Pelastusopisto

B-sarja:
Tutkimusraportit
[1/2014]

Tiedontuotannosta viestintäprosesseihin

Kari Pylväs
Laura Hokkanen
Pekka Paananen
Terhi Kankaanranta
Hanna-Miina Sihvonen

PELASTUSOPISTO

Tiedontuotannosta viestintäprosesseihin

Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa -hanke, osaraportti II

Kari Pylväs
Laura Hokkanen
Pekka Paananen
Terhi Kankaanranta
Hanna-Miina Sihvonen

Pelastusopisto
PL 1122
70821 Kuopio

www.pelastusopisto.fi

Pelastusopiston julkaisu
B-sarja: Tutkimusraportit
1/2014

ISBN 978-952-5905-40-3
ISSN 1795-9160

Kari Pylväs[2]
Laura Hokkanen[1]
Pekka Paananen[1]
Terhi Kankaanranta[2]
Hanna-Miina Sihvonen[1]

[1]Pelastusopisto [2]Poliisiammattikorkeakoulu

Tiedontuotannosta viestintäprosesseihin. Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa -hanke, osaraportti II
Julkaisu/Tutkimusraportti, 49 s., 2 liitettä (10 s.)
Helmikuu 2014

Tiivistelmä

Pelastusopiston ja Poliisiammattikorkeakoulun yhteisprojektissa "Sosiaalinen media (some) ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa" tarkasteltiin kansainvälisiä ja kansallisia sosiaalisen median ja älypuhelinsovellusten käyttötarkoituksia ja parhaita käytäntöjä hätä- ja häiriötilanneviestinnässä sekä ennaltaehkäisevässä viestinnässä. Sosiaalista mediaa ja älypuhelinsovelluksia lähestyttiin myös kanavakohtaisten strategioiden ja käytäntöjen sekä palveluiden tuottamisen näkökulmista. Lisäksi projektissa selvitettiin, miten sosiaalisen median kanavien hyödyntämistä hätä- ja häiriötilanneviestinnässä sekä ennaltaehkäisevässä viestinnässä voitaisiin kehittää.

Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa -projektin toinen osaraportti koostuu kahdesta osiosta. Osiossa I avataan hätä- ja häiriötilanteissa viestintään käytettävien älypuhelinsovellusten mahdollisia tietomalleja sekä käsitellään tiedon tuotannon näkökulmia. Lisäksi osiossa I tarkastellaan hankkeen ensimmäisen osaraportin perusteella vaaratiedottamisessa käytettävää WEA-järjestelmää. Osiossa II selvennetään sosiaalisen median palveluiden tuottamiseen liittyviä reunaehtoja sekä pohditaan näiden soveltamista viranomaistoiminnan näkökulmasta. Osiossa tarkastellaan sosiaalisen median palveluiden toimintaperiaatteiden pohjalta muodostuvia monitahoisia asiakkuus- ja sopimussuhteita ja keskitytään erityisesti pohtimaan sosiaalisen median uusia viestintäprosesseja suhteessa perinteiseen viranomaisviestintään liittyviin viestintäprosesseihin. Lisäksi osiossa esitellään mahdollisuuksia uudenlaisten viestintätapojen ja välineiden hyödyntämiselle hätä- ja häiriötilanneviestinnässä.

Älypuhelinsovellusten avulla on mahdollista paitsi jakaa ennalta ehkäisevää, luonteeltaan staattista viranomaistietoa esimerkiksi opassovellusten muodossa, myös reaaliaikaista ohjeistusta hätä- tai häiriötilanteen vaikutuspiiriin kuuluville henkilöille. Viranomaisten lisäksi kansalaiset voivat toimia tiedon tuottajina – sovellusten avulla tätä tietoa voidaan johtaa viranomaisten ja kansalaisten käyttöön. Älypuhelinsovellukset voivatkin hyödyntää ja yhdistää toiminnassaan moninaista tietoa, jota voivat tuottaa niin teknologiset sensorit kuin sovellusta käyttävät henkilöt. Älypuhelinten ja niihin luotujen sovellusten avulla varoitusviestinnässä voitaisiin käyttää apuna esimerkiksi Cell broadcasting -järjestelmää alueellisessa varoittamisessa.

