MAANPUOLUSTUSKORKEAKOULU

SOSIAALISEN MEDIAN MUODOSTAMA UHKA TAISTELUOSASTON OPERAATIOTURVALLISUUDELLE JOUKKOJEN PERUSTAMIS-VAIHEESSA

Kandidaatintutkielma

Kadetti
Aito Paloheimo

Kadettikurssi 98
Johtamisjärjestelmälinja

Maaliskuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Kadettikurssi 98	Maavoimien johtamisjärjestelmälinja
Tekijä Kadetti Aito Paloheimo	
Tutkielman nimi **Sosiaalisen median muodostama uhka taisteluosaston operaatioturvallisuudelle joukkojen perustamisvaiheessa**	
Oppiaine, johon työ liittyy Taktiikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika Maaliskuu 2014	Tekstisivuja 31 Liitesivuja 3

TIIVISTELMÄ

Operaatioturvallisuus (OPTU) nykyajan konseptina on suhteellisen tuore. Aihetta on tutkittu Persianlahdensodan ajoilta asti. Suomen Puolustusvoimat tulkitsee operaatioturvallisuutta yleisesti ottaen samalla tavalla kuin Yhdysvaltojen asevoimat. Sosiaalinen media (SOME) on konseptina myös tuore ilmiö (2007). Sosiaalisen median käyttöaste yhteiskunnassamme on merkittävä. Sosiaalinen media mahdollistaa vaivattoman tiedon jakamisen, joka puolestaan vaikuttaa operaatioturvallisuuteen. Sosiaalista mediaa ja operaatioturvallisuutta on tutkittu laajasti joko yksittäisinä konsepteina tai osana muita kokonaisuuksia. Operaatioturvallisuutta ei ole kuitenkaan käsitelty sosiaalisen median näkökulmasta laajamittaisesti. Suomessa aihealuetta on tarkasteltu rauhanturvaajien toimintaympäristössä ja sen yleiskäyttöä rauhan aikana. Joukkojen perustamisvaihetta ei ole käsitelty. Modernina ilmiönä on syytä ymmärtää sosiaalisen median mahdollistamaa uhkaa taisteluosaston (TSTOS) operaatioturvallisuudelle joukkojen perustamisvaiheessa.

Päätutkimuskysymys on: Millainen uhka sosiaalinen media on taisteluosaston operaatioturvallisuudelle ja miten siltä voidaan suojautua joukkojen perustamisvaiheen aikana? Alakysymykset, jotka tukevat tutkimusta ovat: Mitä operaatioturvallisuus tarkoittaa konseptina? Minkälainen sosiaalinen media on toimintaympäristönä? Miten vastustaja tiedustelee sosiaalisessa mediassa (OSINT)? Minkälaisen vaikutuksen operaatioturvallisuuden puute sosiaalisen median toimintaympäristössä luo taisteluosastolle?

Aineisto koostuu internetlähteistä sekä kirjallisista lähteistä oppaiden, artikkelien ja uutisten muodossa. Johtopäätöksenä on todettavissa, että operaatioturvallisuuden kannalta on syytä kieltää sosiaalisen median käyttöä sekä poistaa sosiaalisen median palveluita mahdollistavat laitteet joukkojen perustamisvaiheessa. Operaatioturvallisuuden laiminlyöminen sosiaalisen median toimintaympäristössä jo rauhanajan koulutuksessa voi johtaa pahimmassa tapauksessa siihen, että joukot on saatettu toimintakyvyttömään tilaan ennen laajamittaista sotaa. Operaatioturvallisuuden tärkeyttä sosiaalisessa mediassa on koulutettava henkilökunnalle ja varusmiehille jo rauhan aikana. Tutkija kehottaa Puolustusvoimia ottamaan tarkemmin kantaa älypuhelimien ja sosiaalisen median käyttöön rauhan- ja joukkojen perustamisvaiheen aikana.

AVAINSANAT
OPSEC, OSINT, OPTU, SOME, TSTOS, JOUKKOJEN PERUSTAMISVAIHE

SOSIAALISEN MEDIAN MUODOSTAMA UHKA TAISTELUOSASTON OPERAATIOTURVALLISUUDELLE JOUKKOJEN PERUSTAMIS-VAIHEESSA

SISÄLLYS

SOSIAALISEN MEDIAN MUODOSTAMA UHKA TAISTELUOSASTON OPERAATIOTURVALLISUUDELLE JOUKKOJEN PERUSTAMIS-VAIHEESSA

1 JOHDANTO

1.1 Aihealueen esittely

Sosiaalinen media (SOME) käsitteenä syntyi vuonna 2007, ja on ollut hyvin keskeinen osa yhteiskuntaa ja sen toimintatapoja 2000-luvun alusta alkaen. Sosiaalinen media käsittää web 2.0- verkkoympäristön (internet), jonka palvelut mahdollistavat esteettömän tiedon jakamisen eri yhteisöissä ja sovelluksissa[1]. Tunnetuimmat ja käytetyimmät yhteisöpalvelut Suomessa ovat esimerkiksi Twitter, Facebook, Youtube, sähköpostipalvelut Gmail ja Hotmail, sekä yleiset keskustelufoorumit kuten Suomi24. Sosiaalisen median kautta mikä tahansa taho pystyy vastaanottamaan ja tuottamaan tietoa. Tämä ilmiö on muodostanut uuden tavan kommunikoida, markkinoida, myydä, tiedottaa sekä vaikuttaa yhteiskuntaan globaalilla tasolla.

Koska sosiaalisesta mediasta on muodostunut vahvasti arkipäiväinen työkalu, ovat sen vaikutukset merkittäviä myös sotilaallisesta näkökulmasta. Suomessa älypuhelimen käyttö (vrt. 2013 n.61 % kun 2012 n. 44 %) tai muun internetpalveluita tarjoavan laitteen kuten tabletin (vrt. 2013 16 % kun 2012 oli 6 %) on kasvanut merkittävästi. Suomessa älypuhelimien kautta sosiaalista mediaa käyttävät jo 45 % väestöstä.[2,3]

Tietoa voidaan helposti ja nopeasti levittää älypuhelimien kautta, jotka mahdollistavat uusia turvallisuusriskejä. Turvallisuusriski sotilaallisesta näkökulmasta voidaan käsittää operaatioturvallisuuden laiminlyöntinä. Taisteluosaston näkökulmasta nämä riskit ovat paikkatietoi-

[1] Kaplan, Andreas M. ja Haenlein, Michael: *Users of the world, unite! The challenges and opportunities of Social Media*, Business Horizons, 2010, ss. 59-68.
[2] TNS Mobile Life Gallup, 2013, http://www.tns-gallup.fi/uutiskirje2013/05/otsikko2, 14.12.2013.

hin, kokoonpanoon, kalustoon, tehtävään ja toimintatapoihin liittyvät asiat, joita ei haluta saattaa vastustajan tietoon.

Tämä tutkielma tarkastelee taisteluosastoa, jossa sosiaalisen median käyttö älypuhelimien välityksellä muodostaa operaatioturvallisuuteen liittyvän uhan joukkojen perustamisvaiheessa, ennen laajamittaista sotaa. Tämä vaihe on kriittisin, sillä infrastruktuurin, viesti- ja sähköverkkojen ollessa vielä toimintakunnossa on riskialttius vastustajan tiedusteluun ja tiedonkeruuseen suurin. Tässä vaiheessa vastustaja suorittaa laajamittaista tiedustelua käyttäen perinteisen tiedustelun lisäksi myös avointen lähteiden tiedustelua sosiaalisessa mediassa. Tietoja voidaan käyttää esimerkiksi johtamiskyvyn lamauttamiseen, disinformaation tuottamiseen, moraalin vaikuttamiseen psykologisten operaatioiden (PSYOPS) kautta, fyysiseen tuhoamiseen tai harhauttamiseen.

Sosiaalisen median vaikutusta Puolustusvoimien toimintaan on tutkittu lähinnä rauhan ajan ympäristössä ja osittain kriisinhallintatehtäviin liittyen. On tärkeää tutkia sosiaalisen median vaikutusta operaatioturvallisuudelle kriisin aikana samalla kun joukkoja perustetaan. Tällöin vihollinen suorittaa psykologista sodankäyntiä sekä avointen lähteiden tiedustelua laajimmillaan. Täten on syytä ymmärtää ns. virtuaaliuhat perinteisten uhkien lisäksi.

Tässä tutkimuksessa käsitellään operaatioturvallisuutta konseptina ja prosessina, esitellään sosiaalisen median nykypäivän toimintaympäristö, havainnoidaan tiedustelumahdollisuuksia sosiaalisessa mediassa avointen lähteiden tiedustelun muodossa, analysoidaan esimerkkitapauksia sosiaalisessa mediassa ja luodaan pohja operaatioturvallisuuden suhteesta sosiaalisen mediaan joukkojen perustamisvaiheessa.

1.2 Aikaisempi tutkimus ja keskeiset käsitteet

Sosiaalista mediaa on tutkittu lähinnä rauhanajan näkökulmasta sekä siviili että sotilaspuolella[4]. Operaatioturvallisuutta on pääsääntöisesti tarkasteltu sodanajan[5] ja kriisinhallintatehtävien näkökulmasta. Operaatioturvallisuus konseptina on syntynyt Yhdysvalloissa, jossa sitä on tutkittu laajemmin jo Persianlahden sodasta asti. Suomen Puolustusvoimat ovat ottaneet kon-

[3] Digitoday: *Älypuhelimet ponnistavat yli haamurajan Suomessa*, 2013, http://www.digitoday.fi/pdf/20136702, 14.12.2013.
[4] Holopainen, Jari: *Sosiaalisen median mahdollisuudet ja riskit puolustusvoimissa*, Esiupseerikurssi 63, Maanpuolustuskorkeakoulu, 2011.
[5] Turunen, Jarkko: *Esikunta- ja viestipataljoonan operaatioturvallisuus*, Esiupseerikurssi 57, Maanpuolustuskorkeakoulu, 2004.

septin käyttöön osaksi operaatiotoimintaa. Yhdistetysti aihetta ei ole juurikaan tutkittu operaatiotaidon ja taktiikan näkökulmasta.

Puolustusvoimissa sosiaalisen median strategiaa on lähinnä kehitetty ja jalostettu rauhanajan toiminnalle varusmiesten SOME strategian muodossa, josta on laadittu asiakirja[6]. Sosiaalisen median strategiaa ei ole selkeästi laadittu kriisin- tai sodanajan toiminnalle. Jari Holopaisen ”Sosiaalisen median mahdollisuudet ja riskit”, Torsti Sirénin ”Strateginen kommunikaatio ja informaatio-operaatiot 2030” sekä Kimmo Pispan ”Psykologiset operaatiot sosiaalisessa mediassa” luovat alustavan käsityksen tutkielmaan liittyvistä yksittäisistä aihealueista, mutta eivät tarjoa kokonaisvaltaista käsitystä sosiaalisen median luomasta uhasta operaatioturvallisuudelle.

Edellä mainitun kahden teeman yhteinen kohtaaminen on osittain uutta ja tuo lisäarvoa operaatioturvallisuuden ja sosiaalisen median ymmärtämiselle. Vaikka operaatioturvallisuutta ja sosiaalista mediaa on tutkittu erikseen, ei näiden yhtenevyyttä ole tutkittu joukkojen perustamisvaiheen aikana.

Käsitteet

Sosiaalinen media (SOME) käsittää web 2.0 verkkoympäristön (internet), jonka palvelut mahdollistavat esteettömän tiedon jakamisen eri yhteisöissä ja sovelluksissa. Tämä tutkimus keskittyy tarkastelemaan niitä julkisia sovelluksia joita tutkimuksen kannalta käytetään v. 2013–2014 eniten Suomessa, esim. Facebook, Youtube ja Twitter. Näihin on mahdollista saada yhteys eteenkin modernien älypuhelinten, tietokoneiden ja muiden laitteiden kautta.

Operaatioturvallisuudella (OPTU) tarkoitetaan informaatioita, joita pyritään pitämään salassa vastustajan tiedustelulta, jotta operaation tavoitteita ja toimintaa voidaan suojella. Näitä ovat mm. paikkatiedot, kokoonpanot, kaluston ja joukkojen lukumäärät, joukkojen tehtävät sekä toimintatavat ja taktiikka. Operaatioturvallisuuteen kuuluvat myös ulkopuoliset vaikutteet, jotka voivat haitata operaatioturvallisuutta disinformaation ja propagandan muodossa (esim. PSYOPS/INFO-OPS → sosiaalisen median kautta). Tässä tutkimuksessa operaatioturvallisuutta tarkastellaan sosiaalisen median näkökulmasta. Operaatioturvallisuus tunnetaan myös kansainvälisesti termillä OPSEC (Operational Security), jota käytetään tässä tutkielmassa.

[6] Pääesikunnan asiakirja AH27977, Sosiaalisessa mediassa toiminnan ohje varusmiehille ja reserviläisille.

Operaatioturvallisuusohje pyrkii määrittämään rajoitteita, ohjeita ja toimintatapoja, joilla suojataan omaa toimintaa vihollisen tiedustelulta ja vaikutukselta. Käytännössä tämä tarkoittaa taisteluosaston operaatioturvallisuusupseerin/ -komentajan laatimaa käskyä operaatioturvallisuudesta, joka voi sisältää mm. ohjeita tietokoneiden, sähköpostin, sosiaalisen median ja älypuhelimien käytöstä. Tämän lisäksi operaatioturvallisuusohje käskee mitä tietoa saa jakaa esimerkiksi älypuhelimien kautta ja miten tiedustelulta sekä tietoturvauhilta suojaudutaan.

Open Source Intelligence (OSINT) eli avointen lähteiden tiedustelu perustuu julkisesti saatavilla olevan lähteiden tiedon keräämiseen sekä analysointiin. OSINT käsittää sanomalehdet, radion, television, julkaistut tutkimukset sekä internetin kokonaisuudessaan. Tutkielman tarkastelun painopisteessä on internetpohjainen avointen lähteiden tiedustelu, eteenkin sosiaalisen median eri yhteisöpalveluiden muodostamat tiedonkeruukohteet. OSINT menetelmää tarkastellaan pääsääntöisesti Yhdysvaltojen asevoimien muodostaman OSINT-manuaalin kautta.

