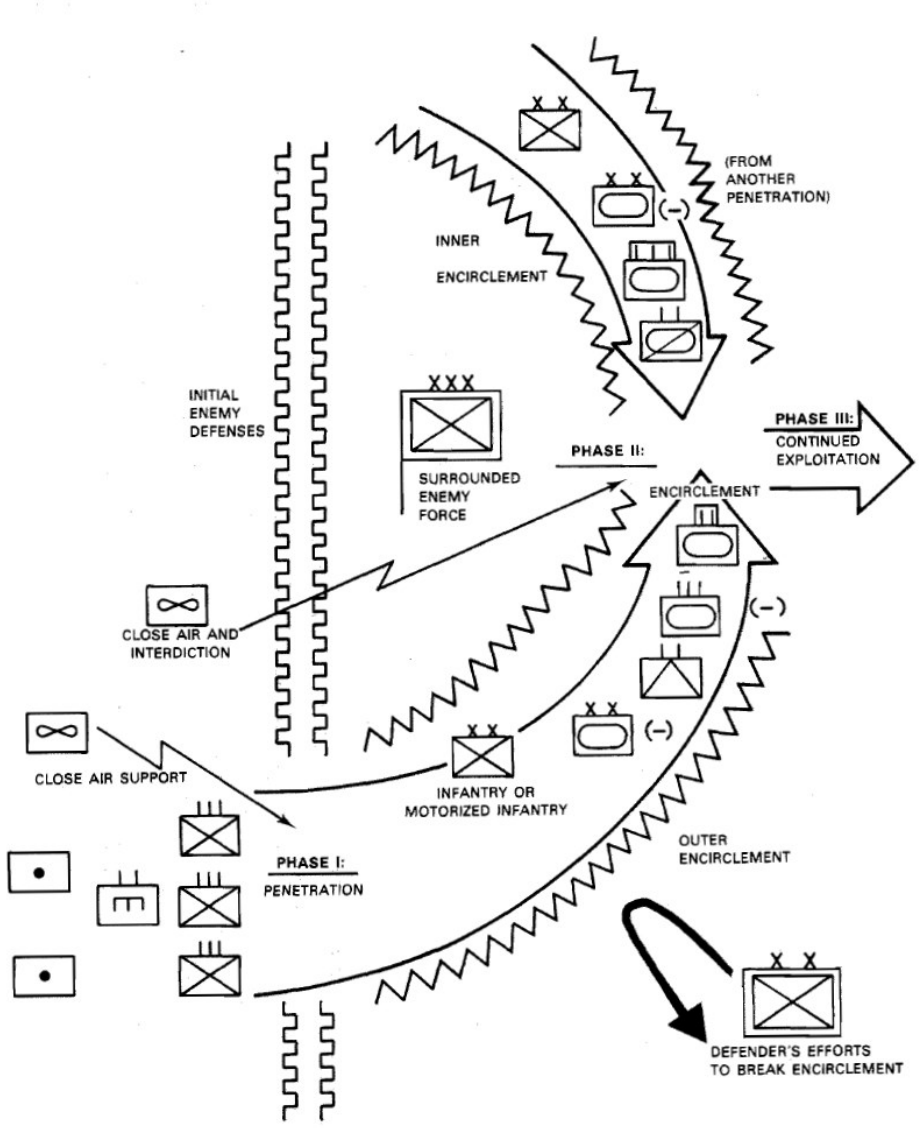
2.1. Perusteet ja historia

Sodankäynnin luonne on vuosisatojen saatossa muuttunut merkittävästi. Ennen ensimmäistä maailmansotaa maavoimien vallitsevana trendinä oli ryhmittää joukot divisiooniin tai armeijakuntiin. Euroopassa oli pääsääntöisesti hyväksytty perustaistelujoukoksi divisioona, jossa kyettiin yhdistämään jalkaväen ja tykistön suorituskyvyt. Ratsuväki oli pääsääntöisesti järjestetty erillisiksi joukoikseen, jotka suorittivat esimerkiksi tiedustelu- ja suojaustehtäviä. Jalkaväkidivisioonien koko vaihteli jonkin verran, kun esimerkiksi ranskalaiseen divisioonaan kuului vuonna 1914 15000 miestä, 36 tykkiä ja 24 konekivääriä, kun venäläiseen divisioonaan kuului 21000 miestä, 48 tykkiä ja 32 konekivääriä.[34]

Ehkä ensimmäiset viitteet nykyaikaisen taisteluosaston tyylisestä toiminnasta esiintyivät helmikuussa 1918, kun saksalaisten pääesikunnan päällikkö Erich von Ludendorff julkaisi ohjeistuksen hyökkäyksiä varten. Tässä ohjeessa ohjeistettiin jalkaväkeä hyökkäämään itsenäisesti käyttäen konekivääreitä, kivääreitä, kranaatteja, kevyitä heittimiä ja joukon mukana toimivaa suora-ammuntatykistöä. Maaliskuussa 1918 saksalaiset aloittivat hyökkäyksen eversti Georg Bruckmüllerin johdolla, kun operaatio Michael alkoi. Hyökkääviksi joukoiksi oli koottu rynnäkköpataljoonia (Sturm-Bataillon), jotka koostuivat tyypillisesti 3-4 jalkaväkikomppaniasta, heitinkomppaniasta, tykistöpatterista tai -puolipatterista, liekinheitinpuolijoukkueesta, viestiosastosta ja pioneeripuolijoukkueesta.[34]

Sotien välisenä aikana kukin valtio kehitti omaa taistelutapaansa ylimpien johtojensa näkemysten mukaisesti, mutta tulivoiman ja liikehtimiskyvyn lisääminen olivat merkittäviä trendejä ensimmäisen maailmansodan kokemusten pohjalta. Joukkorakenteet kevenivät mieslukumäärältään, mutta kulkuvälineitä ja aseita tuli merkittävästi lisää, etenkin panssarivaunujen kehittyessä käytännöllisemmiksi taisteluvälineiksi. Tämä tarjosi paremman mahdollisuuden taisteluosastotyyliselle toiminnalle, ja toisen maailmansodan alkuvuosina saksalaisissa panssaridivisioonissa olikin tapana muodostaa erilaisia tehtäviä varten uusia tehtäväorganisaatioita divisioonatasolta aina pataljoonatasolle asti. Näissä tehtäväorganisaatioissa yhdistyivät panssarivaunut, jalkaväki, tykistö, pioneerit ja joskus jopa ilmatorjunta, ja niiden painotukset vaihtelivat tehtävän, maaston ja vihollisjoukkojen mukaan. Ranskalaiset olivat tässä osa-alueessa merkittävästi saksalaisia jäljessä, ja panssaridivisioonat olivat jäykkiä organisaatioita, joissa oli neljä panssaripataljoonaa, jalkaväkipataljoona ja kaksi tykistöpatteristoa. Tämän organisaation muuttaminen taisteluiden aikana ei onnistunut, koska muita joukkoja ei ollut koulutettu taistelemaan panssarivaunujen kanssa.[34]

Blitzkrieg-taktiikassa, suoritettaessa saarrostustaistelua, näitä taisteluosastoja käytettiin osana laajempaa hyökkäystä selkeissä tehtävissä. Kun puolustajan puolustuslinja oli ensin murrettu jalkaväen, pioneerien, tykistön ja ilmaiskujen yhteysvaikutuksella, eri aselajeista muodostettu pataljoona- tai rykmenttipohjainen taisteluosasto toimi etujoukkona panssarijoukkojen hyökkäyksessä jonka tavoitteena oli saarrostaa puolustava joukko yhteistyössä toisen läpimurtokohdan kautta tulevan vastaavan joukon kanssa. Lopuksi molemmat saarrostavat joukot muodostavat kehät sisään- ja ulospäin kuluttaakseen saarrostettua joukkoa ja estääkseen sen tukemisen ja saarrostuksen murtamisen (Kuva 2).[34]



Kuva 2: Blitzkrieg-sodankäynnin saarrostustaktiikka.[34]

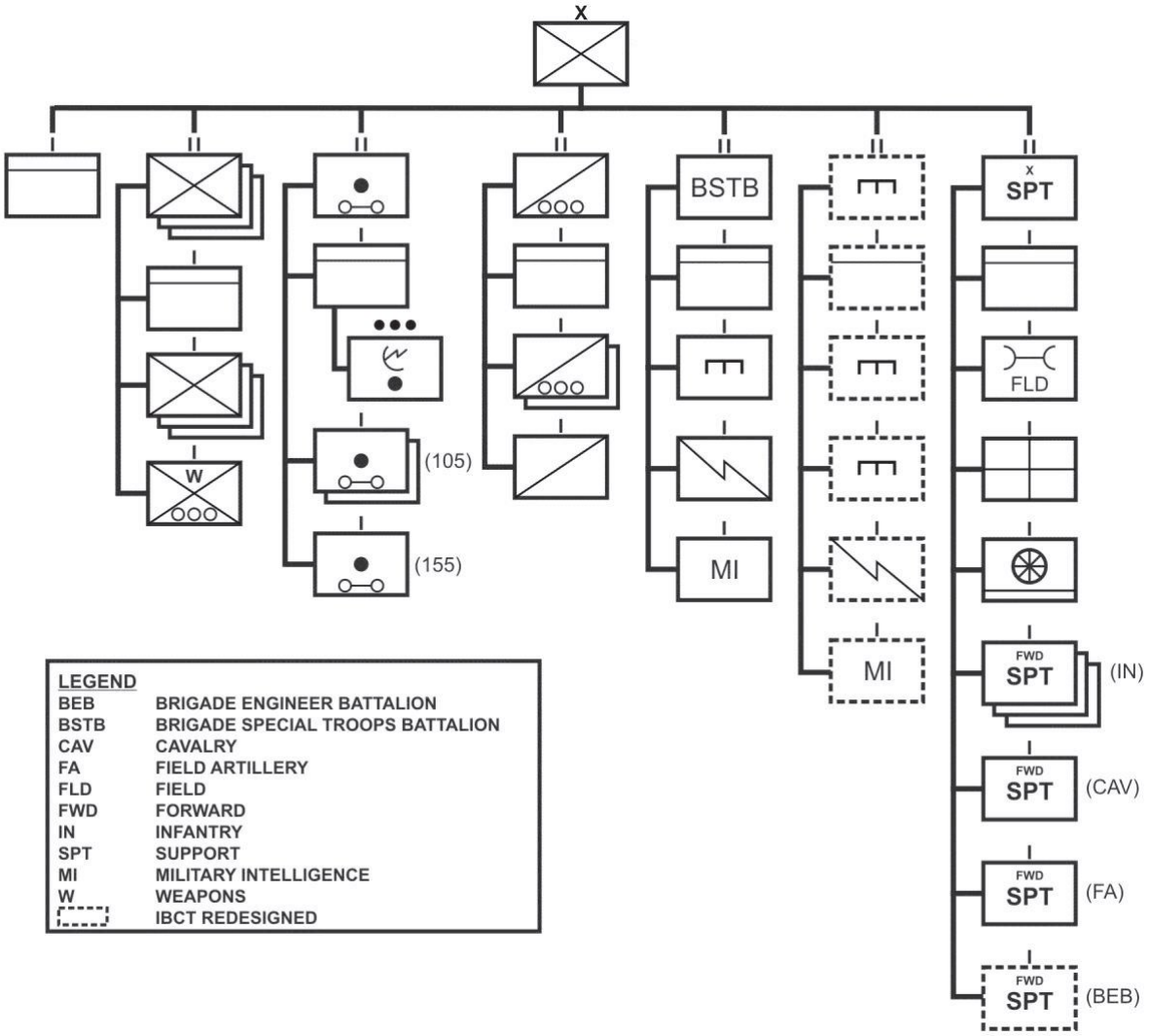
Toisen maailmansodan jälkeen eri valtiot kokeilivat erilaisia konsepteja, jotka mahdollistaisivat esimerkiksi joukkojen itsenäisen taistelun erillään muista omista joukoista. Yhdysvalloissa kokeiltiin muun muassa viisijakoista jalkaväkidivisioonaa, jossa päätaisteluvoiman muodostivat viisi taisteluosastoa, kooltaan hieman pienempiä kuin rykmentti mutta suurempia kuin pataljoona, ja niihin kuului orgaanisesti viisi jalkaväkikomppaniaa, esikunta ja heitinkomppania, ja lisänä usein panssarikomppania ja tiedusteluosia. Tämä kuitenkin osoittautui äärimmäisen hankalaksi johtamistoiminnan kannalta, koska divisioonan komentajalla oli valtava määrä suoria alaisia, samoin kuin taisteluosastojen komentajilla, kun pataljoonan esikunnat oli poistettu välistä johtamisrakenteessa.[34]

Kaiken kaikkiaan taisteluosaston merkittävin tekijä ei ole se, minkä kokoinen se on – niitä pystytään rakentamaan periaatteessa mille tahansa pataljoona-prikaatikokoiselle joukolle. Se, mikä tekee taisteluosastosta taisteluosaston, on eri aselajien yhdistäminen yhden johdon alle joukoksi, joka kykenee itsenäiseen taisteluun erilaisissa olosuhteissa ja erilaisia vihollisia vastaan.

2.2. Taisteluosaston organisaatio

Taisteluosastojen yksi merkittävimmistä eduista verrattuna muihin perinteisiin taisteleviin yksiköihin on niiden kyky muuntautua tilanteen vaatiessa ja ylemmän johtoportaan resurssien mahdollistaessa sen. Näin ollen on lähtökohtaisesti äärimmäisen vaikeaa sanoa, mikä pitäisi olla taisteluosaston varsinainen, kiinteä organisaatio. Yhdysvaltojen maavoimien kenttäohjesääntö FM 3-96 (Brigade Combat Team) ilmoittaakin heti organisaatiota käsittelevän päälukunsa alussa, että BCT:t toimivat usein osana divisioonaa tai Joint Task Forcea, jonka johdossa voi olla kaikkiaan jopa 6 BCT:a. Näitä taisteluosastoja voidaan muokata tehtäväkohtaisesti irrottamalla niistä osia tai lisäämällä niihin osia muista taisteluosastoista tai suoraan ylemmän johtoportaan alaisista muista joukoista. Kaikkiin taisteluosastoihin kuuluu kuitenkin liikkuvuutta, tykistöä, tiedustelua, viestiä, pioneereja, CBRN-kykyä ja ylläpitokykyä, ja näiden lisäksi voidaan tuoda uusia kyvykkyyksiä tai vahvistaa tiettyjä osa-alueita.[24]

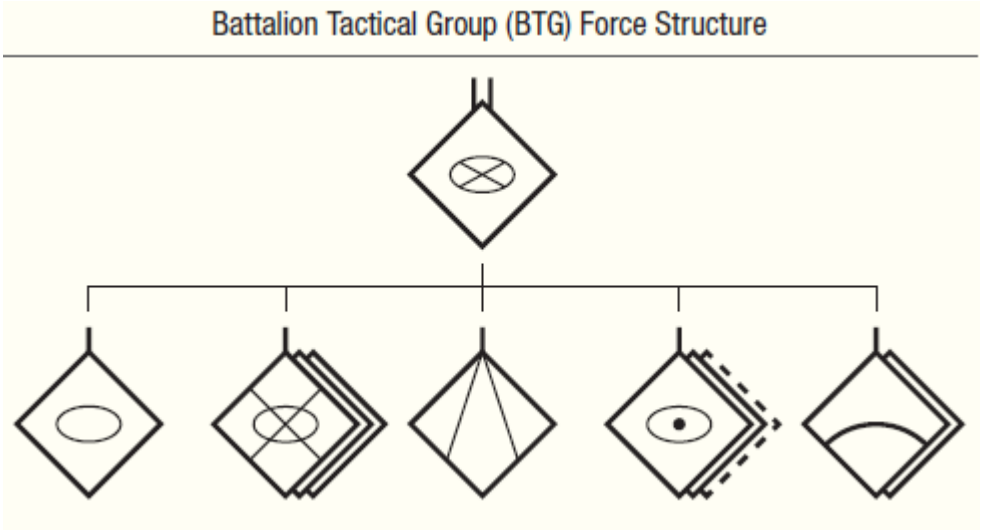
Hyvä esimerkki prikaatikokoisesta taisteluosastosta on Yhdysvaltalainen Infantry Brigade Combat Team (IBCT). Sen organisaatio muodostuu esikunnasta, kolmesta jalkaväkipataljoonasta, tykistöpatteristosta, tiedustelupataljoonasta, erikoisaselajipataljoonasta (BSTB) ja huoltopataljoonasta (Kuva 3). Katkoviivalla on merkitty uuden suunnittelutyön tuottama pioneeripataljoona, joka korvaisi erikoisaselajipataljoonan, lisäten taisteluosastoon yhden pioneerikomppanian ja yhden huoltokomppanian. Tämä kokoonpano tuottaa monipuolisissa ympäristöissä itsenäiseen taisteluun kykenevän kokonaisuuden. BSTB:n alla toimiva viestikomppania on tarkoitettu taisteluosaston ulkopuolisten yhteyksien muodostamiseen, ja sen avulla taisteluosasto liitetään Yhdysvaltojen puolustusministeriön tietoverkkoon (DODIN).[24]



Kuva 3: US Army Infantry Brigade Combat Team.[24]

Sellaisenaan IBCT ei ole kovinkaan tulivoimainen yksikkö, mutta se kykenee monipuoliseen toimintaan haastavissakin maastoissa kevyehköstä kalustostaan johtuen. Pääasiallisesti se taistelee jalkautuneena sellaisella maantieteellisellä alueella, joka sisältää yhden asutuskeskuksen ja kaksi tai useampaa toimintaa rajoittavaa maasto- tai ympäristötekijää. Tulivoimaisempi taisteluosasto onkin Armored Brigade Combat Team (ABCT), jossa jalkaväkipataljoonien tilalla on ”combined arms battallioneja”, jotka muodostuvat kahdesta mekanisoidusta jalkaväkikomppaniasta ja kahdesta panssarivaunukomppaniasta. Lisäksi koko tykistöpatteristo toimii tela-alustaisilla 155-millisillä aseilla, ja tiedustelu on muutettu panssaritiedusteluksi.[24]

Venäläinen sotilasajattelu on johtanut toisenlaiseen lähestymistapaan rakennettaessa taisteluosastoa. Taisteluosasto on rakennettu mekanisoidun pataljoonan päälle prikaatin sijaan, mutta se koostuu puhtaasti tulivoimaisista yksiköistä. Pataljoonan taisteluosaston organisaatio on yksinkertainen: yksi panssarivaunukomppania, kolme mekanisoitua jalkaväkikomppaniaa, yksi panssarintorjuntakomppania, 2-3 tykistöpatteria, yksi raketinheitinpatteri ja kaksi ilmatorjuntapatteria (Kuva 4). Pääesikunnan päällikkö Valery Gerasimovin mukaan näitä taisteluosastoja on tarkoitus olla käytössä 120 vuoden 2018 aikana.[26]



Kuva 4: Venäläinen pataljoonan taisteluosasto.[26]

Tällaisesta taisteluosastosta puuttuu Yhdysvaltalaiseen vastinkappaleeseen verrattuna orgaaninen kyky laajamittaiseen huoltoon sekä mahdolliset ylempään johtoportaaseen liittymisen mahdollistavat viestiosat, ellei liittyminen tapahdu johonkin komppaniaan tai patteriin lähtökohtaisesti kuuluvilla viestijärjestelmillä. Tulivoimaa sen sijaan riittää suorittamaan kohtalaisen suuriakin hyökkäyksiä vastustajan puolustukseen ja sen läpi, mikäli käyttötarkoituksena on saavuttaa jokin tasa ja luottaa muiden omien joukkojen saapuvan tueksi taisteluiden jälkeen.

Muut valtiot eivät ole julkaisseet juurikaan julkista tietoa taisteluosastoista, sillä niiden mainitaan usein olevan modulaarisia, tilanteenmukaisesti rakennettuja tilapäisiä organisaatioita, joissa esimerkiksi Kanadan tapauksessa perusrakenteena toimivaa pataljoonaa tai prikaatia vahvistetaan tykistöllä, pioneereilla, logistiikalla, lääkinnällä tai muilla tilanteeseen sopivilla joukoilla[37].

Tämän tutkielman viitekehyksessä on käytännöllisintä tarkastella ainakin organisaationa Yhdysvaltalaista IBCT:a, koska se pitää sisällään verrattain laajan määrän erityyppisiä joukkoja, selkeän johtamisrakenteen ja paljon viestijärjestelmiä. 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.

2.3. Johtaminen

Prikaatin taisteluosasto pohjautuu pitkälti siihen, että Yhdysvaltojen asevoimien uudistuksessa päätaistelujoukoksi vaihtui divisioonan sijaan prikaatin taisteluosasto. Tämän seurauksena ennen divisioonalle kuuluneet kyvykkyydet siirtyivät orgaanisesti prikaatin taisteluosaston johtoon. Kooltaan taisteluosastot ovat pienempiä kuin entiset prikaatit, mutta niillä on noin puolitoistakertainen taisteluvoima. Näin ollen taisteluosastojen esikunnilla on tarve entisten divisioonan tai armeijakunnan esikuntien tasoisille upseereille suunnitteluprosessissaan, ja tähän on perinteisesti kouluttauduttu Advanced Military Studies Program (AMSP) -ohjelmassa.[57]

Nykyaikaisen prikaatin taisteluosaston komentajan johtamistoimintaa ohjaa pitkälti tehtävätaktiikka. Yhdysvalloissa korostetaan jatkuvasti tehtävätaktiikan merkitystä kaikessa komentajan johtamistoiminnassa, ja termi Mission Command on selitetty ja tarkennettu useammassakin kenttäohjesäännössä (esim. FM 3-0 ”Operations” ja FM 3-96 ”Brigade Combat Team”)[24][23]. Sinnekin termi on kuitenkin rantautunut kaukaa historiasta, 1800-luvun Saksasta, jossa kenraali Helmut von Moltke kehotti nuorempia upseereja ymmärtämään, milloin on järkevää jättää tottelematta ylempää tulleita käskyjä, mikäli tilanne vaati sitä[31].

Johtamisprosessi perustuu paljolti käytettävissä olevan tiedustelutiedon hyödyntämiseen suunnittelun välineenä. Prikaatin taisteluosastolla on yhdysvaltalaisessa konseptissa käytössää yli kolmekymmentä erillistä tietojärjestelmää, jotka tarjoavat esikunnalle tilannetietoa ja vaikuttavat päätöksentekoon [76][25]. Suurin osa näistä on käytössä hitaasti liikkuvalla, vahvasti miehitetyllä ja kattavin viestiyhteyksin varustetulla pääkomentopaikalla, joka lähtökohtaisesti vastaa prikaatin johtamistoiminnasta kaikilla eri toimialoilla[24]. Näiden lisäksi taisteluosastolla on tarvittaessa käytössään ainakin taktinen komentopaikka, joka perustetaan usein jonkin alayksikön komentopaikan yhteyteen tai muutoin operaatiolle merkitykselliseen paikkaan[24].

Liitteessä 1 on esitetty BCT:n esikunnassa työskentelevä henkilöstö. Siitä on selkeästi nähtävissä, kuinka valtava määrä ihmisiä on lähtökohtaisesti käytössä suunnittelun työkaluina taisteluosaston taistelua suunniteltaessa. Kaiken kaikkiaan esikuntaan kuuluu 54 henkilöä, joista 14 on majuri-everstitasoisia, 26 luutnantti-kapteenitasoisia ja 14 toimiupseeria (tasoilla 2-4). Käytössä on kaikkea tiedustelusta ruokaan ja CBRN:stä sotilasilmailuun, eli esikunnassa olevan informaation määrä on massiivinen.[18] Tämän kokoisella esikunnalla, yhdistettynä alayksiköiden johtoihin on harvoin kykyä suorittaa koko joukolla kokoontumisia tilannetiedon vaihtamiseksi ja uusien suunnitelmien päivittämiseksi, ja usein erilaisin briefeihin osallistutaan käytössä olevin viestivälinein, joko radioilla tai puhe- tai videoyhteyksillä verkon yli[24].

Johtamisen tärkeä osa-alue on jatkuva tiedonvaihtaminen eri johtamistasojen välillä[7]. Tärkeän osan tästä muodostaa etenkin suunnitteluvaiheessa riittävän informaation saaminen ylemmältä johtoportaalta, jonka suunnittelu ohjaa alempien portaiden suunnittelua voimakkaasti. Tätä ohjausta voidaan toteuttaa esimerkiksi antamalla valmistautumistehtäviä suunnitteluun jo siinä vaiheessa, kun kokonaisuus ei ole vielä täysin selkeä[25]. Kun alemmat johtoportaat ovat saaneet suunnitelmansa valmiiksi ja saavutetaan sopiva vaihe suunnittelussa, potentiaaliset vaihtoehdot sotapelataan niiden vaikutusten tarkastelemiseksi, ja sen jälkeen päätetään lopullinen toimintavaihtoehto[25]. Esikunnan henkilöstön tulee jatkuvasti ylläpitää tietoisuuttaan ja arvioita läpi operaation siitä, kuinka suunnitelman etenemiseen vaikuttavat tekijät muuttuvat taisteluiden edetessä, koska niiden muutokset saattavat vaikuttaa merkittävästi siihen, miten seuraavat vaiheet tulisi toteuttaa[25].

Mikäli suunnitteluvaiheessa käytössä oleva tieto on väärää, se saattaa johtaa katastrofaaliseen lopputulokseen, kun suunnitelmia aletaan siirtää käytäntöön. Pahimmassa tapauksessa vastustajan joukkojen määrä on aliarvioitu tai sijainti on täysin väärä, ja taisteluosasto hyökkää merkityksettömälle alueelle. Taisteluosaston tehokkainta tulivoimaa edustavat sen epäsuoran tulen joukot, ja näin ollen myös niille päätyvän maalitiedon virheellisyys saattaa johtaa omiin tappioihin tai ammusten tarpeettomaan kuluttamiseen, joka aiheuttaa rasitteen huoltojoukoille.

2.4. Johtamisjärjestelmä

Nykyaikaisessa sodankäynnissä taktisen tason verkot ovat merkittävä osa kaikkea taistelua, ja ne liittyvät aina informaation jakamiseen eri osa-alueilla ja eri tasoilla. Käytännössä mistä valtiosta tahansa puhutaan, kun vaan on kyse taktisen tason viestijärjestelmistä, nousee esiin termi MANET – Mobile Ad Hoc Network. MANET on käytännössä itsestään muodostuva mesh-verkko, jota on mahdollista käyttää liikkuvassa ympäristössä, koska koko infrastruktuuri muuttuu osien liikkuessa, toisin kuin perinteisessä verkossa.[68] Tämä tarkoittaa käytännössä sitä, että verkon solmut ovat taisteluosaston mukana kulkevia laitteita, ja ne saattavat minä ajanhetkenä tahansa liittyä verkkoon tai poistua siitä vallitsevien maasto-, sää- tai sähkömagneettisen spektrin olosuhteista johtuen[13].

Britannian asevoimilla on käytössään Bowman-johtamisjärjestelmä, joka kattaa alleen dataterminaaleja, ohjelmistoja ja dataradioita, joiden avulla rakentuu laajan liitettävyyden omaava kokonaisuus[51]. Järjestelmällä on kyky jakaa taktisella tasalla johtamis- ja tiedustelutietoa, ja siirtää sitä jopa joint-esikuntiin tai muille yhteistyökumppaneille[27]. Käytössä ovat muun muassa automaattinen paikkatieto-, navigointi- ja raportointijärjestelmä, äänikommunikaatio ja datansiirto, ja taktinen internet langallisesti ja radioiden välityksellä[27][47].

Yhdysvallat on valinnut käyttöönsä taktisten verkkojen luomiseksi Warfighter Information Network-Tactical (WIN-T) -järjestelmän, joka kattaa alleen kaiken esimerkiksi prikaatin taisteluosaston tapauksessa massiivisen määrän laitteita (Kuva 5)[15]. Kuvasta nähdään, että yksittäinen IBCT saa käyttöönsä jopa 87 erilaista yhteyspistettä verkkonsa rakentamiseksi, ja nämä eri yhteyspisteet sisältävät vaihtelevan määrän erilaisia yhteystekniikoita, joita selvennetään hieman.