Tieto- ja viestintäteknologian kehittyminen on tuonut viestintään uusia sisältöjä sekä uusia vuorovaikutuksen muotoja. Vuorovaikutteisen teknologian ja viestintävälineiden kehittymisen myötä käyttäjät voivat olla viestintäprosessien käynnistäjiä, ja viestinnän keskiössä voivat olla

monimuotoiset informaatiosisällöt, kuten videot, valokuvat, blogikirjoitukset, uutiset, sosiaaliset verkostomme, yms. Myös vuorovaikutuksen tavat ovat moninaiset. Tykkäämiset, jakamiset, kommentoinnit, yms. ominaisuudet sekä mukana kulkevat mobiililaitteet tekevät osallistumisesta vaivatonta ja nopeaa, sekä mahdollisesti madaltavat kynnystä osallistua vuorovaikutukseen. Esimerkiksi sosiaaliseen mediaan keskittyvässä hätä- ja häiriötilanneviestinnässä tulisi huomioida ja hyödyntää mahdollisuudet vuorovaikutuksen aikaansaamiselle sekä siitä saatavalle hyödylle.

Vaikka viestintäprosessit ovat muuttuneet sosiaalisen median myötä sisällöltään ja viestinnän muodoiltaan monimuotoisemmiksi sekä tavoittavuudeltaan kattavammiksi, on muistettava että sosiaalinen media ei vielä tavoita kaikkia kansalaisia. Aiemmat käytännöt hätä- ja häiriötilanneviestinnässä ovat myös osoittautuneet toimiviksi, eikä niitä tulisi hylätä uuden edessä. Tärkeää olisikin huomioida, että sosiaalisen median aktiiviset käyttäjät voivat olla tehokkaita toimijoita tiedon levittämisessä, tiedotettavan informaation rakentamisessa sekä palautteen antamisessa. Tämän resurssin hyödyntäminen ei kuitenkaan ole mahdollista ilman sitoutumista vuorovaikutukseen sosiaalisen median käyttäjien kanssa.

Viestintäprosesseja ja -teknologioita tarkastelemalla voitaneen löytää nykyisiin käytäntöihin niveltyviä uusia tapoja hyödyntää sosiaalista mediaa ja mobiiliteknologiaa viranomaisviestinnässä.

Avainsanat: Hätä- ja häiriötilanneviestintä, älypuhelinsovellukset, sosiaalinen media, viestintäprosessit, turvallisuusviestintä

Esipuhe

Pelastusopiston ja Poliisiammattikorkeakoulun yhteisprojektissa "Sosiaalinen media (some) ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa" tarkasteltiin kansainvälisiä ja kansallisia sosiaalisen median ja älypuhelinsovellusten käyttötarkoituksia ja parhaita käytäntöjä hätä- ja häiriötilanneviestinnässä sekä ennaltaehkäisevässä viestinnässä. Sosiaalista mediaa ja älypuhelinsovelluksia lähestyttiin myös kanavakohtaisten strategioiden ja käytäntöjen sekä palveluiden tuottamisen näkökulmista. Lisäksi projektissa selvitettiin, miten sosiaalisen median kanavien hyödyntämistä hätä- ja häiriötilanneviestinnässä sekä ennaltaehkäisevässä viestinnässä voitaisiin kehittää.

Raportin ensimmäisessä osassa käsitellään tiedon tuotantoa sekä sovellusten tietomalleja. Raportissa avataan hätä- ja häiriötilanteissa viestintään käytettävien älypuhelinsovellusten tietomalleja sekä tarkastellaan tiedon tuotannon näkökulmia. Tarkempaan esittelyyn valittiin osaraportin I perusteella Wireless Emergency Alert -järjestelmän toimintaperiaatteet ja -vaatimukset. WEA-järjestelmän tietomallien pohjalta esitetään mahdollisuuksia tietomalleista esimerkiksi vaaratiedottamisen sovelluksille Suomessa. Aihe on ajankohtainen, sillä nykyisessä varoitusviestinnässä käytettävä tekniikka ei mahdollista alueellista tai paikallista vaaratiedottamista, jolloin esimerkiksi paikallisista karhuhavainnoista hälytetään valtakunnallisesti.