Informaatio-operaatiot (INFO-OPS) muodostuvat seuraavista kokonaisuuksista: operatiivinen harhauttaminen, kansallinen informaatiosodankäynti, psykologinen sodankäynti, elektroninen sodankäynti, tukevat osa-alueet (fyysinen vaikuttaminen ja turvallisuus), tietojärjestelmäsodankäynti, sekä operaatioturvallisuus.

Joukkojen perustamisvaiheessa muodostetaan sodan-ajan joukot, kalustetaan, ja varustetaan ne, sekä aloitetaan joukkojen kouluttaminen. Rauhan- ja sodanajan välistä aikaa voidaan käsittää ns. harmaaksi vaiheeksi tai kriisinajaksi. Joukkojen perustamisvaihe sijoittuu tähän vaiheeseen.

Taisteluosasto (TSTOS) käsittää maavoimien uudistetun taistelutavan 2015 mukaan n. vahvennetun pataljoonan kokoisen osaston, joka kykenee itsenäiseen taisteluun. Taisteluosaston kokoonpanoon kuuluu neljä jalkaväki- tai jääkärikomppaniaa, tykistöpatteristo, kranaatinheitinkomppania, huoltokomppania, pioneerikomppania, sekä esikunta- ja viestikomppania. Taisteluosastoa johtaa taisteluosastonkomentaja yhdessä esikunnan kanssa. Taisteluosasto voi olla alueellinen, puolustava, mekanisoitu tai hajautettu.

1.3 Tutkimusongelma, tutkimuksen tavoite ja tutkimuskysymykset

Tutkimus kartoittaa sosiaalisen median uhat ja selvittää miten näitä uhkia ennaltaehkäistään ja miten niiltä suojaudutaan operaatioturvallisuuden näkökulmasta. Lopputuloksena on syvennetty käsitys avointen lähteiden tiedustelusta sosiaalisessa mediassa, ja miten tämä vaikuttaa taisteluosaston operaatioturvallisuuteen.

Päätutkimuskysymys: Millainen uhka sosiaalinen media on taisteluosaston operaatioturvallisuudelle ja miten siltä voidaan suojautua joukkojen perustamisvaiheen aikana?

Alakysymykset:

- Mitä operaatioturvallisuus tarkoittaa konseptina?
- Minkälainen sosiaalinen media on toimintaympäristönä?
- Miten vastustaja tiedustelee sosiaalisessa mediassa (OSINT)?
- Minkälaisen vaikutuksen operaatioturvallisuuden puute sosiaalisen median toimintaympäristössä luo taisteluosastolle?

1.4 Tutkimusmenetelmät

Tutkielma toteutetaan laadullisen tutkimuksen periaatteella hermeneuttisesta näkökulmasta ja menetelmänä käytetään aineistolähtöistä analyysiä perustuen aiempiin tutkimuksiin ja kirjallisiin lähteisiin. Tämän lisäksi tutkimusaiheeseen syvennytään kahdella avoimella haastattelulla. Haastateltavaksi on valittu kaksi asiantuntijaa, jotka ovat toimineet operaatioturvallisuuden ja avointen lähteiden tiedusteluun liittyvissä ympäristöissä.

Sisältöanalyysin avulla tutkimuksessa selitetään sosiaalisen median mahdollisia uhkia ja vaikutteita operaatioturvallisuuteen ja mitä asioita operaatioturvallisuussuunnitelma pitäisi sisältää vastatakseen näihin haasteisiin. Täten on mahdollista ymmärtää ilmiötä paremmin. Tulokset muodostuvat analysoimalla teoriaa ja tapauksia sosiaalisessa mediassa, joiden pohjalta on laadittu kolme toimintamallia. Lopputuloksena on usean lähteen muodostama teoriapohja, josta on mahdollista kehittää sosiaalisen median operaatioturvallisuuskonseptia Puolustusvoimissa.

1.5 Viitekehys, rajaukset ja näkökulma

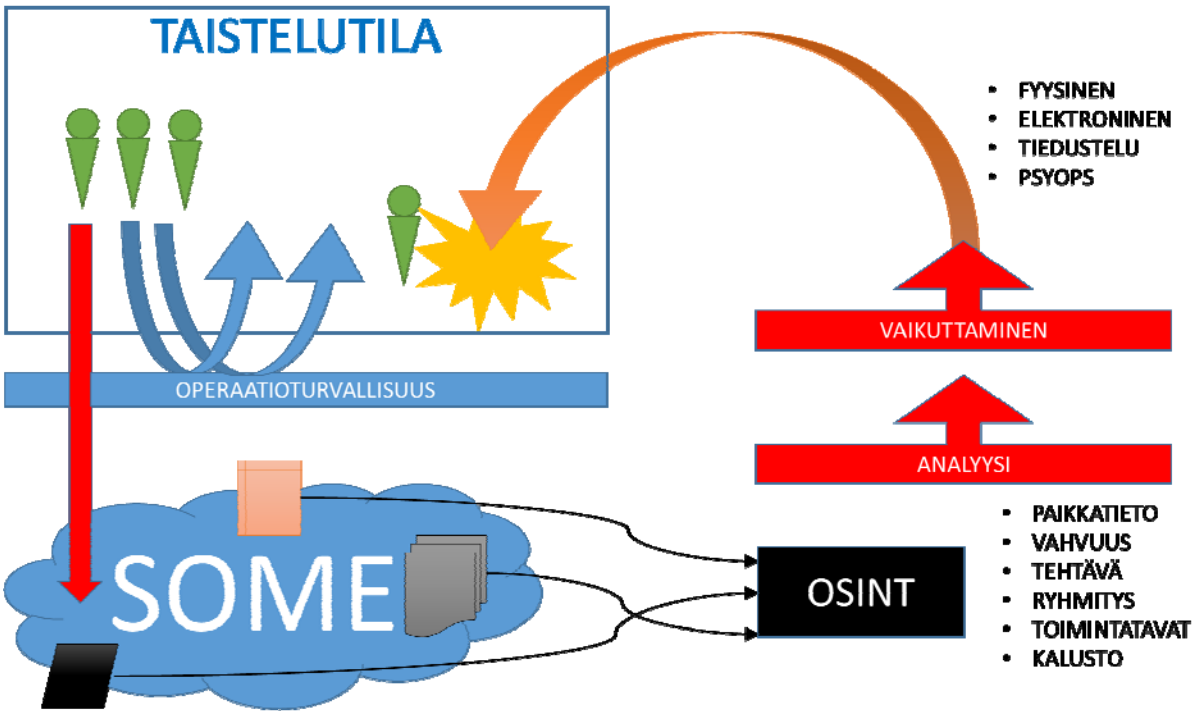
Tutkimuksen näkökulma muodostuu kolmesta tekijästä: operaatioturvallisuus osana taisteluosaston kokoista organisaatiota joukkojen perustamisvaiheessa, sosiaalisen median muodostama uhka operaatioturvallisuudelle, sekä vastustajan avointen lähteiden tiedustelu sosiaalisen median kautta. Näiden tekijöiden kautta muodostuu yhdistetty sosiaalisen median vaikutus operaatioturvallisuuteen–näkökulma. Näitä tekijöitä tarkastellaan sekä yksittäisen taistelijan että taisteluosaston komentajan tasolla.

Tutkielma rajataan taisteluosaston kokoiseen kokoonpanoon joukkojen perustamisvaiheessa. Aihetta rajataan operaatiotaidon ja taktiikan näkökulmasta tiedusteluun ja tiedon keruuseen uhkakuvien ja näiltä suojautumisen osalta yksittäisen taistelijan näkökulmasta. Tiedustelu rajataan avointen lähteiden tiedusteluun internetissä. Tässä tutkimuksessa ei käsitellä disinformaation uhkia tai psykologista vaikuttamista (PSYOPS) tai muita vaikutuskeinoja tarkemmin. Tutkimuksessa vastustajalla tarkoitetaan yleisesti ottaen minkä tahansa valtion asevoimien avoimen tiedustelun yksikköä. Vastustajaa ei ole rajattu tiettyyn valtioon tai organisaatioon.

Tässä tutkielmassa ei käsitellä operaatioturvallisuuden tai sosiaalisen median laillisia tai psykologisia taustoja. Sosiaalisen median sovelluksia ja yhteisöpalveluita rajataan yleisimpiin sovelluksiin: Twitter, Facebook, Youtube, Skype, sekä GPS-tyyppiset sovellukset. Näitä sovelluksia tarkastellaan kansainväliselle tasolla operaatioturvallisuusesimerkkien valossa. Painopisteenä on suomalaisten sosiaalisen median käyttö. Taisteluosasto organisaationa toimii viitekehyksenä, mutta sen organisaatiota ei tutkita tarkemmin.

Tutkimuksen viitekehys on havainnoitu kuvassa 1 (liite 1). Kuvassa ilmenee taistelutila, joka käsittää taisteluosaston fyysisen toiminnan alueen ja rajat. Taisteluosaston alueella toimivat taistelijat käyttävät sosiaalista mediaa pääsääntöisesti älypuhelimillaan. Operaatioturvallisuus toimii taisteluosaston suojana, jonka vaikutus perustuu taistelijoiden ymmärrykseen siitä, mitä saa ja ei saa tehdä sosiaalisessa mediassa. Takaisin kimpoilevat nuolet ilmaisevat sitä, että taistelijat ymmärtävät operaatioturvallisuuden asettamat sosiaalisen median rajoitteet, ja toimivat niiden rajoissa ylläpitääkseen operaatioturvallisuutta.

Kuvan yksi taistelija on laiminlyönyt operaatioturvallisuutta, ja vuotaa tärkeää tietoa sosiaaliseen mediaan kuvan, blogin, paikkatiedon tai muun tiedon muodossa. Kuvan punainen viiva osoittaa tiedon läpäisyä operaatioturvallisuudesta suoraan sosiaalisen median toimintaympäristöön, jossa erilaisia tietoja on saatavilla. Tiedot havaitaan avointen lähteiden tiedustelulla (OSINT), jota musta laatikko kuvaa. Tiedustelu pyrkii selvittämään paikkatietoa, joukon vahvuutta, tehtävää, ryhmitystä, toimintatapoja ja kalustoa. Analysoinnin kautta vastustaja määrittelee tärkeän tiedon, jonka pohjalta on mahdollista vaikuttaa takaisin. Vaikutus voi ilmetä tiedusteluna tai fyysisenä, elektronisena ja psykologisena sodankäyntinä. Vaikutusta voidaan kohdentaa tavoitteesta riippuen takaisin taisteluosastoon, tai muualle.



Kuva 1: Tutkimuksen viitekehys - sosiaalisen median muodostama uhkakuva taisteluosaston operaatioturvallisuudelle.

2 OPERAATIOTURVALLISUUS OSANA INFORMAATIO-OPERAATIOITA

Ymmärtääksemme sosiaalisen median muodostamia uhkia taisteluosaston operaatioturvallisuudelle, on tutkittava aiheeseen liittyvää ympäristöä ja siihen liittyviä konsepteja: informaatio-operaatiota ja operaatioturvallisuutta. Tämä luku pyrkii luomaan kuvan tästä ympäristöstä, joka puolestaan mahdollistaa uhkakuvien tarkastelun seuraavissa luvuissa. Lisäksi luvun tarkoituksena on luoda teoriapohja tutkimukselle. Ensimmäisenä käsitellään informaatio-operaation ja operaatioturvallisuuden välistä suhdetta. Toiseksi tarkastellaan operaatioturvallisuusprosessia konseptina. Kolmantena konsepteja tarkastellaan sosiaalisen median näkökulmasta.

Vaikka operaatioturvallisuussuunnitelma-, sekä informaatio-operaatiokonseptit perustuvat strategisen tason ajatteluun ne luovat perustan taktisen tason tarkasteluun. Informaatio-operaatioiden tarkastelulla pyritään selvittämään se viitekehys, missä taktisen tason elementit myös liikkuvat. Operaatioturvallisuusprosessi toimii taisteluosaston komentajan työkaluna, jota apuna käyttäen voi laatia perustat operaatioturvallisuuden ylläpitämiseksi.

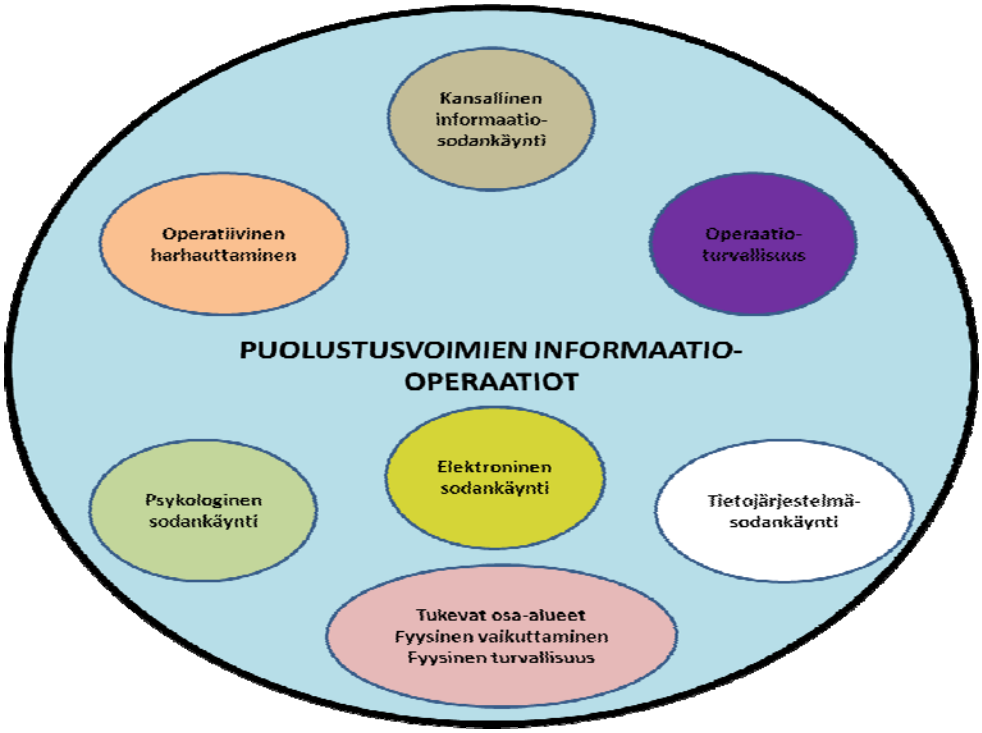
2.1 Informaatio-operaatiot ja operaatioturvallisuus

Vaikka sosiaalinen media käsitteenä ei ollut vielä olemassa 2000-luvun alussa, oli selkeää, että internetin ja sosiaalisen median yhteisöpalvelut tulevat olemaan osa tulevaisuuden informaatiosodankäyntiä[7]. Informaatio-operaatiot käsittävät seitsemän osa-aluetta. Operaatioturvallisuus on yksi osa vaikeasti määriteltävissä olevaa informaatio-operaatiot –konseptia. Sirén määrittää Puolustusvoimien informaatio-operaatioiden muodostuvan seuraavista kokonaisuuksista: Operatiivinen harhauttaminen, kansallinen informaatiosodankäynti, psykologinen sodankäynti, elektroninen sodankäynti, tukevat osa-alueet (fyysinen vaikuttaminen ja turvallisuus), tietojärjestelmäsodankäynti, sekä operaatioturvallisuus.[8] On siis todettavissa, että operaatioturvallisuus liittyy vahvasti informaatio-operaatioihin, johon sosiaaliset mediat kuuluvat informaatiokanavana. Konsepti on havainnoitu kuvassa 2.