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							

Kuva 5: WIN-T laitteiston jako eri joukkotyypeille.[15]

WIN-T:n laitteiston yhteyspisteinä toimivat seuraavat:

- **TCN(-L):** Tactical Command 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.[15]

- **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.[15]

- **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[28]. SNE:n tiedonsiirto perustuu satelliittitiedonsiirtoon liikkeestä ja paikallaan, ja tällöin kaistanleveys rajoittaa jonkin verran käyttöön saatavia tietojärjestelmiä esimerkiksi komppanian päälliköiden päätöksenteon tueksi[15]. SNE:ien avulla voidaan myös laajentaa taisteluosaston verkkoa alueellisesti tai tarjota lisää liityntämahdollisuuksia raskaasti liikennöidyille alueille[15].

- **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.[15]

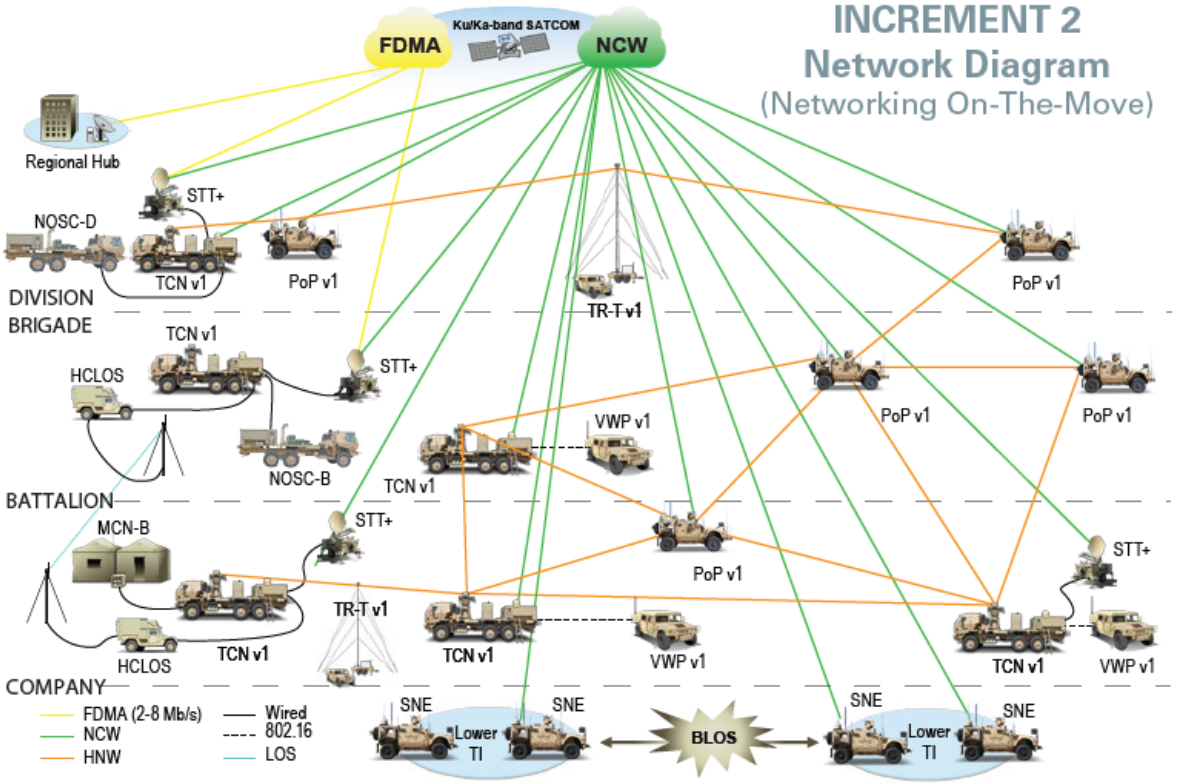
Näistä osista muodostuu laaja, monin eri tekniikoin varmennettu viestijärjestelmä prikaatin taisteluosaston alueelle, ja se tarjoaa myös yhteysmahdollisuuden ylempiin johtoportaisiin (Kuva 6). Kuvassa on esitetty myös edellisessä taulukossa mainitsematta jääneet komponentit:

- **HCLOS:** High Capacity Line of Sight, joka on tiedonsiirtokanava kahden JNN:n (Joint Network Node) välillä.[15]

- **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.[15]

- **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.[15]

- **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 valtavan määrän erilaisia ohjelmistoja reitittimien, kytkinten ja muiden verkkolaitteiden hallintaan, sekä esimerkiksi tulevien operaatioiden verkkosuunnitteluun.[15]



Kuva 6: WIN-T -verkko prikaatin taisteluosaston alueella.[28]

Suomalainen Bittium on myös valmistanut oman versionsa taistelukentälle sopivasta MANET-ratkaisusta. TAC WIN on johtamisjärjestelmäkokonaisuus, joka muodostuu point-to-point, point-to-multipoint ja ympärisäteilevistä radioyhteyksistä ja niitä yhdistävistä taktisista reitittimistä. Kokonaisuudella voidaan rakentaa taistelukentälle hyvin paljon WIN-T:ia muistuttava verkkokokonaisuus, pois luettuna satelliittiyhteydet. Järjestelmä mahdollistaa taktisten reitittimien kautta liikennöinnin taktisen verkon sisällä OLSR-reitityksen avulla ja ulkoiset yhteydet OSPF/BGP-reitityksen avulla. Se sallii myös VLAN:ien käyttämisen verkossa ja sisältää jonkinlaisen palomuuriratkaisun itsessään.[43]

Pääasiallinen trendi on selkeästi se, että valtiosta ja valmistajasta riippumatta taistelukentälle pyritään luomaan jonkinlainen MANET-verkko, johon alayksiköt ja jopa yksittäiset taistelijat kykenevät liittymään dynaamisesti minä tahansa ajankohtana ja missä tahansa taisteluosaston alueella, riippumatta siitä, minkä tukiaseman alueella toimivat. Verkkotopologia vaikuttaisi useimmiten muodostuvan mesh-tyyppiseksi, sillä erilaisia tukiasemia levitetään verkon alueelle laajasti, ja miltei kaikki yksittäisen taistelijan tasoa tehokkaammat laitteet kykenevät toimimaan verkon releasemina vähintään lähialueelle, ja verkko kykenee itsenäisesti suorittamaan soveltuvan reitityksen, mikäli yksittäiset solmut poistuvat verkosta.

2.5. Taisteluosaston tietoliikenne ja tiedon tallennus

Taisteluosaston sisällä tapahtuu valtava määrä tietoliikennettä jatkuvasti. Pelkästään verkon valvontaan ja hallintaan liittyvää dataa liikkuu johtamisjärjestelmässä jatkuvasti edestakaisin verkon eri solmujen välillä. Esimerkiksi Bittiumin taktisten reitittimien taktisessa verkossa käyttämä OLSR-protokolla (Optimized Link State Routing) lähettää jatkuvasti sanomia verkkonaapureilleen selvittääkseen verkon tilaa ja mahdollisia uusia naapureita. Lisäksi reitittimet jakavat keskenään tietoa omista naapureistaan.[40] Tämän lisäksi useat eri taistelunjohtojärjestelmät jakavat keskenään tietoa esimerkiksi tilannekuvasta, erilaiset puhepalvelut tuottavat jatkuvasti liikennettä taisteluosaston kommunikoidessa keskenään, ja näiden lisäksi voidaan olettaa, että taisteluosaston sisällä toimii jonkinlainen tiedostopalvelin, joka tuottanee suuren määrän liikennettä molempiin suuntiin itsestään[7].

Pääasiallisesti taisteluosastojen tietoliikenne ei kuitenkaan rajoitu taisteluosaston sisäiseen liikennöintiin, vaan ne saattavat olla viestijärjestelmien kautta liitettynä ylempään johtoportaaseen tai naapureihinsa, tai ne voivat olla liittyneenä alueelliseen verkkoinfrastruktuuriin kaapeliteitse. Esimerkiksi IBCT:n tapauksessa yhteys puolustusministeriön tietoverkkoon (DODIN) on olennaista siksi, että näin se pääsee osaksi LandWarNet:iä, joka tarjoaa tällöin taisteluosaston käyttöön erilaisia sovelluksia, dataa ja laskentapalveluita[24]. LandWarNetin kautta taisteluosaston verkkoon liittyy muun muassa taktiset johtamisjärjestelmät, ilma- ja ohjuspuolustuksen suunnittelu- ja hallintajärjestelmä, tykistödatajärjestelmä, blue force tracking ja taktinen ilmatilanhallintajärjestelmä[24]. Lisäksi järjestelmästä löytyy yksilöidyt verkkotallennusmahdollisuudet eri johtamistasoille, tietokantoja, tiedostopalvelimia, verkkosivustoja ja sähköpostipalveluita[24].

Tietoliikenteen määrää on myös arvioitu Yhdysvaltojen kongressin budjettitoimiston tutkimuksessa ”The Army’s Bandwidth Bottleneck” vuodelta 2003. Suurimman pullonkaulan tiedonsiirrossa näyttivät tuolloin muodostavan nimenomaan pataljoonan ja prikaatin tasoilla tapahtuva tiedonsiirto, kun matalammat tasot tarvitsivat vähemmän siirtokaistaa tarvittavan tiedon siirtämiseksi ja ylemmillä tasoilla oli paremmat viestijärjestelmät käytössään. Sen sijaan arvioissa vuoden 2010 tasoihin armeijakunnan ja divisioonan arvioitiin kärsivän eniten riittämättömästä tiedonsiirtokapasiteetista (Kuva 7). Prikaatin tapauksessa nuolilla on osoitettu joko ylempiin johtoportaisiin tai johdettaviin joukkoihin tapahtuva liikennöinti, ja ylärajojen on oletettu toteutuvan, mikäli prikaatitasoisten joukkojen operaatiokeskusten välillä tapahtuu jatkuvaa tiedonjakoa.[73]

Effective Bandwidth Supply Versus Peak Demand in 2010, by Command Level

Command Level[a]	Relative Supply Versus Peak Demand (S : D)[b]
Corps[c]	1 : 10 to 30
Division[c]	1 : 10 to 30
Brigade[c,d]	1 : 3 to 10↑ 1 : 5 to 15↓
Battalion	1 : 1.5 to 3
Company	1 to 4 : 1
Platoon	4 to 10 : 1
Squad/Vehicle	7 to 20 : 1

Kuva 7: Arvioitu tiedonsiirtokapasiteetin riittävyys vuonna 2010.[73]

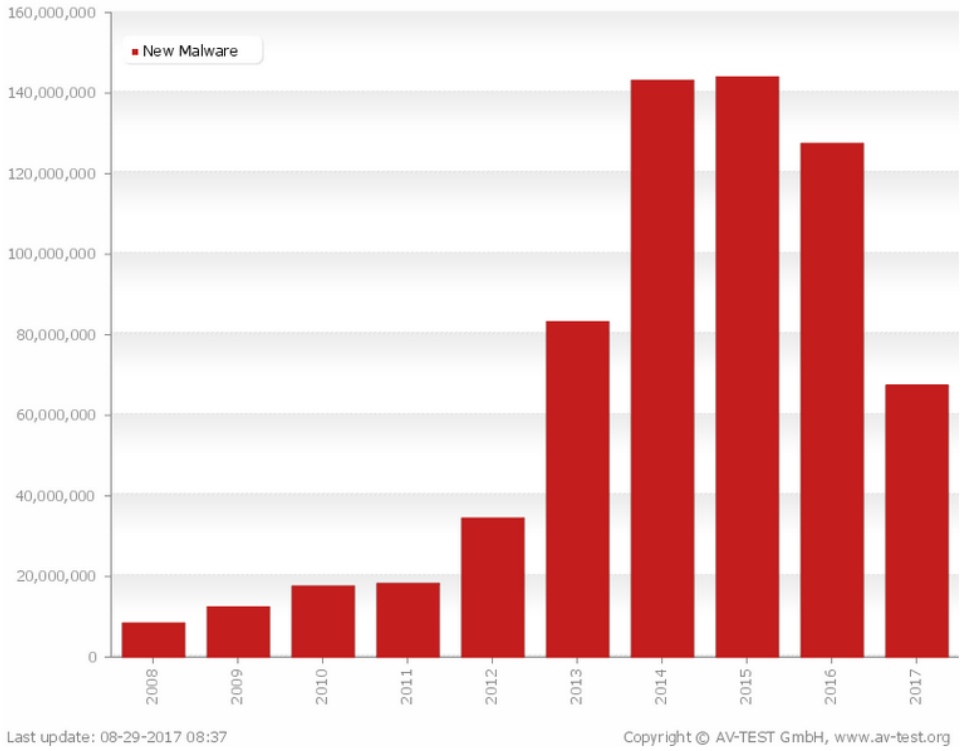
Koska voidaan olettaa, että taisteluosaston kokoisella joukolla on käytössään jonkinlainen tiedostopalvelinjärjestelmä, voidaan myös olettaa, että tietoa on tällöin tallennettu sekä suoraan palvelimelle, että työasemille. Tämä toimenpide auttaa siinä tapauksessa, että verkko ei jostain syystä ole kaikkina ajanhetkinä käytettävissä. Tämä tarkoittaa, että ainakin laadittuja käskyjä ja suunnitelmia on tallennettu useampaan sijaintiin verkon eri osissa ja erityyppisissä laitteissa. Tällöin potentiaalisella hyökkääjällä on yksi hyökkäysvektori lisää, kun saman tiedon voi löytää useaa eri lähdettä tarkastelemalla.

Taisteluosaston toiminnasta johtuen suunnitelmat ja käskyt ovat usein hyvin aikakriittisiä. Tämä tarkoittaa sitä, että vaikka pääteasemille tai palvelimille on usein tallennettuna paljon dataa, on suurin osa siitä todennäköisesti vanhentunutta sisällöltään. Tästä johtuen potentiaalista hyökkääjää ajatellen saatavilla on paljon dataa, mutta vain osa siitä on ajankohtaista sisällöltään. Käskyjen osalta tämä voi hyvinkin pitää paikkansa, mutta BCT:n esikunnassa ylläpidetään myös paljon tiedustelutietoa raporttien, dokumenttien, kuvien ja tietokantojen muodossa[24]. Tällaisessa tapauksessa hyökkääjällä on mahdollisuus vaikuttaa siihen, minkälaista tietoa siitä itsestään on saatavilla tai muokata toimintaansa sen pohjalta, minkä taisteluosasto on tiedustelullaan havainnut.

3. NYKYAIKAISET KYBERUHKAT

3.1. Kyberhyökkäysten kehitys

Kyberhyökkäykset ovat aikojen saatossa muuttuneet paljon niin rakenteeltaan kuin käyttötarkoitukseltaan, eikä kehitys ole aina ollut selkeästi suuntautunutta kummankaan osalta. Ensimmäinen tapaus haittaohjelmasta lienee Creeper vuodelta 1971, ohjelma joka liikkui ARPANET:n sisällä TENEX-käyttöjärjestelmällä varustetulta päätelaitteelta toiselle ja tulosti kohdekoneen kaukokirjoittimella viestin ”I’m the creeper: catch me if you can”[35]. Tämän jälkeen uusien haittaohjelmien ilmestyminen on ollut selkeässä kasvussa viime vuosiin asti, kuten AV-Testin kuvaaja kertoo (Kuva 8).[42] Vuodesta 2015 eteenpäin havainnot uusista haittaohjelmista ovat vähenemään päin, ja määrän sijaan haittaohjelmissa on keskitytty laatuun – monet uusista haittaohjelmista ovat merkittävästi aikaisempia monimutkaisempia ja vaarallisempia, eikä niiden tarkoitus olekaan iskeä välittömästi vaan tarjota edellytykset hyvin suunnitellulle laajemmalle käytölle[32].



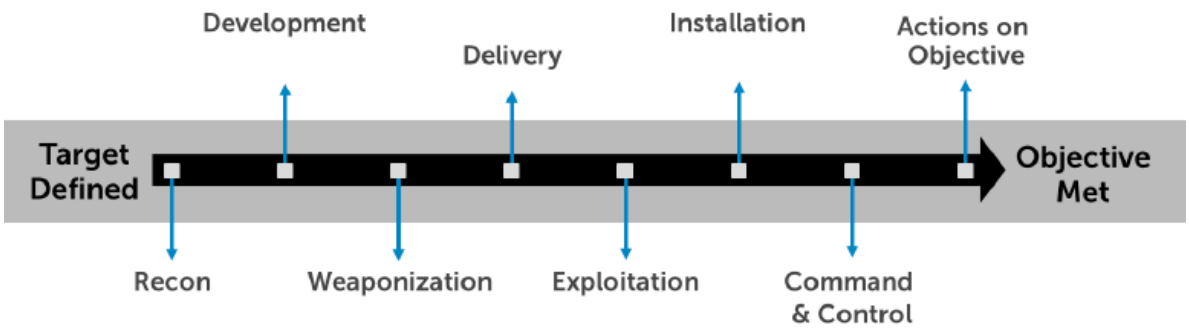
Kuva 8: AV-Testin vuotuiset havainnot uusista haittaohjelmista[42].

Nykypäivän kyberuhkat kohdistuvat usein käyttäjän harhauttamiseen varsinaisen teknisen kyberhyökkäyksen sijaan. Tästä johtuen erityyppiset spear-phishing -hyökkäykset ovat myös vaivanneet etenkin yrityksiä ja valtiollisia toimijoita, joiden työntekijöiden tietoturvakäyttäytyminen on johtanut ongelmallisiin tilanteisiin. Tämän lisäksi näkyviä tekijöitä uhkakuvan muuttumisessa ovat esimerkiksi ransomware-ohjelmien määrän merkittävä kasvu vuonna 2016, samoin kuin Internet of Things -ilmiön myötä esiin noussut heikko tietoturvan taso laitteissa, joita ei aiemmin oletettu käytettävän minkäänlaiseen haitalliseen toimintaan. [55]

Näistä monet tapaukset eivät kuitenkaan sovellu sotilaalliseen toimintaympäristöön, sillä käyttäjät eivät ole suoraan yhteydessä internetiin tai sähköpostiin, eivätkä siten kykene avaamaan haitallisia linkkejä tai mahdollista erilaisten haittaohjelmien latautumista verkon yli ilman todella edistyneitä toimintoja. Jotkin haittaohjelmat kuitenkin kykenevät monenlaisiin erilaisiin toimintoihin hyödyntäen haavoittuvuuksia eri järjestelmissä, joita varsinkin kohdistetut advanced persistent threat (APT) -tyyppiset hyökkäykset hyödyntävät edistyneessä koodissaan[4].

Erilaisissa kyberhyökkäyksissä on korostunut entistä voimakkaammin tarve piilottaa itsensä. Koska monet virustorjuntaohjelmistot sekä ohjelmisto- tai laitteistopohjaiset palomuurit toimivat havaitsemalla tietynlaisia käyttäytymismalleja tietoliikenteessä tai ohjelmistojen toiminnassa, täytyy hyökkääjän usein naamioitua käyttäytymään mahdollisimman paljon tavallisen käyttäjän tavoin[8].

Vaikka ei puhuttaisi suoranaisesta APT-hyökkäyksestä, sotilaallisessa kontekstissa on kuitenkin syytä puhua advanced threatista, edistyneestä uhkasta. Tämän erottaa tavanomaisesta uhkasta se, että se on aina kohdistettu johonkin tiettyyn kohteeseen, ja sen valmistelu ja toteuttaminen perustuvat kohteesta saatuihin tietoihin. Toisin kuin geneerisissä uhkissa, näiden takana on myös havaittavissa selkeä motiivi, tavoitteet ja toimijat. Ne rakennetaan selkeän kaavan mukaisesti (Kuva 9), ja niiden käyttö on selkeästi tavoitehakuista. [4]



Kuva 9: Edistyneen uhkan toimintaketju.[4]

Tässä kuvassa on esitetty selkeästi hyökkäyksen suunnittelu, rakentaminen ja käyttö aikajanalla. Sen eri vaiheet ovat kaikki kriittisiä halutun tavoitteen saavuttamiseksi, vaikka joitain niistä kyetään karsimaan tavoiteltaessa vain rajallista vaikutusta. Kohdat on esitelty Dell Secure Worksin julkaisussa seuraavasti:

1. Tiedustelu (Reconnaissance): Hyökkääjä kerää tietoa kohteestaan ennen hyökkäystä ja sen aikana hyödyntäen avointen lähteiden tiedustelua, skannausta, Webiä, ihmislähteitä tai varastamalla tietoja.
2. Kehitys (Development): Hyökkääjä kerää hyödyllistä tietoa kohteen infrastruktuuri ja käytössä olevien välineiden kehityksestä.
3. Aseistaminen (Weaponization): Yhdistetään etähallintaan soveltuva troijalainen haittaohjelman muuhun hyötykuormaan yhdeksi paketiksi.
4. Toimitus (Delivery): Tämä vaihe kuvaa haittaohjelman saattamista uhrin organisaatioon eri välinein joko verkkoteitse tai fyysisesti.
5. Hyödyntäminen (Exploitation): Tässä vaiheessa kuvataan haitallisen koodin suorittamisen keinot, ja tarkastellaan käyttääkö hyökkääjä uusia vai muilta hankittuja nollapäivähaavoittuvuuksia, vai turvautuuko se käyttäjien sosiaaliseen manipulointiin.
6. Asennus (Installation): Tässä vaiheessa kuvataan hyökkääjän toimenpiteet ja mahdollisesti jättämät jäljet asennettaessa haittaohjelmaa haavoittuviin järjestelmiin.
7. Hallinta (Command and Control): Tässä vaiheessa kuvataan hyökkääjän toimenpiteitä saastuneen järjestelmän kanssa kommunikointiin. Tämä käsittää muun muassa sisäänkirjautumiset eri menetelmin ja datan lähettämiseen tarkoitetut reitit.
8. Toiminta kohteessa (Action on Target): Kun hyökkääjä on saavuttanut sisäänpääsyn kohteeseen, tässä vaiheessa hyökkääjä toteuttaisi haluamansa vaikutuksen, esimerkiksi tietojen varastamisen kohteen kovalevyltä.[4]

3.2. Palveluiden käytön estämiseen tähtäävät hyökkäysmenetelmät

Yksi toteutukseltaan yksinkertaisimmista ja vaikutukseltaan kohtalaisen tehokkaista menetelmistä on DoS (Denial of Service) eli palvelunestohyökkäys. Palvelunestohyökkäyksiä on erityyppisiä, mutta kaikkien yhteisenä tavoitteena on estää hyötyliikenteen kulku joko kokonaan, tai ohjata se uudelleen hyökkääjän haluamaan kohteeseen.[63]

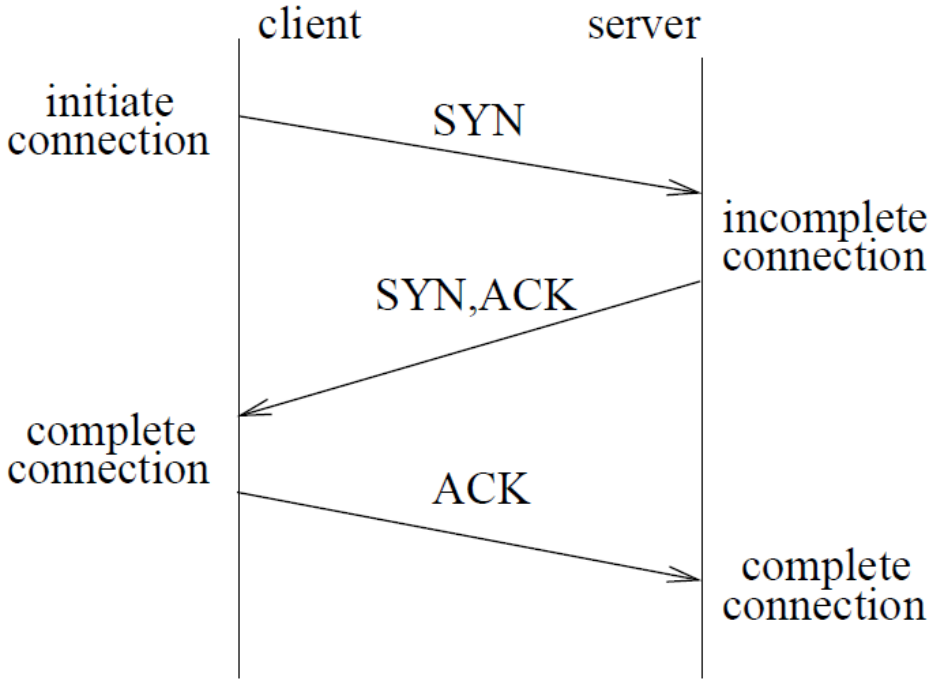
Yksinkertaisin ja perinteisin hyökkäysmalli perustuu käytössä olevan siirtokaistan tukkimiseen ohjaamalla merkittävä määrä liikennettä yhteen kohteeseen.[63] Vaikka käytössä olisi minkälainen nykyaikainen verkkolaite tahansa, esimerkiksi Mirain kaltainen botnet-verkkoon perustuva palvelunestohyökkäys tuottaa parhaimmillaan liikennettä jopa 623 gigatavua sekunnissa. Tämän lisäksi hyökkäys suuntautui yksittäiseen kohteeseen parhaimmillaan jopa 158 839 IP-osoitteesta kerrallaan.[69][6] Tällaisessa tilanteessa ilman valtavaa, laajennettavaan infrastruktuuriin perustuvaa palvelin- ja reititinkapasiteettia verkkoliikenne kohteeseen pysähtyy väistämättä.

Mirai oli haittaohjelma, jonka avulla toteutettiin valtavia DDoS-hyökkäyksiä valikoituja verkkosivustoja, teleoperaattoreita ja datakeskuksia vastaan elokuusta 2016 helmikuuhun 2017[6]. Itse haittaohjelma oli perusrakenteeltaan lähimpänä matoa eri haittaohjelmatyypeistä, mutta sen funktio oli saastuttaa haavoittuvia IoT-laitteita ja luoda niistä palvelunestohyökkäyksiin käytettävä botnet-verkko[6][71]. Kohteina olivat esimerkiksi erilaiset verkkoon kytketyt valvontakamerat, kotireitittimet ja tallentavat digiboksit, joissa oli käytössä oletuskäyttäjänimet ja -salasanat, koska niitä ei koettu suoranaisena uhkana verkkohyökkäykselle[6].

Mirain lähdekoodi muodostui kolmesta osasta: Bot, CNC server ja Loader[71]. Bot oli haavoittuneissa laitteissa toimiva ohjelman suorittajaosio, joka toteutti hyökkäykset, sammutti toimintaan vaadittavia portteja varaavat prosessit ja skannasi satunnaisia ip-osoitteita löytääkseen uusia hyökkäyskohteita. Bot käynnistyi kertaalleen, jonka jälkeen se poisti oman ohjelmatiedostonsa ja jäi käyntiin vain laitteen välimuistiin, näin vähentäen havaitsemistodennäköisyyttään. CNC server oli Mirain käsittely- ja tietokantaosio, jonka tarkoituksena oli toimia bottien luomien yhteyksien vastaanottajana ja välittää niille hyökkäyksen toteuttamiseksi tarvittavia komentoja. Loader vastaanotti tietoa verkossa havaituista haavoittuvista laitteista ja toimitti niihin Bot-hyötykuorman.[71] Mirai saastutti ensimmäisen kymmenen minuutin aikana 11 tuhatta laitetta, ja ensimmäisten 20 tunnin aikana kaiken kaikkiaan 64,500 laitetta, ja parhaimmillaan botnet koostui noin 600 tuhannesta laitteesta[6].