Älypuhelinsovellusten avulla on mahdollista paitsi jakaa tietoa viranomaisilta kansalaisille, myös hyödyntää onnettomuusalueella olevia henkilöitä. Onnettomuuden vaikutuspiiriin kuuluvia henkilöitä voidaan pyytää osallistumaan tiedon tuotantoon tai johtamaan tiedon tuotantoa automaattisesti esimerkiksi sosiaalisen median päivityksistä. Kansalaiset voivat siis toimia tehokkaina antureina hätä- ja häiriötilanteissa ja tuottaa tietoa viranomaisten tueksi. Raportissa tarkastellaankin älypuhelinsovellusten toimintaa myös tiedon tuottamisen näkökulmista ja analysoidaan tarkemmin, millaista (kenen tuottamaa ja missä muodossa olevaa) tietoa sovellukset käyttävät ja millaista tietoa ne välittävät eteenpäin.

Raportin toisessa osassa keskitytään sosiaalisen median palveluntuotantoon sekä viestintäprosesseihin. Osiossa selvennetään sosiaalisen median palveluiden tuottamiseen ja käyttämiseen liittyviä reunaehtoja sekä pohditaan sosiaalisen median soveltamista hätä- ja häiriötilanneviestinnässä. Tässä yhteydessä sosiaalisella medialla viitataan yleisesti välineeseen, sillä se käsittää terminä paremmin ne kaikkien eri palveluiden tarjoamat mahdollisuudet välittömän, ajantasaisen, sisällöltään monimuotoisen, paikasta ja ajasta riippumattoman sekä tasavertaisen viestinnän erilaatuisten ja kokoisten yleisöjen välillä.

Sosiaalisen median palveluiden toimintaperiaatteiden pohjalta muodostuu monitahoisia asiakkuus- ja sopimussuhteita. Tyypillisimpiä muotoja ovat sosiaalisen median palveluntarjoajien ja käyttäjien välinen suhde, käyttäjien väliset keskinäiset suhteet, sekä palveluntarjoajan ja kolmannen osapuolen – kuten mainostajan tai palvelun ja sen käyttäjien suhde ulkopuoliseen tahoon. Pohdimme raportissa lyhyesti näitä suhteita muun muassa rekisteröitymisen, käyttämisen, tiedonhallinnan sekä lainsäädännön osalta.

Lopuksi raportissa tarkastellaan sosiaalisen median palveluiden tuomaa muutosta viestinnälliseen toimintaan ja toimintakenttään ja pohditaan sosiaalisen median uusia viestintäprosesseja suhteessa perinteiseen viranomaisviestintään liittyviin viestintäprosesseihin. Viestintäprosesseja tarkastellaan viestintävälineiden, viestintätapojen sekä viestinnällisten näkemysten muutoksen pohjalta sekä esitellään mahdollisuuksia uudenlaisten viestintätapojen ja välineiden hyödyntämiselle hätä- ja häiriötilanneviestinnässä.

Sisällys

Osa I – Keskeisten sovellusten tietomallikuvaukset ja tiedontuotannon näkökulmat

1 Johdanto

"Uudet vaaratiedotteet hämmentävät ja ärsyttävät" (Yle Uutiset 26.8.2013)
"Lukuisat vaaratiedotteet ärsyttävät kansalaisia" (Yle Uutiset 12.7.2013)
"Vaaratiedotteet aivan liian laajassa jakelussa" (Kaleva, 29.7.2013)

Hätä- tai häiriötilanteessa viranomaisviestinnän tulee olla luotettavaa, ymmärrettävää ja yhdenmukaista – samalla sen tulisi tavoittaa häiriötilanteen vaikutuspiirissä olevat nopeasti. Olennaista on käyttää viestinnän eri kanavia mahdollisimman tehokkaasti ja monipuolisesti. Internetiä ja sosiaalisen median palveluja käytetään yhä enemmän mobiilisti. Tilastokeskuksen (2012) mukaan jo 49 prosenttia 16–74-vuotiaista suomalaisista omistaa älypuhelimen. Marketvision ennusteen mukaan vuonna 2014 jo 90 %:lla suomalaisista on älypuhelin (Marketvisio 2012). Sosiaalinen media ja älypuhelinsovellukset tarjoavatkin käytössä olevien viestintätapojen rinnalle uuden, täydentävän kanavan myös hätä- ja häiriötilanteiden aikaiseen viestintään.

Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa -hankkeen osaraportissa I tarkasteltiin, kuinka sosiaalista mediaa sekä erityisesti älypuhelinsovelluksia on hyödynnetty ennakoivassa viestinnässä sekä hätä- ja häiriötilanteissa kansallisesti ja kansainvälisesti. Viranomaisten tarjoamia maksuttomia ja maksullisia älypuhelinsovelluksia on maailmalla kehitetty laajasti. Ne tarjoavat käyttäjälleen sekä ennaltaehkäisevää turvallisuusinformaatiota, ennakoivaa ohjeistusta että viestintäkanavan häiriötilanteissa. Suurta osaa näiden sovellusten toimintalogiikasta voitaisiin hyödyntää onnettomuuden elinkaaren eri vaiheissa myös Suomessa. (Hokkanen, Pylväs, Kankaanranta, Paananen, Sihvonen & Honkavuo 2013.)

Tässä raportissa avataan hätä- ja häiriötilanteissa viestintään käytettävien älypuhelinsovellusten tietomalleja sekä tarkastellaan tiedon tuotannon näkökulmia. Tarkempaan esittelyyn valittiin hankkeen osaraportin I perusteella Wireless Emergency Alert -järjestelmän toimintaperiaatteet ja -vaatimukset. WEA-järjestelmän tietomallien pohjalta esitetään mahdollisuuksia tietomalleista esimerkiksi vaaratiedottamisen sovelluksille Suomessa. Aihe on ajankohtainen, sillä nykyisessä varoitusviestinnässä käytettävä tekniikka ei mahdollista alueellista tai paikallista vaaratiedottamista, jolloin esimerkiksi paikallisista karhuhavainnoista hälytetään maanlaajuisesti.

Älypuhelinsovellusten avulla on mahdollista paitsi jakaa tietoa viranomaisilta kansalaisille, mutta myös hyödyntää viestinnässä onnettomuusalueella olevia henkilöitä. Onnettomuuden vaikutuspiiriin kuuluvia henkilöitä voidaan pyytää osallistumaan tiedon tuotantoon tai johtamaan sitä automaattisesti esimerkiksi sosiaalisen median päivityksistä. Kansalaiset voivat siis toimia tehokkaina antureina hätä- ja häiriötilanteissa ja tuottaa tietoa viranomaisten tueksi. Tässä osiossa tarkastellaankin älypuhelinsovellusten toimintaa myös tiedon tuottamisen näkökulmista ja analysoidaan tarkemmin, millaista (kenen tuottamaa ja missä muodossa olevaa) tietoa sovellukset käyttävät ja millaista tietoa ne välittävät eteenpäin.

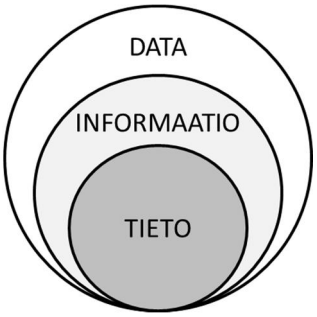
2 Käsitteet

Seuraavassa esitellään lyhyesti raportissa käytetyt keskeiset käsitteet ja nimikkeet, joiden tunteminen helpottaa raportin lukemista. Määritelmien rakentamisessa noudatettiin mahdollisuuksien mukaan aikaisemmassa tutkimuskirjallisuudessa esiintyneitä määritelmiä aihetta koskevan terminologian yhdenmukaisuuden ja yksiselitteisyyden takaamiseksi.

2.1 Tieto, data ja informaatio

Tietoon liittyvät läheisesti käsitteet data ja informaatio. *Data*lla tarkoitetaan, kirjaimia, numeroita ja symboleja sekä niiden muodostamia kokonaisuuksia jotka ovat koneellisesti luettavassa, viestittävässä tai käsiteltävässä muodossa (ks. esim Oxford Dictionaries 2014, Sanastokeskus TSK:n termipankki 2014). Datalla voidaan viitata myös tietokoneen käyttämään ja käsittelemään tietoon (Jaakohuhta 1999, 192). *Informaatio* on datasta eli merkeistä koostuva kokonaisuus, johon liittyy jokin merkitys tai tulkinta (Suurla 2001, 31). Data ja informaatio voivat olla esimerkiksi sähköisessä muodossa tallennettuna tietokoneen muistiin. Informaatiosta tulee tietoa vasta, kun ihminen on prosessoinut sen, ja tieto on siten kontekstiinsa sidottua. Tällaisesta tiedostoa käytetään myös termiä *tietämys*. Mikäli tieto erotetaan kontekstistaan, se on informaatiota. (Suurla 2001, 31)