---

[7] Liimatainen, Heikki ja Rantapelkonen: *Informaatioajan viestitaktisia ajatuksia*, Viestikoulu, Riihimäki, 2000, ss. 213–215.

[8] Sirén, Torsti: *Strateginen kommunikaatio ja informaatio-operaatiot 2030,* Juvenes Print Oy, Helsinki, 2011, s.130.



Kuva 2: Puolustusvoimien informaatio-operaatioiden kokonaisuus.[9]

Suomen Puolustusvoimat määrittää operaatioturvallisuuden seuraavasti:

”Operaatioturvallisuus on operatiivisen toiminnan kannalta kriittisten tietojen ja tavoitteiden määrittämistä sekä niiden käytettävyyden ja saatavuuden turvaamista oman päätöksenteon tukena sekä niiden paljastumisen estämistä vastustajalle. Yleisesti kriittiseen tietoon voidaan lukea kuuluvaksi tilannekuvaan, operatiivisiin suunnitelmiin sekä puolustusjärjestelmän keskeisiin osiin liittyvät tiedot.”[10]

Operaatioturvallisuus voidaan jakaa strategiseen, operatiiviseen ja taktiseen tasoon. Tutkimuksen rajauksen kannalta keskitytään taktiseen tasoon. Taktisella tasolla tarkoitetaan yksittäisen sotilaan kriittisen tiedon turvaamista, joka paljastuttuaan voi aiheuttaa turvallisuusvaaran niin yksittäiselle taistelijalle kuin koko hänen joukolleen. Tämä on huomioitu esimerkiksi rauhanturvausoperaatioissa, joissa suomalaisilla rauhanturvaajilla ei ole oikeutta jakaa toimialueella kuvattua materiaalia internetin kautta.[11]

[9] Sirén (2009), s. 92.
[10] Pääesikunnan suunnitteluosasto: *Informaatio-operaatiot (INFOOP) konsepti 2.0*, Helsinki, 2011, s.4.
[11] Puolustusvoimien kansainvälinen keskus: *ISAF, Suomalainen kriisinhallintajoukko Afganistanissa*, Kaarinan Tasopaino oy, Kaarina, 2007, s.57.

Valtionvarainministeriön sosiaalisen median tietoturvaohjeessa todetaan sosiaalisen median olevan uusiluontoinen uhka taktisella tasolla, jolla voi olla jopa strategisia vaikutuksia[12]. Vuonna 2006 perustettu Wikileaks, jota voidaan pitää salaisen tiedon avoimen jakelun edelläkävijänä, osoittaa tämän uhan todeksi. Sivuston paljastuksiin kuuluu vuonna 2010 julkaistun Apache helikopterin ”teloitusvideo” ja siitä seurannut viattomien sivullisten tappaminen herätti maailmanlaajuista kritiikkiä.[13]

CIA:lle ja NSA:lle tietoteknikon töitä tehnyt Edward Snowden osoitti kesäkuussa 2013 paljastettuaan Yhdysvaltain tiedustelupalvelun huippusalaisen PRISM-tiedusteluohjelman, että tietoturvauhka voi olla hyvinkin mahdollista niin ulko- kuin sisäpuolelta[14]. Molemmat esimerkit osoittavat yksittäisten taktisen tason tekijän vaikutuksen strategisella tasolla ja kuinka todellinen uhka sekä mahdollisuus sosiaalinen media voi olla. Tämä myös osoittaa yhteyden sosiaalisen median potentiaalisista uhista suhteessa operaatioturvallisuuteen.

2.2 Operaatioturvallisuusprosessi osana operaatioturvallisuutta

Yhdysvaltojen puolustushaarakomentajien neuvoston (JCOS - Joint Chiefs of Staff) mukaan operaatioturvallisuus (OPTU) käsittää operaatioturvallisuusprosessin, josta voidaan muodostaa operaatioturvallisuussuunnitelma. Operaatioturvallisuusprosessi koostuu viidestä osa-alueesta: kriittisen informaation identifioiminen, uhkien analysointi, heikkouksien analysointi, riskien arviointi sekä sopivien vastatoimien soveltaminen.[15] Suomen Puolustusvoimien ja Yhdysvaltojen asevoimien näkemys operaatioturvallisuudesta ja siihen liittyvästä prosessista ovat käytännössä samanlaiset. Yhdysvallat ovat tutkineet ja kehittäneet kyseistä aluetta ensimmäisenä jonka jälkeen Suomi on ottanut metodin käytäntöön.[16]

Tämän turvallisuusprosessin myötä on mahdollista kartoittaa esimerkiksi taisteluosaston omat uhat ja mahdollisuudet. Tutkielman kontekstissa on kyse siitä, miten taisteluosastossa tulisi toimia ja suhtautua sosiaalisen median luomaan erilaiseen uhkakuvaan perinteisen operaatioturvallisuuden kannalta. Tämä prosessi toimii työkaluna hyvin samalla tavalla kuin SWOT analyysi, jossa tulkitaan kohteen vahvuudet, heikkoudet, mahdollisuudet ja uhat. Taistelu-

[12] Valtionvarainministeriö: *Sosiaalisen median tietoturvaohje (VAHTI 4/2010)*, vm-julkaisutiimi, Helsinki, 2010.
[13] *Huffington Post*, WikiLeaks ‘Insurance’ File:Julian Assange’s Group Posts Huge Encrypted File to Web, 5.8.2010, http://www.huffingtonpost.com/2010/08/05/wikileaks-insurance-file-_n_672094.html, 15.12.2013.
[14] Ewen MacAskill: Edward Snowden: how the spy story of the age leaked out, *The Guardian*, 12.6.2013.
[15] Joint Chiefs of Staff: *Operations Security*, Joint Publication 3-13, 2012, ss. 1-2.
[16] Leskinen, Aleksi: *Informaatiosodankäynti, operaatioturvallisuus ja puolustusvoimien turvallisuusprosessi*, 2006 ss. 84–86.

osaston komentaja pystyy määrittelemään tarvittavat rajaukset ja toimintatavat operaatioturvallisuuden näkökulmasta käyttäen tätä prosessia.

Kriittisen informaation identifioiminen: prosessin ensimmäisessä vaiheessa identifioidaan kriittinen informaatio. Kriittinen informaatio muodostuu niistä tiedoista, jotka vastustaja tarvitsee kiistääkseen operaatioturvallisuuden. Kriittinen informaatio koostuu mm. käytettävistä resursseista, kalustosta, ajoituksesta, logistisista mahdollisuuksista, kohteista, viestiyhteyksistä, taktiikasta, tekniikasta ja muista prosesseista. Kriittisistä informaatioista muodostetaan lista, jota voidaan prosessin mukaan analysoida. Kriittisen informaation tekijät voivat ulottua myös organisaation ulkopuolelle, mikä pitää ottaa myös huomioon.[17]

Uhkien analysointi: prosessin toisessa vaiheessa analysoidaan kaikki uhat, jotka liittyvät pelkästään edellä mainittuihin kriittisiin informaatioihin. Analysointiin käytetään keskeisiä kysymyksiä, jotta on mahdollista muodostaa kokonaiskuva erilaisista uhista. Analysoinnissa otetaan huomioon seuraavat tekijät: kuka vastustaja on, mitä vastustaja yrittää saavuttaa, minkälaisia toimenpiteitä vastustaja käyttää saavuttaakseen tiedon, mitkä kriittiset tiedot vastustajalla on jo hallussa, mitä keinoja vastustajalla on käytettävissä kerätessään tietoa, ja keiden tahojen kanssa vastustaja aikoo jakaa tietoa.[18]

Heikkouksien analysointi: prosessin kolmannessa vaiheessa analysoidaan omia heikkouksia. Heikkouksia analysoidessa on otettava huomioon ne organisaatioon liittyvät toiminnat, jotka ovat vihollisen kannalta helposti tiedusteltavissa, ja jotka yhdistettäessä muodostavat kriittistä informaatiota. Eri avoimet lähteet sekä omien joukkojen toiminta voi myös luoda uutta kriittistä tietoa, jonka vastustaja voi havaita. Näiden lähteiden ja organisaation toimintojen olemassaolo voi toimia myös organisaatiota vastaan, jos tieto osoittaa selkeitä heikkouksia ja toimintatapoja vastustajalle, joka pystyy analysoimaan tiedon sekä toimimaan riittävän nopeasti tehtävän kumoamiseksi.[19] Taisteluosaston näkökulmasta voidaan analysoida, onko mahdollista estää tai kontrolloida älypuhelimien käyttöä.

Riskien arviointi: prosessin neljännessä vaiheessa arvioidaan riskit. Arviointi voidaan jakaa kolmeen osaan, joista ensimmäisessä määritellään vastatoimenpide jokaista edellä mainittua heikkoutta kohtaan. Toisessa osassa arvioidaan hyöty/haitta-suhde vastatoimenpiteiden suunn-

[17] Joint Chiefs of Staff (2012), ss. 2-3.
[18] Sama, ss. 3-4.
[19] Sama, ss. 4-5.

ittelun, resurssien ja henkilöstön käytön suhteen suhteessa vastustajan saaman kriittisen informaation merkittävyyteen ja sen käytettävyyteen operaatioturvallisuuteen verrattuna. Kolmannessa osassa valitaan kaikki kriittisimmät ja toteutuskelpoisimmat vastatoimenpiteet, jotka toteutetaan.[20] Riskejä arvioidessa on todettava, pystyykö taisteluosasto ylläpitämään operaatioturvallisuutta jos älypuhelimet ovat käytössä, vai pitäisikö ne poistaa kokonaan.

Sopivien vastatoimien soveltaminen: prosessin viidennessä vaiheessa sovelletaan ja analysoidaan vastatoimia. Hyvä vastatoimenpidestrategia vähentää omien toimintojen ennalta-arvaamattomuutta, määrittää havaittavissa olevat tekijät ja suojelee niitä poistamisen, ohjaamisen tai hämäyksen keinoin, peittää ratkaisevat tekijät ja potentiaaliset tavoitteet sekä torjuu tehtäväprosessin suorittamisen sisäiset heikkoudet ja siihen liittyvän teknologian heikkoudet.

Tehtävän aikana on suositeltavaa mitata suunnitelman toimivuutta MOE (Measure of Effectiveness) ja MOP (Measure of Performance) -analyysien kautta. MOE analyysi osoittaa miten vastustaja reagoi vastatoimenpiteisiin, joka osoittaa vastatoimenpiteen tehokkuuden suhteessa siihen käytettyihin resursseihin. MOP analyysi osoittaa operaatioturvallisuuteen liittyvien vastatoimenpiteiden toteutuksen toimivuutta käytännössä. Näiden analyysien pohjalta on mahdollista muokata ja kehittää operaatioturvallisuussuunnitelmaa tulevaisuuden toimenpiteitä varten.[21] Prosessin viimeisessä osassa voidaan laatia suunnitelma älypuhelimien käyttöön liittyen taisteluosastossa. Tämä voi sisältää useita vaihtoehtoja, joista valitaan tehokkain ja turvallisin operaatioturvallisuuden näkökulmasta.

Operaatioturvallisuusprosessi kiteyttää taisteluosaston komentajan toimintaympäristön ja siihen tarvittavien suunnittelutyökalujen merkityksen osana isompaa kokonaisuutta. Taktisella tasolla tämä tarkoittaa sitä, että usean taisteluosaston operaatioturvallisuuden laiminlyönti sosiaalisessa mediassa voi vaikuttaa vastustajan tiedusteluun merkittävästi. Informaatiooperaatiot suunnitellaan ja toteutetaan isossa mittakaavassa, ja ne voivat vaikuttaa myös taisteluosaston toimintaan riippuen halutusta vaikutuksesta. Tämä on selkeästi huomioitava uhka jopa yksittäisen taisteluosaston tasolla. Taktisen tason tarkastelu edellyttää erilaisia työkaluja, joilla sosiaalisen median vaikutusta operaatioturvallisuuteen voidaan mitata taisteluosaston tasolla. Kun nämä uhat, mahdollisuudet, heikkoudet ja vahvuudet otetaan huomioon, on mahdollista laatia räätälöity operaatioturvallisuussuunnitelma yksittäiselle taisteluosastolle.

[20] Joint Chiefs of Staff (2012), ss. 5-6.
[21] Sama, ss. 6-8.

3 SOSIAALINEN MEDIA OSANA OSINT MENETELMÄÄ

Informaatio-operaatioiden, operaatioturvallisuuden ja operaatioturvallisuussuunnitelman viitekehyksen lisäksi on tärkeää ymmärtää sosiaalisen median toimintaympäristöä ja vastustajan toimintatapoja sosiaalisen median ympäristössä. Taisteluosaston tasolla on ymmärrettävä, miten taktisen tason toimet yksittäisestä taistelijasta lähtien voivat vaikuttaa vastustajan strategisen tason toimintaan, kun tarkastellaan asiaa sosiaalisen median näkökulmasta. Tämä tarkoittaa avointa tiedustelua ja vaikuttamista sosiaalisen median kautta, jolla voi mahdollistaa strategisen tason toimeenpanoa. Tämän luvun tarkoituksena on luoda teoriapohja sosiaalisen median toimintaympäristöstä ja avointen lähteiden tiedustelukeinoista.