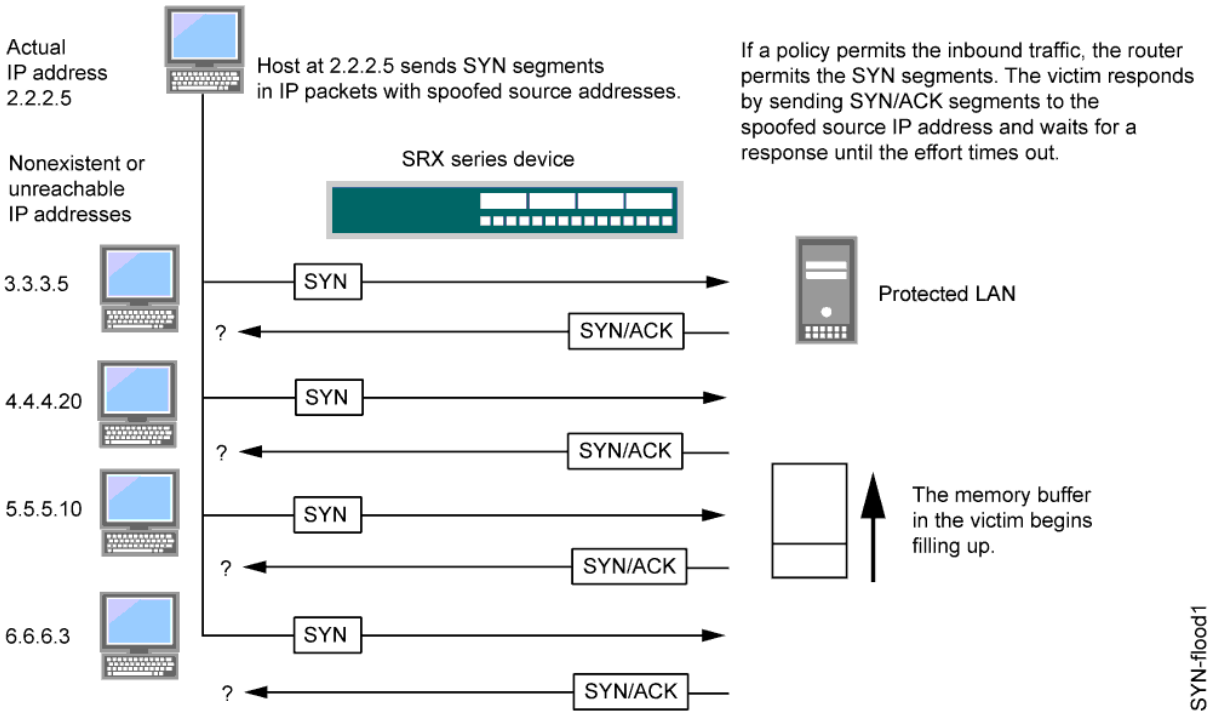
Toinen vaihtoehto palvelunestohyökkäyksen päämääräksi on kohdejärjestelmän resurssien kuluttaminen. Tällaisessa tapauksessa kohdejärjestelmään kohdennetaan sellaisia toimintoja, joilla pyritään pakottamaan se ottamaan käyttöön enemmän käyttömuistia tai prosessorin laskentatehoa siihen pisteeseen asti, että se ei kykene enää suorittamaan varsinaista toimintaansa. Tähän johtavia vaikutuksia voivat olla esimerkiksi laskentatehon tai käyttömuistin loppuminen, tiedostojärjestelmän täyttäminen turhalla datalla, tai yksinkertaisesti käyttöjärjestelmän kaatuminen. Tällaisen hyökkäyksen etu verrattuna siirtokaistan kuormittamiseen on se, että sen voi suorittaa pienenkin siirtokapasiteetin laitteella, koska se ei perustu valtavaan liikennemäärään vaan kohdelaitteiden hämäämiseen.[63]

Yleinen ja verrattain yksinkertainen menetelmä resurssien kuluttamiseksi on SYN Flood -hyökkäys, jossa hyökkääjän tarkoituksena on työllistää kohteena oleva järjestelmä puoliavoimiksi jätetyillä yhteyspyynnöillä siihen pisteeseen, ettei se kykene vastaanottamaan todellisia hyöty-yhteyksiä todellisilta käyttäjiltä. Normaalissa tapauksessa muodostettaessa TCP-yhteys haluttuun kohteeseen, lähetetään sille ensin synkronointi- eli SYN-paketti, jolloin kohdekone saa tiedon siitä, että siihen halutaan ottaa yhteys. Tämän jälkeen kohde palauttaa lähteelle SYN-ACK -paketin kertoakseen, että se on saanut yhteyspyynnön ja on valmis muodostamaan yhteyden. Lopuksi lähdekone lähettää vielä acknowledgement- eli ACK-paketin kuittauksena, ja näin muodostuu TCP-yhteys (Kuva 10).[63][60][12]



Kuva 10: TCP 3-way handshake, normaali yhteyden muodostaminen.[60]

SYN Flood -hyökkäyksen voi toteuttaa kahdella eri tapaa. Yksinkertaisimmillaan kyseessä on suora hyökkäys, jolloin yksi tai useampi lähde lähettävät SYN-paketteja kohteelle mutta eivät vastaa SYN-ACK pakettiin enää ACK-paketilla, vaan kohde jää odottamaan vastausta ja varaa näin ollen resursseja potentiaalista yhteyttä varten[12]. Tällainen hyökkäys on kuitenkin verrattain helppo ehkäistä pakottamalla vastaanottava järjestelmä estämään yhteyspyynnöt, mikäli sama lähde lähettää niitä jatkuvasti[10]. Tehokkaampi menetelmä onkin spoofing-hyökkäys, jossa lähdejärjestelmä väärentää oman ip-osoitteensa jokaiseen lähetettävään SYN-pakettiin, lähtökohtaisesti sellaiseksi osoitteeksi joka ei ole tavoitettavissa[10][63]. Tällöin kohde lähettää SYN-ACK pakettinsa tavoittamattomaan osoitteeseen ja jää odottamaan joko yhteyden avaavaa ACK-pakettia tai yhteyden muodostamisen peruuttavaa RST-pakettia, ja sen muistipuskuri alkaa täyttyä puoliavoimista yhteyksistä (Kuva 11)[48].



Kuva 11: SYN Flood -hyökkäys.[48]

Kolmas, ja potentiaalisesti yksi haitallisimmista palvelunestohyökkäysten tyypeistä on reititykseen ja DNS-palveluihin kohdistuva hyökkäys. Mikäli kohteella on käytössään DNS-palvelin, hyökkääjä pyrkii muokkaamaan sen tietokannassa olevia URL-osoitteen ja IP-osoitteen muodostamia pareja haluamikseen siten, että haluttuun kohteeseen suunnattu pyyntö ohjautuu uudelleen hyökkääjän haluamaan kohteeseen. Mikäli taas käytössä on puhdas reititinverkko, voidaan yksittäisten reitittimien reititintauluja muokata sellaisiksi, että hyökkääjä saa ohjattua liikenteen haluamaansa osoitteeseen.[63]

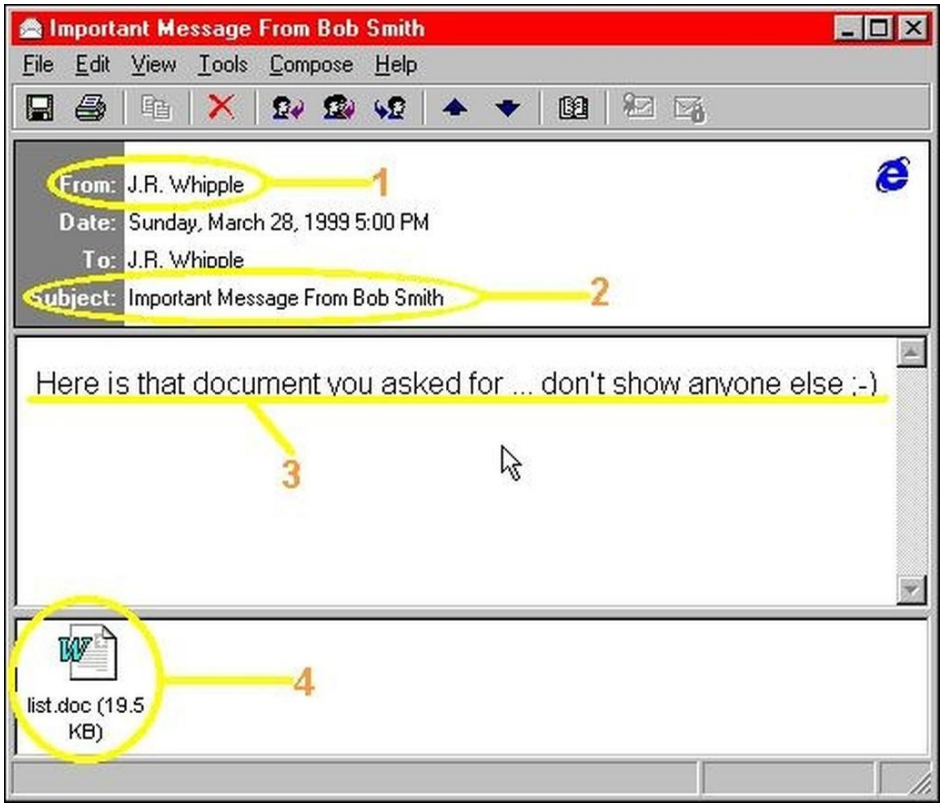
3.3. Järjestelmään tunkeutumiseen perustuvat hyökkäykset

Suoran, verkkopohjaisen hyökkäyksen lisäksi yhtenä hyökkäysvektorina ovat erilaiset haitta-ohjelmat. Niiden toiminta voi olla samankaltaista kuin manuaalisessa verkkohyökkäyksessä, tai ne voivat tarjota verkkohyökkäykselle reitin sisäänpääsyyn. Tämän kaltaisia uhkia ovat esimerkiksi virukset, madot, rootkitit ja troijalaiset.[32]

Virukset

Virukset ovat yksinkertaisia, pieniä ohjelmia tai koodin osia, jotka tartuttavat kohdekoneen tiedostoja. Viruksen päätarkoituksena on monistautua ja toimittaa hyötykuormansa kohteeseen. Käytännössä virus on vain välittäjä, jonka kohteeseen välittämä hyötykuorma voi olla käytännössä mitä tahansa, mutta itse viruksen tehtävänä on vain monistuminen ja saastuttaminen. Virusten tartuttamismekanismit ovat erilaisia, ja niitä voivat olla esimerkiksi makrovirukset, joita voi esiintyä esimerkiksi makroja sisältävissä Microsoft Office -dokumenteissa tai bootsector-virukset, jotka muokkaavat käyttöjärjestelmän käynnistymisen yhteydessä ajettavia prosesseja.[32]

Melissa on yksinkertainen esimerkki perinteisestä tietokoneviruksesta. Se havaittiin vuonna 1999, ja se oli siihen mennessä nopeimmin ympäri maailmaa levinnyt virus[46]. Se oli Microsoft Wordilla luoduissa .doc-tekstitiedostoissa toimiva makrovirus, ja sen käyttötarkoitus oli levittää itsensä sähköpostitse 50 uudelle uhrille[50][53]. Saastunut tiedosto oli ensin jaossa internetin keskustelufoorumilla, ja kun käyttäjä latasi sen ja avasi sen Microsoft Wordilla, se käynnisti makron joka lähetti sen sähköpostitse Microsoft Outlookin osoitekirjassa 50 ensimmäiselle yhteystiedolle saatetekstin kera (Kuva 12)[46]. Se tarkasti lisäksi itse luomansa rekisteritiedon arvon, jotta sama kone ei toistaisi lähetystä useammin kuin kerran, ja piilotti Wordin valikoista makrojen käyttöön liittyvät asetukset[46][53]. Virus saastutti myös uhrikoneella luodut uudet .doc-tiedostot, ja vaikka saastunut kone lähettääkin tiedoston vain kerran 50 uudelle uhrille, mikäli tämä uusi .doc-tiedosto avataan jollain muulla tietokoneella, se toistaa saman lähetyksen[53]. Lisäksi virus käynnisti erillisen prosessin aina, mikäli Wordissa oli avoinna tekstidokumentti silloin, kun sen ajanhetken minuutit täsmäsivät päivämäärän kanssa (esimerkiksi 12:15 huhtikuun 15. päivänä), ja kirjoitti avoimeen dokumenttiin: ”Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here”, joka on viittaus Simpsoneissa esiintyneeseen keksittyyn sanaan Kwyjibo, jota viruksen kehittänyt David L. Smith käytti nimimerkkinään[46][50].



Kuva 12: Melissa-viruksen toimitusmenetelmä tunnusmerkkeineen.[36]

Madot

Madot ovat monilta osin samankaltaisia kuin virukset, mutta niissä on yksi merkittävä ero. Madot ovat itsenäisiä ohjelmia, eivätkä ne tarvitse isäntätiedostoa, kuten virukset. Ne kykenevät liikkumaan järjestelmien sisällä ja monistamaan itsensä riippumatta kohteesta, ja monet nykyaikaisista haittaohjelmista ovat joko matoja tai sisältävät madon toiminnallisuudet osana laajempaa kokonaisuutta.[32]

Yksi esimerkki kuuluisasta madosta on Conficker. Se oli verkkomato, jonka ensimmäiset variantit Conficker.A ja Conficker.B ilmestyivät marras-joulukuussa 2008, ja uudemmat versiot B++, C, D ja E alkuvuodesta 2009[52]. Conficker hyödynsi tarttumisessaan ja leviämisessään Windowsiin rakennettua palvelinpalvelua, jonka kautta se sai suoritettua tarttumiseensa vaadittavan .dll-tiedoston[59]. Ensimmäiset versiot monistuivat Windowsin tiedostonjakamisjärjestelmän avulla sekä siirrettävän median laitteita saastuttamalla, mutta C-variantti tarjosi Confickerille mahdollisuuden jakaa tiedostoja peer-to-peer -menetelmällä saastuneiden kohdekoneiden välityksellä[22]. Conficker sisälsi monia suojausmenetelmiä poistamisen ja havaitsemisen estämiseksi – se muun muassa lukitsi tiedostonsa useaan eri kansioon tiedostojärjestelmässä, ja esti rekisteriavaimensa muokkaamisen tai lukemisen[22]. Tämän lisäksi se esti Windowsin turvallisuustoiminnallisuuksien automaattisen käynnistymisen, virheraportoinnin ja automaattiset päivitykset, kuten myös vikasietotilassa käynnistymisen[22]. Havaitsemisriskin pienentämiseksi sen päivitysten noutamiseen käytössä olevalta satunnaiselta ip-skannaukselta oli estetty muun muassa tietoturvayhtiöiden ja Microsoftin osoitteita, jotteivat ne havaitsisi haittaohjelmaa verkossa[59]. Kaikesta hienostuneisuudestaan huolimatta Conficker osoittautui verrattain vaarattomaksi madoksi itsessään, sillä se tarjosi lähinnä toimituskanavan muiden haittaohjelmien potentiaaliseen käyttöön, lähinnä valmistellen kohdekoneita johonkin tehokkaampaan käyttöön[11].

Troijalaiset

Troijalaiset eroavat perusrakenteeltaan viruksista ja madoista siten, että ne eivät monistu tai levitä itseään uusiin kohdekoneisiin omilla toiminnallisuuksillaan, vaan ne vaativat käyttäjää käynnistämään uskottavalta vaikuttavan sovelluksen omalla tietokoneellaan[49][41]. Troijalaiset ovat usein nimetty jonkin normaalin ohjelman mukaisesti, ja saattavat jopa käynnistää halutun ohjelman, mutta suorittavat samalla jonkin muun toiminnon järjestelmähaavoittuvuuden hyödyntämiseksi[77][49]. Tällaisia voivat olla muun muassa järjestelmänvalvojan oikeuksien saavuttaminen, jonkin muun haittaohjelman asentaminen tai takaportin avaaminen järjestelmään haitallisen liikenteen mahdollistamiseksi[63][77].

Zeus, toiselta nimeltään Zbot on yksi pahamaineisimmista ja laajalle levinneimmistä informaatiovarkauksiin käytetyistä troijalaisista[78]. Se oli käytännöllisesti saatavilla suoraan foorumeilta ostamalla, normaalisti noin 700 dollarin hintaan mutta joskus jopa ilmaiseksi[21]. Zeus oli sinänsä yksinkertainen ohjelma, jonka päätarkoitus oli useimmiten varastaa kohdekoneelta käytettyjä käyttäjätunnus-salasanayhdistelmiä sekä pankkitunnuksia tai sosiaaliturvatunnuksia sellaisilta sivustoilta, joissa niitä käytettiin sisäänkirjautumiseen[20][78]. 2009 mennessä Zeuksen arvioitiin vaarantaneen jopa yli 74 tuhatta FTP-tiliä verkkosivuilta tai yrityksiltä, mukaan lukien muun muassa NASA, Amazon ja Oracle[20].

Zeuksen levittämiseen on käytetty useita erilaisia menetelmiä, joista yleisimpiä ovat olleet:

- Drive-by downloadit suoraan verkkosivustoilta, jossa käyttäjän vierailema verkkosivusto sisältää toiminnallisuudet, joilla se tunnistaa kohdejärjestelmän haavoittuvuuksia ja lataa itsensä kohteeseen[21].

- Sähköpostispammi, jossa on hyödynnetty sosiaalisen manipuloinnin keinoja käyttäjän luottamuksen voittamiseksi. Hyökkääjä on saattanut naamioitua muun muassa Yhdysvaltain veroviranomaisen, Facebookin tai Microsoftin edustajaksi ja sisällyttänyt viestiin valheellisen linkin hyökkääjän haluamalle sivustolle[21][20].

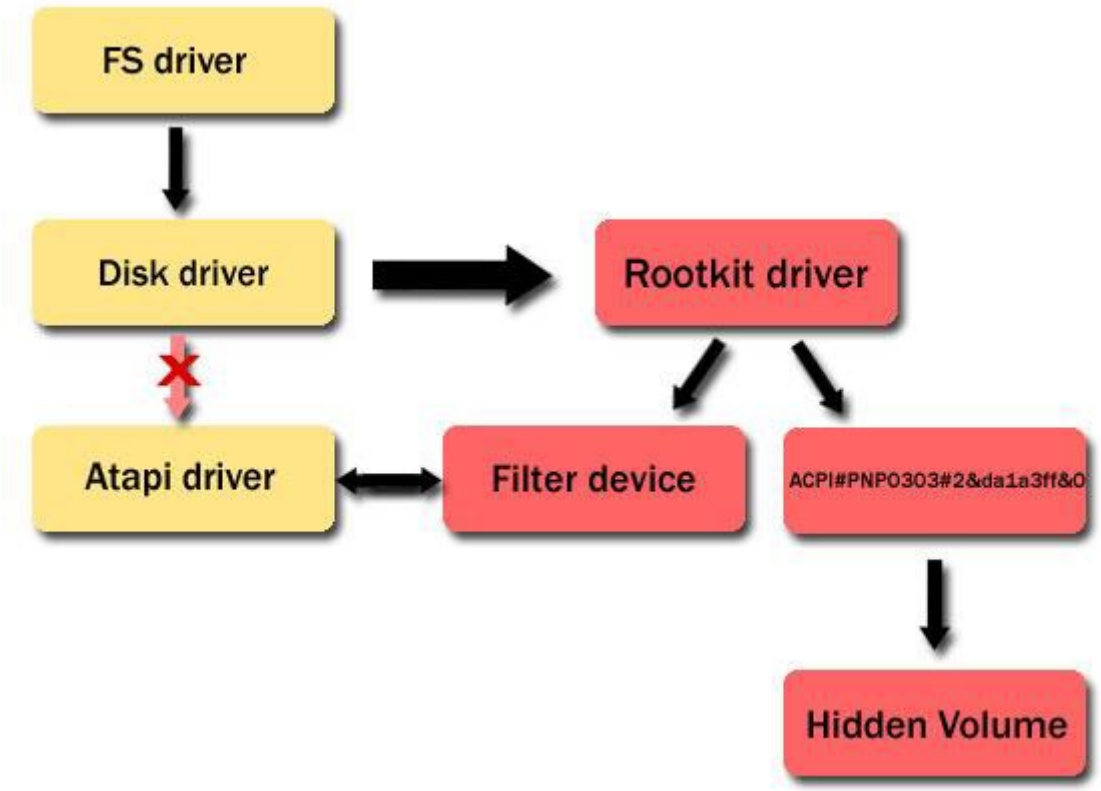
Käynnistyttyään kohdekoneessa Zeus kopioi itsensä tiedostokansioon, ja etsii Windowsin sisäänkirjautumisprosessin, eli winlogon.exen[21]. Kun se on löytänyt kohteensa, se injektoi oman koodinsa tähän kohdeprosessiin ja sulkee oman pääprosessinsa[21][72]. Tämän lisäksi se injektoi lisää koodia Windowsin eri palveluista vastaavaan svchost.exe-prosessiin, jonka avulla se kykenee vaihtamaan internet-selaimen näyttämän sisällön omakseen valitsemillaan verkkosivustoilla, ja näin ollen keräämään muun muassa käyttäjän syöttämät tunnukset omiin kryptattuihin ja piilotettuihin tiedostoihinsa[21][20][72][78]. Valheellisten verkkosivustojen kautta tehtyjen tekstikaappausten lisäksi Zeus kykenee myös tallentamaan yksittäisiä näppäimistön painalluksia tai ottamaan ruutukaappauksen[20][72]. Zeus kykenee lisäksi kommunikaatioon hallintapalvelimen kanssa, jolta se voi vastaanottaa komentoja eri toimintojen suorittamiseksi tai kerättyjen tietojen lähettämiseksi hyökkääjälle[21][78].

Rootkitit

Rootkitit ovat käytännössä paketti työvälineitä, jotka asennetaan kohdejärjestelmään, kun se on kyetty ensin saastuttamaan. Rootkit asennetaan kohdejärjestelmään siinä vaiheessa, kun siihen on saavutettu riittävät käyttöoikeudet, ja sen tarkoituksena on usein asentaa jonkinlainen takaovi järjestelmän autentikoinnin ohittamiseksi, tuottaa muita haluttuja vaikutuksia ja pyrkiä peittämään saastumisen jäljet järjestelmästä. Ne voivat muokata käyttöjärjestelmän omia järjestelmätyökaluja ja komentoja tai pyyhkiä tietoja järjestelmälokeista salatakseen olemassaolonsa, ja samalla pyrkivät piilottamaan muita kohdejärjestelmässä mahdollisesti toimivia haittaohjelmia.[32]

ZeroAccess oli haittaohjelma, joka havaittiin ensimmäisen kerran vuonna 2011[65], ja se tunnetaan eri lähteissä erityyppisenä, koska se muodostui useammasta osasta. Symantecin tuottamissa analyyseissa se tunnetaan lähinnä troijalaisena tai botnetinä[65][33], mutta esimerkiksi Prevx on tehnyt analyysin ZeroAccessista nimenomaan rootkitinä[29]. Millä tahansa nimellä ZeroAccessia haluaa kutsua, se sisältää joka tapauksessa rootkit-toiminnallisuuden, ja tässä tutkielmassa tarkastellaan nimenomaan tätä osiota.

ZeroAccess tartutti kohdekoneen joko troijalaisen tapaan käyttäjän ladattua ja käynnistettyä tiedoston, jonka sisältö ei vastannutkaan tiedostonimeä, tai drive-by downloadina.[77][29][33]. Kun ZeroAccess käynnistyy ensimmäisen kerran, se valitsee satunnaisen ajurin Windowsin tiedostoista ja tallentaa itsensä sen päälle, arkistoiden alkuperäisen ajurin kryptatulle ja käyttöjärjestelmän tiedostojärjestelmään piilotetulle omalle levyasemalleen, jonka se luo samalla[29][33]. Tämän jälkeen se luo suodattimet kaikelle kiintolevyjen ja käyttöjärjestelmän väliselle liikenteelle, jolloin se kykenee näyttämään käyttäjälle tai ohjelmistoille alkuperäisen ajurin omalta levyasemaltaan sen sijaan, että ne havaitsisivat muutoksen (Kuva 13)[65][33]. Lisäksi se luo itsestään varmuuskopion, ja rekisteriavaimia muokkaamalla varmistaa sen, että vaikka ohjelma poistettaisiin, se asentaa itsensä uudelleen tietokoneen sammuttamisen yhteydessä[65][33]. Jotta löytäminen olisi virusskannereille entistä hankalampaa, se muokkaa rekisteriavaimia myös siten, että mikäli jokin prosessi skannaa yli 50 rekisteriavainta lyhyen ajanjakson aikana, prosessi keskeytetään[33].



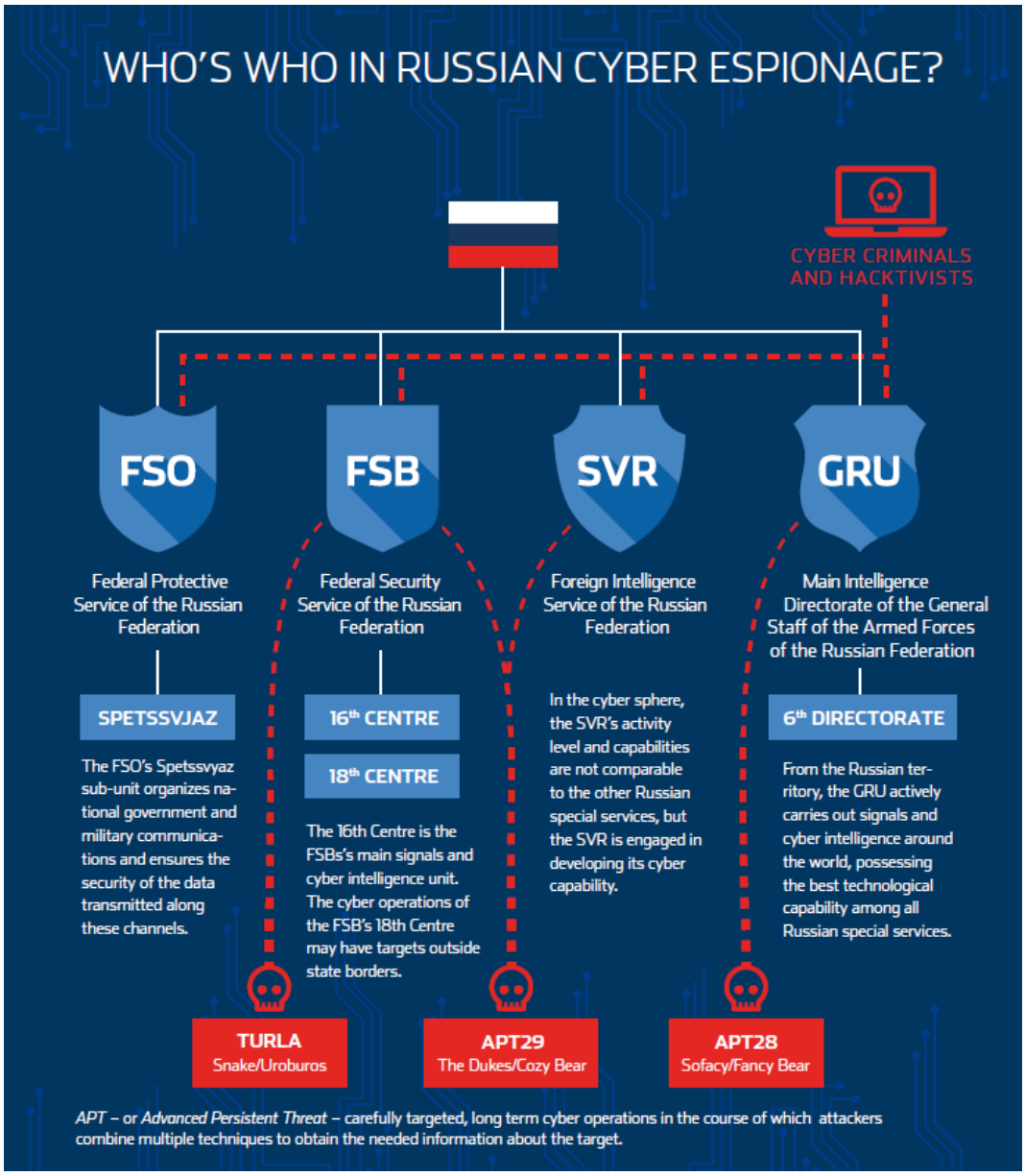
Kuva 13: ZeroAccess-rootkitin toimintaperiaate.[29]

3.4. APT-hyökkäykset

APT-hyökkäykset ovat pitkään tunnettu, poikkeuksellisen vaarallinen uhkatyyppi. Niiden ero tavanomaisiin hyökkäyksiin on useimmiten se, että ne ovat selkeästi jonkin hyökkääjäryhmittymän toteuttamia, eivätkä vain yksittäisten henkilöiden. Niiden tärkeä ominaisuus on myös se, että ne pyrkivät usein monin eri menetelmin tunkeutumaan kohdejärjestelmäänsä, piilottavat itsensä mahdollisimman tehokkaasti ja pyrkivät sitten luomaan itsellensä suotuisan toimintaympäristön. APT-termin P, persistent, viittaakin siihen, ettei hyökkääjällä ole suoranainen kiire suorittaa toimintojaan heti järjestelmään tunkeuduttuaan, vaan pystyy odottamaan suotuisaa hetkeä toteuttaa toimintonsa.[32] Tämän tyyppinen uhka on siitä vaarallinen, että se kyetään pahimmassa tapauksessa toimittamaan kohdejärjestelmään jo varastoinnin tai kalusto testauksen yhteydessä, jolloin joukko saattaa tietämättään olla saastunut jo ennen taisteluiden alkua.