Tieto voidaan jakaa sen esitysmuodon mukaan esimerkiksi kahteen muotoon: 1) rakenteiseen ja 2) vapaamuotoiseen tietoon. *Rakenteisella tiedolla* on tarkasti kuvattu rakenne, missä muodossa tieto esitetään (Saari 2006, 25). Esimerkiksi syntymäajan rakenne voidaan kuvata PP.KK.VVVV, jolloin tiedetään että syntymäaika tulee kuvata juuri kyseisellä tavalla. *Vapaamuotoisella tiedolla* ei ole vastaavaa tiettyä rakennetta. Tällöin syntymäaika voidaan antaa muodoilla 01.01.1990, 010190, 01011990, 1190 tai sanallisesti kirjoitettuna.



Kuva 1. Tietoon liittyvät termit

Tiedon rakenteen täsmällisyys voi kuitenkin vaihdella; esimerkiksi tässä raportissa rakenteisuutta on toteutettu jäsentämällä tekstiä pää- ja alaluvuin sekä lyhyin kappalein. Kappaleiden sisällöllä ei kuitenkaan ole tarkempaa rakennetta ja esimerkiksi sanojen järjestystä, sana- tai lausemääriä tai muuta spesifimpää rakennetta ei ole määritelty. Tiedon rakenteen määrittely helpottaa kuitenkin tiedon käsittelyä. Jos esimerkiksi tiedetään missä järjestyksessä tiettyyn asiaan viittaavat merkit, sanat tai ilmaisut ovat yhdellä tekstirivillä, on hakutoiminnon toteuttaminen huomattavasti yksinkertaisempaa.

2.2 Tietomalli (data model)

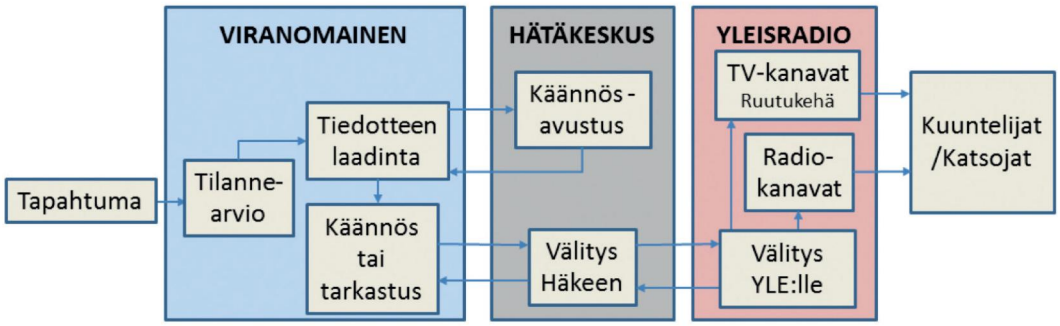
Tietomallin avulla kuvataan tietoja ja niiden välisiä suhteita. (Julkisen hallinnon tietohallinnon neuvottelukunta - JUHTA 2012) Tietomallia voidaan käyttää sekä teknisellä tasolla (esimerkiksi tietokantojen sisältämien tietojen jäsentelyyn) että loogisella tasolla kuvattaessa mitä tietoja sovellus käyttää. Tässä raportissa keskitytään loogiseen näkökulmaan: mitä tietoja ensimmäisestä osaraportista valitsemamme sovellus käyttää ja kuinka näiden tietojen käyttämistä voisi kehittää.

3 Nykyinen vaaratiedotus

Laki vaaratiedotteesta (466/2012) tuli voimaan 1.6.2013. Lakia sovelletaan viranomaisen radiossa ja televisiossa välitettäväksi antamaan vaaratiedotteeseen. Vaaratiedotteen tarkoitus on varoittaa vaarallisesta tapahtumasta, sekä tarpeen vaatiessa ohjeistaa suojautumiseen ja vaaratilanteen välttämiseen.