Tämä luku avaa nykyajan sosiaalisen median toimintaympäristön ja siihen liittyvät konseptit, avointen lähteiden tiedustelun kantavan periaatteen siitä mitä ja miten vastustaja kerää tietoa sekä tiedustelee sosiaalisessa mediassa, ja yhdistää edellä mainitut teoriat ja konseptit yhteen. Lopputuloksena on ymmärrys siitä, mitä vaikutusta tai tehtävää vastustaja pyrkii saamaan aikaan sosiaalisen median kautta, sekä millä keinoin ja mitä konkreettisia uhkia näistä muodostuu.

3.1 Sosiaalisen median toimintaympäristö

Sosiaalinen media voidaan käsittää usealla eri tapaa termin käytöstä tai näkökulmasta riippuen. Sosiaalinen media käsittää verkkoviestintäympäristön, jossa eri käyttäjät ja käyttäjäryhmät voivat toimia aktiivisina viestijöinä ja sisällöntuottajina perinteisen tiedon vastaanottajan roolin lisäksi.[22] Sosiaalisen median ja siihen liittyvän tietoturvan ja tiedustelun kannalta on syytä käsitellä sekä ymmärtää sosiaalinen mediaan liittyviä teknologioita, eteenkin sen mahdollistamia sovelluksia ja palveluita. Sosiaalisen median teknologiat voidaan tulkita professori Andreas M. Kaplanin ja Michael Haenleinin mukaan ”*joukkona internetsovelluksia, joiden ideologinen ja tekninen perusta on web 2.0:ssa ja jotka mahdollistavat loppukäyttäjien tuottaman sisällön luomisen ja välittämisen*”[23]. Sosiaalisen median palveluihin kuuluu muun muassa linkkien ja uutisten jakopalvelut, blogi- ja mikroblogipalvelut, wiki- ja muut yhteisöpalvelut, mediapalvelut, yhteisöt, virtuaalimaailmat, ja verkkoyhteisöt[24].

[22] Kalliala, Eija & Toikkanen, Tarmo: *Sosiaalinen media opetuksessa*, Finn Lectura, 2009.
[23] Kaplan Andreas M., Haenlein Michael: *Users of the world, unite! The challenges and opportunities of Social Media*, Business Horizons, 2010, ss. 59–68.

[24] Kalliala, Eija & Toikkanen, Tarmo: *Sosiaalinen media opetuksessa*, Finn Lectura, 2009.

Palveluiden käyttö vaihtelee vuosittain ja maittain trendien mukaan. Tutkimuksen kannalta on olennaista tarkastella Suomen nykypäivän trendejä. YLE:n teettämän tutkimuksen mukaan vuonna 2013 käytetyimmät sosiaalisen median palvelut olivat Facebook (n. 2 100 000 aktiivista käyttäjää), Suomi24 (1 700 000 rekisteröityä käyttäjää), IRC-Galleria (451 000 rekisteröityä käyttäjää), LinkedIn (444 000 rek. käyttäjää), Twitter (300 000), Foursquare (74 600 rek. käyttäjää) ja Google+ (47 600 rek. käyttäjää). Näistä sosiaalisen median palveluista Facebook ja Twitter luovat ylivoimaisen osan kokonaisyhteisöistä, jonka päivittäinen käyttäjämäärä ja tietoliikenne ovat suuria.[25]

Sosiaalisen median ympäristö Suomessa on keskittynyt yhteisöihin, joissa tiedonjakaminen sekä viestittäminen ovat helppoa, laadukasta ja jotka tavoittavat suuren yleisön. Facebook, joka on Suomen käytetyin sosiaalisen median palvelu käyttää jo 55 % kaikista 13–64 vuotiaista suomalaisista. Suurin käyttäjäryhmä on 21-vuotiaat nuoret. Tutkimus osoittaa, että etenkin Facebookkia käytetään pääsääntöisesti viestintään ja 20 % käyttää Facebookia pelkästään mobiililaitteella. Suomen toiseksi eniten käytetyllä reaaliaikaisella viestintäpalvelulla, Twitterillä on jo yli 516 000 käyttäjää, joista 116 000 on aktiivisia. Tiedon jakaminen tapahtuu nk. Tweeteillä, joita keskimääräinen käyttäjä on luonut 283 kappaletta. Käyttäjällä on n. 70 seuraajaa jotka aktiivisesti vastaanottavat tietoa.[26]

Tutkimuksen kannalta etenkin mobiililaitteiden käyttö sosiaalisen median ympäristössä on merkittävää, sillä joukkojen perustamisvaiheessa suurin osa taisteluosaston joukoista kykenee suurimmaksi osaksi pelkästään mobiiliyhtieyteen sosiaalisen median kannalta. 41 % suomalaisista internetinkäyttäjistä on sosiaalisessa mediassa mobiilisti. 98 % käyttäjistä lähettää tekstiviestejä esimerkiksi Whatsapp-sovelluksella, joka on internetyhteyttä käyttävä ilmainen viestintäsovellus. 82 % on lähettänyt kuva- tai videotiedostoja toiselle mobiilikäyttäjälle tai julkisesti sosiaaliseen mediaan. 60 % käyttäjistä tarkistaa sähköpostinsa mobiililaitteella. 53 % ovat käyttäneet karttapalveluita, kuten GPS-pohjaista GoogleMaps-sovellusta. 51 % käyttäjistä on ladannut laitteeseen sovelluksen, kuten esimerkiksi interaktiivisen pelin. 49 % ovat jakaneet langattomalla Bluetooth tiedonjakomenetelmällä tiedostoja. 35 % katsovat videoita

[25] *YLE uutiset*: Täällä somelaiset elävät – katso lista historiallisesta Facebookista juuri avattuun Pheediin, 5.3.2013, http://yle.fi/uutiset/taalla_somelaiset_elavat_-_katso_lista_historiallisesta_facebookista_juuri_avattuun_pheediin/6518189, 18.12.2013.
[26] Pönkä, Harto: *Sosiaalisen median katsaus 09/2013*, 10.9.2013, http://www.slideshare.net/hponka/sosiaalisen-median-katsaus-092013, 18.12.2013.

tai tv-ohjelmia. 18 % käyttäjistä on käyttänyt GPS-paikannusohjelmia kuten Foursquare-sovellusta. 12 % käyttäjistä on käyttänyt Spotifyita älypuhelimella musiikin kuunteluun.[27]

Suomalaisista 16–60 -vuotiaista 61 % omistaa älypuhelimen[28]. Ikäluokittain tämä luku on 16–24 vuotiailla 65 %, 25–34 -vuotiailla 73 %, 35–44 -vuotiailla 72 %, 45–54 -vuotiailla 55 % ja 55–64 -vuotiailla 33 % vuonna 2012. Näistä ikäluokista 16–24 -vuotiaat ovat 75 % viikoittain netissä älypuhelimien kautta, ja 25–51 -vuotiaat miehet 70 %.[29] Nämä ikäluokat ovat verrattavissa Suomen reserviläisten lukumäärien kanssa. Lukumäärät ovat suuntaa antavia koska tarkkoja lukuja ei ole määritelty. Sovellettuna taisteluosaston raamiin tämä tarkoittaa sitä, että n. 70 % taisteluosastosta käyttää älypuhelima ja 71 % heistä käyttää sovelluksia. Tämä arvio mahdollistaa potentiaalisen riskin kartoittamisen taisteluosaston henkilöstön keskuudessa.

3.2 OSINT osana vastustajan tiedustelua ja tiedonkeruuta

Vastustajan avointen lähteiden tiedustelun (OSINT - Open Source Intelligence) päämääränä on kerätä kriittistä tietoa joukkojen toiminnasta ja tilasta oman operaation kannalta. Tieto luokitellaan eri luokkiin sen tärkeyden, sisällön ja tarpeen mukaan luoden erilaisia tiedustelutuotteita. Toteuttaakseen annetun tehtävän, vastustaja käyttää pääsääntöisesti avointen lähteiden tiedustelukonseptia työkaluna osana tiedustelua ja tiedonkeruuta. Päätös tiedustella eri kohteita, kuten tarkasteltavaa taisteluosastoa, muodostetaan resurssien, kriittisyyden ja tavoitteiden mukaan. On syytä huomauttaa, että vaikka avointen lähteiden tiedustelu on tarkoitettu pääsääntöisesti tiettyjen kriittisten kohteiden ja tärkeiden henkilöiden maalittamiseksi voi tämä kohdistua myös taisteluosaston kokoiseen organisaatioon riippuen siitä, miten hyvin tai huonosti sen operaatioturvallisuutta ylläpidetään ja miten organisaatio vaikuttaa isossa mittakaavassa.

Avointen lähteiden tiedustelumenetelmä käsittää kaiken julkisen materiaalin ja lähteen keräämistä, analysointia sekä käyttöä operaation tarpeiden mukaan. Avointen lähteiden tiedustelu koostuu tiedonkeruun suunnitteluprosessista, tiedonkeruun valmistelevasta osasta, tiedonkeruuprosessista sekä analysoidun tiedon tuottamisprosessista. Avointen lähteiden tiedustelun tarkastelu keskittyy medioiden osalta sosiaalisen mediaan ja sen tiedonkeruuprosessiin.

---

[27] Pönkä (2013).
[28] TNS Mobile Life Gallup, 2013, http://www.tns-gallup.fi/uutiskirje2013/05/otsikko2, 14.12.2013.
[29] Suomen virallinen tilasto (SVT): Väestön tieto-ja viestintätekniikan käyttö 2012. 3.Internetin käyttö muualla kuin kotona tai työpaikalla, Helsinki, http://www.stat.fi/til/sutivi/2012/sutivi_2012_2012-11-07_kat_003_fi.html, 14.12.2013.

Avointen lähteiden tiedustelun päämääränä on tukea taistelun neljää osa-aluetta: joukkojen muodostamista, yleisen tilannekuvan muodostamiseen tarvittava tuki, tiedonkeruun, valvonnan ja tiedustelun suorittaminen, sekä henkilö- ja kohdemaalittamisen ja informaatioylivoima[30].

3.2.1 OSINT tiedonkeruuprosessi

Avointen lähteiden tiedustelun tiedonkeruuprosessi (OSINT) koostuu neljästä tekijästä: informaation ja tiedustelutarpeiden tunnistaminen, tiedustelutarpeiden luokittelu tyypeittäin, informaatiolähteen tunnistaminen ja tiedonkeruumetodin valinta[31]. Tämä prosessi on osoitettu kuvassa 3.

Informaation ja tiedustelutarpeiden tunnistaminen luo rajoitukset tiedonkeruulle operaation tarpeiden mukaan[32]. Tämä voisi tarkoittaa esimerkiksi mielialan, kaluston, tehtävän tai joukkojen sijoitusten tiedustelua eri sosiaalisten medioiden sovellusten kautta, kuten Facebook.

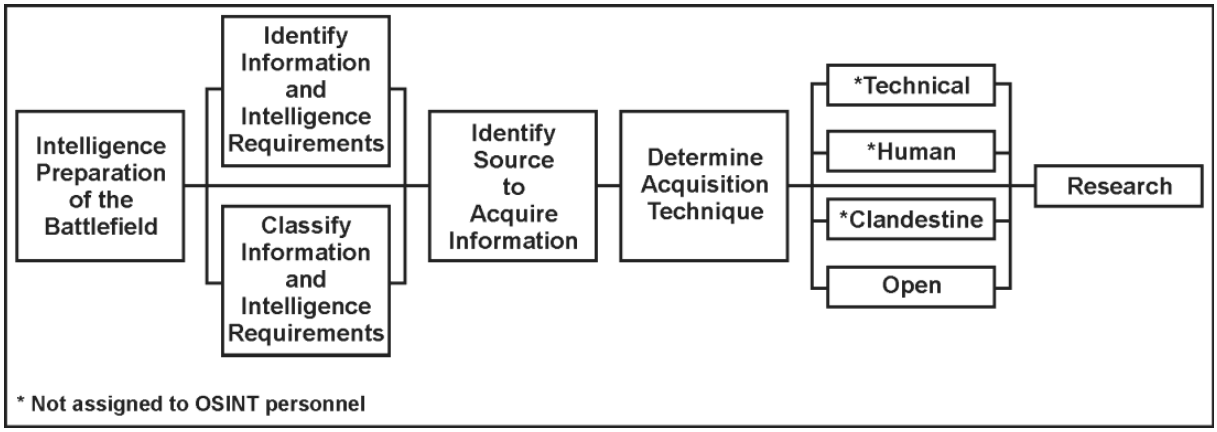
Tiedustelutarpeiden luokittelu tyypeittäin muodostuu yksityisen ja julkisen tiedon kategorioista[33]. Sosiaalisessa mediassa yksityiset tiedot muodostuvat sovelluksen käyttäjän henkilökohtaisista tiedoista, jotka ovat yleisesti suojattua tietoa. Julkisen tiedon kategoria käsittää suojaamatonta, julkaistua informaatiota.

Informaatiolähteen tunnistaminen perustuu luottamuksellisen ja julkisen tiedon kategorioihin. Luottamukselliset tiedonlähteet koostuvat tiedoista, joita voidaan luovuttaa tarkasteltavaksi ilman julkaisuoikeutta. Avoimet tiedonlähteet koostuvat yksityishenkilöistä tai ryhmistä, jotka jakavat tietoa julkiseen käyttöön[34]. Tutkimuksen kannalta sosiaalinen media toimii tarkastelukohteena informaatiolähteiden suhteen.