Yleisesti ottaen APT-hyökkäykset ovat nimenomaan jotain tiettyä kohdetta varten rakennettuja haittaohjelmakokonaisuuksia. Niille ominaista on usein kyky piiloutua useammalla eri menetelmällä, ja mahdollinen kyky muuntautua joiltain osin liikkumisensa ja monistumisensa helpottamiseksi. Kohteeseen tunkeutumista voi olla pahimmillaan hyvinkin vaikea havaita, sillä APT-ohjelmia testataan usein mahdollisimman monia puolustuskeinoja vastaan ennen käyttöönottoaan, ja ne pyrkivät luomaan useita mahdollisuuksia etähallintayhteyden luomiseksi. Järjestelmään tunkeutumiseen on käytössä lukemattomia eri keinoja fyysisesti tai verkon yli, ja niiden kaikkien estäminen on liki mahdotonta. Näin ollen yksi varmimmista vaihtoehdoista puolustuskeinoksi olisikin monitoroida reaaliajassa kaikkea verkossa tai päätelaitteilla tapahtuvaa liikennöintiä.[32]

Monet APT-hyökkäykset ovat luonteeltaan erittäin monisyisiä. Tästä johtuen ne havaitaan usein vasta vuosien jälkeen siitä, kun niillä on hyökätty. Tuoreista tapauksista, kuten esimerkiksi Turlasta ja Red Octoberista on saatavilla paljonkin teknistä tietoa, mutta vain vähän selkeitä julkaisuja, vaikka niistä on ollut havaintoja jo vuosina 2012 ja 2014[38][39]. Yleinen nimeämistapa erilaisille APT-uhkille on antaa niille numero ja jonkinlainen lempinimi, ja yhdistää ne johonkin toimijaan, joka voi toteuttaa useampia erilaisia uhkia eri kohteisiin samojen tekijöiden toimesta[44]. Yksi esimerkki tällaisesta APT-ryhmittymästä on APT28, joka on tunnettu myös nimillä ”Fancy Bear” tai ”Sofacy”, joka on linkitetty vuoden 2016 Yhdysvaltain demokraattipuolueen sähköpostihakkerointitapaukseen[70]. Viron ulkomaiden tiedustelupalvelu Välisluureamet on raportissaan osoittanut kolmen tunnetun APT-uhkan yhteydet Venäjän federaation tiedustelupalvelun eri haaroihin (Kuva 14)[54].



Kuva 14: Viron tiedustelupalvelun näkemys APT-toimijoiden ja Venäjän federaation tiedustelupalvelun yhteyksistä.[54]

3.5. Tulevaisuudennäkymät

Useat tietoturvayhtiöt ja muut kyberturvallisuudesta kiinnostuneet yritykset ja yhteisöt laativat vuosittain arvion tulevan vuoden potentiaalisesta uhkatilanteesta ja edeltävän vuoden trendeistä, joista voidaan päätellä eri uhkatyyppien määrän kasvua tai vähenemistä. Vuoden 2018 ennusteiden osalta tarkasteluun on tässä tutkielmassa huomioitu Kaspersky, Thales, CyberArk, FireEye, Mindstar ja Canadian Security Intelligence Service (CSIS). Näitä lähteitä tarkastelemalla voidaan saada kohtalaisen laaja näkemys edellisvuonna vallinneesta kyberturvallisuustilanteesta ja potentiaalisista uhkista tulevalle vuodelle.

Sotilaallisten organisaatioiden eduksi voitaneen nähdä, että suuri osa hyökkäyksistä tullee suuntautumaan pilvipalveluita kohtaan niiden jatkuvasti kasvavan suosion myötä[16]. Suuria pilvipalveluntarjoajia kohtaan koetaan olevan enemmän luottoa niiden valtavien resurssien takia, mutta etenkin pienempien yhtiöiden omien pilvipalveluiden uskotaan olevan hyökkääjille erittäin houkutteleva kohde tietojen varastamiseen[16][17][61].

Yksi suurimmista nousussa olevista riskeistä on palveluntuottajiin ja -toimittajiin kohdistuvat iskut[56]. Sen sijaan, että pyrittäisiin iskemään korkean tietoturvan omaavaa organisaatiota vastaan suoraan, haluttu vaikutus pyritään toimittamaan jollekin kolmannelle osapuolelle, joka toimittaa esimerkiksi asevoimien käyttöön tiettyjä ohjelmistoja[56][16][2]. Kohteeksi valitaan esimerkiksi ohjelmien tuotannossa käytettävät palvelimet, mahdolliset päivityspalvelimet tai muut kehitysympäristön osa-alueet, ja tämän jälkeen haitallinen koodi injektoidaan tuotteeseen[61]. Koska lähtökohtaisesti vastaanottaja on joko auditoinut omien käytäntöjensä mukaisesti toimittajan tai muutoin luottaa siihen, ei suoriteta riittävää omaa tarkastusta ohjelmakoodin sisältöön ja näin ollen hyökkääjällä on tapa ohittaa kohdeorganisaation tietoturvatoimenpiteet[61][56]. Vuonna 2017 tällainen hyökkäys toteutettiin verrattain luotettavaa CCleaner-ohjelmistoa vastaan, kun arviolta noin kaksi miljoonaa konetta ympäri maailman saastui luotettavan toimittajan toteuttaman ohjelmistopäivityksen kautta[56].

Muita merkittäviä uhkia seuraavan vuoden ajalle on arvioitu olevan muun muassa seuraavat:

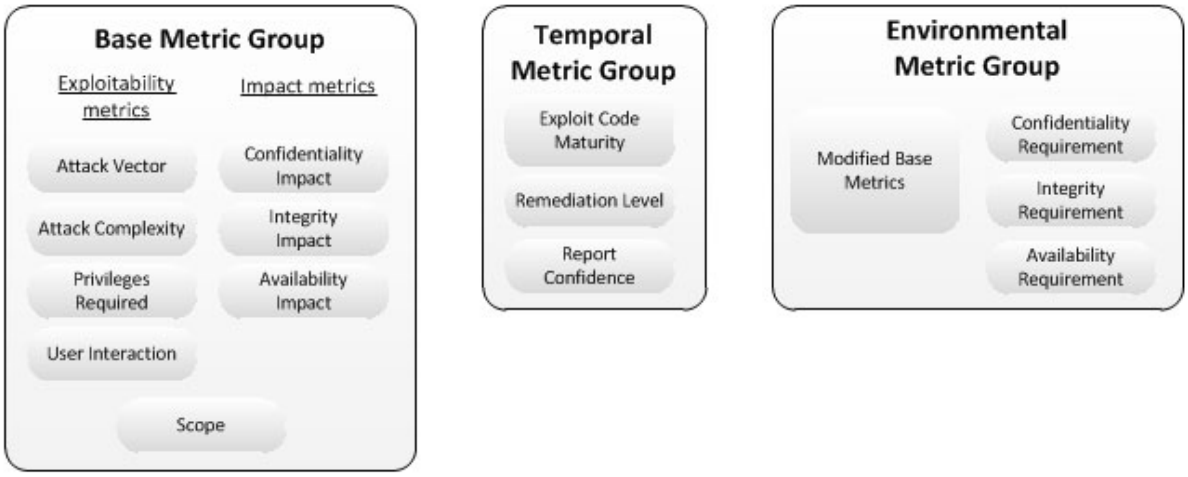
- UEFI-hyökkäykset: aikaisemmin tietokoneissa on ollut käytössään käynnistyksen yhteydessä BIOS (Basic input-output system). BIOS:ssa ei pystynyt käynnistämään ohjelmia, ottamaan yhteyttä verkkoihin tai käyttämään kryptografisia ominaisuuksia. BIOS:in seuraaja UEFI (Unified Extensible Firmware Interface) kykenee suorittamaan näitä toimintoja, ja se tarjoaa hyökkääjälle täysin uuden rajapinnan toiminnalle. Koska UEFI käynnistyy ennen käyttöjärjestelmää tai minkäänlaista tietoturvaohjelmistoa, sen kautta tapahtuvia hyökkäyksiä on miltei mahdoton torjua muutoin kuin ennakkoon toteutetulla testauksella.[56]

- APT-uhkat: APT-uhkien uskotaan kasvavan etenkin odottamattomia laitteita vastaan. Kun järjestelmien kriittisimmät ja suorituskykyisimmät laitteet ovat usein suojattu hyvin potentiaalisia hyökkäyksiä vastaan, APT-uhkien odotetaan suuntautuvan verkossa olevia huomaamattomia komponentteja vastaan, joiden ei odoteta vaikuttavan toimintaan merkittävästi.[1]

- Datan tuhoamiseen suuntautuvat hyökkäykset: Kaspersky on arvioinut datan tuhoamiseen suuntautuvien hyökkäysten lisääntyvän vuonna 2018. Niiden merkittävä kasvu alkoi vuonna 2016, ja monet näistä hyökkäyksistä oli naamioitu näyttämään jonkinlaiselta ransomware-hyökkäykseltä, joka vaati lunnaita käyttäjältään tietojen palauttamiseksi. Todellisuudessa kyseessä oli kuitenkin hyökkäys, joka tuhosi tiedot kohdelaitteen kovalevyltä eikä sillä ollut todellista kykyä palauttaa tietoja, vaikka uhri olisikin maksanut vaaditun lunnassumman.[56]

4. CVSS-ARVIONTIKRITEERISTÖ

Informaation menetyksen tai siihen tehtyjen muutoksien vaikutuksien arviointiin on tarjolla useita eri vaihtoehtoja, perinteisestä riskianalyysistä Open Groupin julkaisemaan Open Information Security Management Maturity Modeliin (O-ISM3)[66]. Yksi menetelmä on arvioida informaation luotettavuutta, eheyttä ja saatavuutta (CIA: confidentiality, integrity, availability). Tätä kolmen muuttujan mallia hyödyntää esimerkiksi FIRST:n julkaisema CVSS (Common Vulnerability Scoring System), jossa on lisäksi tarkasteltavana useita muita tekijöitä (Kuva 15)[14].



Kuva 15: CVSS v3.0:n arviointikriteeristö[14].

Tämän kriteeristön avulla voidaan luoda melko kattava analyysi siitä, minkälaiset uhkat aiheuttavat merkittävintä haittaa taisteluosaston toiminnalle. FIRST tarjoaa uhka-arvioiden laskentaan sivustollaan laskentatyökalun, kun uhkille on ensin määritelty riittävän monta edellä mainituista kriteereistä[45]. Näin voidaan helpottaa laskentatyötä, vaikka eri uhka-arviot onkin luotava itse. Seuraavaksi esitellään analyysissa käytettävät kriteerit.

4.1. Kriteerien esittely

Attack Vector (AV)

Attack Vector -kriteerillä määritellään sitä, kuinka kaukaa verkon yli hyökkääjä kykenee vaikuttamaan kohdejärjestelmään. Mitä kauempaa hyökkääjä pystyy toimimaan, sitä korkeamman arvon AV saa. Mahdolliset arvot ovat seuraavat:

- Network (N): Hyökkääjä kykenee hyökkäämään kohdejärjestelmään verkkokerroksen kautta, yhden tai useamman reititinhypyn päästä kohteesta,
- Adjacent (A): Hyökkääjän täytyy olla samassa fyysisessä (bluetooth, wi-fi) tai loogisessa verkossa (sama ip-aliverkko),

- Local (L): Hyökkääjä ei pysty suorittamaan hyökkäystä verkon yli, vaan vaikutus vaatii tarvittavat tiedostojen käyttöoikeudet,
- Physical (P): Haavoittuvuuden hyväksikäyttö vaatii hyökkääjän fyysisen pääsyn kohdelaitteelle.[14]

Tämän kriteerin tarkastelu on erityisen tärkeää sotilaallisen joukon kontekstissa, koska se vaikuttaa suoraan siihen, kuinka kriittisesti pitää suhtautua tietoliikenteeseen langallisissa sekä langattomissa verkoissa, ja minkälaisella todennäköisyydellä näitä voidaan käyttää ilman suurta pelkoa vastustajan kyberuhkasta. On ratkaisevaa, voiko vastustaja suorittaa iskun omalta maaperältään, joutuuko se tulemaan viestiaseman langattoman verkon kantamalle tai joudutaanko pääsemään fyysisesti laitteeseen käsiksi.

Attack Complexity (AC)

Attack Complexity kuvaa niitä olosuhteita, joihin hyökkääjä ei voi vaikuttaa, mutta joiden täytyy toteutua hyökkäyksen onnistumiseksi, kuten tiettyjen ohjelmistojen olemassaolo kohdelaitteella. Mahdolliset arvot ovat seuraavat:

- Low (L): Erityisiä pääsyoikeuksia ei ole, eikä hyökkäyksen kannalta lieventäviä olosuhteita ole olemassa. Hyökkääjä voi olettaa onnistuvansa toistuvasti hyökkäyksissään.
- High (H): Onnistunut hyökkäys ei ole hyökkääjän hallinnassa. Hyökkäyksen onnistumiseksi tarvitaan kohdesidonnaista tiedustelua, kohdejärjestelmän valmistelua tai kohteen loogisen verkkoliikenteen kuuntelua tarvittavan tiedon kaappaamiseksi.[14]

Lähtökohtaisesti sotilaskohteita vastaan toimittaessa on varmasti syytä olettaa, että kriteerin arvo tulee aina olemaan arvolla High, koska ainakin reititin- ja päätelaitetasolla minkä tahansa asevoimien laitteisto on oletettavasti lähtökohtaisesti suojattu erilaisilla käyttäjähallinnan menetelmillä. Riskin tarjoaa kuitenkin ainakin konseptuaalisella tasolla se, että MANET-verkot muodostuvat itsestään siihen soveltuvien laitteiden tullessa kantamalle. Vaikka käytössä olisi jonkinlainen turvallisuusalgoritmi verkkoon kuulumattomien laitteiden poissulkemiseksi, ei ole mahdotonta, että hyökkääjä olisi tiedustelun keinoin saanut käyttöönsä soveltuvat parametrit oman laitteensa muokkaamiseksi oikean näköiseksi.

Privileges Required (PR)

Privileges Required kuvaa hyökkääjältä vaadittuja käyttöoikeuksia, jotka vaaditaan ennen hyökkäyksen onnistumista. Mahdolliset arvot ovat seuraavat:

- None (N): Hyökkääjällä ei ole käytössään käyttöoikeutta järjestelmään, mutta hyökkäys ei vaadi pääsyä asetuksiin tai tiedostoihin hyökkäyksen onnistumiseksi,
- Low (L): Hyökkääjällä on tarvittavat käyttöoikeudet peruskäyttäjän hallinnassa oleviin asetuksiin ja tiedostoihin,
- High (H): Hyökkääjällä on hallussaan korkean tason (esimerkiksi järjestelmänvalvojan) käyttöoikeudet, ja pystyy vaikuttamaan kaikkiin kohteen asetuksiin ja tiedostoihin.[14]

Tämän kriteerin tarkastelu tulee sitouttaa hyvin arvioitavaan uhkaan taisteluosaston kyberuhkaa analysoidessa. Monimutkaiset ja suurta tuhoa aiheuttavat hyökkäykset saattavat vaatia pääsyoikeuden huoltokäyttöliittymään ja riittävän korkeat käyttöoikeudet esimerkiksi konfiguraatioiden ja salasanojen muuttamiseksi tai varastamiseksi. Koska suunnitteluun käytettäviä päätelaitteita tuskin käytetään järjestelmänvalvojan tunnuksin, niihin tallennettu data on lähtökohtaisesti käytettävissä ilman korotettuja käyttöoikeuksia.

User Interaction (UI)

User Interaction kuvaa sitä, vaaditaanko hyökkäyksen onnistumiseksi jonkin muun käyttäjän, kuin hyökkääjän toimintaa hyökkäyksen onnistumiseksi. Tämä tarkoittaa sitä, voiko hyökkääjä suorittaa hyökkäyksensä puhtaasti itse, vai täytyykö käyttäjän osallistua jollain tavoin hyökkäykseen (avata tiedosto, klikata linkkiä). Mahdolliset arvot ovat seuraavat:

- None (N): Hyökkääjä voi toteuttaa hyökkäyksen ilman käyttäjän osallistumista,
- Required (R): Käyttäjän täytyy suorittaa jokin toiminto hyökkäyksen onnistumiseksi (esimerkiksi ohjelman asennus järjestelmänvalvojan oikeuksin).[14]

Tämän kriteerin osalta on oletettava, ettei hyökkääjä lähtökohtaisesti toteuta sellaista hyökkäystä, joka vaatisi kohdelaitteella käyttäjän osallistumista. Puhuttaessa verkkolaitteista tai johtamisjärjestelmän päätelaitteista, on hyvin epävarmaa ainakin ajallisesti, että käyttäjän saisi toteuttamaan jonkin toiminnon luotettavasti niin usein, että hyökkäyksen voisi olettaa toimivan luotettavasti.

Scope (S)

Scope kuvaa sitä, voiko haavoittuvan osan avulla hyödyntää mahdollisuutta edetä järjestelmän sisällä toiseen kohteeseen siten, että haavoittuva osa mahdollistaa joidenkin sellaisten asetusten tai tiedostojen muokkauksen, joihin ei muuten olisi pääsyä sen hetkisellä pääsynhallinnalla. Yhtenä tapauksena olisi esimerkiksi kyky vaikuttaa kohdelaitteella toimivan virtualisoidun laitteen kautta suoraan todelliseen käyttöjärjestelmään. Mahdolliset arvot ovat seuraavat:

- Unchanged (U): Haavoittuvuus mahdollistaa vain samoilla käyttöoikeuksilla olevien asetusten tai tiedostojen muuttamisen,
- Changed (C): Haavoittuvuus mahdollistaa korkeampien käyttöoikeuksien käytön kuin kohteella muuten olisi käytössään.[14]

Tämän kriteerin osalta tarkastelu ei yhdestä näkökulmasta ole kovin kriittinen, sillä lähtökohtaisesti monet uhkat on suunnattu selkeään tavoitteeseen ja näin ollen suunniteltu joko hankkimaan korkeammat käyttöoikeudet tai tyytyvän peruskäyttäjän ominaisuuksiin. On toki mahdollista, että mikäli matalampia käyttöoikeuksia vastaan suunnatulla hyökkäyksellä kyetään avaamaan reitti monimutkaisemmille ja vaikuttavammille hyökkäyksille, sitä hyödynnetään. Toisaalta taas uusiin kohteisiin leviäminen voi aiheuttaa hallitsemattoman uhkatilanteen koko verkossa.

Confidentiality Impact (C)

Confidentiality Impact kuvaa hyökkäyksen vaikuttavuutta tietojen luottamuksellisuutta kohtaan. Luottamuksellisuudella tarkoitetaan tässä tapauksessa tiedon saatavuuden rajaamista vain halutuille käyttäjille. Mahdolliset arvot ovat seuraavat:

- High (H): Täydellinen luottamuksellisuuden menetys, jolloin hyökkääjä saa pääsyn kaikkiin kohteensa tietoihin. Myös sellaiset tapaukset, joissa hyökkääjä saa vain rajallisen määrän tietoja, mutta ne ovat vaikutukseltaan suuria (järjestelmänvalvojan salasana, salausavaimet).
- Low (L): Jonkinasteinen luottamuksellisuuden menetys, jossa hyökkääjä saa pääsyn joihinkin luottamuksellisiin tietoihin, mutta ei joko pysty kontrolloimaan mitä tietoa saa, tai tietojen määrä tai laatu on rajallinen. Ei aiheuta vakavaa uhkaa.
- None (N): Ei luottamuksellisuuden menetystä.[14]

Tämän kriteerin tarkastelu on ehdottomasti yksi tärkeimmistä kaikkien tiedostoihin ja sovelluksiin vaikuttavien uhkien osalta. Koska sotilasympäristössä operatiiviset käskyt ja suunnitelmat ovat lähtökohtaisesti aina turvaluokiteltuja johtuen niiden arkaluontoisuudesta ja vaikuttavuudesta taistelun kulkuun, on ensiarvoisen tärkeää että tietojärjestelmiin tallennettuun tietoon voi luottaa. Low-tasoinen riski on vielä hallittavissa, johtuen pääluvussa 2 mainitusta aikakriittisyydestä, mikäli vastustaja ei pysty hallinnoimaan mitä tietoa kykenee järjestelmästä hankkimaan. Arkistoidun datan määrä on tällaisessa tapauksessa selkeä etu, mikäli haittaohjelma ei kykene toimintansa aikana siirtämään kaikkia kohdejärjestelmän tiedostoja hyökkääjän haltuun.

Integrity Impact (I)

Integrity Impact kuvaa sitä, kuinka suuri vaikuttavuus hyökkäyksellä on tiedon luotettavuuteen. Mahdolliset arvot ovat seuraavat:

- High (H): Täydellinen luotettavuuden tai suojauksen menetys, jolloin hyökkääjä kykenee muokkaamaan kaikkia kohteensa tietoja. Myös sellaiset tapaukset, joissa hyökkääjä pystyy muokkaamaan vain rajallista määrää tietoja, mutta niiden vaikutukset olisivat suuria.
- Low (L): Tietojen muokkaus on mahdollista, mutta hyökkääjällä ei ole kontrollia muutosten seurauksista, tai muutokset ovat rajallisia. Ei aiheuta välitöntä, vakavaa uhkaa.
- None (N): Ei luotettavuuden menetystä.[14]

Luottamuksellisuuden tavoin myös luotettavuus on erittäin oleellinen arviointikriteeri. Tietojen haltuun saamista jopa vaarallisempaa voi olla tietojen muuttaminen, etenkin jos kyetään hallitsemaan sitä, mitä tietoja muutetaan. Vaikka muutettavat tiedot olisivat vain pieniä vaikutuksiltaan, saattaa järjestelmässä olevan tiedon luotettavuus romahtaa välittömästi. Pienetkin muutokset kellonajoissa tai muissa numeraalisissa arvoissa saattavat aiheuttaa perustavanlaatuisia ongelmia taisteluosaston taistelussa. Tämä taas johtaa seurannaisvaikutuksiin koko valtakunnan alueella.

Availability Impact (A)

Availability Impact kuvaa hyökkäyksen aiheuttamaa vaikutusta jonkin kohdepalvelun saatavuuteen. Kyseessä ei ole siis tiedostojen, vaan palvelun saatavuuden arviointi, voidaanko erilaisilla hyökkäyksillä jotka vaikuttavat esimerkiksi prosessorin käyttöön, verkon kuormitukseen tai tallennustilaan aiheuttaa sama vaikutus. Mahdolliset arvot ovat seuraavat:

- High (H): Täydellinen saatavuuden menetys, jolloin hyökkääjä kykenee estämään pääsyn haluttuun resurssiin kokonaan. Voi olla joko jatkuva hyökkäys, tai sellainen hyökkäys, joka aiheuttaa saatavuuden menetyksen loppumisensa jälkeenkin. Myös sellaiset tapaukset, joissa hyökkääjä pystyy estämään resursseihin pääsyn vain rajallisesti, mutta saatavuus on kriittinen tekijä kohteen kannalta,
- Low (L): Resurssien saatavuus on heikentynyt tai siinä on katkoksia. Vaikka hyökkäys olisi mahdollista toteuttaa toistuvasti, hyökkääjä ei pysty täysin estämään pääsyä haluttuihin resursseihin. Ei vakavia seurauksia,
- None (N): Ei vaikutusta saatavuuteen.[14]

Tämän kriteerin tarkastelu on taisteluosaston viitekehyksessä hyvin perusteltua. Osassa hyökkäyksistä tällä kriteerillä ei ole suurta merkitystä, koska kaikkien hyökkäysten kohteena ei ole estää pääsyä resursseihin vaan nimenomaan pysyä havaitsemattomana käyttäjälle. High-arvon saavista hyökkäyksistä on syytä tarkastella myös sitä, pystyykö hyökkäys aiheuttamaan saatavuuden menetyksen loppumisensa jälkeenkin.

Exploit Code Maturity (E)

Exploit Code Maturity kuvaa haavoittuvuutta kohtaan toteutettavaan hyökkäykseen vaadittavan koodin kypsyyttä ja todennäköisyyttä, jolla kyseistä haavoittuvuutta kohtaan hyökätään. Haavoittuvuuden alkuvaiheessa hyökkäysmetodi voi olla vain karkea proof-of-concept -muotoinen koodi, joka myöhemmissä kehitysvaiheissa kehittyy automatisoiduksi hyökkäysjärjestelmäksi. Mahdolliset arvot ovat seuraavat:

- Not Defined (X): Ei arvioitu, eikä vaikuta näin kokonaisuhkan laskelmaan.
- High (H): On olemassa toimivaa, autonomista koodia, tai minkäänlaista haavoittuvuutta ei tarvita ja yksityiskohdat ovat laajasti saatavilla. Haittakoodi toimii aina, tai toimitetaan kohteeseen autonomisen toimijan (esimerkiksi virus) avulla. Haittaohjelman kehitys on tasolla, jolla tuotetaan luotettavia, helposti saatavilla olevia ja helppokäyttöisiä automatisoituja työkaluja.

- Functional (F): Toimivaa haittakoodia on saatavilla, ja se toimii useimmissa tapauksissa haavoittuvuutta vastaan
- Proof-of-Concept (P): Proof-of-concept -tasoista haittakoodia on saatavilla, tai hyökkäysdemonstraatio ei ole käytännöllinen useimpia järjestelmiä kohtaan. Koodi tai tekniikka ei ole toimiva kaikissa tapauksissa tai vaatii paljon muokkaamista taitavalta hyökkääjältä.
- Unproven (U): Haittakoodia ei ole saatavilla, tai haavoittuvuus on teoreettinen.[14]

Tämän kriteerin tarkastelu voi tuottaa monenlaisia näkemyksiä lopputuloksen arvioinnissa. Toisaalta tunnettu haavoittuvuus, jonka haittakoodi on saatavilla voi olla äärimmäisen vaarallinen tapa vaikuttaa kohdejärjestelmään. Toisaalta sen tunnettavuus aiheuttaa todennäköisemmin uhkan estämisen tai kiertämisen erilaisella teknisellä tai ohjelmistopohjaisella ratkaisulla. Tämän pitäisi ainakin vähentää potentiaalisten hyökkäysten määrää merkittävästi, niin kauan mikäli hyökkäys kohdistuu työasemiin.