Ratkaisun vaaratiedotteen antamisesta tekee toimivaltainen viranomainen. Se annetaan aina maanlaajuisesti, sillä alueelliseen tai paikalliseen jakeluun ei tällä hetkellä ole teknisiä mahdollisuuksia. Vaaratiedotteen käytön on perustuttava vakaaseen harkintaan ja kynnys sen antamiseen tulee olla riittävän korkea. (Sisäasiainministeriö 2012, 5–9)

Vaaratiedote välitetään valtakunnallisesti kaikille Yleisradio Oy:n radiokanaville sekä pitkäaikaisen toimiluvan saaneille kaupallisille radiokanaville. Vaaratiedotteen antava viranomainen voi päättää, että vaaratiedote välitetään tiedoksi myös televisiossa, jolloin sen teksti kulkee kuvaruudun yläosassa. Tekstin ohessa kuuluu aluksi varoitusääni. Vaaratiedotteet välitetään "pakkosyöttönä", jolloin ne katkaisevat kaikki muut radio- ja televisiolähetykset koko maassa (Ahvenanmaan maakuntaa lukuun ottamatta). Kielilain mukaisesti vaaratiedote annetaan suomeksi ja ruotsiksi sekä saamen kielellä silloin, kun vaarallinen tapahtuma tai sen seuraukset kohdistuvat saamelaisten kotiseutualueelle. (Sisäasiainministeriö 2012, 5)



Kuva 2. Vaaratiedotteen laatiminen ja välittäminen (Sisäasiainministeriö 2012, 4)

Vaaratiedotteen antava viranomainen vastaa aina tiedotteen ja sen käännöksen oikeellisuudesta. Sen tulee vastata viiteen kysymykseen: missä – milloin – mitä – miten – kuka on tiedotteen antaja. Vaaratiedotteen kohteena on ensisijaisesti vaara-alueella oleva väestö, ja ensisijaisesti se on väestölle osoitettu varoitus ja toimintaohje. (Sisäasiainministeriö 2012, 6,11)

3.1 Vaaratiedotteen tietomalli

Vaaratiedote koostuu kuudesta tietoelementistä: 1) otsikosta, 2) paikka- tai aluetiedosta, 3) päivämäärästä ja kellonajasta, 4) vaaratilanteen kuvauksesta, 5) toimintaohjeista, sekä 6) tiedottavasta viranomaisesta (ks. taulukko 1).

Vaaratiedotteen tietoelementit ovat sekä staattisia että dynaamisia. Otsikko on kaikista staattisin eli pysyvin; vaaratiedotteen otsikko on aina "VAARATIEDOTE". Päiväys ja kellonaika annetaan aina muodossa "pp.kk.vvvv kello tt.mm", esimerkiksi "5.5.2012 kello 13.40".

Tiedottava viranomainen on aina jokin laissa määritellyistä toimivaltaisista viranomaisista. Tiedottavan viranomaisen nimenä näytetään sen yleisesti käytetty nimi, kuten Varsinais-Suomen pelastuslaitos. (ks. taulukko)

Taulukko 1. Nykyisen vaaratiedotteen tietomalli

Otsikko	Paikka tai alue	Pvm ja kellonaika	Kuvaus	Toimintaohjeet väestölle	Tiedottava viranomainen
VAARATIEDOTE:	Turku, keskusta	5.5.2012 kello 13.40.	Terveydelle vaarallista savua ilmassa. Tulipalo Turun keskustassa.	Alueen ihmisiä kehotetaan pysymään sisätiloissa ja sulkemaan ilmanvaihto, sekä odottamaan tiedotetta vaaratilanteen päättymisestä.	Varsinais-Suomen pelastuslaitos