Tiedonkeruumetodin valinta. Tiedonkeruulla tarkoitetaan raakadatan ja informaation keräämistä, josta muodostetaan karsinnan ja analysoinnin kautta käytettävää tietoa. Metodeilla tarkoitetaan erityisiä informaatiopyyntöjä, tavoitteita, prioriteetteja, tiedostetun toiminnan tai tapahtuman aikataulua, viimeisintä käyttöpäivämäärää, jolloin tiedolla on vielä arvoa ja rapor-

[30] Headquarters Department of the Army: *Open Source Intelligence 2012*, Army Technique Publication No. 2-22.9, Washington DC, 2012, s. 2.
[31] Headquarters Department of the Army (2012), s. 23.
[32] Sama, s. 23.
[33] Sama, s. 24.

tointiohjeita.[35] Sosiaalisen median sovellusten kannalta tarkastellaan päivityksiä, kuvia, GPS-dataa ja muuta analysoitavaa raakaa dataa.



Kuva 3: OSINT tiedonkeruuprosessi.[36]

Neliosainen prosessi mahdollistaa tutkimustyön aloittamisen. Tutkimustyö mahdollistaa tietokantojen muodostamisen, joilla voidaan muodostaa haluttu tilannekuva sekä ymmärtää tiettyjä trendejä. Sosiaalisen median kontekstissa tämä voi tarkoittaa Facebookin ja Twitterin tilannepäivitysten merkittävyyttä, moraalin muutosta sidottuna aikaan sekä kuvia ja tietoja liittyen tehtäviin. Tässä vaiheessa prosessia muodostetaan tutkimuskysymys (mitä vastustaja haluaa selvittää), tutkimussuunnitelma sekä tutkimuksen käynnistäminen.[37]

Kuva 4 osoittaa avoimen lähteiden tiedustelun mahdollistamat tiedustelukanavat ja keinot. Tutkielmassa avoimen lähteiden tiedustelua tarkastellaan internetsivustojen ja sosiaalisen median alueelta, joka kuvaajassa on merkitty punaisella ruudulla. Internettiedustelun neljä tärkeintä osa-aluetta ovat viestintä (communications), tietopankit (databases), informaatio/tieto (information) ja palvelut (services).

[34] Sama, s. 25.
[35] Headquarters Department of the Army (2012), s. 25.
[36] Sama, s. 24.
[37] Sama, s. 26.

Media	Components	Elements	
Public Speaking	Speaker	• Sponsor • Relationship	• Message
	Format	• Conference • Debate • Demonstration • Speeches	• Lecture • Rally • Loud speakers • Talk shows
	Audience	• Location	• Composition
Public Documents	Graphic	• Drawing • Engraving • Painting • Graffiti	• Photograph • Print • Posters
	Recorded	• Compact data storage device • Digital video disk	• Hard disk • Tape
	Printed	• Book • Brochure • Newspapers • Magazines • Government releases • "Dumpster diving" • Annuals	• Periodical • Pamphlet • Report • Novelties • Non-government releases • Leaflets • Business cards
Public Broadcasts	Radio	• Low frequency AM radio • Medium frequency AM radio • Short wave radio	• VHF FM radio • Satellite radio • Standard wave radio
	Television	• Ku band satellite television • VHF and UHF terrestrial television • Advertisements	
Internet Web Sites	Communications	• Chat • E-mail • News; newsgroup	• Web cam • Web cast • Web log
	Databases	• Commerce • Education	• Government • Military organizations
	Information (Web page content)	• Commerce • Education	• Government • Military organizations
	Services	• Dictionary • Directory • Downloads • Financial	• Geospatial • Search and URL lookup • Technical support • Translation
FM frequency modulation UHF ultrahigh frequency		VHF very high frequency	

Kuva 4: OSINT tiedon tuottaminen.[38]

Viestinnällä pyritään kartoittamaan tietoa chat-, sähköposti-, ja uutiskirje liikenteestä, sekä webkamera, webcast ja weblog käytöstä. Näistä tärkeimmät käyttäjän näkökulmasta ovat sähköposti- ja kamerasovellusten tiedot, joita älypuhelimien käyttäjät jakavat. Esimerkkinä tästä mm. tilannekuvat joukkojen perustamisvaiheessa kun siirrytään panssaroiduissa miehistönkuljetusajoneuvoissa väistöalueella ja sähköpostiviestit ystäville ja perheelle, joissa voi käydä ilmi esimerkiksi missä henkilö on ja minne on menossa.

Tietopankit ja informaatio jakautuvat taloudellisiin, sotilaallisiin, valtiollisiin ja opetuksellisiin tietokantoihin. Näistä tärkeimmät tiedustelun kannalta ovat sotilaallisten tietokantojen murtaminen, joka rajautuu tietokantojen osalta tämän tutkimuksen ulkopuolelle, koska ei ole sosiaalisen median alle soveltuva käsite.

[38] Headquarters Department of the Army (2012), s. 27.

Palveluilla pyritään selvittämään eri internetpohjaisten palveluiden käyttöä, joista ilmenee tiettyjä trendejä. Näihin palveluihin kuuluu mm. sanakirjat, luettelot, tiedostojen lataushubit, taloudelliset palvelut ja URL-lähteet.

3.2.2 OSINT työkalut

Avointen lähteiden tiedusteluun on mahdollista käyttää tuhansia ilmaisia sekä kaupallisia palveluja. Työkalujen laajuuden puitteissa tutkimukseen on valittu muutama keskeinen esimerkki, jonka kautta luodaan ymmärrys miten avoimia lähteitä voidaan hankkia.

Wayback machine kykenee etsimään internetsivustoja, jotka on poistettu käytöstä.

Who.is mahdollistaa tietyn henkilön tunnistamisen sivuston informaation, liikenteen ja sen historian analysoinnin sekä DNS arkistojen kautta.

Maltego rakentaa haetusta tiedosta kirjaston ja luo visuaalisen analysointimallin, jolla on mahdollista toteuttaa internetlinkkianalyysiä sekä datalouhintaa. Maltego mahdollistaa ihmisten, ryhmien, yritysten, organisaatioiden, tietojen ja monen muun tiedon yhdistämisen.

IP Location mahdollistaa IP osoitteiden huomaamattoman paikantamisen ja ilmaisee käyttäjän tiedot, joihin kuuluu: maa, lääni, kaupunki, koordinaatit, aikavyöhyke, liitynnän nopeus ja monia muita piirteitä.

Social mention tuottaa reaaliaikaista sosiaalisen median yhteisöpalveluiden analysointia, kuten Twitter, Facebook, YouTube, ja Google.

Google ja monet muut vastaavat hakukonepalvelut mahdollistavat laajamittaisen yleisen tiedonhankinnan internetsivustoilta.

3.3 Pohdinta sosiaalisen median ja avointen lähteiden tiedustelun muodostamasta uhkakuvasta

Vastustaja pyrkii käyttämään sosiaalisen median toimintaympäristöä kerätäkseen tietoa (Open Source Intelligence - OSINT) sekä vaikuttaakseen joukkoihin fyysisesti tuli-iskulla, elektronisesti häirinnällä, tiedustelemalla tai suorittamalla psykologisia operaatioita. Tiedonkeruun mahdollistaa avointen lähteiden tiedonkeruukonsepti (OSINT). Avointen lähteiden tiedustelumenetelmän avulla vastustaja pyrkii selvittämään paikkatiedot, joukkojen kokoonpanon ja kaluston, toimintatavat ja taktiikan sekä tehtävän. Vaikka avointen lähteiden tiedustelua käytetään lähtökohtaisesti strategisen tason toimintaa ajatellen, on syytä ottaa huomioon tiedustelu myös taisteluosaston kokoisessa kokoonpanossa. Kerätyn tiedon kautta vastustaja pyrkii muodostamaan tilannekuvan, tuottamaan tietopalveluita joukoilleen sekä vaikuttamaan joukkoihin sosiaalisen median kautta esimerkiksi psykologisen sodankäynnin vaikutuksella.[39]

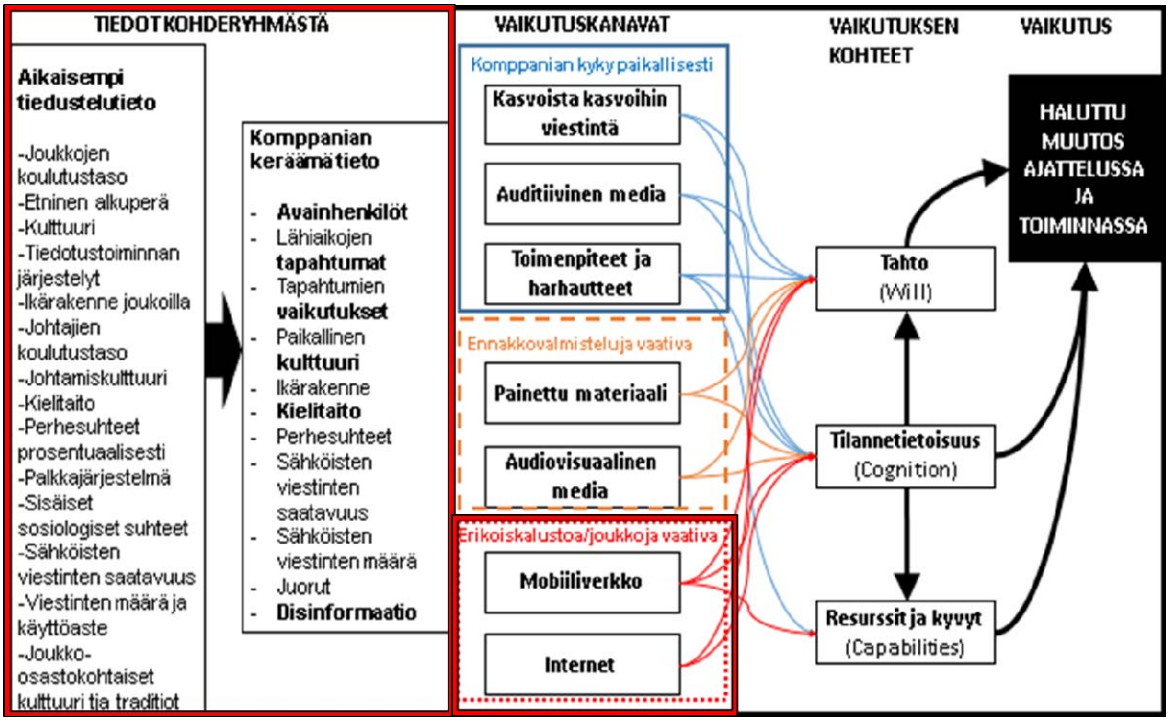
Viitaten liitteeseen 2, sosiaalisen median uhkakuvat muodostuvat vihollisen ensisijaisista tarpeista. Ymmärtääksemme näitä uhkia, on ymmärrettävä vastustajan aikeet ja tavoitteet; mitä vastustaja pyrkii saamaan aikaan? Sosiaalisen median näkökulmasta voidaan vaikuttaa tai kerätä tietoa. Vaikuttaminen liittyy vahvasti psykologiseen sodankäyntiin, jolla pyritään aktiivisesti vaikuttamaan vastustajan taistelutahtoon, päätöksentekoon sekä levittää disinformaatiota. Vaikutus voi olla myös fyysistä, esimerkiksi ohjusisku kriittiseen kohteeseen tai joukkojen keskittäminen uudelle alueelle.

Vastustajan tavoitteena on kerätä tietoa psykologisia operaatioita tai tärkeiden kohteiden ja joukkojen maalittamista varten tai tuottaa tilannekuvaa ja ymmärrystä valmiustilasta. Näihin tietoihin sisältyy **paikkatiedot** (GPS, koordinaatit, ryhmitys), **kokoonpanot** (osaston vahvuus, kalusto, määrä ja laatu), **taktiikan ja käytännön ymmärrys** (taktiikka, rutiinit, miten joukot toimivat ja käyttäytyvät), sekä mikä **tehtävä** (puolustus, hyökkäys, koulutus, suojaus) eri joukoilla on. Tiedot on saatavilla sosiaalisessa mediassa tilanneilmoitusten, viestiketjujen ja kuvien muodossa. Paikkatieto ilmenee GPS-datana, jota esimerkiksi Facebook käyttää tilapäivityksen yhteydessä. Lisäksi älypuhelimien kameroiden ottamissa kuvissa on usein automaattisesti Geotagging-ominaisuus, joka sisällyttää kuvan tiedostoon paikkatiedot jopa koordinaattien tarkkuudella.[40]

---

[39] Headquarters Department of the Army (2012), s. 23.
[40] *BBC News*, US Army: Geotagged Facebook posts put soldiers' lives at risk, 9.3.2012, http://www.bbc.co.uk/news/technology-17311702, 14.12.2013.

Tiedustelun lähtökohtana on aikaisemman tiedustelutiedon kartoittaminen ja trendien luominen. Kuva 6 osoittaa mitä psykologisen sodankäynnin operaatioissa tarkastellaan taktisella tasolla. Kuva on ote psykologisen sodankäynnin vaikutuksista rauhanturvausoperaatioissa. Kuvassa punaiset viivat rajaavat tarkastelun avointen lähteiden tiedustelun tarkastelussa pelkästään tiedustelun ja informaation käyttöön. On olennaista kartoittaa ja käyttää vanhaa tietoa jo olemassa olevista tietokannoista, jotta voidaan perustaa lähtökohta uuden tiedon keräämiselle ja tarkastelulle. Kuvan tärkein osio, ”komppanian keräämä tieto” on vastustajalle tärkeää tietoa. Vaikka kuva on räätälöity rauhanturvausoperaatioihin, joissa joukkojen määrä on merkittävästi pienempi verrattuna Suomen kriisinajan perustettaviin joukkoihin ja toimintaympäristö erilainen joukkojen perustamisvaiheessa, on sen vaikutus yhtä oleellinen myös tutkimuksen kannalta.



Kuva 6: Psykologiset operaatiot taktisella tasolla rauhanturvausoperaatioissa.[41]

[41] Kilpeläinen, Lauri: *Psykologiset operaatiot kriisinhallinnan toimintaympäristössä, ISAF, Afganistan*, 2014.

4 ESIMERKKITAPAUKSET JA OPITUT ASIAT

Tutkielman esimerkkitapaukset ja opitut asiat osiossa tarkastellaan kolmea erilaista sosiaalisessa mediassa konkreettista vaikutusta joukkojen operaatioturvallisuuteen. Esimerkit sitovat operaatioturvallisuuden (OPTU), sosiaalisen median (SOME) ja avointen lähteiden tiedustelun (OSINT) toimintaympäristöt ja käyttöperiaatteet yhteen. Esimerkit mahdollistavat käsitteiden tarkastelun käytännön tasolla ja avaavat näkemyksen operaatioturvallisuuden sekä sosiaalisen median merkityksestä modernissa sodankäynnissä.