Remediation Level (RL)

Remediation Level kuvaa haavoittuvuuden paikkaamisen tasoa. Usein ilmestyessään haavoittuvuuksia vastaan ei ole korjausta, ja ennen virallista ongelman poistamista tilannetta paikataan vaihtoehtoisella toiminnalla tai hotfixeillä. Mahdolliset arvot ovat seuraavat:

- Not Defined (X): Ei arvioitu, eikä vaikuta näin kokonaisuhkan laskelmaan.
- Unavailable (U): Haavoittuvuuteen ei ole saatavilla korjausta, tai sitä ei voida käyttää.
- Workaround (W): Epävirallinen, muun kuin alkuperäisen tekijän ratkaisu on saatavilla. Joissain tapauksissa käyttäjät tekevät itse tarvitsemansa päivityksen tai esittävät toimintatapoja haavoittuvuuden estämiseksi tai sen vaikutusten vähentämiseksi.
- Temporary Fix (T): Virallinen, mutta väliaikainen korjaus on saatavilla. Alkuperäinen tekijä julkaisee hotfixin, työkalun tai W-kohdan mukaisen toimintatavan.
- Official Fix (O): Virallinen korjaus on saatavilla. Alkuperäinen valmistaja on julkaissut päivityksen.[14]

Tämä kriteeri voi osoittautua monissa tapauksissa odotettua tärkeämmäksi. Niin kauan kun kriteerin arvo ei ole U, on Puolustusvoimilla mahdollisuus kriisin vaiheesta riippumatta hankkia tai toteuttaa itse korjaus haavoittuvuutta vastaan. Sen toimittaminen kokonaisen taisteluosaston laitteistoon ei tapahdu nopeasti, mutta mikäli hallintaryhmällä on mahdollisuus hallinnoida lähes koko laitteistoa verkon ylitse, uhka voidaan eristää tai sen vaikutukset minimoida hyvinkin nopeasti, mikäli korjaus saadaan toimitettua perille riittävän aikaisin.

Report Confidence (RC)

Report Confidence kuvaa sitä, kuinka luotettavia ja yksityiskohtaisia haavoittuvuudesta julkaistut tiedot ovat. Joissain tapauksissa kerrotaan vain haavoittuvuuden olemassaolosta, mutta ei sen teknisistä yksityiskohdista. Mitä pidemmälle tutkimus etenee, sitä varmemmin voidaan kuvata haittaohjelman olemassaoloa ja vaikutuksia. Mahdolliset arvot ovat seuraavat:

- Not Defined (X): Ei arvioitu, eikä vaikuta näin kokonaisuhkan laskelmaan.
- Confirmed (C): On olemassa yksityiskohtaisia raportteja, tai toiminnallisuus kyetään toisintamaan. Lähdekoodi on saatavilla arvioitavaksi, tai kohteen valmistaja vahvistaa haavoittuvuuden olemassaolon.
- Reasonable (R): Paljon yksityiskohtia on julkaistu, mutta tutkijoilla ei ole pohjimmaisesta syystä täyttä varmuutta tai pääsyä lähdekoodiin toimintojen vahvistamiseksi. On kuitenkin kohtalainen varmuus, että toiminto on toistettavissa ja vähintään yksi vaikutus on kyetty todistamaan.
- Unknown (U): On olemassa ilmoituksia havaituista vaikutuksista, jotka osoittavat haavoittuvuuden olemassaolon. Raportoijat eivät ole varmoja haavoittuvuuden todellisesta luonteesta, eikä toimintaa välttämättä kyetä toistamaan.[14]

Tämä kriteeri tullee olemaan monissa tapauksissa joko R tai U. Hyvin dokumentoidut haittaohjelmat on usein estetty joko laite- tai ohjelmistovalmistajan toimesta, eikä niiden avulla kyetä murtautumaan suunnitelmallisesti suojattuun kohteeseen. Kaikki hyökkäykset eivät varmasti tule kuitenkaan olemaan uusia nollapäivähaavoittuvuuksia, vaan osa saattaa hyvinkin hyödyntää tunnettuja haavoittuvuuksia joihin ei ole löytynyt toistaiseksi soveltuvaa korjausvaihtoehtoa, ja vaikka uhka tunnetaan jollain tasolla, sillä on vielä potentiaalia suorittaa joitain ennestään tuntemattomia toimintoja.

Turvallisuusvaatimukset

Organisaatiosta riippuvaiset kriteerit ovat Confidentiality Requirement (CR), luottamuksellisuuden vaatimustaso, Integrity Requirement (IR), luotettavuuden vaatimustaso ja Availability Requirement (AR), saatavuuden vaatimustaso. Nämä vaikuttavat painokertoimina aiemmissa kohdissa mainittuihin kriteereihin C, I ja A, ja ne määrittyvät sen mukaan, miten organisaatio painottaa näitä osa-alueita omassa toiminnassaan. Mahdolliset arvot kaikille ovat seuraavat:

- Not Defined (X): Ei arvioitu, eikä vaikuta näin kokonaisuhkan laskelmaan.

- High (H): Kriteerin C, I tai A menetys johtaa katastrofaalisiin haittavaikutuksiin organisaatiolle tai siihen kuuluville yksilöille
- Medium (M): Kriteerin C, I tai A menetys johtaa vakaviin haittavaikutuksiin organisaatiolle tai siihen kuuluville yksilöille
- Low (L): Kriteerin C, I tai A menetys johtaa rajallisiin haittavaikutuksiin organisaatiolle tai siihen kuuluville yksilöille

Tämän kriteerin tarkastelu on hieman ristiriitainen tämän kaltaisessa tapauksessa, sillä se vastaa sisällöltään hyvin lähelle perinteisiä suojaustasovaatimusten kriteereitä. Kuitenkin puhuttaessa sodan ajan joukosta, sen johtajalla on aina oma näkemyksensä siitä, kuinka kriittistä minkälainen data on. Näin ollen tarkastelussa on pyrittävä lähestymään asiaa mahdollisimman objektiivisesta näkökulmasta, painottaen potentiaalisten haittojen todellista vaikutusta niin taisteluosaston taistelussa kuin suuressa mittakaavassa.

4.2. Kritiikki

Vaikka pääsääntöisesti CVSS-asteikko toimii monilta osin erinomaisena analyysityökaluna erilaisia uhkatyyppejä tarkasteltaessa, siinä on omat haasteensa kuvauksien ja niiden vaikutusten yhteyksistä lopputulokseen joissain tapauksissa. On selkeää, että esimerkiksi suurempi kyky vaikuttaa tietojen luottamuksellisuuteen tai hyökkäyksen vaikutusten estämisen mahdottomuus nostavat uhka-arviota. Sen sijaan suurimman ristiriidan uhkaa laskettaessa aiheuttaa RC-kriteeri, Report Confidence.

Report Confidence tarkastelee uhkasta saatavilla olevien raporttien yksityiskohtaisuutta ja luotettavuutta tarkasteluhetkellä. Arvot on luokiteltu määrittelemättömästä aina tarkasti dokumentoituun ja analysoituun uhkaan, jonka toimintaperiaatteet tunnetaan tarkasti ja kyetään toisintamaan. Tuntuu kuitenkin jokseenkin väärältä, että mitä huonommin uhka tunnetaan ja mitä vähemmän siitä on kyetty tuottamaan tutkittua tietoa, sitä pienemmäksi uhkaksi se koetaan. Esimerkiksi nollapäivähaavoittuvuuden tapauksessa täyttyisivät varmasti matalimman uhka-arvon antavan Unknown-arvon ehdot: uhkaa ei juuri tunneta, mutta on olemassa havaintoja mahdollisen uhkan olemassaolosta eikä sen toimintaa kyetä toisintamaan omin keinoin. Uskallan kuitenkin väittää, että tällainen tapaus olisi monen puolustajan kannalta suurin mahdollinen uhkatilanne, sillä hyvin dokumentoitu ja raportoitu uhka olisi todennäköisesti myös ensimmäisenä tietoturvapäivitysten listalla, ja sen toiminta olisi pyritty estämään jo ennen kuin joku hyökkääjä käyttäisi sitä uudessa hyökkäyksessä.

5. UHKA-ANALYYSI

Uhka-analyysin toteuttamiselle tämänkaltaisessa, tieto- ja tietoliikennejärjestelmiä täynnä olevassa ympäristössä voisi itsessään tuottaa lukemattomia analyyseja, mikäli kaikki mahdollisuudet huomioitaisiin. Tämän tutkielman viitekehyksessä on kuitenkin syytä keskittyä toiminnan kannalta kriittisimpiin laitteisiin tai ohjelmistoihin, joihin päässeellä haittaohjelmalla olisi merkittävin vaikutus taisteluosaston taistelulle. Taisteluosaston taistelulle välittömän uhkan muodostavat pääsy reitittimiin, työasemiin tai tiedostopalvelimelle. Näitä kolmea tullaan tarkastelemaan sekä todennäköisen että vaarallisimman hyökkäyksen näkökulmasta. Verkonvalvontaohjelmisto tarjoaa vielä yhden sinänsä mielenkiintoisen uhkavektorin, jota ei kuitenkaan tarkastella tämän tutkimuksen viitekehyksessä.

Pisteytys on toteutettu, kuten CVSS:n omassa laskimessa siten, että uhka saa kolme erillistä pistemäärää. Ensimmäinen, Base Score, määräytyy vain uhkan ominaisuuksien mukaan. Temporal Scoressa huomioidaan uhkan lisäksi myös uhkan, siitä saatujen ilmoitusten ja raporttien, sekä sen vastatoimenpiteiden kypsyyttä ajallisesti. Lopullinen arvosana, Environmental Score, huomioi myös kohteen tietoturvan vaatimukset kolmella kriittisimmällä (luotettavuus, eheys, saatavuus) osa-alueella. Näin ollen Environmental Score on se pistemäärä, jota tullaan käyttämään vertailukohteena eri uhkien välillä.[14]

5.1. Reititin

Reititin / Todennäköinen

Taisteluosaston johtamisjärjestelmän kannalta reititin on laitetyyppinä hyvin potentiaalisesti vaarallisin ja mahdollisesti halutuin kohde, sillä sen kautta on mahdollista saavuttaa paljon tietoa verkon rakenteesta ja siellä liikkuvasta tiedosta. Ne muodostavat koko taisteluosaston verkon rungon, ja välitystiestä riippumatta ne ohjaavat tietoliikenteen lähettäjältä vastaanottajalle reititysprotokollan mukaista reittiä pitkin. Todennäköinen hyökkäys tällaisessa tilanteessa olisi jokin verkon yli toimitettava haittaohjelma haluttuun reitittimeen. Oletetaan puolustajan kannalta edullisesti niin, että runkoverkkoyhteys on toteutettu erittäin korkean teknisen tietoturvan keinoin. Näin ollen reititinverkkoon pääsemiseksi tarvitsisi päästä käsiksi vähintään samassa fyysisessä tai loogisessa verkossa oleviin laitteisiin. Täten AV-kriteerin arvoksi tulee A.

Hyökkäyksen täytyisi olla kohtalaisen hienostunut tiedustelultaan, koska sen täytyisi tunnistaa ennalta joko laitetyyppi, jossa aktivoitua tai tarkka IP-osoite, johon hakeutua verkossa liikkuessaan. Sinänsä itse hyötykuorman ei välttämättä tarvitse reitittimen kaltaisessa laitteessa suorittaa äärettömän monimutkaisia operaatioita muutoin kuin itsensä peittämiseksi, mutta nimenomaan oikean kohteen löytäminen voi olla suurin haaste tässä ympäristössä. Kertaalleen onnistuneen hyökkäyksen voidaan kuitenkin olettaa onnistuvan myös muissa vastaavissa tilanteissa. Lopputuloksena kuitenkin AC-kriteerin arvoksi tulee tässä tapauksessa H.

Koska reitittimet ovat niin keskeisessä roolissa taisteluosaston verkon rakenteessa ja tietoliikenteen ohjaamisessa, niiden kriittisimmät ominaisuudet on todennäköisesti lukittu järjestelmänvalvojan käytettäväksi. Varsinkin keskeisiin järjestelmäasetuksiin tai reititystauluihin liittyvät ominaisuudet on lähes varmasti poistettu käytöstä normaalilta käyttäjältä, mikäli sellaisia on reitittimen tapauksessa ylipäänsä olemassa. Tämä riippunee voimakkaasti johtamisjärjestelmän muusta toimintaperiaatteesta. Tässä tapauksessa kriteeri PR saa kuitenkin arvon H.

Reitittimiä harvoin operoidaan jatkuvasti, vaan ne toimivat itsenäisesti niihin asetettujen perusteiden ja reititysprotokollien mukaan. Tällöin olisi vaikea kuvitella luotettavaa hyökkäystä reititintä vastaan toteutettavan siten, että se vaatisi jonkinlaista käyttäjän interaktiota toteutuakseen. Ainut tällainen tilanne olisi se, että jostain syystä reitittimelle haluttaisiin päästä käsiksi esimerkiksi usb-aseman kautta tuotavilla tiedostoilla tai siten, että ennakkovalmisteluna olisi saatu saastutettua reitittimien konfigurointiin käytettävä työasema, jonka välityksellä käyttäjän interaktio voisi toimia laukaisimena hyökkäyksen onnistumiselle. Oletetaan kuitenkin, että UI-kriteerin arvoksi tulee N, eikä käyttäjää tarvita hyökkäyksen onnistumiseksi.

Todennäköisessä uhkakuvassa reititintä vastaan hyökättäessä hyökkäys kohdistunee lähtökohtaisesti itse reitittimeen, eikä sen kanssa samassa verkossa toimiviin muihin laitteisiin. Tämän voi perustella sillä, että pelkkään yksittäiseen reitittimeen vaikuttamalla kyetään parhaimmassa tapauksessa lamauttamaan suurikin osa taisteluosaston alueen johtamisjärjestelmästä, mikäli se sattuu olemaan fyysisesti kriittisessä maantieteellisessä kohdassa. Tähän riittäisi yksinkertaisimmillaan black hole -hyökkäys, jossa hyökkääjä manipuloisi väärennetyillä reititystauluilla ja naapuruustiedoilla muut reitittimet ohjaamaan liikenteen kauttaan, ja tuhoaisi kaikki lävitseen kulkevat paketit[19]. S-kriteerin arvoksi tulee tällöin U.

Koska kriteerin AV osalta oletettiin, että hyökkäyksen sisäänpääsy ei ole mahdollista runkoverkon kautta usean verkkohypyn yli, oletetaan myös, että hyökkäys ei ole niin hienostunut, että se osaisi löytää tiensä ulos julkisiin tietoverkkoihin. Vaikka reititin sinänsä sisältää potentiaalisen hyökkääjän kannalta äärimmäisen hyödyllistä tietoa verkon rakenteesta, sitä ei todennäköisesti saada siirrettyä hyökkääjän haltuun verkon ulkopuolelle. Hyökkäys tullee olemaan monilta osin hyökkääjän kontrolloimattomissa saastuttamisen jälkeen, ja vaikka tietoihin päästäisiin käsiksi, niitä ei saada hyökkääjän tietoon millään välineellä. Tästä syystä C-kriteeri saa arvon N.

Tällaisessa hyökkäyksessä reitittimen sisältämien tietojen eheys on epäilemättä vaarantunut, koska toimiakseen kovin tehokkaasti reititintä vastaan, on hyökkääjän kyettävä muuttamaan sen asetuksia ja reititystauluja kyetäkseen ohjaamaan liikennettä paremmin haluamaansa osoitteeseen. Tässäkin tapauksessa kuitenkin tietoja muuttamalla voidaan lähinnä saavuttaa liikenteen ruuhkautumista verkossa tai pakettien tuhoutumista niiden kulkiessa saastuneen reitittimen läpi, ja tällainen tilanne ei ole välttämättä kovinkaan pitkä ajallisesti. Mikäli hyökkäys on välimuistissa toimiva, vaikeasti havaittava haittaohjelma, sen toiminta lakkaa sammutuksen yhteydessä, ja reititystaulut saavuttavat normaalin tilan reititinten välisen tiedonvaihdon kautta. Muissa tapauksissa reitittimen ohjelmisto saatetaan joutua asentamaan uudelleen, mutta ongelma poistuu silti todennäköisesti tunneissa. I-kriteerin arvoksi tulee näin ollen L.

Saatavuus on reitittimiin kohdistuvissa hyökkäyksissä hyvin kriittinen haavoittuvuus. Aina, kun reititin kyetään saamaan pois käytöstä millä tahansa tavalla, tai sen kautta kulkeva liikenne pysäytettyä tai ohjattua väärään osoitteeseen, hyökkäys on jollain tavalla onnistunut. Koska liikenteen haittaamiseksi on niin monta teknistä vaihtoehtoa, hyökkäys aiheuttaisi todennäköisesti täydellisen saatavuuden menetyksen ainakin siinä laitteessa, johon se alun perin kohdistuu, ja pahimmassa tapauksessa laajemmallekin alueelle verkossa. Kriteerin A arvo on ehdottomasti H, ja näin ollen reitittimen todennäköinen uhka saa Base Scoren 4,8 (Medium).

Reititintä vastaan voisi olla niin tarpeellista hyökätä taistelun vaiheesta riippuen, että sitä vastaan ei välttämättä ole valmisteltu täysin hienostunutta, itsensä piilottavaa ja täysin kohteen rampauttavaa haittaohjelmakokonaisuutta. Toisaalta sellainen ei välttämättä ole edes tarpeen, jos ei ole kyse tietojen varastamisesta tai kontrolloidusta muokkaamisesta ja tietoliikenteen uudelleenohjaamisesta hyökkääjän haluamiin kohteisiin. Koska kohteeseen pääsy saattaa edelleen olla hieman haastavaa suojauksista johtuen, ei kyseessä kuitenkaan ole todennäköisesti minkäänlainen teoreettinen arvaus, joka saattaisi onnistua joissain olosuhteissa. E-kriteeri saa arvon F, jolloin hyökkääjä olettaa onnistuvansa usein.

Samasta syystä, kun reititintä vastaan on helppoa vaikuttaa, on myös sen tehokkain puolustus. Uhkien ei tarvitse olla äärettömän monimutkaisia, ja niiltä on parhaimmillaan mahdollista välttyä jopa ilman kovinkaan vaativia vastatoimia, mikäli verkon rakenne mahdollistaa liikenteen muita reittejä. Moneen erilaiseen hyökkäykseen voidaan vastata uudelleenasentamalla reitittimen ohjelmisto, sillä protokollat mahdollistavat ainakin perusreitityksen toteutumisen, ja ylläpitäjillä ja muulla teknisellä henkilöstöllä on todennäköisesti hallussaan valmis konfiguraatio laitteen uudelleen alustamiseksi. RL-kriteeri saa arvon W, koska ainakin jonkinlaisia väistökeinoja on todennäköisesti käytettävissä.

Vaikka hyökkäysmetodin yksityiskohdat saattavat olla tuntemattomat puolustajalle, niiden vaikutus voi olla hyvinkin analysoitavissa tällaisissa tapauksissa. Mikäli verkkoliikenteessä on selkeitä ongelmia ja ongelma kyetään paikallistamaan johonkin johtamisjärjestelmän fyysiseen sijaintiin, siitä voidaan nopeastikin koota varsin kattava analyysi. Todennäköisesti toimintatapa on ollut myös käytössä muissa vastaavanlaisissa hyökkäyksissä esimerkiksi yrityksiä tai valtiollisia toimijoita vastaan, joten muista lähteistä voidaan koota havaintoja tukevaa tietoa. RC-kriteeri saa näin ollen arvon R. Täten muodostuu Temporal Score 4,4 (Medium), eli nämä olosuhteet huomioiden uhka on pienempi kuin itse hyökkäyksestä muodostuva.

Koska tässä tapauksessa reitittimeen pääsemiseksi hyökkääjä on joutunut todennäköisesti suorittamaan jo jonkin tasoista tiedustelua verkon rakenteesta, ei reitittimen sisältämä tieto välttämättä vuotaessaan paljastaisi mitään kovinkaan ratkaisevaa, uutta tietoa hyökkääjälle. Siksi CR-kriteerin arvo on tässä tapauksessa L. Eheys on hieman tärkeämpi vaatimus reitittimen toiminnalle, sillä mikäli reitittämiseen vaikuttaviin parametreihin päästään tekemään hallittuja muutoksia, liikenne saattaa pahimmillaan häiriintyä pahasti. IR-kriteeri saa arvon M. Ratkaiseva, ja kaiken toiminnan kannalta täysin kriittinen ominaisuus reitittimen toiminnassa on kuitenkin saatavuus, sillä mikäli reititin ei kykene ohjaamaan liikennettä lävitseen, se rampauttaa ainakin oman toimipisteensä kaikki verkkoyhteydet, ja pahimmillaan koko johtamisjärjestelmän alueellisesti. AR-kriteeri saa reitittimen tapauksessa arvon H. Lopulliseksi arvosanaksi, Environmental Scoreksi muodostuu tällöin **5,7** (Medium), joka on jo siinä määrin korkea, että uhka kannattaa ottaa varsin vakavasti. Kokonaisuus on esitetty alla (Kuva 16).

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 Requirement	**CR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Integrity Requirement	**IR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Availability Requirement	**AR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	

Kuva 16: Todennäköinen uhka reititintä vastaan.

Reititin / Vaarallisin

Koska reititin on erittäin keskeinen tekijä kaikelle taisteluosaston tietoliikenteelle, siihen voi suuntautua pahimmillaan uskomattoman vaarallisia hyökkäyksiä. Potentiaalisesti vaarallisin olisi sellainen hyökkäys, joka suuntautuisi reitittimeen runkoverkon kautta, siten että hyökkääjä pääsisi murtautumaan virtuaaliseen lähiverkkoon ja mahdollisesti ohjaamaan kaiken reitittimen läpi kulkevan liikenteen julkiseen verkkoon tai hyökkääjän omaan verkkoon. Lisäksi hyökkäyksen tavoitteena olisi leviäminen vähintään kaikkiin samassa verkossa oleviin muihin reitittimiin, ja mahdollisuuksien mukaan muihin verkossa oleviin laitteisiin. Näin ollen hyökkääjän olisi mahdollista toteuttaa hyökkäyksensä maantieteellisesti mistä tahansa, monenkin verkkohypyn yli ja näin ollen jäädä täysin tunnistamattomaksi parhaassa tapauksessa. AV-kriteeri saa vaarallisimmassa tapauksessa arvon N.

Tällaisessa tapauksessa hyökkäyksen täytyy olla äärimmäisen hienostunut, sillä sen täytyy sisään päästäkseen pystyä ensin murtautumaan johonkin runkoverkon reitittimeen, jotta se kykenee löytämään oikean kohteen ja läpäisemään verkkoa suojaavat toimenpiteet. Lisäksi, jotta hyökkääjä kykenee liikennöimään mahdollisuuksien mukaan haluamiinsa kohteisiin, hyökkäyksen täytyy kyetä naamioimaan liikenteensä mahdollisimman normaalisti jäädäkseen havaitsematta verkonvalvonnalta. Aiemmin hyökkäysten yhteydessä puhuttiin pakettien ip-spoofingista, mutta tässä tapauksessa esimerkiksi hyökkäyksen toteuttama arp-spoofing voisi saada reitittimen ohjaamaan kaiken liikenteen mielestään oikeaan ip-osoitteeseen, mutta fyysinen osoite olisi hyökkääjän haluama, eikä ip-osoitteen todellinen. AC-kriteeri saa arvokseen H.

Vaikka hyökkäyksen pääsy reitittimeen ei välttämättä sinänsä vaadi käyttöoikeuksia lainkaan, niitä todennäköisesti tarvitaan viimeistään siinä vaiheessa, kun verkkoliikenteeseen halutaan alkaa vaikuttaa hallitusti. Hyökkäys tullee toteuttamaan jonkinlaisen käyttöoikeuksien korottamiseen johtavan haavoittuvuuden hyödyntämisen, jolloin sen saavutettua kohteen sillä on kyky saavuttaa kaikki tarvittavat oikeudet toimintojensa suorittamiseen. Nämä oikeudet kuitenkin tarvitaan kokonaisuuden toiminnan varmistamiseksi, ja näin ollen PR-kriteerin arvo on selkeästi H.

Kuten edellisessä kohdassa, ei tässäkään tapauksessa voida vaatia käyttäjän interaktiota toiminnan varmistamiseksi. Vedoten todennäköisessä uhkassa käytettyihin perusteluihin kriteerin UI arvo on tässäkin tapauksessa N.

Vaarallisin hyökkäys reitittimiä kohtaan on sellainen, että se ei pyri pysymään yhdessä reitittimessä. Koska sotilasorganisaatioiden tehokkuus ja käyttövarmuus pohjautuu varsin pitkälti siihen, että laitteisto on yhteneväistä erilaisista ryhmistä ja joukkotyypeistä riippumatta, tämä tarkoittaa vaarallista potentiaalia erilaisten haittaohjelmien leviämiselle. Kun yksi reititin on saastutettu, se tarjoaa välittömästi koko taisteluosaston reititinverkon uudeksi hyökkäysvektoriksi. Esimerkiksi Bittiumin reitittimen käyttämä OLSR-protokolla toimii proaktiivisesti välittämällä jatkuvasti tietoa verkon tilasta kaikille siinä oleville reitittimille, ja lähtökohtaoletuksena on aina se, että kaikki verkossa olevat reitittimet ovat luotettavia[3]. Näin hyökkäys pyrkisi vaikuttamaan vähintään kaikkia reitittimiä vastaan, ja niistä saamiensa osoitetietojen perusteella, sillä olisi kyky tiedustella ja mahdollisesti vaikuttaa myös kaikkiin muihin verkossa oleviin laitteisiin. S-kriteeri on vaarallisimman uhkan tapauksessa ehdottomasti C, ja samalla se tuo koko uhkaan täysin uuden ulottuvuuden.

Koska aiemmin tehtiin oletus, että vaarallisin uhka kykenee läpäisemään eristetyn sotilaallisen verkon suojaukset ja näin ollen liikuttamaan dataa sekä sen sisään että ulos siitä, tietojen luottamuksellisuuden merkitys muuttuu täysin. Vaikka reitittimen itsensä sisältämä tieto ei olisi niin käyttökelpoista hyökkääjälle, sen läpi kulkeva tieto saattaa sisältää äärimmäisen arkaluontoista tietoa. Vaikka tieto onkin todennäköisesti miltei aina suojattu jonkinlaisella päätelaitteiden välisellä salauksella, se ei takaa, etteikö hyökkääjä voisi riittävällä panostuksella saada siitä ainakin sodan kokonaiskuvaa merkittävästi hyödyntävää informaatiota. Jos liikenne saadaan ohjattua hyökkääjän kannalta edulliseen osoitteeseen, kaikki luotettavuus menetetään välittömästi. C-kriteeri saa arvon H.

Tämä koskettaa yhtä lailla reitittimen sisältämän informaation eheyttä. Jos hyökkäys mahdollistaa yhteyden esimerkiksi ulkoiseen hallintapalvelimeen, hyökkääjä voi kontrolloida reitittimen parametreihin tehtäviä muutoksia haluamikseen. Reitittimen eheys menetetään täysin, mikäli hyökkäys onnistuu. Tästä syystä kriteeri I saa arvon H.

Saatavuuden osalta tarkastelu on hieman kaksijakoinen tällaisessa tapauksessa. Toisaalta hyökkäyksen tarkoituksena on tuskin keskeyttää tietoliikennettä missään kohdassa verkkoa, mutta toisaalta liikenteen ohjaaminen odottamattomiin osoitteisiin aiheuttaa yhtä lailla saatavuuden menetyksen reitittimen palveluille. Tällaisella hyökkäyksellä olisi kuitenkin mahdollista parhaimmillaan estää kaikki tietoliikenne suoria yhteyksiä lukuun ottamatta koko taisteluosaston alueella, mikäli hyökkääjä päättäisi joko käyttää reitittimiä pakettien tuhoamiseen niiden välittämisen sijaan, tai jakamalla niitä broadcast-osoitteella koko verkkoon, estäen kaiken muun tietoliikenteen ja tukkien koko kaistanleveyden. A-kriteerin arvoksi tulee H. Näillä arvoilla vaarallisin hyökkäys reititintä vastaan saa Base Scoren 8,0 (High).