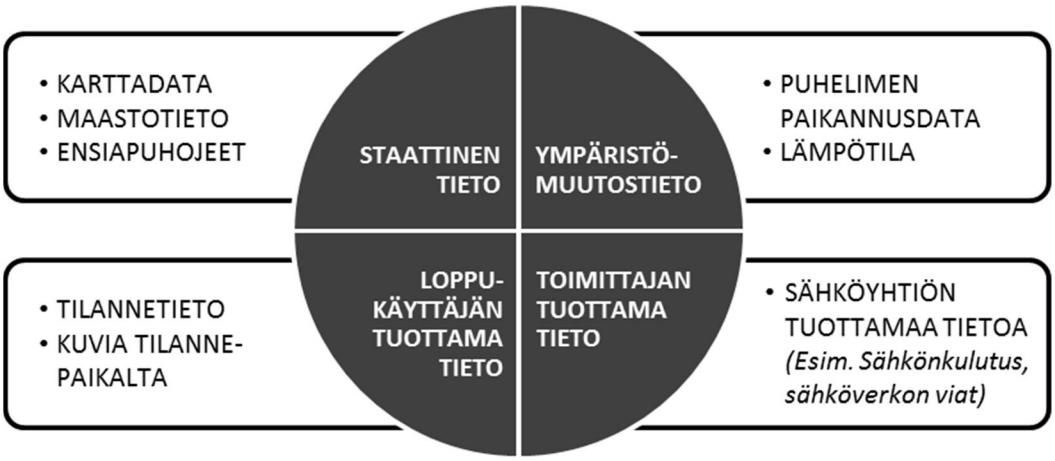
Vaaratiedote on saanut osakseen paljon kritiikkiä. Yleisradion mukaan negatiivinen palaute on liittynyt muun muassa vaaratiedotteiden tunnusmusiikkiin, ruotsinkielisten käännösten heikkoon tasoon ja vaaratiedotteiden alhaiseen lähettämiskynnykseen. Esimerkiksi heinäkuun 2013 puoliväliin mennessä vaaratiedotteita oli lähetty kesän 2013 aikana jo yli 12, kun vastaava luku vuotta aiemmin oli kaksi. Kritiikkiä on saanut osakseen erityisesti se, ettei käytettävä tekniikka mahdollista alueellista tai paikallista vaaratiedottamista, jolloin esimerkiksi paikallisista karhuhavainnoista hälytetään maanlaajuisesti. Näiden seikkojen pelätään vaikuttavan edelleen vaaratiedotteen tehoon ja merkitykseen. (Yle, 2013)

4 Älypuhelinten tiedonkäsittelymahdollisuudet

Seuraavassa esitellään älypuhelinten sekä älypuhelinsovellusten mahdollisuuksia tiedontuottamisessa, -hallinnassa ja -käsittelyssä. Älypuhelinten ja -sovellusten sisältäviä sekä niissä käytettäviä tietoja tarkastellaan tiedontuotannon sekä tiedon ominaisuuksien mukaan. Tiedontuottajalla tarkoitetaan tahoa, joka syöttää tietoa älypuhelinsovellukseen tai sen käytettäväksi. Tässä tiedon ominaisuuksilla tarkoitetaan raporttia varten tarkastelluista sovelluksista havaittuja oleellisia tietokategorioita. Nämä tarkastelukulmat eivät ole toisiaan poissulkevia ja osaltaan limittyvät toisiinsa.

4.1 Tiedon kategoriat

Mobiilisovellusten käyttämät tiedot voidaan luokitella ominaisuuksien pohjalta neljään kategoriaan (ks. kuva 3): 1) staattiseen tietoon, 2) ympäristömuutostietoon, 3) toimittajan syöttämään tietoon sekä 4) loppukäyttäjän syöttämään tietoon. Älypuhelinsovellus voi yhtäaikaisesti yhdistää eri tietolähteistä ja eri kategorioista tulevaa tietoa. Toisaalta yksittäinen tieto voi kuulua useampaan kuin yhteen kategoriaan.



Kuva 3. Älypuhelinsovelluksen tiedon kategoriat esimerkkeineen

Staattinen tieto

Staattisella tiedolla tarkoitetaan pääosin muuttumatonta tietoa, jonka oikeellisuuteen ja käyttökelpoisuuteen eivät vaikuta merkittävästi ympäristössä tapahtuvat muutokset. Esimerkiksi karttapohjia, maastotietoja tai auto-onnettomuuden tai ensiavun antamiseen muodostettuja valmiita ohjeita voidaan pitää staattisena tietona. Staattinen tieto voi toimia pohjana muuttuvan tai päivittyvän tiedon havainnollistamisessa. Hätä- ja häiriötilanteita varten suunnitellut älypuhelinsovellukset voivat hyödyntää staattista tietoa: esimerkiksi tilanteesta päivittyvät tiedot voidaan havainnollistaa puhelimen muistissa olevalla kartalla verkkoyhteyden ollessa käytössä, mikäli käyttäjä on ladannut kartat puhelimeensa. Älypuhelimen hyödyntämä staattinen tieto voi myös olla puhelimeen ennalta ladatun ohjeistavan sovelluksen sisältöä, joka ohjeistaa käyttäjää esimerkiksi ensiavun antamisessa viimeisimpien ensiapusuositusten mukaisesti. Staattisen tiedon muuttuessa tietoja voidaan päivittää puhelimiin verkkoyhteyden välityksellä. Mikäli puhelin on offline-tilassa, käytössä on viimeisin laitteen omassa muistissa oleva tieto.