4.1 Esimerkkitapaus 1: GEOTAG-ominaisuus paljastaa Apache helikoptereiden paikan

Vuonna 2007 neljä Yhdysvaltalaista AH-64 ”Apache” helikopteria tuhottiin Irakissa käyttäen älypuhelimen kuvien Geotag-ominaisuutta. Helikoptereissa matkustaneet sotilaat ottivat itsestään ja helikoptereista kuvia asematason ja hallien alueella. Kuvat ladattiin sosiaalisen median sovellukseen, jonka metatiedostoja tutkimalla vastustaja paikansi helikoptereiden tarkan sijainnin lentotukikohdan sisällä. Tietoa käyttäen vastustaja suoritti tuli-iskun heittimillä tuhoten helikopterit.[42]

Esimerkkitapaus paljastaa suuren haavoittuvuuden älypuhelimien kautta jaettavasta mediasta. Tätä kautta videot, kuvat ja muut jaetut tiedostot voivat sisältää paikkatietoa metatiedon sisällä. Käyttäjällä on mahdollisuus kontrolloida GPS-signaalin käyttöä tiettyyn pisteeseen asti, mutta jotkut sovellukset voivat käyttää GPS-tietoa ilman käyttäjän lupaa tai tämän tiedostamatta.

4.2 Esimerkkitapaus 2: Facebook päivitys pysäyttää operaation

Israelilainen tykistön ampuja jakoi operaatiosuunnitelmat koskien IDF:n (Israel Defence Forces) iskua Länsirannan alueella, Palestiinan Ramallah kaupungin lähettyvillä. Tiedot Qatannan kylän operaatiosta oli julkaistu käyttäjän toimesta hänen Facebook sivustollaan. Sotilas kommentoi tietojen yhteydessä: ”Keskiviikkona siistimme Qatannan ja torstaina, jumalan armosta, pääsemme kotiin”. Sotilaan Facebook-sivustolla oli julkaistu tietoja hänen yksiköstään sekä tarkat operaatioon liittyvät kohteet sidottuna aikaan. Saman yksikön muut sotilaat huo-

[42] Reed, John: Used Cell Phone Geotags to Destroy AH-64s in Iraq, *Defencetech*, 15.3.2012, http://defensetech.org/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq/#ixzz1pDRqzKSB, 18.12.2013.

masivat operaatioturvallisuusrikoksen ja raportoivat tästä esimiehilleen. Saatuaan tiedon divisioonan komentaja päätti peruuttaa operaation vedoten tiedon päätymiseen vihamielisille ryhmille, jotka käyttäisivät tietoa Israelin puolustusvoimia vastaan. Operaatioturvallisuusrikkomuksesta sotilaalle lankesi 10 päivän vankeusrangaistustuomio, hänet poistettiin pataljoonasta ja häneltä evättiin kaikki oikeudet sotilaallisiin tehtäviin.[43]

Israelilaisen sotilaan esimerkkitapaus osoittaa sosiaalisen median vääränlaisen käytön olevan erittäin todellinen ja suuri uhka operaatioturvallisuudelle. Yksittäinen taistelija vaikutti omalla toiminnallaan koko divisioonan operaatioon, sekä vaaransi muiden sotilaiden hengen. Tapaus myös osoittaa, että on syytä tarkastella operaatioihin koskevan tiedon levittämistä vain tietyille henkilöillä nk. ”need to know basis”-menetelmällä.

4.3 Esimerkkitapaus 3: Facebook viesti rikkoo jokaista operaatioturvallisuuden kohtaa

Tunnettu sotilasjournalisti Michael Yon julkaisi kesällä 2010 Facebook sivuillaan saamansa viestin Afghanistanissa palvelevalta sotilaalta (ks. liite 1), jossa rikotaan jokaista operaatioturvallisuuteen liittyvää kohtaa. Viestin sisällöstä ilmenee joukkojen liikkeet, ja sen toiminta-alue, yksikön tunnus, vastustajan hyökkäysten teho, puolustavan joukon järjestelmien viat, joukkojen reagointiajat, turvallisuuden kannalta heikot kohdat, sekä tukikohdan puolustusjärjestelyt.[44]

Julkaisu herätti kiihkeää keskustelua operaatioturvallisuudesta Facebookissa. Suuri huolenaihe oli anonyymin sotilaan välinpitämättömyys operaatioturvallisuuden suhteen julkaistessaan tukikohdan puutteet tunnetulle journalistille. Myös journalistin päätöstä kritisoitiin, sillä vaikka tarkoituksena oli saada aikaan nopeita toimia tukikohdan turvallisuuden korjaamiseksi, tieto oli silti liian tuoretta ja helposti saatavilla, mikä nostatti turhaa paniikkia alueella palvelevien omaisten keskuudessa.[45]

[43] *ABC News*, Soldier posts military plans on Facebook, 4.3.2010, http://www.abc.net.au/news/2010-03-04/soldier-posts-military-plans-on-facebook/350284, 18.12.2013.
[44] *War on Terror News*, Yon OPSEC Violations, 2.10.2011, http://waronterrornews.typepad.com/ps/2011/02/yon-opsec-violations.html ja http://waronterrornews.typepad.com/.a/6a00e551d9d3fd88330147e275cfed970b-popup, 18.12.2013.
[45] Yon, Michael: A Soldier Emails from Afghanistan, 12.6.2010, https://www.facebook.com/MichaelYonFanPage/posts/118317618212252, 18.12.2013.

4.4 Opitut asiat

Opitut asiat osio pyrkii vastaamaan esimerkkitapausten operaatioturvallisuuden ongelmiin sosiaalisessa mediassa esittämällä ratkaisuja sekä menetelmiä, jotka ovat muodostuneet rikkeiden seurauksina. Esimerkkitapaukset osoittavat kuinka merkittävästi sosiaalinen media voi vaikuttaa operaatioturvallisuuteen. Esimerkkitapausten perusteella mahdollisiin menetyksiin ja uhkiin voidaan lukea asejärjestelmien tuhoutuminen; paikkatiedot helposti saatavilla GPS- ja metadatan kautta kuvissa, video ja äänitiedostoissa; operaatiosuunnitelmien ja aikataulujen julkaiseminen; ja joukkojen liikkeet, toiminta-alue, yksikön tunnus, vastustajan hyökkäysten tehon, puolustavan joukon järjestelmien viat, joukkojen reagointiajat, turvallisuuden kannalta heikot kohdat sekä tukikohdan puolustusjärjestelyt.

Edellä mainituilta uhilta voidaan välttyä usealla tavalla. Ensimmäisessä tapauksessa käsiteltiin Yhdysvaltojen Apache taisteluhelikoptereihin kohdistunutta hyökkäystä yksinkertaisen Geotag-ominaisuuden takia[46]. Tapahtumien jälkeen Yhdysvaltojen asevoimat ovat keskittyneet entistä enemmän kampanjoimaan sosiaalisen median hyödyistä, haitoista ja uhista niin palveluksessa oleville kuin myös heidän omaisilleen. Kampanjointia suoritetaan niin sosiaalisessa mediassa kuin työpaikoillakin mm. sosiaalisen median käyttöoppaan muodossa.[47]

Toisessa esimerkissä käsiteltiin israelilaisen sotilaan julkaisemaa operaatioon liittyvää tietoa ja aikataulua, joka johti operaation peruuttamiseen. Tapahtuma synnytti Israelin puolustusvoimissa uutta kannanottoa sosiaalisen median ja älypuhelimien käyttöön operaatiotehtävissä oleville. Lopputuloksena oli hyvin yksinkertainen ratkaisu: kaikki sosiaaliseen mediaan liittyvä toiminta on ankarasti kiellettyä. Tämän lisäksi perustettiin osasto levittämään myönteistä propagandaa Israelin puolustusvoimien toiminnasta, sekä poistamaan ja kontrolloimaan internetissä julkaistua huonoa propagandaa. Toinen perustettava osasto sai tehtäväkseen tarkkailla ja tiedustella Israelin puolustusvoimien henkilökunnan ja sotilaiden toimintaa sosiaalisessa mediassa, antaen valtuudet tarkkailuun, raportointiin sekä vastatoimenpiteisiin.[48,49]

---

[46] BBC News, US Army: Geotagged Facebook posts put soldiers' lives at risk, 9.3.2012, http://www.bbc.co.uk/news/technology-17311702, 19.12.2013.
[47] *Online and Social Media Division*: The United states Army Social Media Handbook Version 3.1. 2013, http://www.25idl.army.mil/Social_media_handbook.pdf, 19.12.2013.
[48] ArabCrunch, "Israel's" army bans its soldiers from using facebook, Twitter and other social media sites, 12.7.2011, http://arabcrunch.com/2011/07/israels-army-bans-its-soldiers-from-using-facebook-twitter-and-other-social-media-sites.html, 19.12.2013.
[49] *Times of Israel*, IDF plans social media clampdown for soldiers, 7.6.2013, http://www.timesofisrael.com/idf-plans-social-media-clampdown-for-soldiers/, 19.12.2013.

Kolmannessa esimerkissä esiteltiin klassinen tapaus operaatioturvallisuuden laiminlyömisestä. Tapauksessa turhautunut sotilas ilmiantoi oman tukikohtansa turvallisuuspuutteet julkisesti. Tapauksella olisi voinut olla kriittisiä seurauksia, sillä vastustaja olisi helposti voinut lukea julkista tietoa Michael Yonin sivuilla, joka on hyvin tunnettu Afganistanissa toimiva journalisti. Toisaalta tieto oli laadultaan sellaista, jota vastustaja (Taleban) pystyy omatoimisesti selvittämään mm. kokeilemalla eri toimintatapoja kellottamalla tai yleisellä tiedustelulla.

Tulevaisuuden sosiaalisen median uhkakuvat pysyvät todennäköisesti samanlaisina, jos ihmisten verkkokäyttäytyminen pysyy samalla tasolla ja internetin käyttötarve yhä kasvaa. Vaikka sosiaalisen median palveluista Facebook ja Twitter ovat vuoteen 2014 mennessä onnistuneet luomaan laajan globaalin yhteisöpalvelun, on todennäköistä että näistä molemmat tullaan korvaamaan jollain muulla palvelulla tulevaisuudessa. Näistä tulevaisuuden palveluista löytyy todennäköisesti samanlaiset erityispiirteet, jotka mahdollistavat sanomien, kuvien, videon, paikkatiedon ja sähköisten tiedostojen entistä helpomman ja reaaliaikaisemman jakamisen. Sosiaalinen media on kasvava trendi, joka ei ole poistumassa yhteiskunnan laajamittaisesta käytöstä. Täten tulevaisuudessa on otettava huomioon suhtautuminen sen aiheuttamaan riskiin operaatioturvallisuudelle.

5 JOHTOPÄÄTÖKSET

5.1 Pohdinta

Sosiaalinen media on suosittu julkinen median toimintaympäristö, josta suurimpana käyttäjäryhmänä ovat nuoret aikuiset. Sosiaalisen median eri sovelluksia ja palveluita käytetään globaalisella tasolla ja sen toimintaympäristö kokonaisuudessaan tulee vahvistumaan entisestään lähitulevaisuudessa. Sosiaalinen media on myös turvallisuusriski ja konkreettinen osa modernia operaatioturvallisuusajattelua. Kappaleen 4 esimerkit osoittavat vain murto-osan mahdollisista uhista operaatioturvallisuuden kannalta.

Avointen lähteiden tiedustelu itsessään on suhteellisen vanha konsepti, mutta sosiaalisen median aikakaudella johdosta on avautunut uusia mahdollisuuksia ja lähteitä OSINT-tiedustelumenetelmälle. Sosiaalisen median yhteisöpalvelut mahdollistavat suurien internetpohjaisten tietokantojen tarkkailun helposti ja ilmaiseksi. Vaikka käyttäjä pystyy rajoittamaan itse tiedon julkisuutta ja näkyvyyttä on osoitettavissa, että turvallisuutta laiminlyödään yleensä tiedostamatta. Tämä osoittaa sosiaalisen median olevan tärkeä ja huomioitava osa operaatioturvallisuutta nykysodankäynnissä. Puutteellinen operaatioturvallisuus suhteessa sosiaaliseen mediaan voi mahdollistaa vastustajan avointen lähteiden tiedustelutoimintaa. Avointen lähteiden tiedustelutoiminta voi johtaa johtamiskyvyn häirintään, lamauttamiseen tai tuhoamiseen, väärien tietojen tarkoitukselliseen tuottamiseen; vastustajan johtamistoiminnan suuntaamiseksi halutulla tavalla, taistelutahdon tai moraalin vaikuttamiseen, elektroniseen sodankäyntiin, fyysiseen tuhoamiseen, harhauttamiseen ja muihin vaikutuksiin operaatioalueella.

5.2 Haastattelut

Tutkielman teoriapohjan ja tutkimuskysymysten kautta muodostettiin haastatteluita varten syventävät kysymykset. Haastattelukysymysten (liite 3) tavoitteena on syventää tutkijan ymmärrystä sosiaalisen median toimintaympäristöstä, älypuhelimien riskeistä ja operaatioturvallisuuden suhteesta sosiaaliseen mediaan. Tutkija haastatteli Puolustusvoimien operaatioturvallisuuden asiantuntijaa Majuri Ville Porrasta sekä F-Securen tietoturvapäällikköä Camillo Särsia. Haastattelun yhteydessä esiteltiin myös alaluvun 5.3 kolme toimintavaihtoehtoa joihin haastateltavat ottivat kantaa. Haastatteluissa käyty keskustelun pohjalta voidaan todeta seuraavat alla olevat piirteet, jotka täydentävät tutkimusta sekä johtopäätöksiä.