Lähtökohtaisesti tällaisen uhkan tapauksessa on syytä olettaa, että haittakoodi tai muut hyökkäykseen käytettävät menetelmät ovat äärimmäisen hienostuneita ja hyvin tarkkaan suunniteltu toimimaan potentiaalisia puolustuksia vastaan. Toiminta tuskin pohjautuisi puhtaan manuaaliseen tai automatisoituun toimintaan ilman haittaohjelman asennuksen tarvetta, johtuen MANET-verkon mobiilista luonteesta ja muuttuvasta infrastruktuurista, ja näin ollen todennäköisesti leviämiseen käytettäisiin jonkinlaista matoa tai virusta muiden hyötykuormien välittämiseksi. Havaitsemattomuuden varmistamiseksi vaaditaan myös paljon suunnittelua ja testausta erilaisissa ympäristöissä, joten E-kriteeri saa arvon H.

Koska hyökkääjä pyrkii toimimaan mahdollisimman huomaamattomasti kohteessaan niin pitkään, kun se on mahdollista, on syytä olettaa, että käytössä on vähintään yksi, jopa useampi nollapäivähaavoittuvuus, joita vastaan ei ole kyetty tekemään valmisteluja tuoreistakin tietoturvapäivityksistä ja -tekniikoista huolimatta. Myöskään siinä tapauksessa, että verkonvalvonnan avulla kyettäisiin havaitsemaan potentiaalisesti haitallista liikennettä tai muuta epäilyttävää ja yksittäinen laite kyettäisiin puhdistamaan, se saastuisi todennäköisesti nopeasti uudelleen muiden reitittimien avustuksella. Kriteeri RL saa arvon U.

Tarkasteltaessa tällaisen hyökkäyksen raporttien tarkkuutta joudutaan useimmiten toteamaan, että minkäänlaisia raportteja ei ole olemassa. Joitain hyökkäyksen osia saattaa olla tunnistettavissa tietyntyyppisiä käyttäytymismalleja seuraamalla, mutta käyttäjätason ilmoituksia ei välttämättä ole lainkaan tai ne ovat hyvin vaihtelevia, jos jonkinlaisia ongelmia esiintyy. Verkonvalvonta pystyy hyvässä tapauksessa analysoimaan jonkinlaisia ilmiöitä normaalista poikkeavasta liikenteestä, mutta havaintoja ei pystytä yhdistämään mihinkään tunnettuun uhkaan eivätkä automaattiset tietoturvatyökalut tuota minkäänlaisia havaintoja. Tässä kohtaa mielestäni täyttyvät kriteerit RC-kriteerin arvolle U, mutta koska se laskee uhkan vaarallisuutta CVSS-laskurissa, annetaan arvoksi X, koska tällainen tilanne on paljon vaarallisempi kuin selkeästi dokumentoidussa ja analysoidussa uhkassa. Näin myös Temporal Scoreksi muodostuu 8,0 (High).

Koska reitittimien kautta liikkuu käytännössä kaikki taisteluosaston sisällä tapahtuva tietoliikenne järjestelmästä riippumatta, ovat niille asetetut turvallisuusvaatimukset ehdottomasti oltava riittävän korkeat kuvastamaan niiden puuttumisesta aiheutuvaa uhkaa. Koska niin suuri osa liikenteestä sisältää jossain määrin kriittistä tietoa, mukaan lukien tilannetietoa, tiedustelutietoa ja käskyjä tuleviin toimintoihin, CR-kriteerin arvo on tässä tapauksessa H.

Myös tietojen eheys on ehdottoman korkealla vaatimustasolla, sillä mikäli esimerkiksi reititystauluja muokataan hyökkääjälle edullisiksi, reitittimet muuttuvat välittömästi hyökkääjän käytössä oleviksi aseiksi, joilla voidaan haitata kaikkea tietoliikennettä taisteluosaston sisällä. IR-kriteerin arvo on H. Tämän lisäksi, kuten jo todennäköisen uhkan tapauksessa todettiin, on reititinten pääfunktio tiedonsiirron takaaminen taisteluosastossa. Koska tästä vaatimuksesta ei voi säästää tilanteesta riippumatta, senkin arvo on H. Lopullinen Environmental Score on **8,0** (High), eli uhka on todella vaarallinen toiminnalle, ja kokonaisuus on esitetty alla (Kuva 17).

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 Requirement	**CR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Integrity Requirement	**IR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Availability Requirement	**AR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	

Kuva 17: Vaarallisin uhka reitititintä vastaan.

5.2. Työasema

Työasema / Todennäköinen

Työasemat ovat esikuntien tärkein suunnittelutyökalu, sillä ne sisältävät itsessään suunnitteluun tarvittavat perusvälineet, kuten tekstin- ja kuvankäsittelyyn tarvittavat ohjelmistot, tallentamismahdollisuuden sekä mahdolliset käytössä olevat taistelunjohto- ja tietojärjestelmät. Ne ovat samalla kuitenkin verkon kauimmaisessa reunassa eri verkkolaitteista nähden, ja niihin käsiksi päästäkseen täytyy ohittaa monta muuta laitetta. Todennäköisin hyökkäysvektori työasemaa vastaan suuntautunee tuotantoketjussa, johon vaikuttaakseen hyökkääjällä täytyy todennäköisesti olla pääsy vähintään ohjelmistovalmistajan tuotantovälineisiin suorasti tai epäsuorasti kyetäkseen vaikuttamaan ohjelmistoon sen tuotanto- ja jakeluvaiheessa. Tästä syystä AV-kriteeri saa arvon L.

Saavuttaakseen kyvyn toteuttaa hyökkäyksen taisteluosaston käytössä olevaa työasemaa kohtaan, tai siinä olevaan ohjelmistoon, vaaditaan kattavaa tiedustelua käytössä olevasta ohjelmistosta tai siihen liittyvästä laitteistosta. Lisäksi hyökkääjä ei voi olettaa hyökkäyksensä toimivan toistuvasti, koska valmistaja tai asiakas pystyvät tarkastamaan ohjelmiston sisällön esimerkiksi laboratorio-olosuhteissa, ennen kuin hyökkäys ehtii välttämättä edes vaikuttaa. Näin ollen AC-kriteeri saa arvon H.

Käyttöoikeuksien tarve hyökkäyksen onnistumiselle on hieman riippuvainen hyökkäyksen tarkoituksesta. Lähtökohtaisesti hyökättäessä työasemaa kohtaan voidaan kuitenkin olettaa, että tarkoituksena olisi poistaa tai muokata sen sisältämiä tietoja, sillä pelkällä käytön estämisellä ei välttämättä saavutettaisi merkittävää vaikutusta. Poistamisen ja muokkaamisen takaamiseksi vaadittaneen vähintään käyttäjätason pääsyoikeudet, joten kriteeri PR saa arvon L.

Puhuttaessa haittaohjelmasta, jolla on tarkoitus vaikuttaa sotilasorganisaatiota vastaan, on jokseenkin vaikea nähdä sellaista haittaohjelmaa, joka vaatisi käyttäjältään mitään toimenpiteitä onnistuakseen. Lähtökohtana kaikille työasemille kohdistuville haittaohjelmille on se, että ne toimivat itsenäisesti ja pyrkivät toimimaan mahdollisimman huomaamattomasti. Kriteeri UI saa siis arvon N.

Kun tarkastellaan sitä, miten todennäköinen hyökkäys työasemaa kohtaan toimisi, on tarkasteltava sitä, mikä sen vaikutukseksi on alun perin arvioitu. Koska edellisen kohdan arvion mukaan hyökkääjä pyrkisi minimoimaan havaittavuutensa, hyökkäyksen voidaan olettaa pitäytyvän nimenomaan työasemassa, eikä pyrkiä etsimään lisähaavoittuvuuksia muista verkossa toimivista laitteista. Ylimääräinen liikennöinti verkon sisällä saattaisi herättää huomiota verkonvalvonnassa, mikäli se poikkeaisi selkeästi työaseman toiminnasta, ja siksi hyökkäys pyrkisi välttämään tätä. Tästä syystä kriteeri S saa arvokseen U.

Tiedon luottamuksellisuuden säilyttäminen on tämän kaltaisessa tapauksessa kaikista helpoin näistä kolmesta tietoturvan osa-alueesta, koska taktinen verkko ei välttämättä ole kytkettynä mihinkään laitteeseen, josta olisi pääsy ulkoiseen verkkoon, ja vaikka olisikin, on yhteyden muodostaminen ilman todella edistynyttä uhkaa todella vaikea toteuttaa yhden hyökkäyksen turvin. Kriteeri C saa siis arvokseen N, koska luottamuksellisuus ei laske lainkaan.

Vaikka tiedon eheyteen pystytään varmasti vaikuttamaan tämän kaltaisella hyökkäyksellä, sen kontrollointi voi olla samasta syystä hankalaa, kuin luottamuksellisuuden kanssa. Jos hyökkääjällä ei ole kykyä kommunikoida työasemalla olevan haittaohjelman kanssa, se kykenee kyllä muokkaamaan tiedostoja, mutta vain ennalta suunniteltujen algoritmien mukaisesti eikä siten, miten hyökkääjä saattaisi siinä tilanteessa haluta. Näin ollen kriteeri I saa arvokseen L.

Saatavuuteen on mahdollista vaikuttaa voimakkaastikin tämän kaltaisessa skenaariossa, mutta sen vaikutukset voivat silti jäädä melko vähäisiksi käyttäjän kannalta. Mikäli hyökkäys estäisi joko tiedostojen, sovellusten tai koko työaseman käytön tilapäisesti tai pysyvästi, se pystytään todennäköisesti korvaamaan uudella tai sen toiminnallisuudet kyetään toteuttamaan toisella työasemalla. Vain siinä tapauksessa, että hyökkäys vaikuttaisi useisiin työasemiin kerralla, sillä kyettäisiin saavuttamaan merkittävä vaikutus saatavuuteen. Kriteerin A arvoksi tulee siis L. Näillä arvoilla todennäköinen uhka työasemaa vastaan saa Base Scoren 3,6 (Low).

Haittaohjelman tai muun hyökkäyksen voidaan olettaa olevan teknisesti hyvin edistyneellä tasolla, koska lähtökohtaisesti hyökkääjä on jokin toinen valtio, jolla on riittävät resurssit hyvinkin laadukkaaseen kehitystyöhön. Hyökkäys on todennäköisesti räätälöity toimimaan nimenomaan tietynlaisessa ympäristössä ja tiettyä ohjelmistoa tai järjestelmää vastaan, eikä sen toiminnan varmuudesta pitäisi olla epävarmuutta. Näin ollen kriteeri E saa arvokseen H.

Koska hyökkäys on todennäköisesti tarpeeseen räätälöity, kuten edellisessä kohdassa mainittiin, ei siihen ole myöskään valmista, valmistajan kehittämää parannuskeinoa saatavissa. Moneen työaseman tietoja muokkaavaan tai poistavaan ongelmaan on kuitenkin mahdollista kehittää jonkinlainen tilapäisratkaisu ongelman väistämiseksi. Tekstitiedostot voidaan tallentaa eri tiedostomuotoon, mikäli normaalisti käytössä olevissa esiintyy hyökkäyksen merkkejä, kuvatiedostoja voidaan liittää tekstitiedostojen sisään, jotta niiden katoamiselta välttyisi tai taistelunjohtojärjestelmistä voidaan ottaa ruutukaappauksia, mikäli niissä havaitaan poikkeamia. RL-kriteeri saa näin ollen arvokseen W.

Raportoinnin luotettavuudesta puhuttaessa on melko varmaa, että minkäänlaista julkaistua tietoa kyseisestä hyökkäyksestä ei löydy. Käyttäjät saattavat raportoida samantapaisista ongelmista useissa eri työasemissa, joka antaa indikaation ongelman olemassaolosta, mutta ei ole riittävä tieto analysoimaan hyökkäyksen laatua sen tarkemmin. RC-kriteeri saa arvokseen U. Nämä lisäkriteerit huomioiden uhka saa Temporal Scoren 3,3 (Low).

Tietoturvallisuusvaatimukset työasemaa käsiteltäessä eivät ole kovinkaan korkeat, koska oletusarvoisesti kaikista kriittisimmät tiedot ovat tallennettuna muualle, tai ne liikkuvat jonkin järjestelmän sisällä yhteistyössä muiden taisteluosaston toimijoiden kanssa. Luotettavuuden menetys saattaisi aiheuttaa vakavan vaaran joukon toiminnalle, joten kriteeri CR saa arvon M. Eheyden menetys aiheuttaisi yhtä lailla vakavan vaaran, joten myös kriteeri IR saa arvon M. Saatavuuden menetys ei olisi yhtä kriittinen toiminnan kannalta, sillä muilla välineillä pystyttäisiin korvaamaan työaseman käyttökyvyttömyydestä johtuvat haittatekijät, ja kriteeri AR saa näin ollen arvon L. Näin ollen, ympäristötekijät huomioiden työasemaan kohdistuva todennäköinen uhka saa Environmental Scoren **2,8** (Low), eikä uhka ole näin ollen kovinkaan merkittävä. Kokonaisuus on esitetty alla (Kuva 18).

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 Requirement	**CR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Integrity Requirement	**IR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Availability Requirement	**AR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	

Kuva 18: Todennäköinen uhka työasemaa vastaan.

Työasema / Vaarallisin

Kun pohditaan vaarallisinta työasemaan vaikuttavaa hyökkäystä, sen täytyy tapahtua odottamatta. Tällöin tilanne ei mahdollista sitä, että hyökkäys olisi saatavilla kohteeseen vain paikallisessa lähiverkossa tai fyysisesti syöttämällä. Vaarallisimman tällaisesta hyökkäyksestä tekisi se, että se kyettäisiin saattamaan kohteeseensa verkon yli, potentiaalisesti jostain aivan muualta kuin taisteluosaston fyysiseltä lähialueelta. Hyökkäys olisi sellainen, että se kykenisi saavuttamaan työaseman joko taisteluosaston langattoman verkon yhteyspisteitä hyödyntäen tai runkoverkosta, siten, että se pystyisi kulkemaan reititinten ja palomuurien läpi. AV-kriteeri saa arvon N.

Kuten todennäköistä uhkaa arvioitaessa, tilanne hyökkäyksessä sotilasorganisaatiota vastaan vaatii valtavan määrän tiedustelua ja valmistelua ennen melko varmaa onnistumista, eikä silloinkaan hyökkäys ole välttämättä toistettavissa kovin montaa kertaa. AC-kriteerin arvo on tässäkin tapauksessa H.

Vaarallisimmat hyökkäykset vaativat usein käyttöönsä korkeat käyttöoikeudet, jotta ne kykenevät toteuttamaan maksimaalisen vaikutuksen kohteessaan. Hyökkäykseen voi liittyä esimerkiksi uusien ohjelmien asennusta työasemalle, järjestelmäasetusten muokkaamista tai muuta sellaista, jota ei voi suorittaa voimakkaasti rajoitetuin peruskäyttäjän oikeuksin. Vaikka hyökkäys todennäköisesti pyrkisi saavuttamaan korotetut käyttöoikeudet hyödyntämällä jonkinlaista escalation of privileges -haavoittuvuutta, se ei poista niiden tarvetta. Näin ollen PR-kriteerin arvoksi tulee H.

Tässäkään tapauksessa, kuten todennäköisessä uhkassa, ei oleteta käyttäjän toimenpiteillä olevan vaikutusta siihen, toimiiko hyökkäys vai ei. UI-kriteerin arvo on näin ollen N.

Vaarallisimman hyökkäyksen tapauksessa on lähes varmaa, että tavoitteena ei ole pelkästään työasemaan vaikuttaminen, etenkään kun oletetaan, että hyökkäys on saavuttanut työaseman verkon ylitse. Työasemaan päätynyt hyökkäys tullee skannaamaan muita verkossa olevia laitteita, selvittäen niistä mahdollisimman paljon tietoa tai käyttäen niitä hyökkäysvälineenä esimerkiksi palvelunestohyökkäyksen toteuttamiseksi taisteluosaston taktisen verkon sisällä. On myös mahdollista, että itse hyökkäys ei ole suunnattu työasemaa vaan jotain muuta verkossa olevaa laitetta vastaan, mutta hyökkäyksen toteuttamiseksi käytetään työasemissa esiintyvää haavoittuvuutta. S-kriteeri saa arvokseen C.

Jos hyökkäys pääsee reitittimien lävitse sisään työasemaan, sillä on todennäköisesti myös reitti ulos sieltä. Tällöin mikäli verkonvalvonnassa ei paljastu mitään liian epätavallista, se pystyy todennäköisesti siirtämään kaiken haluamansa tiedon kohdekoneelta haluamaansa kohteeseen verkon mahdollistaessa. Mikäli runkoverkon kautta ei ole mahdollista siirtää tietoa suoraan julkisen internetin puolelle, on silti olemassa mahdollisuus jakaa dataa vähintään taisteluosaston omia tukiasemia hyödyntäen. Kaikki tallennettu tai työasemalla toimivassa ohjelmistossa liikkuva tieto on näin ollen vuodettavissa ja järjestelmän luotettavuus on täysin menetetty. Kriteeri C saa arvokseen H.

Samaa periaatetta hyödyntäen hyökkääjällä on todennäköisesti mahdollisuus toimittaa komentoja haittaohjelmalle työasemassa, tai mikäli kyseessä ei edes ole suoranainen haittaohjelma, niin hyökkääjällä on suora pääsy työaseman sisältöön verkon kautta. Näin ollen hyökkääjä pystyy vaikuttamaan siihen, mitä informaatiota ja miten halutaan muokattavan, ja siten vaikuttaa vähintään epäsuorasti taisteluosaston päätöksentekoon. Tietojen eheys on täysin menetetty, eikä mihinkään työaseman sisällä olevaan informaatioon voi suhtautua varauksetta luotettavana. Kriteeri I saa arvon H.

Jos haittaohjelma on onnistunut saavuttamaan korkeat käyttöoikeudet, kuten vaarallisimman tapauksen oletetaan saavuttavan, sillä on kyky katkaista saatavuus tiedostoihin tai palveluihin kokonaan kohdetyöasemassa. Järjestelmänvalvojan oikeuksin hyökkääjän on mahdollista poistaa sovelluksia tai tiedostoja, sulkea tietyn tyyppisen verkkoliikenteen vaatimia liikennöintiväyliä tai kryptata koko kovalevyn sisältö niin halutessaan. Saatavuus on täysin menetetty, mikäli hyökkääjä niin haluaa, ja siksi kriteeri A:n arvo on H. Näistä perustekijöistä muodostuu Base Score 8,0 (High).

Hyökkäysmetodi on teknisesti hienostunut, ja sen käyttö tulee onnistumaan käytännössä kaikissa tapauksissa johtuen kattavasta tiedustelusta ja suunnittelusta. Hyökkäys pyrkii leviämään itsenäisesti verkossa vähintään kaikkiin vastaavanlaisiin laitteisiin, ja pyrkii selvittämään ympäröivän verkon rakennetta ja mahdollisia muita laitteita. Kriteeri E saa arvoksi H.

Hyökkäys on mahdollisesti täysin uudenlainen toiminnaltaan, tai se toteuttaa kohteeseen päästyään useita erilaisia toimintoja. Se voi jopa muuttaa omaa toimintaansa hyökkääjän havaitessa vastatoimenpiteiden yrittämistä, koska hyökkäystä on mahdollista muokata niin kauan kun siihen on yhteys verkon yli. Minkäänlaista vastatoimenpidettä ei ole mahdollista toteuttaa, muutoin kuin rajoittamaan joitain yksittäisiä ominaisuuksia, mutta hyökkäyksen jatkuminen on edelleen todennäköistä. RL-kriteeri saa arvoksi U.

Tällaisesta hyökkäyksestä ei ole saatu tuotettua minkäänlaista luotettavaa tietoa hyökkäyksen luonteen selvittämiseksi, ja koska se ei välttämättä toimi joka kerta kaavamaisesti, siitä kerättyjen ilmoitusten sisältö saattaa vaihdella. Koska uhkan luonteesta ei ole varmuutta, RC-kriteeri saa arvoksi U. Näillä lisämuuttujilla uhka saa Temporal Scoren 7,4 (High).

Koska ympäristötekijät eivät muutu uhkan mukana, CR-kriteerin arvo on edelleen M, IR-kriteerin arvo on M ja AR-kriteerin arvo L. Kun nämä kriteerit huomioidaan aiempien lisäksi, lopputuloksena on Environmental Score **7,4** (High), joten uhka on erittäin vaarallinen toteutuessaan. Kokonaisuus on esitetty alla (Kuva 19).

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 Requirement	**CR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Integrity Requirement	**IR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Availability Requirement	**AR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	

Kuva 19: Vaarallisin uhka työasemaa vastaan.

5.3. Tiedostopalvelin

Tiedostopalvelin / Todennäköinen

Taisteluosaston tiedostopalvelin, oli kyseessä sitten taisteluosaston omalla laitteistolla toimiva tiedostonjakojärjestelmä tai verkkoyhteyden kautta käytettävä asevoimien hallinnassa oleva etäpalvelin, on äärimmäisen tärkeä väline tiedonjakoon ja arkistonhallintaan taisteluosaston sisällä. Kuten muiden laitteiden tapauksessa, on syytä olettaa, että lähtökohtaisesti hyökkääjällä ei ole mahdollisuutta aktiiviseen ja luotettavaan yhteyteen itsensä ja hyökkäyskohteen välillä, vaan hyökkäyksen on toimittava itsenäisesti kohteessa. Todennäköisin uhka tällaisessa tapauksessa on tiedostojen tuhoamiseen, niiden sisällön muokkaamiseen tai kryptaamiseen perustuva haittaohjelma, jonka tarkoituksena on vaikeuttaa tiedostojen keskitettyä jakamista taisteluosaston sisällä. Toimitusmenetelmänä kohteeseen toimisi todennäköisesti hyökkäys joko tuotantoketjussa tai ylläpitohenkilöstön laitteiston avulla, vaatien vähintään pääsyn laitteelle tai sitä hallinoivalle laitteelle, jotka eivät toimi verkoissa. Näin ollen AV-kriteeri saa arvon L.

Tällaisen hyökkäyksen kompleksisuutta arvioitaessa joudutaan tarkastelemaan monia eri näkökulmia. Toisaalta hyökkäyksen toimintamekaniikka voisi olla hyvinkin yksikertainen, perustuen vain siihen, että se poistaisi määriteltynä ajanhetkenä kaikki tiedostot halutusta kohteesta tai kaikista tiedostopalvelimen mahdollisista levyasemista. Toisaalta taas hyökkäys paljastuisi tällöin välittömästi ja uhka kyettäisiin todennäköisesti poistamaan kohteesta verrattain nopeasti. Koska ajastaminen on muutenkin hyökkäyshetken määrittelemisessä hyvin epäluotettava metodi tulosten saavuttamisen näkökulmasta, hyökkäyksen täytyisi kyetä tunnistamaan selkeitä tunnusmerkkejä tiedostojen määrässä tai tyypissä hyökkäyksen toteuttamiseksi. Lisäksi sen tulisi pyrkiä piiloutumaan siten, että se kykenisi laukaisemaan hyötykuormansa useammin kuin kerran varmistetun vaikutuksen saavuttamiseksi. AC-kriteeri saa arvokseen H.

Tiedostoihin vaikuttavan hyökkäyksen etuna tällaisessa tapauksessa on se, että se ei vaadi korkeita käyttäjäoikeuksia kyetäkseen toimimaan haluamiaan tiedostoja vastaan. Levyasemille on todennäköisesti asetettu jonkinlaisia pääsyrajoituksia, mutta ne täytyy olla toteutettu käyttäjäoikeuksin jotta niiden laajamittainen käyttö kyetään takaamaan niitä käyttäville joukoille. Oletetaan, että hyökkäys vaatii peruskäyttäjän oikeudet kyetäkseen toteuttamaan kaiken tarvitsemansa, joten PR-kriteeri saa arvon L.

Periaatteessa tällaisessa tapauksessa vaarallisimman vaikutuksen saamiseksi hyökkäyksen olisi mahdollista luottaa käyttäjän toimintoihin. Tekstitiedostoon piilotettu makrovirus voisi toimia aktivointimekanismina käyttäjän avatessa tiedoston, mutta toisaalta tiedoston nimeämiskäytännön hyödyntäminen tiedoston avaamisen takaamiseksi voisi olla hankalaa. Lähtökohtaisesti olisi syytä olettaa, että hyökkäyksen kompleksisuudesta johtuen se kykenisi aktivoimaan hyötykuormansa ilman käyttäjän toimintaa, vaikka sitä voisikin hyödyntää tarvittaessa. UI-kriteerin arvoksi muodostuu N.

Vaikka tiedostopalvelin itsessään tarjoaa massiivisen potentiaalin hyökkäyksen leviämiselle moniin kohteisiin, todetaan tässä tapauksessa kuitenkin hyökkäyksen keskittyvän tiedostopalvelimen sisältöön. Näin ollen, ilman laajempaa analyysia todetaan S-kriteerin olevan tässä tapauksessa U.

Koska aiemmin todettiin, että hyökkäyksellä ei ole kykyä luotettavaan kommunikaatioon hyökkääjän kanssa, ei silloin kyetä myöskään varastamaan tiedostopalvelimella olevia tiedostoja. Vaikka kyseessä oli taisteluosaston laitteistoon kuuluva palvelin, sieltä saattaisi kattavan verkkotiedustelun jälkeen kyetä lähettämään tiedostoja satunnaisiin verkkokohteisiin ja näin aktivoida alueella toimivia langattomia verkkoja, lähetetyt tiedostot olisivat silti satunnaisia tiedostoja ja niiden saattaminen hyökkääjän haltuun olisi ennemmin satunnaisuuden varassa kuin hyökkäyksen toiminnan. Tietojen luottamuksellisuus ei kärsi, ja C-kriteeri saa arvokseen N.

Samasta syystä tiedostojen eheyteen vaikuttaminen on haastavaa hyökkääjän kannalta. Niiden sisältöä kyetään mahdollisesti muuttamaan, mutta muutoksia ei kyetä hallitsemaan täysin, vaan ne saattavat olla satunnaisia ja puolustajan kannalta ilmeisiä ja epäilyksen herättäviä. Näin ollen kriteeri I saa arvokseen L.

Hyökkäyksen luonteesta riippumatta, oli kyseessä sitten tiedostoja poistava, salaava tai kryptaava haittaohjelma, se aiheuttaa väistämättä jonkinlaisen haasteen tietojen saatavuudelle. Tietojen poistaminen aiheuttaa välittömän, täydellisen saatavuuden menetyksen kaikkiin menetettyihin tietoihin, ja sitä ei kyetä korvaamaan ilman saatavilla olevia varmuuskopioita tai tiedostojen uudelleen vientiä palvelimelle työasemilta tai vastaavilta. Jopa tietojen eheyteen vaikuttaminen saattaa aiheuttaa informaation saatavuudelle selkeän esteen, jolloin tiedostojen käyttöarvo laskee nollaan. A-kriteerin arvoksi tulee H, ja näin ollen uhka saa Base Scoren 5,3 (Medium).

Tällaiseen hyökkäykseen vaadittavat ominaisuudet eivät välttämättä ole vaatimuksiltaan korkeimmalla tasolla, sillä tarpeen tullen hieman viimeistelemättömämpi hyökkäyskin voi saavuttaa riittävän vaikutuksen. Jos tavoitteena ei ole toteuttaa toistuvasti onnistuvaa ja äärimmäisen vaikeasti poistettavaa haittaa, vaan saavuttaa vaikutus korkeintaan muutamia kertoja tilapäiseksi saatavuuden minimoimiseksi, tähän saattaa riittää monilta ominaisuuksiltaan hieman keskeneräinenkin hyökkäys. Etenkin sellaisessa tapauksessa, että hyökkäysajankohtaa ei kyetä tarkasti määrittelemään tai tarkka ajankohta ei välttämättä ole otollinen hyökkäyksen käynnistämiselle, se saattaa silti aiheuttaa odottamattoman uhkan. E-kriteeri saa arvon F.