Mainosyritykset pyrkivät profiloimaan kaikkia älypuhelimien käyttäjiä käyttäen mainosbannereita eri internetsivustoissa. Näitä painamalla käyttäjä lähettää tiedostamatta omia tietoja, joita mainosyritykset käyttää profiloimaan käyttäjää ja tämän suhdetta muihin käyttäjiin ja verkostoihin. Mainosohjelmat pystyvät poimimaan käyttäjän ainutlaatuisen tunnisteen, puhelinnumeron, IMEI tunnisteen, sähköpostin ja GPS datan. Täten mainosohjelmat mahdollistavat kohteiden tiedustelun sekä laajamittaisen verkoston rakenteen eri käyttäjien välillä. Tämä tarkoittaa sitä, että yhden käyttäjän paljastuttua vastustajan tiedustelun kautta myös muutkin käyttäjät voivat paljastua.[50]

Android käyttöjärjestelmät ovat edelleen suurin uhka muihin järjestelmiin verrattuna. Suomessa uhka on vielä tilastollisesti pieni, mutta Venäjällä tämä on todettu suureksi ongelmaksi, koska käyttäjät ostavat ja lataavat tiedostoja virallisten ja turvallisten verkkokauppojen ulkopuolelta. IOS on turvallisempi järjestelmä, koska käyttäjä ei pysty ostamaan tai lataamaan tietoja Applen verkkokaupan ulkopuolelta. Toisaalta on mahdollista ohjata käyttäjä linkkien kautta haitalliselle sivulle, jonka kautta voidaan ottaa älypuhelin hiljaisesti haltuun.[51]

Haastateltavat toteavat, että sosiaalinen media on propagandan ja viestinnän kanava. Tätä kautta on mahdollista ylläpitää sosiaalinen yhteys ystäviin ja kotiin, sekä hoitaa muita tärkeitä asioita. Operaatioturvallisuuden näkökulmasta olisi syytä aloittaa joukkojen perustamisvaiheen aikana laajamittainen viestintä kampanja, jossa todetaan mitä kanavia saa käyttää. Tämän lisäksi tulisi määrittää toimintaohjeet älypuhelimien ja sosiaalisen median käytön suhteen, johon myös sisältyvät mahdolliset kurinpitomenetelmät. Lisäksi Puolustusvoimien tulisi keskittää voimavaroja sosiaalisen median hallitsemiseen, eli olla aktiivinen osa toimintaympäristöä. Tämä kokonaisuus muodostaisi myös sisäisen paineen yhteisössä, joka tiettyyn pisteeseen asti kykenee ylläpitämään ryhmäkuria sosiaalisen median käytön suhteen. On tärkeää selvittää, onko Puolustusvoimilla tarpeeksi joukkoja valvomaan verkkoja, joilla olisi toimintakykyä suunnitteella ja toteuttaa myös ennaltaehkäisevää toimintaa.[52,53]

[50] Särs Camillo, F-Securen tietoturvapäällikkö, älypuhelimiin liittyvät tietoturvauhat ja operaatioturvallisuus sosiaalisessa mediassa, haastattelu 7.3.2014, materiaali kirjoittajalla.
[51] Sama, 7.3.2014.
[52] Sama, 7.3.2014.
[53] Porras Ville, majuri, Täydennyskoulutus- ja kehittämiskeskus (TKKK), älypuhelimiin liittyvät tietoturvauhat ja operaatioturvallisuus sosiaalisessa mediassa, haastattelu 6.3.2014, materiaali kirjoittajalla.

Operaatioturvallisuuden suhteen haastateltavat totesivat, että sosiaalisen median täyskielto on mahdottomuus. Sosiaalinen media on vahva osa nykyajan toimintatapoja ja käytön kieltäminen tuottaisi ongelmia moraalin suhteen. Tämän lisäksi sosiaalisen median käyttöä on vaikeaa valvoa. Molemmat haastateltavista tukivat kolmen vaihtoehtoisen toimintamallin yhdistelmäratkaisua. Sosiaaliseen mediaan tulisi olla käyttöoikeus, mutta ei operaation aikana. Tämä tarkoittaisi esimerkiksi valvottuja ja suojattuja päätelaitepisteitä esimerkiksi joukko-osastoihin sidottuna. Näiden ulkopuolella sosiaalisen median käyttö olisi kiellettyä.[54,55]

5.3 Kolme vaihtoehtoista toimintamallia

Joukkojen perustamisvaiheessa on useita vaihtoehtoja, joilla suojaudutaan vihollisen avointen lähteiden tiedustelulta sekä rajoitetaan omien joukkojen sosiaalisen median väärinkäyttöä. Ensimmäinen vaihtoehto on rajoittaa omien joukkojen pääsyä sosiaaliseen mediaan asettamalla halutut sosiaalisen median palvelut käyttökieltoon valtakunnallisesti, sekä vahvistaa kieltoa rangaistusmenetelmillä. Tämä vaatii yhteistoimintaa maassa toimivien teleoperaattorien kanssa. Tämä vaihtoehto ei ole aukoton, sillä eri sovelluksilla ja konfiguraatioilla on mahdollista kiertää sovellusestot. Tätä vaihtoehtoa ei ole tutkijan tiedon mukaan vielä kokeiltu.

Tämän lisäksi on huomioitava, että vaikka sosiaalisen median eri yhteisöpalvelut estettäisiinkin, on paikka- ja henkilötiedot silti tiedusteltavissa SIGINT (Signal Intelligence) muodossa. Älypuhelimet ja muut mobiililaitteet lähettävät paikkatietoaan operaattorille/tukiasemalle tietyin väliajoin. Tätä signaalia on mahdollista tiedustella, etenkin jos teleoperaattorit ovat vastustajan hallussa tietoisesti tai tiedostamatta. Esimerkkinä voidaan mainita Iranin suorittama signaalitiedusteluoperaatio Syyriassa vuonna 2006, jolla tuettiin Hizbollahin iskuja Libanonin konfliktissa. Israelilaisten viestien salausta ei tiettävästi ollut purettu tai viestejä vastaanotettu, mutta sotilaiden henkilökohtaiset mobiilipuhelimet antoivat ilmi joukkojen kokoontumispaikat, joista oli mahdollista päätellä hyökkäyssuunnat ja ajankohdat.[56]

[54] Porras Ville, majuri, Täydennyskoulutus- ja kehittämiskeskus (TKKK), älypuhelimiin liittyvät tietoturvauhat ja operaatioturvallisuus sosiaalisessa mediassa, haastattelu 6.3.2014, materiaali kirjoittajalla.
[55] Särs Camillo, F-Securen tietoturvapäällikkö, älypuhelimiin liittyvät tietoturvauhat ja operaatioturvallisuus sosiaalisessa mediassa, haastattelu 7.3.2014, materiaali kirjoittajalla.
[56] Darlene Storm, Pocket Spies: Smartphone actionable intelligence, *Computer World*, 29.11.2011 http://blogs.computerworld.com/19348/pocket_spies_smartphone_actionable_intelligence, 20.12.2013.

Toinen vaihtoehto on kieltää älypuhelimet, mobiililaitteet ja muut elektroniset laitteet joilla on mahdollista tuottaa ja jakaa kuvia, videoita tai muuta mediaa sosiaalisessa mediassa. Käytännössä tämä voisi tarkoittaa näiden laitteiden kieltämistä käskykorttien yhteydessä etukäteen, sekä laitteiden takavarikoimista joukkojen perustamisvaiheen yhteydessä. Tämä käytäntö poistaisi sosiaalisen median uhan operaatioturvallisuudelle kokonaan. Taktisesti tämä vaihtoehto on kannattavin, sillä riskit minimoidaan kokonaan, ja se on perusteltavissa tutkielman kolmen eri esimerkkilopputuloksien suhteen. Tästä huolimatta on huomautettava, että joukkojen taistelutahdon ja psyykkeen ylläpitämiseksi on suositeltavaa luoda myönteinen ja salliva linjaus sosiaalisen median käytön suhteen. Sosiaalinen media toimii erittäin vahvana nykyajan tunteiden ja yhteenkuuluvuuden tekijänä. Sen kieltäminen voi aiheuttaa negatiivista ilmapiiriä taisteluosaston sisällä. IDF (Israel Defence Forces) on ottanut käytäntöön tämän vaihtoehdon vaihtelevalla menestyksellä.

Kolmas vaihtoehto on luoda myönteinen ilmapiiri sosiaalisen median käyttöön Puolustusvoimissa. Operaatioturvallisuutta ylläpidetään ja tehostetaan laajamittaisella ja tehokkaalla sosiaalisen median kampanjalla sekä Puolustusvoimien organisaation muodostamalla tukitoiminnalla. Tämä konsepti vaatii sosiaalisen median ja operaatioturvallisuuden koulutusta henkilökunnalle ja varusmiehille. Konsepti tulisi sisällyttää sosiaalisen median ja avointen lähteiden tiedustelu-ohjesääntökirjan, jota jaetaan henkilökunnalle sekä varusmiehille, ja joka on saatavilla mm. Puolustusvoimien virallisilta verkkosivuilta sekä joukko-osastojen virallisilta sosiaalisen median kanavilta. Yhdysvaltojen asevoimat ovat ottaneet tämän käytännön käyttöön vaihtelevalla menestyksellä. Ohjetta päivitetään vuosittain ja se on sisällöltään laadukas. Operaatioturvallisuutta sosiaalisessa mediassa käsitteenä on nähtävillä USA:n eri varuskuntien omilla sivuilla, Facebookissa sekä muilla foorumeilla, eteenkin palvelevien sotilaiden puolisoiden toiminnassa.[57]

Sosiaalisen median täyskielto, jota Israelin puolustusvoimat ovat toteuttaneet, on taktiselta kannalta turvallisempi. Kun kielletään älypuhelimien käyttö rangaistuksen uhalla, pienenee käyttöriski lähes olemattoman pieneksi. Täyskiellon haittavaikutuksena on moraalin ja psyykkisen hyvinvoinnin potentiaalinen lasku joukoissa. Tämä on perusteltavissa yksilön tarpeella viestiä sekä jakaa elämäänsä ystävien, läheisten ja perheen kanssa. Kun keino täyttää tarve poistetaan, on mahdollista että syyt taistella katoavat.

[57] Dao, James: Military Announces New Social Media Policy, *The New York Times*, 26.2.2010,http://atwar.blogs.nytimes.com/2010/02/26/military-announces-new-social-media-policy/?_r=0, 20.12.2013.

Toisaalta Yhdysvaltojen asevoimien soveltama avoin lähestymistapa sosiaalisen median käyttöön ei ole aukoton. Vaikka Yhdysvaltojen asevoimat ovat laatineet ja jalkauttaneet sosiaalisen median toimintatavat joukoille, on luottamus yksittäiseen taistelijaan valtava. Sosiaalisen median kampanjointiin, ohjeistamiseen, tukemiseen sekä valvomiseen on panostettu erittäin paljon. Tämän huomaa valtavalla asevoimien läsnäololla Facebookissa ja Twitterissä.

5.4 Päätelmä

Edellä mainittujen näkökulmien varjossa on todettava, että ratkaisu sosiaalisen median luomaan turvallisuusriskiin riippuu strategisen tason päätöksistä. Jos päätös on tehtävä strategisella tasolla, niin turvallisin vaihtoehto operaatioturvallisuuden näkökulmasta on sosiaalisen median täyskielto, sekä sen mahdollistaman elektroniikan kieltäminen ja takavarikointi. Taktisesta näkökulmasta katsottuna tilanteessa, jossa taisteluosaston komentajalla on mahdollisuus päättää itse sosiaalisen median käytöstä omassa osastossaan, on mahdollista soveltaa sääntöä kolmen edellä mainitun vaihtoehdon väliltä.

Suomen reserviläisikäisestä väestöstä n. 70 % omistaa älypuhelimen ja 75 % näistä käyttää sosiaalisen median sovelluksia sekä yhteisöpalveluita päivittäin. On todettavissa, että taisteluosastossa käyttäjämäärä sekä käyttötarpeet ovat keskimäärin samanlaiset kuin keskivertokansalaisellakin. Jos taisteluosaston organisaatioon kuuluu n. 2500 taistelijaa, tarkoittaa tämä sitä, että n. 1750 taistelijaa omistaa älypuhelimen, ja näistä n. 1300 on päivittäin sosiaalisessa mediassa, jos mahdollista. Täten yksittäisen taistelijan operaatioturvallisuuden laiminlyönti on todellinen riski, sillä käyttäjien määrän kasvaessa riski kasvaa samalla kuin kontrolli heikkenee.

Riski kasvaa käyttäjämäärän lisäksi myös käyttäjien älypuhelinten osaamisen tason takia. Suurella osalla voi olla paikantamispalvelut koko ajan käytössä, koska käyttäjät eivät vielä tiedosta älypuhelimien asetuksia tai käyttömahdollisuuksia, etenkin Android- ja IOS käyttöjärjestelmää käyttävissä älypuhelimissa. Tämän takia taisteluosaston sosiaalisen median lisäkoulutuksen yhteydessä olisi hyvä tuoda esille sekä sosiaalisen median riskit, että eri käyttöjärjestelmien riskit sekä ratkaisut.

Tutkijan päätelmä on, että operaatioturvallisuuden optimoinnin kannalta on ehdottomasti siirryttävä sosiaalisen median ja älypuhelimien täyskieltoon joukkojen perustamisvaiheessa operaation aikana. Sosiaalinen media on taisteluosaston operaatioturvallisuudelle todellinen uhka. Modernit avointen lähteiden tiedustelun työkalut sekä reserviläisten sosiaalisen median käyttäytyminen luovat edellytykset vastustajan tiedustelutoiminnalle. Sosiaalisen median rajallinen käyttöoikeus operaatioalueen ulkopuolella on mahdollista, jos valvontaan ja tietoturvaan on resursseja. Operaatioturvallisuuden tärkeyttä sosiaalisessa mediassa on koulutettava henkilökunnalle ja varusmiehille jo rauhan aikana. Tämä mahdollistaisi suojautumisen sosiaalisen median ja avointen lähteiden tiedustelun muodostamasta uhkakuvasta. Tutkija kehottaa Puolustusvoimia ottamaan tarkemmin kantaa älypuhelimien ja sosiaalisen median käyttöön rauhan- ja joukkojen perustamisvaiheen aikana.

Kaikissa vaihtoehdoissa on suotavaa laatia operaatioturvallisuus-suunnitelma, jossa otetaan sosiaalinen media huomioon. Tutkielman perusteella on todettavissa tarve jatkotutkimukselle, jossa ilmenee varusmiesten sosiaalisen median käyttö sotaharjoituksissa. Lisätutkimusta tarvitaan myös siksi, että saataisiin konkreettista tietoa tämänhetkisestä sosiaalisen median käyttötrendistä Puolustusvoimissa. Tämän perusteella voidaan ymmärtää miten ilmiötä tulisi ottaa huomioon operaatioturvallisuuden kannalta.