Lähtökohtaisesti jo tuotantovaiheessa kohdelaitteelle toimitettua haittaohjelmaa voi olla äärimmäisen vaikeaa estää minkäänlaisin vastatoimin. Estämisen sijaan hyökkäyksen vaikutuksia voidaan kuitenkin pyrkiä minimoimaan ensimmäisen havainnon jälkeen, tällaisessa tapauksessa esimerkiksi varmistamalla se, että kaikki tiedostopalvelimen tiedostot varmuuskopioidaan jatkuvasti myös jollekin verkosta irralliselle laitteelle, josta ne voidaan tietojen menettämisen jälkeen tarvittaessa palauttaa tiedostopalvelimelle sen puhdistamisen jälkeen. RL-kriteeri saa arvon W.

Toiminnastaan riippuen tiedostojen muokkaamiseen perustuva haittaohjelma tulee varmasti ennemmin tai myöhemmin herättämään taisteluosaston henkilöstön huomion. Tiedostojen erikoiselta näyttävät muokkauksen jättämät aikaleimat, satunnaiset havainnot mahdollisten asiakirjojen erikoisesta sisällöstä tai tiedostojen katoaminen aiheuttavat varmasti ilmoituksia johtamisjärjestelmähenkilöstölle. Niiden sisältö saattaa kuitenkin vaihdella voimakkaasti, ja niiden pohjalta voi olla vaikea paikallistaa todellista syypäätä näille tapahtumille. Riittävän monta havaintoa riittää kuitenkin syyksi epäillä jonkinlaista hyökkäystä, tuntematta sen tarkempaa aiheuttajaa, ja tällöin hyökkäyksellä on aina riski paljastua. RC-kriteeri saa arvon U, ja näin ollen tiedostopalvelimeen kohdistuvan todennäköisen uhkan Temporal Score on 4,6 (Medium).

Tiedostopalvelimet ovat luonteeltaan luottamuksellisen tiedon keskittymiä. Niille tallennetaan jatkuvasti kuvia, käskyjä, suunnitelmia ja muuta tiedostomuodossa syntyvää dataa taisteluosaston tueksi. Jos hyökkääjä pääsee käsiksi niiden sisältöön, koko taisteluosaston toiminta on vaarassa ja seuraamukset voivat olla katastrofaaliset. CR-kriteerin arvo on väistämättä tässä tapauksessa H, mutta koska todennäköisen uhkan tapauksessa luottamuksellisuuden menetystä ei tapahdu, ei tämä myöskään vaikuta lopulliseen arvosanaan.

Eheysvaatimus on hieman ristiriitainen pohdittava riippuen siitä, että eheyden muutoksen sisällöllä on ratkaiseva merkitys tämän vaatimuksen tasossa. Satunnaiset muutokset tuhoavat kyllä eheyden, mutta se ei välttämättä johda merkittäviin seuraamuksiin taisteluosaston taistelussa. Hallitut muutokset sen sijaan voisivat olla täysin tuhoisia. Selkeyden vuoksi käsitellään eheysvaatimusta juuri tämän tyyppiseltä uhkalta, ja annetaan IR-kriteerille arvo M.

Saatavuuden osalta vaatimus on helppo määrittää. Mikäli tiedostopalvelimen tietoihin ei pääse käsiksi, on käytännössä kaksi vaihtoehtoa: taisteluosasto menettää kykynsä jakaa tietoa laajalle joukolle nopeasti, tai se alkaa käyttää aktiivisesti kaikkia viestijärjestelmiään, kuormittaen verkkoa vielä enemmän, kun ei pystytä yksiselitteisesti määrittämään, mihin osoitteisiin mitäkin tietoa täytyy lähettää taistelun onnistumiseksi, eivätkä tarvitsijat voi itse käydä hakemassa oma-aloitteisesti tietoa. AR-kriteerin arvo on H, ja näin ollen lopullinen Environmental Score on **5,8** (Medium). Uhka on syytä huomioida suunnittelussa, mutta sitä vastaan on kohtalaisen hyvin toimintamahdollisuuksia. Kokonaisuus on esitetty alla (Kuva 20).

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 Requirement	**CR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Integrity Requirement	**IR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Availability Requirement	**AR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	

Kuva 20: Todennäköinen uhka tiedostopalvelinta vastaan.

Tiedostopalvelin / Vaarallisin

Vaarallisimman uhkan tiedostopalvelimella, ajatellen taisteluosaston toimintaa aiheuttaa väistämättä sellainen uhka, joka kykenee leviämään sen kautta muihin laitteisiin. Geneerisen tiedostopalvelimen näkökulmasta tarkasteltuna sen paikallistaminen taisteluosaston laitteistosta voi olla äärimmäisen vaikeaa, puhumattakaan siitä, että se toimisi ulkoisen verkkoyhteyden takana, fyysisesti muualla. Lähtökohtana voisi pitää, että suurimmassa osassa tapauksia olisi mahdotonta saavuttaa kunnollista hallintayhteyttä hyökkäyksen hallitsemiseksi, mutta silti hyökkäyksellä olisi kyky liikkua esimerkiksi taisteluosaston laitteistojen välillä kohteeseensa pääsemiseksi. Koska tällainenkin liikenne kuitenkin täyttää korkeimman uhkatason vaatimukset hyökkäysvektoria arvioitaessa, AV-kriteeri saa arvon N.

Tässä tapauksessa uhka tulee myös olemaan äärimmäisen hienostuneesti toteutettu, sillä sen tulee samanaikaisesti pyrkiä piiloutumaan niin verkonvalvonnalta kuin perinteisiltä tietoturvaohjelmistoilta, kyetä toteuttamaan oma liikkumisensa joko autonomisesti tai saastuttamalla tiedostopalvelimen tiedostoja ja siirtyä jokaisen latauksen mukana, ja lisäksi toteuttamaan erilaisia haittavaikutuksia kohdelaitteissa. Tämä vaatii valtavan määrän valmistelua, suunnittelua ja testausta, ja AC-kriteerin arvo on ehdottomasti H.

Jotta tällainen hyökkäys pystyy toteuttamaan kaikki hienostuneimmat komponenttinsa, se tullee vaatimaan enemmän käyttöoikeuksia kuin äsken tarkasteltu todennäköinen hyökkäys. Itse toimenpiteet tiedostoja kohtaan eivät välttämättä vaadi sen enempää oikeuksia, mutta piiloutumisen kannalta ne saattavat olla elintärkeitä. Tästä syystä PR-kriteeri saa arvon H.

Koska hyökkäys on niin monimuotoinen, käyttäjän interaktiota voi olla hankala analysoida absoluuttisesti. Esimerkiksi tartuttamisen ei pitäisi olla lähtökohtaisesti missään nimessä käyttäjän toiminnasta riippuvaista, mutta hyötykuorman aktivoimisessa sitä voitaisiin hyvin käyttää, mikäli kyseessä olisi esimerkiksi asiakirjaan upotettu makro tai vastaava. Koska halutaan kuitenkin analysoida vaarallisinta uhkaa, todetaan että sen toiminta ei saisi missään vaiheessa olla riippuvainen käyttäjien toiminnasta. UI-kriteerin arvoksi tulee N.

Vaarallisimman uhkan suurin eroavaisuus oletettuun todennäköiseen uhkaan on se, että hyökkäyksen oletetaan leviävän kaikkiin tiedostopalvelimeen yhteydessä oleviin laitteisiin. Riippumatta siitä, miten hyökkäys pääsee leviämään, sen toiminta tulisi varmasti olemaan monilta osin samanlaista esimerkiksi työasemilla. Jos hyökkäys mahdollistaisi minkä tahansa tyyppisten tiedostojen poistamisen tai muokkaamisen, se muuttuisi välittömästi merkittäväksi uhkaksi myös esimerkiksi reitittimille, jolloin sen paikantaminen tai poistaminen muuttuisivat lähes mahdottomiksi realistisessa ajassa. S-kriteeri saa arvon C.

Tietojen luottamuksellisuus voi näin monipuolisen uhkan tapauksessa olla vaarantunut, mutta vain siinä tapauksessa, että hyökkääjä kykenee saavuttamaan reitittimen ja sitä kautta tarvittavan kyvyn muodostaa yhteyden ulos suljetusta verkosta. Oletetaan, että hyökkäys ei ole kohdistettu puhtaasti verkon manipulointiin, mutta johtuen sen kyvystä levitä muihin verkon laitteisiin, sillä on kuitenkin otollisissa olosuhteissa mahdollisuus saada yhteys hyökkääjään hetkellisesti. Tällöin tietojen luottamuksellisuus saatetaan menettää joiltain osin, mutta ei kuitenkaan siten, että kaikki tiedot menetettäisiin tai että haluttua sisältöä pystyttäisiin täysin valikoimaan. C-kriteeri saa arvon L.

Edellisen kohdan perusteisiin vedoten, kuten myös todennäköisimmän uhkan tapauksessa, tietoja tullaan varmasti muokkaamaan tavalla tai toisella, mutta ilman verkkoyhteyttä hyökkääjän ja kohteen välillä on mahdotonta määritellä muokkauksia sellaisiksi, että niillä kyettäisiin tuottamaan merkittävämpää haittaa kuin satunnaisilla muokkauksilla. Tästä syystä I-kriteerin arvo on tässäkin tapauksessa L.

Tässä tapauksessa hyökkääjällä on äärimmäisen edullinen asema saatavuuteen vaikuttamiseksi. Jo pelkästään tiedostopalvelimeen ja sen sisältöön vaikuttamalla kyetään estämään tiedon saatavuus lähes varmasti, kuten todennäköisen uhkan analyysissa todettiin. Mikäli tiedostopalvelin on verkkoarkkitehtuurissa vain yhden reitittimen kautta tavoitettavissa, esimerkiksi jossain taisteluosaston omassa laitteessa, voitaisiin tähän reitittimeen vaikuttamalla kyetä estämään kaikki liikenne tiedostopalvelimelle ja tuottaa vastaava saatavuuden menetys. A-kriteeri saa ehdottomasti arvon H. Näin saadaan tälle uhkakuvalle Base Score 7,2 (High).

Vaikka tiedostopalvelin tarjoaa loistavan mahdollisuuden levittää haittaohjelmaa verkkoympäristössä ilman hyökkääjän toimenpiteitä johtuen jatkuvasta tiedostojen siirrosta, olisi jokseenkin naiivia olettaa sen olevan ainut leviämismenetelmä korkealaatuisessa, kohdennetussa hyökkäyksessä. On hyvin oletettavaa, että hyökkäys pyrkisi selvittämään mahdollisimman nopeasti kaikki palvelimen kanssa yhteydessä olevat muut laitteet, ja leviämään mahdollisuuksien mukaan itsenäisesti myös niihin. Mikäli hyökkäys löytäisi näin uuden kohteen, se mahdollistaisi jälleen vastaavanlaisen ympäristön skannauksen, ja paljastaisi siten lisää potentiaalisia tartuntakohteita verkosta. Kaikki tämä toiminta olisi todennäköisesti täysin automatisoitua ja luotettavaa toiminnaltaan, jolloin E-kriteerin arvoksi tulee H.

Koska hyökkäyksen on oletettu olevan luonteeltaan ympäristöönsä levittäytyvä ja teknisesti edistynyt, siihen kohdistuvat vastatoimenpiteet ovat äärimmäisen haastavia toteuttaa. Tiedostopalvelin kyetään tyhjentämään sisällöstä ja asentamaan täysin uutta vastaavaan tilaan, mutta mikäli uhkaa ei tunneta tarkalleen, ja se on edelleen olemassa samassa verkossa olevissa laitteissa, palvelin vain saastuisi välittömästi uudelleen palattuaan verkkoon. Ainut ratkaisu olisi saada kaikkiin verkon laitteisiin hyökkäyksen paljastava tai toiminnan estävä tietoturvapäivitys, joka ei ole liikkuvassa taistelevassa joukossa kovinkaan käyttökelpoinen toimintatapa, vaikka hyökkäyksen yksityiskohtia saataisiinkin tietoon. RL-kriteeri saa arvon U.

Olisi erikoista olettaa, että tällaisen hyökkäyksen toiminta ei rakentuisi yhden tai useamman nollapäivähaavoittuvuuden varaan. Niiden käytöllä kyetään usein takaamaan ainakin hyökkäyksen kannalta kriittisimpien vaiheiden toteutuminen niin, että niitä vastaan ei kyetä ainakaan välittömästi toimimaan, eikä korjausta ole saatavilla. Tästä syystä hyökkäyksestä ei myöskään ole saatavilla minkäänlaista selkeästi raportoitua dataa, vaan pelkästään mahdollisia yksittäisten käyttäjien havaintoja epäilyttävästä toiminnasta mahdollisten poikkeamien muodossa. Muuttuneita sisältöjä on helppo epäillä kirjoitusvirheiksi, ja tiedostojen poistamista saattaa olla vaikeaa jäljittää mihinkään käyttäjien ulkopuoliseen toimintaan. RC-kriteeri saa arvon X, koska muutoin kuvaukseen sopiva U laskisi jälleen uhka-arvion vakavuutta. Temporal Scoreksi muodostuu näin ollen 7,2 (High).

Kun tarkastellaan prikaatin kokoista, suorituskyvyiltään sitäkin tehokkaampaa joukkoa, ovat käskyt ja suunnitelmat usein sisällöltään laajoja ja paljon yksityiskohtia sisältäviä. Vaikka muutoin sotilaskäskyt saattavat olla hyvinkin aikakriittisiä ja menettää suuren osan arvostaan hyökkääjälle, mikäli niitä ei kyetä kaappaamaan ennen niiden toteuttamista, voidaan suurten joukkojen suunnitelmista todennäköisesti kerätä paljon tietoa niiden rakenteesta ja yleisistä toimintamalleista. Näin ollen etenkin suunnitteluun hyödynnettyä dataa ja yleisesti taisteluosaston joukoille jaettavaa tiedostomateriaalia täytyy pyrkiä suojaamaan riittävän tehokkaasti. CR-kriteerin arvoksi tulee H.

Jos oletetaan, että tiedostopalvelimen sisältö on enimmäkseen suunnitelmia ja käskyjä, tai niiden laatimisen tueksi kerättyä materiaalia, niiden sisällöllä voi olla hyvin ratkaiseva merkitys taistelun onnistumisen kannalta. Aiemmin tehtiin oletus, että hyökkääjällä voisi olla ajoittain tilapäinen pääsy haittaohjelmaan sen hallitsemiseksi, mutta pääasiallisesti sen pitäisi toimia autonomisesti kohteessa. Jos muutokset näiden tiedostojen sisältämässä informaatiossa olisivat enimmäkseen sattumanvaraisia, eikä niiden avulla kyettäisi tuottamaan tarkoituksellisesti virheellistä informaatiota taisteluosaston päätöksenteon tueksi, ei niiden sisällön muuttaminen aiheuttaisi peruuttamatonta katastrofia taistelulle. Haitta olisi edelleen olemassa, mutta se olisi luonteeltaan todennäköisesti ennemmin ajallista viivytystä kuin harhaan johtamista. Näin ollen IR-kriteeri saa arvon M.

Tiedostopalvelimen todennäköisen uhkan analyysissa kuvattiin saatavuuden merkitystä koko taisteluosaston taistelua ajatellen, etenkin sen johtamisjärjestelmän osalta. Koska johtamisjärjestelmän siirtokaista on jatkuvasti muutenkin aktiivisessa käytössä viestien, taistelunjohtojärjestelmien, tiedustelutiedon ja muun datan siirrossa, ei olisi suotavaa kuormittaa sitä entisestään pakottamalla tiedonjakoa jatkuvasti useampiin kohteisiin kuin todellinen tarve vaatii. Tämän välttämiseksi olisi äärimmäisen tärkeää, että tiedostopalvelin olisi käytettävissä ja tarvitsijat saisivat sen kautta itselleen kaiken tarvitsemansa tiedon. AR-kriteeri saa tässäkin tapauksessa arvon H. Näin ollen tiedostopalvelimeen kohdistuvan vaarallisimman uhkan Environmental Score on **8,0** (High), ja uhka on todella varteenotettava operatiivisessa suunnittelussa. Kokonaisuus on esitetty alla (Kuva 21), ja sen lisäksi vielä yhteenveto kaikista analyyseista (Kuva 22).

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 Requirement	**CR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Integrity Requirement	**IR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	
Availability Requirement	**AR**	Not Defined (X)	Low (L)	Medium (M)	High (H)	

Kuva 21: Vaarallisin uhka tiedostopalvelinta vastaan.

Uhka	Tulos
Reititin, todennäköinen	5,7 (Medium)
Reititin, vaarallisin	8,0 (High)
Työasema, todennäköinen	2,8 (Low)
Työasema, vaarallisin	7,4 (High)
Tiedostopalvelin, todennäköinen	5,8 (Medium)
Tiedostopalvelin, vaarallisin	8,0 (High)

Kuva 22: Uhka-analyysin yhteenveto.

6. JOHTOPÄÄTÖKSET

6.1. Yleistä

Nykyaikainen taisteluosasto on organisaationa haastava kokonaisuus hallita. Sen organisaatio voi olla kiinteästi määritelty vastaamaan sotilasorganisaation omaa näkemystä toimivasta taistelevasta joukosta, tai se voi olla yleinen konsepti, joka rakentuu joka kerralla erilaiseksi vallitsevan tilanteen mukaan. Se voi olla pataljoonan tai prikaatin pohjalle rakennettu, mutta pääasiallinen ero tavanomaiseen taistelevaan yksikköön on lisätty tulivoima sekä muiden aselajien tuomat mahdollisuudet monimuotoiseen käyttöön.

Näin laajan organisaation johtaminen on monimuotoinen prosessi, jonka onnistumiseksi vaaditaan valtava määrä informaatiota ja sen hallinnoimiseksi ja prosessoimiseksi riittävä määrä erilaisia tietojärjestelmiä. Taisteluosaston esikunnan tulee olla riittävän runsaasti miehitetty, ja siellä tulee olla osaamista kaikilta taistelun edellyttämiltä osa-alueilta ja riittävän syvä ymmärrys taistelun kaikilta eri johtamistasoilta.

Johtamisjärjestelmä rakentuu siten, että taisteluosaston alueella on käytössä MANET-verkko paikallaan oleville sekä liikkuville joukoille, ja ainakin tärkeimmät esikunnat on liitetty johonkin ylempään johtoportaaseen ja mahdollisuuksien mukaan kiinteään verkkoinfrastruktuuriin riittävän tiedonsiirtokapasiteetin takaamiseksi. Verkkorakenne tullee olemaan meshtyyppinen riittävän kattavuuden takaamiseksi, sekä riittävän runsaan reittien määrän yksittäisten solmujen ollessa poissa käytöstä taistelun tai olosuhteiden takia.

Taisteluosaston laitteistoon on tallennettuna ja niiden lävitse liikkuu paljon arkaluontoista tietoa, kuten suunnitelmia ja käskyjä, tilannekuvaa, tiedustelutietoa tai tulikomentoja. Näiden tietojen joutuminen vastustajan haltuun, tai niiden sisällön muuttaminen saattaisi aiheuttaa tuhoisia vaikutuksia taisteluosaston toiminnalle.

Kaiken kaikkiaan tämänhetkisestä kyberuhkien tilasta voidaan todeta päällimmäisenä vain se, että uhkaympäristö on äärimmäisen monipuolinen, ja uhkatyyppien määrä miltei rajaton. Vaikka maailmanlaajuisesti uhkien määrä on laskussa, se ei suinkaan tarkoita, että uhka olisi jollain tavalla pienempi kuin aiempina vuosina. Uhkat ovat siirtyneet yksittäisten ihmisten kiusanteosta jatkuvasti monimuotoisempiin, laajamittaisempiin ja uhrin kannalta haitallisempiin, ja niistä on yhä useammin löydettävissä valtiollinen tai valtion tukema toimija, jolla on käytössään massiiviset resurssit verrattuna yksittäisen henkilön tuottamaan haittaohjelmaan.

Hyökkäysten perustyypit ovat ajan saatossa säilyneet samoina, mutta niiden käyttö on painottunut hieman eri tavalla. Etenkin virukset ovat pääsääntöisesti todellisuudessa historiallisia tapauksia, vaikka niistä puhutaankin usein yleisinä tietoturvauhkina. Sen sijaan troijalaiset, madot ja erilaiset rootkitit ovat hyvin yleisiä nykyaikana, ja niiden toiminnallisuuksia on kehitetty jatkuvasti vastauksena kehittyville tietoturvaohjelmistoille.

APT-ryhmittymät ovat jatkuva uhka valtiollisia toimijoita ja suuryrityksiä kohtaan, ja niiden toiminta tuleekin olemaan todennäköisesti merkittävin uhka myös sotilasorganisaatioita kohtaan kaikissa muissa tapauksissa, kuin taistelun aikaisissa, ilman pitkäaikaista strategista suunnittelua vaatineissa hyökkäyksissä. Niitä on maailmalla useita aktiivisia, ja tällä hetkellä esimerkiksi Kasperskyn Global Research and Analysis Team seuraa yli 100 eri APT-ryhmittymää tai -operaatiota ympäri maailman[56]. Niiden tuottamat uhkat kehittyvät jatkuvasti, ja mikäli jokin uhka suljetaan pois erilaisin tietoturvatoimenpitein, ryhmittymä etsii uuden tavan murtaa järjestelmä, eikä luovuta ennen kuin se saavuttaa haluamansa.

Kun tietoturvan taso on kehittynyt, uudet uhkatyypit nousevat vaarallisemmiksi kuin perinteiset. Tulevan vuoden odotukset vaikuttavat siltä, että APT-ryhmittymät jatkavat toimintaa vähintään samalla aktiivisuudella kuin tähänkin asti. Sotilasympäristöön vaikuttavia uhkia tulevat olemaan etenkin tuotantoketjuun vaikuttavat hyökkäykset, sillä tämän kaltaisilla hyökkäyksillä kyetään monessa tapauksessa ohittamaan sotilasorganisaatioiden äärimmäisen tiukat tietoturvamenetelmät, koska ohjelmistojen toimittajat on turvallisuusauditoitu ja niihin luotetaan, eikä haitallisia koodin osia välttämättä huomaa vertailematta lopputuotteen lähdekoodia toimittajan omaan. Etenkin, mikäli kyberhyökkäysten toteuttajat kykenevät hyödyntämään tehokkaasti UEFI-hyökkäyksiä, ei organisaatiolla ole välttämättä kykyä edes havaita haittaohjelmia laitteillaan, mikäli ne eivät yritä muodostaa yhteyksiä hallintapalvelimiin.

Taisteluosaston laitteisto on erittäin monimuotoinen, ja siihen kohdistuu paljon erilaisia uhkia eri suunnista. Uhkia analysoitaessa eri laitteiden välillä oli havaittavissa selkeästi yhtäläisyyksiä monilta osin, mutta etenkin todennäköisten uhkien tapauksessa oli jokseenkin merkittäviä eroja uhka-arvioiden lopputuloksissa.

Selkeästi pienimmäksi uhkaksi tässä tutkimuksessa osoittautui todennäköinen uhkakuva työasemaa vastaan. Sen arvoksi muodostui 2,8, joka on selkeästi vähemmän kuin seuraavaksi vaarallisimmalla uhkakuvalla. Vaikka työasema on ohjelmistoltaan varmasti äärimmäisen kiinnostava potentiaaliselle hyökkääjälle, sen sijainti taisteluosaston verkkotopologiassa aiheuttaa väistämättä haasteita tehokkaan hyökkäyksen onnistumiselle. Koska työasemat ovat käytännössä aina verkon kauimmassa reunassa potentiaalisista hyökkäysvektoreista, niihin on vaikeaa pyrkiä vaikuttamaan ilman erittäin monipuolista ja edistynyttä hyökkäystä. Tätä vaikeuttaa entisestään kilpajuoksu hyökkäyksen kehitystyön ja työaseman järjestelmäpäivitysten välillä, sillä edistynytkin uhka saattaa olla ominaisuuksiltaan käyttökelvoton soveltuvan turvallisuuspäivityksen jälkeen. Vastaavasti verkon ulkoreunalla sijaitseminen vaikeuttaa myös tietojen varastamista mihinkään suuntaan, jolloin suurin vaikutus olisi lähinnä käytön estäminen tilapäisesti.

Vaarallisimman uhkan osalta sekä reitittimeen että tiedostopalvelimeen suuntautuvat vaarallisimmat uhkakuvat päätyivät tasoihin, pisteisiin 8,0. Vaikka laitteet ovat perusperiaatteeltaan täysin erilaiset kaikin puolin, niillä on paljon yhtäläisiä haavoittuvuuden ilmentymiä. Molemmilta on miltei saumaton pääsy työasemiin, niiden kautta tapahtuu koko taisteluosaston verkon kattavaa liikennettä ja ne toimivat omanlaisinaan tietoliikennesolmuina, vaikka reititin on taisteluosaston verkon keskellä ja tiedostopalvelin mahdollisesti jopa fyysisesti täysin irrallisena ja loogisesti verkon reunalla. Molemmissa tapauksissa pystytään pahimmillaan häiritsemään taisteluosaston johtamista ja päätöksentekoprosessia todella tehokkaasti, mikä voi johtaa taistelun täydelliseen epäonnistumiseen, jos kyberhyökkäykseen yhdistetään muita sotatoimia.

Yksi yhteinen, kriittinen ominaisuus esiintyi kaikissa vaarallisinta uhkaa käsittelevissä analyyseissa – kaikissa oli olennaisena tekijänä se, että hyökkäys ei tule kohdistumaan vain yhtä laitetta vastaan. Vaikka jokin haavoittuvuus esiintyisi ensimmäisenä kohteena olevassa laitteessa, lopullinen ja potentiaalisesti merkittävin vaikutus saattaa syntyä jossain muualla. Etenkin työaseman ja tiedostopalvelimen tapauksessa mahdollisuus levitä reitittimeen kasvattaa välittömästi uhkan vaarallisuutta ja muuttaa sen luonnetta selkeästi uhkaavammaksi. Reitittimessä taas tämä sama uhka saattaa johtaa nopeasti koko taisteluosaston verkkoon leviämisen, joka vuorostaan tekee uhkan poistamisesta ja tilanteen normalisoinnista miltei mahdotonta missään realistisessa aikaikkunassa. Tämä on selkeästi yksi vaarallisimmista ja vaikeimmista aspekteista suunniteltaessa suojaustoimenpiteitä kyberhyökkäyksiä vastaan, koska yksittäistä komponenttia tai laitetta vastaan suunnattu uhka on paljon yksinkertaisempaa puhdistaa järjestelmästä tai ainakin vähentää sen vaikutuksia.

Taisteluosaston johtamisjärjestelmä tarjoaa valtavan määrän erilaisia hyökkäysvektoreita potentiaaliselle hyökkääjälle. Kun käytössä on erilaisia radio-, satelliitti- ja kaapeliyhteyksiä eri taajuusalueilla ja laitteistoilla, olisivat mahdollisuudet hyökkäyksen toteuttamiselle käytännössä rajattomat sähkömagneettisen spektrin, ja etenkin sen aiheuttamien kantamarajoitteiden puitteissa. Yksi, selkeästi myös analyyseissa esiin noussut vaarallisimmista riskeistä tulee kuitenkin hyökkäyksissä tuotantoketjuun. Hyökkääjällä on mahdollisuus vaikuttaa haluamaansa hyökkäyskohteeseen periaatteessa missä tahansa tuotantoketjun vaiheessa, oli kyseessä sitten ohjelmistokehitys tai laitteiden valmistus, mikäli sillä on pääsy edes jossain vaiheessa tähän ketjuun.