LÄHTEET

1. Julkaisemattomat lähteet

1.1 Puolustusvoimien asiakirjat

Pääesikunnan suunnitteluosasto: *Informaatio-operaatiot (INFOOP) konsepti 2.0*, Helsinki, 2011.

1.2 Haastattelut

Porras Ville, majuri, Täydennyskoulutus- ja kehittämiskeskus (TKKK), 6.3.2014, älypuhelimiin liittyvät tietoturvauhat ja operaatioturvallisuus sosiaalisessa mediassa, materiaali kirjoittajalla.

Särs Camillo, F-Securen Tietoturvapäällikkö, 7.3.2014, älypuhelimiin liittyvät tietoturvauhat ja operaatioturvallisuus sosiaalisessa mediassa, materiaali kirjoittajalla.

2. Julkaistut lähteet

2.1 Internet julkaisut

Digitoday: *Älypuhelimet ponnistavat yli haamurajan Suomessa*, http://www.digitoday.fi/pdf/20136702, 10.5.2013.

Ewen MacAskill: Edward Snowden: how the spy story of the age leaked out, *The Guardian*, http://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile, 12.6.2013.

Huffington Post: *WikiLeaks 'Insurance' File: Julian Assange's Group Posts Huge Encrypted File To Web*, 5.8.2010 http://www.huffingtonpost.com/2010/08/05/wikileaks-insurance-file-_n_672094.html, 20.12.2013

TNS Mobile Life Gallup 2013: Arki muuttuu yhä mobiilikeskeisemmäksi, 08.05.2013, http://www.tns-gallup.fi/uutiset.php?aid=14935&k=14320, 20.12.2013.

YLE uutiset: Täällä somelaiset elävät – katso lista historiallisesta Facebookista juuri avattuun Pheediin,5.3.2013,http://yle.fi/uutiset/taalla_somelaiset_elavat_-_katso_lista_historiallisesta_facebookista_juuri_avattuun_pheediin/6518189, 20.12.2013.

Pönkä, Harto: *Sosiaalisen median katsaus 09/2013*, 10.9.2013, http://www.slideshare.net/hponka/sosiaalisen-median-katsaus-092013, 20.12.2013.

BBC News, US Army: Geotagged Facebook posts put soldiers' lives at risk, 9.3.2012, http://www.bbc.co.uk/news/technology-17311702, 20.12.2013.

Reed, John: Used Cell Phone Geotags to Destroy AH-64s in Iraq, *Defencetech*, 15.3.2012, http://defensetech.org/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq/#ixzz1pDRqzKSB, 20.12.2013.

ABC News, Soldier posts military plans on Facebook, 4.3.2010, http://www.abc.net.au/news/2010-03-04/soldier-posts-military-plans-on-facebook/350284, 20.12.2013.

War on Terror News, Yon OPSEC Violations, 2.10.2011, http://waronterrornews.typepad.com/ps/2011/02/yon-opsec-violations.html ja http://waronterrornews.typepad.com/.a/6a00e551d9d3fd88330147e275cfed970b-popup, 20.12.2013.

Yon, Michael: A Soldier Emails from Afghanistan, 12.6.2010, https://www.facebook.com/MichaelYonFanPage/posts/118317618212252, 20.12.2013.

Online and Social Media Division: The United states Army Social Media Handbook Version 3.1. 2013, http://www.25idl.army.mil/Social_media_handbook.pdf, 20.12.2013.

ArabCrunch, ”Israel’s” army bans its soldiers from using facebook, Twitter and other social media sites, 12.7.2011, http://arabcrunch.com/2011/07/israels-army-bans-its-soldiers-from-using-facebook-twitter-and-other-social-media-sites.html, 20.12.2013.

Times of Israel, IDF plans social media clampdown for soldiers, 7.6.2013, http://www.timesofisrael.com/idf-plans-social-media-clampdown-for-soldiers/, 20.12.2013.

Darlene Storm, Pocket Spies: Smartphone actionable intelligence, *Computer World*, 29.11.2011,http://blogs.computerworld.com/19348/pocket_spies_smartphone_actionable_intelligence, 20.12.2013.

James Dao, Military Announces New Social Media Policy, *The New York Times*, 26.2.2010 http://atwar.blogs.nytimes.com/2010/02/26/military-announces-new-social-media-policy/?_r=0, 20.12.2013.

2.2 Tutkimukset ja opinnäytteet

Holopainen, Jari: *Sosiaalisen median mahdollisuudet ja riskit puolustusvoimissa*. Esiupseerikurssi 63:n tutkielma, Maanpuolustuskorkeakoulu 2011.

Kilpeläinen, Lauri: *Psykologiset operaatiot kriisinhallinnan toimintaympäristössä, ISAF, Afganistan*, 2014.

Leskinen, Aleksi: *Informaatiosodankäynti, operaatioturvallisuus ja puolustusvoimien turvallisuustoiminta*, 2006.

Turunen, Jarkko: *Esikunta- ja viestipataljoonan operaatioturvallisuus*, 2004.

2.3 Kirjallisuus

Headquarters Department of the Army: *Open Source Intelligence 2012,* Army Technique Publication No. 2-22.9, Washington DC, 2012.

Joint Chiefs of Staff: *Joint Publication JP3-13.3, Operations Security*, 2012.

Kalliala, Eija & Toikkanen, Tarmo: *Sosiaalinen media opetuksessa*. Finn Lectura, 2009.

Kaplan, Andreas M ja Haenlein, Michael: *Users of the world, unite! The challenges and opportunities of Social Media,* Business Horizons, 53(1), 2010.

Liimatainen, Heikki & Rantapelkonen, Jari (toim.): *Informaatioajan viestitaktisia ajatuksia*, Viestikoulu, Riihimäki, 2000.

Puolustusvoimien kansainvälinen keskus: *ISAF, Suomalainen kriisinhallintajoukko Afganistanissa*, Kaarinan Tasopaino oy, Kaarina, 2007.

Sirén, Torsti: *Strateginen kommunikaatio ja informaatio-operaatiot 2030,* Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, julkaisusarja 2: artikkelikokoelmat N:o 7, Juvenes Print Oy, Helsinki, 2002.

Valtionvarainministeriö: *Sosiaalisen median tietoturvaohje (VAHTI 4/2010),* vm-julkaisutiimi, Helsinki, 2010.

LIITELUETTELO

Michael Yon

A Soldier Emails from Afghanistan

With McChrystal's press war, I'm not there to check out this soldiers claims, so here they are. Take 'em or leave 'em.

Movement

Well

I got only 7 days left here in Afghanistan, and I want to tell you how things are in Logar Province. So far in the 3 months I've been here 17 attacks (counting the 1 just now 30 min ago) total of 5 American wounded and this unit don't do shit about the attacks. They have 3rd ID Aviation Brigade here and every night (1900 to 2100 we are getting rockets. Well the last 2 days we been getting hit (1100 to 1400) most likely someone in the base is calling the rockets. You know what I'm talking about. I really don't know how a unit like this can be permitted so many attacks and don't do anything about it!!!! (The last three attacks within 200 meters of my tent.)

Location

UNIT

Attack Effectiveness

Unit/Equipment Deficiency

The 173rd has a radar system to track the incoming but the alarm doesn't go off after the impact sometimes 5 minutes later. The other night I timed the Apache. It took them 35 minutes to take off!!!

Friendly Timeline

Another situation they sent a platoon size 7km away to search for the launch site, well the Taliban is using them as bait. They place so many IEDs in the road that nobody can get to them. The only way the get supplies is by heli doing maneuver called "speed ball." [Speed balls are prepackaged supplies, such as ammo.] So far 2 units have tried to reach them but they have failed (losing more than 4 MRAPs) each time.

Response to Attack

Enemy effectiveness

The last thing you know when a unit is fucked up is when you see the division commander walking by himself all day without his CSM and when you have higher NCOs (E6 and up) complaining about the unit. I don't worry about the privates because they are always bitching, lol.

Security Vulnerability

At the end of the FOB (southeast) they are 8 towers completely empty!!!! The only security in that end of the fob is 2 Humvees with some Jordanian on it (of course no security) if the same attack the happened to Bagram would happen here it would been a disaster. During the night there are 4 Humvees for that whole perimeter

---

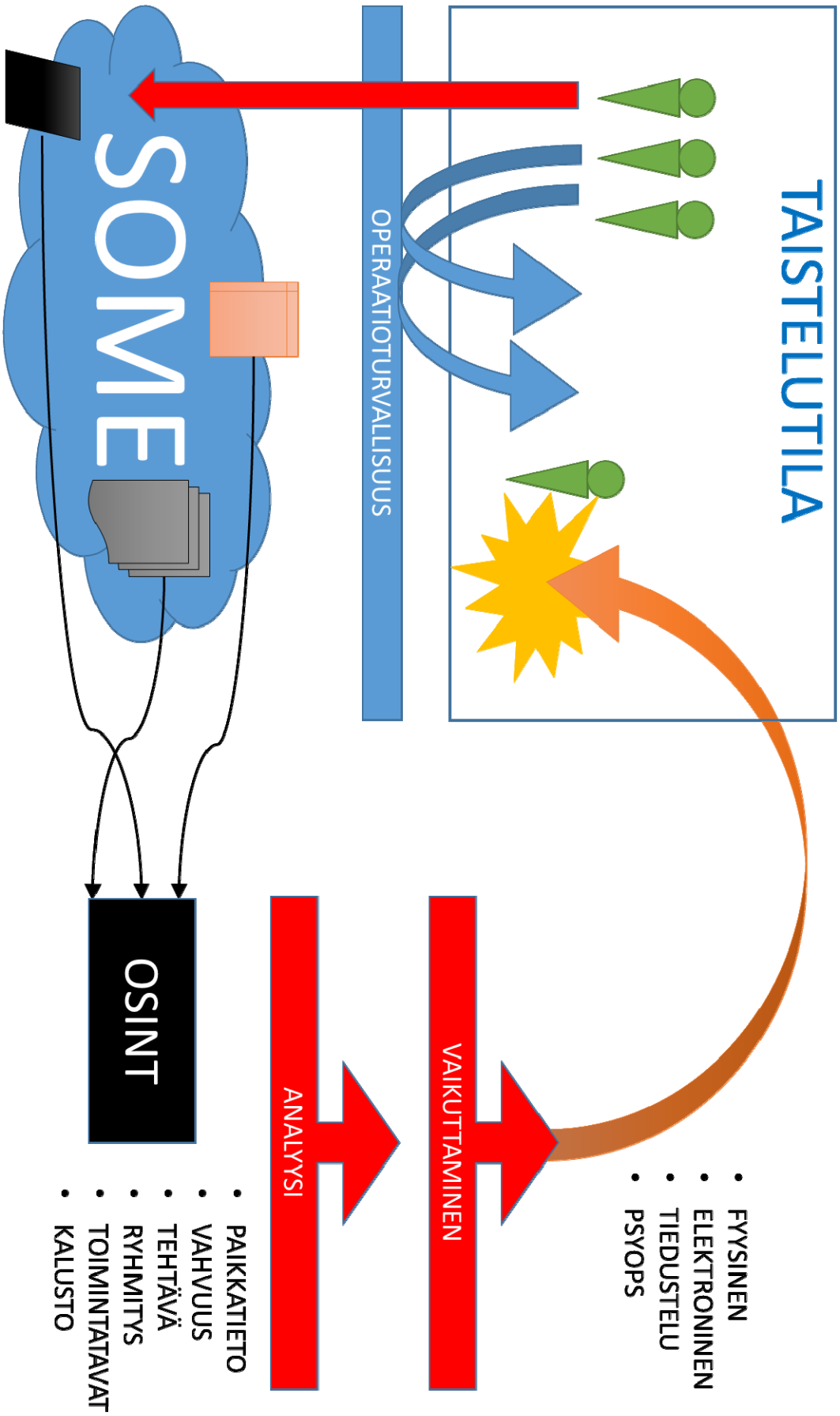
Base Security Measures

(I edited grammar/punctuation a bit.)

Michael Yon - Online Magazine

Michaelyon-online.com

Lähde:http://waronterrornews.typepad.com/.a/6a00e551d9d3fd88330147e275cfed970b-popup


TAISTELUTILA
OPERAATIOTURVALLISUUS
SOME
OSINT
VAIKUTTAMINEN
ANALYYSI
FYYSINEN
ELEKTRONINEN
TIEDUSTELU
PSYOPS
PAIKKATIETO
VAHVUUS
TEHTÄVÄ
RYHMITYS
TOIMINTATAVAT
KALUSTO

Haastattelukysymykset

1.) Kuinka suuri osa mobiilialustojen tietoturvauhista on tullut sosiaalisen median kautta?

2.) Mitkä ovat mobiilikäyttäjien yleisimmät tiedostamattomat tietoturvauhat Suomessa?

3.) Mitä tietoturvariskejä eri käyttöjärjestelmät (IOS, Android, Windows) mahdollistavat?

4.) Miten keskiverto suomalainen suojaa toimintaansa sosiaalisessa mediassa, esimerkiksi Facebookissa? Onko taso mielestänne riittävä sotilastarkoitukseen tietoturvan näkökulmasta?

5.) Millä keinoin on mahdollista kerätä tietoa älypuhelimien käyttäjiltä käyttöjärjestelmäkohtaisesti: IOS, Android, Windows

6.) Miten rajoittaisit sosiaalisen median käyttöä operaatioturvallisuuden parantamiseksi?

7.) Alustavat johtopäätökset – vaihtoehtoiset toimintamallit

I. SOME:n käytön rajoittaminen: Ohje SOME:n käyttörajoituksista operaation aikana, sivujen käyttöestot, rangaistukset, valvottua toimintaa.

II. SOME:n totaalikielto: Älypuhelimet poistetaan palvelukseen astuttaessa ja palautetaan operaation jälkeen.

III. SOME:n käytön hyväksyminen: SOME kampanjointi, henkilöstön ja reserviläisten kouluttaminen, luotto käyttäjään.