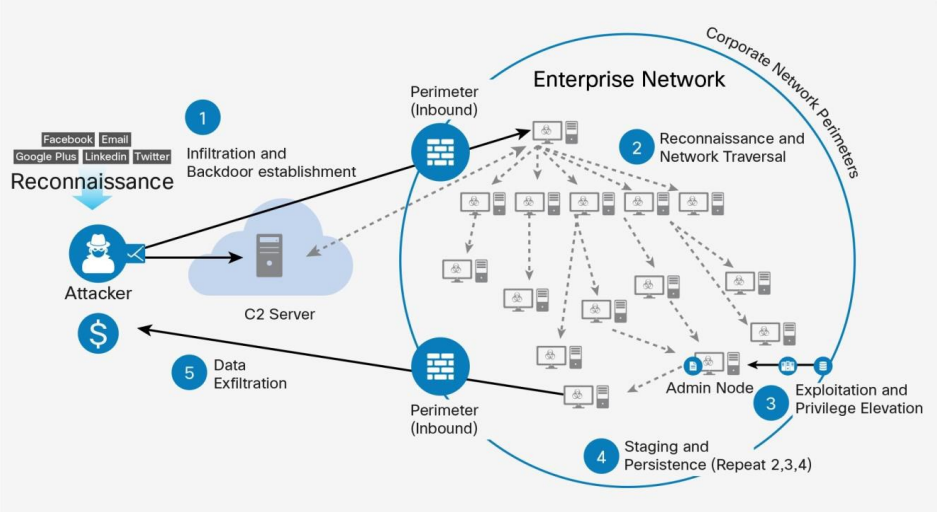
Suuren haasteen tuotteen loppukäyttäjälle aiheuttaa aina se, että periaatteessa jokaisella valmistajalla pitäisi olla riittävät turvatoimet takaamaan asevoimien turvallisuusvaatimukset täyttävä tuotanto täydellisen tietoturvan varmistamiseksi, mutta kaikilla yrityksillä ei varmasti ole tähän resursseja samanlaisessa mittakaavassa. Periaatteessa kuka tahansa yksittäinen henkilö missä tahansa tuotantovaiheessa, tai jopa loppukäyttäjän edustaja, pystyvät vaikuttamaan omalla toiminnallaan siihen, että toimitetussa lopputuotteessa on haittaohjelma sisällään jo ennen taisteluosaston ensimmäiseen tehtävään siirtymistä. Tällaisen uhkan olemassaoloa on mahdoton eliminoida kokonaan, koska fyysinen pääsy laitteeseen pystyy miltei aina takaamaan hyvin suunnitellun ja toteutetun hyökkäyksen onnistumisen.

Asevoimien henkilöstön toteuttamiin sisäisiin hyökkäyksiin on liki mahdotonta vaikuttaa, mutta tuotantoketjun eri vaiheissa potentiaalisesti järjestelmään syötetyn haittaohjelman havaitseminen olisi mahdollista toteuttaa riittävän kattavalla testausympäristöllä. Asevoimilla tulisikin olla käytössään kaikista muista verkoista irrallinen, oman verkkonsa muodostava testausympäristö, jonka verkkoliikennettä ja ohjelmistojen toimintaa kyetään tarkkailemaan kattavasti mahdollisten poikkeamien varalta. Näin pystyttäisiin valtaosassa tapauksia estämään hyökkäys ennen sen pääsyä käytössä olevien joukkojen järjestelmiin. Tämä vaatii verrattain suuren investoinnin kalustoon, tiloihin ja henkilöstöön, mutta mikäli sen avulla kyetään estämään potentiaalisesti katastrofaaliset seuraamukset taisteluosaston toiminnalle, se pitäisi toteuttaa.

Taisteluosaston järjestelmissä liikkuva informaatio on luonteeltaan jopa erittäin arkaluontoista, ja sen sisällön muutokset saattaisivat aiheuttaa merkittävää haittaa taistelun kokonaisuuden kannalta. Johtamisprosessin luonteesta ja tiedon jatkuvasta arkistoinnista johtuen suuri osa järjestelmien sisältämästä informaatiosta on luonteeltaan vanhentunutta, pois lukien tilannekuva ja reaaliaikaiset johtamisyhteydet. Johtamisen peruspilari on tuoreen, sisällöltään oikean tilannekuvan hyödyntäminen päätöksenteossa, ja mikäli tätä tietoa ei ole saatavilla, toiminta hidastuu ja virheellisten päätösten todennäköisyys kasvaa. Tästä johtuen, ehkä jopa hieman yllättäen tietoturvan osa-alueista merkittävämmäksi näyttäisi muodostuvan saatavuus.

Yksi merkittävä tekijä saatavuuden merkityksen kasvattamisessa on myös MANET-verkkojen jatkuvasti muuttuva luonne sekä sotilaallisten joukkojen käytössä olevien runkoverkkojen turvatoimenpiteet. Vaikka kohteessa oleva haittaohjelma kykenisi toiminnoillaan varastamaan kaiken saatavilla olevan informaation, siitä ei ole mitään hyötyä, ellei sitä saada toimitettua hyökkääjän haltuun. Saatavuuden menetys on kuitenkin täysin mahdollista saavuttaa kontrolloimatta hyökkäystä reaaliaikaisesti, tai ilman minkäänlaista kykyä saada yhteyksiä ulkoisiin verkkoihin. Reititinten rooli tietoliikenteen solmuina tekee niistä haavoittuvan ja kriittisen kohteen, koska pahimmillaan yhdenkin laitteen saatavuuden menetys saattaa tuottaa laajamittaisen saatavuuden menetyksen taisteluosaston sisällä. Mesh-verkko tarjoaa joissain tapauksissa hieman sietokykyä tätä vastaan, mutta vain siinä tapauksessa, että saastunut reititin kyetään väistämään reitityksessä.

Suurin osa isoista haasteista ja ongelmista tuntuisi perustuvan yhteen yksinkertaiseen faktaan. Järjestelmät rakennetaan pitkälti vahvoiksi sulkemaan hyökkääjät ulkopuolelle, mutta mikäli ulkokuori on murrettu, sisällä on helppo liikkua uusiin kohteisiin ja tehdä tarvittavaa tuhoa (vrt. esim. OLSR-protokolla). Tätä kutsutaan eggshell-periaatteeksi, munan kuoreksi, jossa ulkoiset puolustukset on toteutettu hyvinkin tehokkaasti, ja niihin luotetaan niin paljon, että sisällä olevia osia ei tarvitse erikseen suojata enää yhtä kattavasti[9][64]. Perusperiaate tällaisesta verkosta on esitetty alla (Kuva 23). Tällaisesta periaatteesta tulisi päästä tehokkaasti irti, siirtyen siihen, että myös verkon sisällä olisi riittävästi passiivisia ja aktiivisia suojaustoimenpiteitä hyökkäysten estämiseksi tai niiden vaikutusten minimoimiseksi. Siirtokaista säilyy tässä haasteena, mutta taistelutoiminnassa tulisi pyrkiä löytämään tasapaino johtamisen kannalta tarpeellisen tiedonsiirron ja teknologian mahdollistamien kyvykkyyksien välillä. Uudet teknologiat mahdollistavat jatkuvasti paremman informaation liikuttamisen ja keräämisen, mutta jossain vaiheessa esikunnat ja komentajat eivät enää pysty käsittelemään kaikkea tarjolla olevaa tietoa ilman merkittäviä muutoksia organisaatiorakenteessa tai taisteluiden johtamisen periaatteessa, joten todennäköisesti tällaiseen tilanteeseen voidaan päästä tulevaisuudessa.



Kuva 23: Eggshell-periaate verkon suojauksessa.[64]

6.2. Tulosten luotettavuus ja validiteetti

Tutkimuksen tarkoituksena oli tarkastella, minkälaisia kyberuhkia taisteluosastoa vastaan kohdistuu, ja tarkentavina alakysymyksinä oli tarkoituksena tarkastella mahdollisia eri hyökkäysvektoreita sekä eri uhkatyyppien vaarallisuutta taisteluosastolle. Toinen pääluku tuo esiin paljon mahdollisia uhkavektoreita taisteluosastossa, mutta niiden varsinainen tarkastelu analyysivaiheessa jää melko vähäiseksi lukuun ottamatta mahdollista runkoyhteyden ja langattoman lähiverkon hyödyntämistä hyökkäyksessä. Analyysiin olisi voinut pyrkiä tuomaan paremmin ilmi erilaisten radiolaitteistojen ja satelliittien tarjoamat mahdollisuudet hyökkäysvektoreina, joskin tarkastelun olisi pitänyt jäädä melko pintapuoliseksi, koska muuten työ olisi venynyt tarpeettoman pitkäksi.

Erilaisten uhkatyyppien vaarallisuutta on arvioitu verrattain kattavasti analyysiluvussa. Uhkia ei ole luokiteltu kovinkaan yksityiskohtaisiin lokeroihin sen mukaan ovatko ne haittaohjelmia, reaaliaikaista manipulointia verkon yli tai jotain muuta, vaan tarkastelussa on keskitytty niiden potentiaalisiin ominaisuuksiin ja vaikutuksiin. Näitä vaikutuksia on kuitenkin tarkasteltu useasta eri näkökulmasta ja niistä on saatu vertailukelpoiset uhka-arvot, jotka on esitetty kuvassa 22. Kolmea eri kohdelaitetta, ja kaikkiaan kuutta eri skenaariota vertailemalla saa jo kohtalaisen käsityksen eri uhkien vaarallisuudesta, ja ennen kaikkea niiden suhteellisesta vaarallisuudesta toisiinsa nähden.

Analyysimenetelmänä CVSS-arviointikriteeristö on sinänsä varsin tehokas työkalu uhkien luokitteluun, mutta väistämättä yksittäisen henkilön tekemät tulkinnat eri uhkatasojen välisissä eroissa ovat joiltain osin subjektiivisia. Myös uhkatyyppien valinnassa ja niiden ominaisuuksien päättämisessä on sama tilanne. Vaarallisimpien uhkien tapauksessa valinta on helpompaa, koska on tarkoitus pyrkiä realistisessa viitekehyksessä luomaan maksimaalista tuhoa aiheuttava uhkakuva, mutta todennäköistä uhkaa arvioitaessa on jouduttu pohjaamaan näkemyksiä tutkijan aiempaan tietoon ja teoriaosiossa esitettyihin mahdollisuuksiin. Useamman henkilön muodostama asiantuntijaryhmä saattaisi saada aikaan monitahoisemman analyysin, mutta toisaalta se voisi myös aiheuttaa täysin vastakkaisia näkemyksiä etenkin arvioitaessa tietoturvan eri osa-alueille asetettuja vaatimuksia.

Tieteen näkökulmasta tämä tutkimus ei suoranaisesti tuota mitään kovinkaan merkittävää tai uutta kontribuutiota, vaan toimii ennemmin kokoavana tarkasteluna kahden eri ilmiön yhteyksistä, joita on tutkittu melko vähän tähän mennessä. Viemällä tarkastelun johonkin yksittäiseen laitteeseen tai teknologiaan ja sitä kohtaan suuntautuviin uhkiin voitaisiin mennä sellaisiin yksityiskohtiin, että tutkimuksessa voitaisiin analysoida haavoittuvuuksia ja niiltä suojautumista hieman tarkemmin. Tämä tutkimus tarjoaa kuitenkin yhdenlaisen lähestymistavan uhka-analyysille ja pohjan potentiaalisten kyberuhkien hahmottamiselle osana taisteluosaston suunnitteluprosessia, jossa sitä ei välttämättä vielä nykypäivänä huomioida riittävän hyvin. Mitä modernimmaksi johtamisjärjestelmät muuttuvat, sitä relevantimmaksi aihe muuttuu, ja silloin jokaisen taisteluosaston käytössä tulee olla jonkinlainen malli uhkien arvioimiselle.

6.3. Aiheita jatkotutkimuksille

Kuten todettua, tämä tutkimus oli laajahko katsaus suuren sotilasjoukon eri teknologioihin, niiden haavoittuvuuksiin ja vaikutukseen taisteluosaston taistelulle. Tältä pohjalta on mahdollista viedä tarkastelu paljon pidemmälle yksityiskohtiin tai tarkastella joitain taisteluosaston osa-alueita entistä tarkemmin. Erityisen hyödyllistä olisi tarkastella tätä aihealuetta suomalaisten joukkotyyppien osalta. Ainakin seuraavia aiheita olisi syytä pyrkiä tutkimaan tulevaisuudessa:

- Taisteluosaston kyberuhkat Suomen toimintaympäristössä
- Taistelijan sulautetut järjestelmät tulevaisuudessa ja niihin kohdistuva kyberuhka
- M18-järjestelmään kohdistuva kyberuhka
- Ilmavoimien taistelutukikohdan kyberuhka

Tutkittavia aiheita olisi tällä hetkellä lähes loputtomasti, koska aiheesta on tehty hyvin vähän tutkimuksia Puolustusvoimien käyttöön toistaiseksi. Uudet teknologiat ja esineiden internetin yleistyminen myös sotilaskäytössä tuottavat jatkuvasti lisää tutkittavia aiheita, joita tulisi tutkia niin sotataidon, kuin sotatekniikan näkökulmasta Maanpuolustuskorkeakoululla. Yksi tutkittava aihe olisi myös hyökkäyksellisten kybersuorituskykyjen käyttö tai aktiivinen kyberpuolustus Puolustusvoimien kontekstissa, niin teknisestä kuin taktisesta näkökulmasta.

LÄHTEET

[1] *2018 Security Outlook: Potential Risks and Threats.* 2016. Canadian Security Intelligence Service.

[2] *2018 Thales Data Threat Report: Trends in Encryption and Data Security Global Edition*.

[3] Adjih, C. et al. (2015). *Securing the OLSR protocol.* INRIA Rocquencourt, Projet Hipercom. Domaine de Voluceau, Ranska.

[4] *Advanced Threat Protection with Dell SecureWorks Security Services* (https://www.secureworks.com/~/media/Files/US/Solution%20Briefs/DellSecureWorksNCO346NAdvancedThreatProtection.ashx)

[5] Agre, J. et al. (2013). *Commercial Technology at the Tactical Edge.* Institute for Defense Analyses. Alexandria, Virginia, USA.

[6] Antonakakis, M. et al. (2016). *Understanding the Mirai Botnet.* (https://static.googleusercontent.com/media/research.google.com/fi//pubs/archive/46301.pdf, viitattu 15.11.2017)

[7] Asman, B. et al. (2011). *Methodology for Analyzing the Compromise of a Deployed Tactical Network.* Proceedings of the 2011 IEEE Systems and Information Engineering Design Symposium, University of Virginia. Charlottesville, VA, USA,

[8] *ATTACK LANDSCAPE H1 2017* (http://images.news.f-secure.com/Web/FSecure/%7B1ddd2e1d-2936-461d-92f9-6232caf2a625%7D_F-Secure_Attack_Landscape_H1_2017_Report_A.pdf?_ga=2.8121394.1885456894.1504541917-2011664237.1504541917)

[9] Attema, T., Sangers, A. & Raspe, S. (2017). *Internal Network Monitoring for Targeted Attack Detection.* Innovating in Cyber Security – Shared Research 2017. TNO.

[10] Bani-Hani, R. & Al-Ali, Z. (2013). *SYN Flooding Attacks and Countermeasures*. Jordan University of Science and Technology, Dept. of Network Engineering and Security. Irbid, Jordan.

[11] BitDefender: *Conficker – One Year After* (http://www.bitdefender.com/files/Main/file/Conficker_-_One_Year_After_-_Whitepaper.pdf, viitattu 28.2.2018)

[12] Bogdanoski, M. & Shuminoski, T. & Risteski, A. (2013). *Analysis of the SYN Flood DoS Attack*. I. J. Computer Network and Information Security, 2013, 8, 1-11.

[13] Bowman, E. & Zimmerman, R. (2010). *Measuring Human Performance in a Mobile Ad Hoc Network (MANET).* ITEA Journal 2010. Army Research Lab, Computational and Information Sciences Directorate. Maryland, USA.

[14] *Common Vulnerability Scoring System v3.0: Specification Document* (v1.8)

[15] *Concept of Operations (CONOPS) for Warfighter Information Network-Tactical (WIN-T).* (2014). Cyber Center of Excellence. Fort Gordon, Georgia, USA.

[16] *Cyber Security: Trends from 2017 and Predictions for 2018.* 2018. Concierge Security Report, Volume 4, Issue 1. Mindstar Security & Profiling, Virginia, USA.

[17] *CyberArk Global Advanced Threat Landscape Report 2018: The cyber security inertia putting organizations at risk*.

[18] Dennis, F. (2014). *Brigade Combat Team the World's Police: Understanding the United States Army Brigade Combat Team's Role in Developing Foreign Police.* United States Army Command and General Staff College. Fort Leavenworth, Kansas, USA.

[19] Dorri, A., Vaseghi, S. & Gharib, O. (2016). *DEBH: Detecting and Eliminating Black Holes in Mobile Ad Hoc Network.* Wireless Networks, huhtikuu 2017.

[20] Etaher, N., Weir, G. & Alazab, M. (2015). *From ZeuS to Zitmo: Trends in Banking Malware.* Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015. IEEE, Piscataway, NJ, USA.

[21] Falliere, N. & Chien, E. (2009). *Zeus: King of the Bots.* Symantec Security Response, California, USA.

[22] Fitzgibbon, N. & Wood, M. 2009. *Conficker.C A Technical Analysis.* Sophoslabs, Sophos Inc.

[23] *FM 3-0: Operations*. (2017). Headquarters, Department of the Army. Washington, DC, USA.

[24] *FM 3-96: Brigade Combat Team*. (2015). Headquarters, Department of the Army. Washington, DC, USA.

[25] *FM 6-0: Commander and Staff Organization and Operations*. (2014). Headquarters, Department of the Army. Washington, DC, USA.

[26] Fox, A. & Rossow, A. (2017). *Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo-Ukrainian War.* The Institute of Land Warfare. Arlington, Virginia, USA.

[27] General Dynamics. (2007). *CWID Update, Summer 2007.* (https://www.generaldynamics.uk.com/wp-content/uploads/2016/08/CWID-Update-web-20-June.pdf, viitattu 18.03.2018).

[28] General Dynamics. (2016). *Warfighter Information Network-Tactical Commander's Handbook.* Version 2.0.

[29] Giuliani, M. *ZeroAccess – an advanced kernel mode rootkit.* Prevx Advanced Malware Research Team.

[30] Gkioulos, V. (2018). *Securing Tactical Service Oriented Architectures.* Väitöskirja, Norwegian University of Science and Technology.

[31] Gunther, M. (2012). *Auftragstaktik: The Basis for Modern Military Command?* School of Advanced Military Studies, United States Army Command and General Staff College. Fort Leavenworth, Kansas, USA.

[32] Harris, S. (2013). *CISSP All-in-One Exam Guide.* McGraw-Hill Education. (6. painos)

[33] Hittel, S. & Zhou, R. (2012). *Trojan.ZeroAccess Infection Analysis.* Symantec Security Response, California, USA.

[34] House, J. (1984). *Toward Combined Arms Warfare: A Survey of 20th-Century Tactics, Doctrine and Organization.* U.S. Army Command and General Staff College. Fort Leavenworth, Kansas, USA.

[35] http://corewar.co.uk/creeper.htm (viitattu 27.2.2017)

[36] http://www.zdnet.com/pictures/ten-computer-viruses-that-changed-the-world/4/ (viitattu 03.03.2018).

[37] https://rusi-ns.ca/battle-group/ (viitattu 16.03.2018).

[38] https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/

[39] https://securelist.com/the-epic-turla-operation/65545/

[40] https://tools.ietf.org/html/rfc3626 (viitattu 18.03.2018).

[41] https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (viitattu 04.03.2018).

[42] https://www.av-test.org/en/statistics/malware/

[43] https://www.bittium.com/download/781/bittium_tactical_wireless_ip_network/pdf (viitattu 18.03.2018).

[44] https://www.fireeye.com/current-threats/apt-groups.html (viitattu 12.03.2018).

[45] https://www.first.org/cvss/calculator/3.0

[46] https://www.f-secure.com/v-descs/melissa.shtml (viitattu 03.03.2018).

[47] https://www.generaldynamics.uk.com/solutions/c4i-systems/bowman/ (viitattu 17.03.2018).

[48] https://www.juniper.net/documentation/en_US/junos/topics/concept/denial-of-service-network-syn-flood-attack-understanding.html (viitattu 01.03.2018).

[49] https://www.kaspersky.com/resource-center/threats/trojans (viitattu 04.03.2018).

[50] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Virus%3AW97M%2FMelissa.A (viitattu 03.03.2018).

[51] https://www.nao.org.uk/report/ministry-of-defence-delivering-digital-tactical-communications-through-the-bowman-cip-programme/ (viitattu 17.03.2018).

[52] https://www.sans.org/security-resources/malwarefaq/conficker-worm (viitattu 28.2.2018)

[53] https://www.symantec.com/security_response/writeup.jsp?docid=2000-122113-1425-99&tabid=2 (viitattu 03.03.2018).

[54] *International Security and Estonia 2018.* 2018. Välisluureamet, Viro.

[55] *Kaspersky Security Bulletin 2016* (https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf)

[56] *Kaspersky Security Bulletin: Kaspersky Lab Threat Predictions for 2018.* 2017. Version 1.1.

[57] Kelly, J. (2011). *Brigade Combat Teams: Designed to Design*. School of Advanced Military Studies, United States Army Command and General Staff College. Fort Leavenworth, Kansas, USA.

[58] Lappalainen, Esa & Jormakka, Jorma. *Tekniset tutkimusmenetelmät Maanpuolustus-korkeakoulussa*. MPKK Tekniikan laitos. Julkaisusarja 5 (2004).

[59] Leder, F. & Werner, T. 2009. *Know Your Enemy: Containing Conficker.* (https://www.honeynet.org/files/KYE-Conficker.pdf, viitattu 25.2.2018)

[60] Lemon, J. (2002). *Resisting SYN flood DoS attacks with a SYN cache.* Proceedings of the BSDCon 2002 Conference. San Francisco, California, USA.

[61] *Looking Ahead: Cyber Security in 2018*. 2017. FireEye, Inc. California, USA.

[62] Marttinen, T. (2010). *Mekanisoidun pataljoonan 2020 operatiiviset suorituskykyvaatimukset.* EUK-tutkielma, Maanpuolustuskorkeakoulu.

[63] McClure, S. & Scambray, J. & Kurtz, G. (1999). *Hacking Exposed: Network Security Secrets and Solutions*. Berkeley, California: Osborne/McGraw-Hill.

[64] *Network as a Security Sensor: Threat Defense with Full NetFlow.* (2016). Cisco White Paper.

[65] Neville, A. & Gibb, R. (2013). *ZeroAccess Indepth.* Symantec Security Response, California, USA.

[66] *Open Information Security Management Maturity Model (O-ISM3)*, Reference C102, US ISBN 1931624860, helmikuu 2011

[67] Pasanen, E. (2015). *Tietoverkkovaikuttamisen suorituskyvyn kuvaus (DOTMLPFIi)*. Pro Gradu -tutkielma, Maanpuolustuskorkeakoulu.

[68] Peacock, B. (2007). *Connecting the Edge: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare.* Blue Horizons Paper, Center for Strategy and Technology, Air War College.

[69] Seaman, C. (2016). *Threat Advisory: Mirai Botnet*. Akamai. (https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-mirai-botnet-threat-advisory.pdf, viitattu 15.11.2017)

[70] *Senate Intelligence Committee: Russia and 2016 Election.* 2017. FireEye, Inc. California, USA.

[71] Sinanović, H. & Mrdovic, S. (2017). *Analysis of Mirai Malicious Software*. Faculty of Electrical Engineering, University of Sarajevo.

[72] *Technical White Paper: Reversal and Analysis of Zeus and SpyEye Banking Trojans*. 2012. IOActive, Inc. Seattle, WA, USA.

[73] *The Army's Bandwidth Bottleneck.* (2003). The Congress of the United States.

[74] Tuomi, J. & Sarajärvi, A. (2009). *Laadullinen tutkimus ja sisällönanalyysi.* Helsinki: Tammi. (6. painos)

[75] Valtioneuvoston periaatepäätös, *Suomen Kyberturvallisuusstrategia*. Helsinki: Forssa print 2013. 44s. ISBN: 978-951-25-2434-1

[76] Villalobos, M. (2016). *Web 2.0 Systems in the Brigade Combat Team as an Enabler of Mission Command: A Dialectic in Information Discourse.* United States Army Command and General Staff College. Fort Leavenworth, Kansas, USA.

[77] Wu, C. (2012). *Introduction to Computer Networks and Cybersecurity.* Florida, USA: Taylor & Francis Group, LLC.

[78] Wyke, J. (2011). *What is Zeus?* A Sophos Labs technical paper. Oxford, Iso-Britannia.

LIITTEET

LIITELUETTELO

LIITE 1: Prikaatin taisteluosaston (BCT) esikunnan henkilöstö

Grade / Rank	Position Code	Position Code Title	Authorized Quantity
O6 / COL	02C00	INFANTRY/ARMOR/FIELD	1
O5 / LTC	11A00	INFANTRY	1
O4 / MAJ	11A00	INFANTRY	1
O4 / MAJ	12A00	ENGINEER	1
O4 / MAJ	15B00	AVIATION COMBINED ARM	1
O4 / MAJ	25A00	SIGNAL, GENERAL	1
O4 / MAJ	27A00	JUDGE ADVOCATE GENERAL	1
O4 / MAJ	30A00	INFORMATION OPERATION	1
O4 / MAJ	35D00	ALL SOURCE INTEL	1
O4 / MAJ	42H00	SENIOR HUMAN RESOURCE	1
O4 / MAJ	46A00	PUBLIC AFFAIRS, GENERAL	1
O4 / MAJ	56A00	CHAPLAIN	1
O4 / MAJ	62B00	FIELD SURGEON	1
O4 / MAJ	90A00	LOGISTICS	1
O3 / CPT	01A00	OFFICER GENERALIST	1
O3 / CPT	02A00	COMBAT ARMS GENERALIST	1
O3 / CPT	11A00	INFANTRY	3
O3 / CPT	12A00	ENGINEER	1
O3 / CPT	14A00	AIR DEFENSE ARTILLERY	1
O3 / CPT	15B00	AVIATION COMBINED ARM	1
O3 / CPT	27A00	JUDGE ADVOCATE GENERAL	2
O3 / CPT	29A00	ELECTRONIC WARFARE OFF	1
O3 / CPT	31A00	MILITARY POLICE	1
O3 / CPT	35D00	ALL SOURCE INTELLIGEN	2
O3 / CPT	35F00	HUMAN INTELLIGENCE	1
O3 / CPT	35G00	SIGNALS INTELLIGENCE	1
O3 / CPT	36A00	FINANCIAL MANAGER	1
O3 / CPT	38A00	CIVIL AFFAIRS	1
O3 / CPT	53A00	INFORMATION SYSTEMS	1
O3 / CPT	57A00	SIMULATIONS OPERATION	1
O3 / CPT	70H67	HEALTH SERVICES PLANS	1
O3 / CPT	74A00	CBRNE	1
O3 / CPT	90A00	LOGISTICS	1
O3 / CPT	90A92	LOGISTICS	1
O2 / LT	02B00	INFANTRY/ARMOR	1
O2 / LT	42B00	HUMAN RESOURCES OFF	1

LIITE 1: Prikaatin taisteluosaston (BCT) esikunnan henkilöstö

Grade / Rank	Position Code	Position Code Title	Authorized Quantity
W4 / CW4	150U0	UNMANNED AIRCRAFT SYS	1
W3 / CW3	153AI	ROTARY WING AVIATOR	1
W3 / CW3	255S0	INFORMATION PROTECTION	1
W2 / CW2	125D0	GEOSPATIAL ENGINEERING	1
W2 / CW2	140A0	COMMAND AND CONTROL	1
W2 / CW2	255A0	INFORMATION SERVICES	1
W2 / CW2	255N0	NETWORK MANAGEMENT TECH	1
W2 / CW2	290A0	ELECTRONIC WARFARE TECH	1
W2 / CW2	350F0	ALL SOURCE INTELLIGENCE	1
W2 / CW2	351M0	HUMAN INTELLIGENCE	1
W2 / CW2	420A0	HUMAN RESOURCES TECH	1
W2 / CW2	882A0	MOBILITY OFFICER	1
W2 / CW2	920A0	PROPERTY ACCOUNTING TECH	1
W2 / CW2	922A0	FOOD SERVICE TECH	1