Ympäristömuutostiedot

Ympäristömuutostiedot ovat älypuhelimen ympäristöön liittyvää muuttuvaa ja päivittyvää tietoa. Ympäristömuutostietoa saadaan muun muassa älypuhelinten erilaisten sensoreiden kautta. Sensorilla eli anturilla viitataan yleisesti teknisiin mittalaitteisiin, jotka muuntavat erilaisia ympäristön muutoksia tietotekniikan hyväksikäytettävään muotoon.

Useimmat älypuhelimet sisältävät esimerkiksi liikkeentunnistus-, kuva-, valaistuksentunnistus- ja etäisyyssensorin, kuva-, ääni- ja monikosketussensorin, digitaalisen kompassiominaisuuden ja GPS-paikannusmahdollisuuden. Käyttäjä voi myös itse liittää erilaisia lisälaitesensoreita (kuten sykemittarin tai lämpötilan mittaavan sensorin[1]) omaan älypuhelimeensa vaikkapa Bluetooth-, NFC[2]- tai WLAN yhteyden avulla. Erilaisten sensorien tuottamaa tietoa voidaan välittää verkkoyhteyden avulla älypuhelinten ja niiden sovellusten käyttöön. Tutuin esimerkki ympäristömuutostiedoista lienee säätieto, jota jo tällä hetkellä hyödynnetään älypuhelinsovelluksissa hyvin monipuolisesti.

Toimittajan tuottama tieto

Toimittajan tuottamalla tiedolla voidaan tarkoittaa ulkoisten toimijoiden keräämää informaatiota, jota älypuhelinsovellus hyödyntää tietojen esittämisessä. Toimittajan tuottama tieto voi olla esimerkiksi sensoridataa, jota sovellus vielä esittää sovelluksen tuottajan haluamalla tavalla. Tällöin esimerkiksi säätieto on ulkopuolisen toimittajan keräämää sensoridataa, jota sovellus hyödyntää käyttäjän haluamalla tavalla.

Loppukäyttäjän tuottama tieto

Loppukäyttäjän tuottamalla tiedolla tarkoitetaan nimensä mukaisesti sovelluksen käyttäjän luomaa tietosisältöä. Sovelluksesta riippuen tämä tieto voi kulkea edelleen muille sovelluksen käyttäjille tai sovelluksen palveluntarjoajalle. Loppukäyttäjän tuottamaa tietoa voi olla esimerkiksi onnettomuusalueelta julkaistu kuvamateriaali, tilanteen kuvaaminen sanallisesti tai paikkatiedon julkaiseminen älypuhelinsovelluksen kautta.

Avoin data

Älypuhelinsovellusten toimintaperiaate pohjautuu usein erilaisten avointen tietovarantojen hyödyntämiseen. Avoimella datalla tarkoitetaan informaatiota, johon on avattu maksuton ja vapaa pääsy kaikille halukkaille. Avoin data voi olla niin kutsuttua raakadataa, kuten tilastoja, julkaisuja, videotallenteita, kuvia tai karttoja.

Avointa dataa sisältävät tietovarannot ovat kenen tahansa saatavilla ja vaihtelevin luvin käytettävissä eri tarkoituksiin. Avoimen datan periaatteeseen kuuluu oletus, että avatessaan tietovarannot niiden julkaisija sallii aineistojen uudelleenkäytön. Tämä edellyttää myös avattujen tietovarantojen sisältämän datan rakenteen ja merkityksen kuvailua niin, että käyttäjä voi tietosisällöt ymmärtää. (Helsinki Region Infoshare 2013) Avoimen datan kanssa voidaan käyttää valmiita, vapaasti käytettävissä olevia lisenssejä (esimerkiksi Creative Commons), joissa määritellään tekijänoikeuksiin liittyvät sopimusehdot. Esimerkiksi avoimen datan tarjoaja voi viitata "Nimeä (CC BY)" -nimiseen lisenssiin, jonka mukaan kyseistä aineistoa saa käyttää vapaasti niin kaupallisiin kuin epäkaupallisiin tarkoituksiin, kunhan alkuperäinen

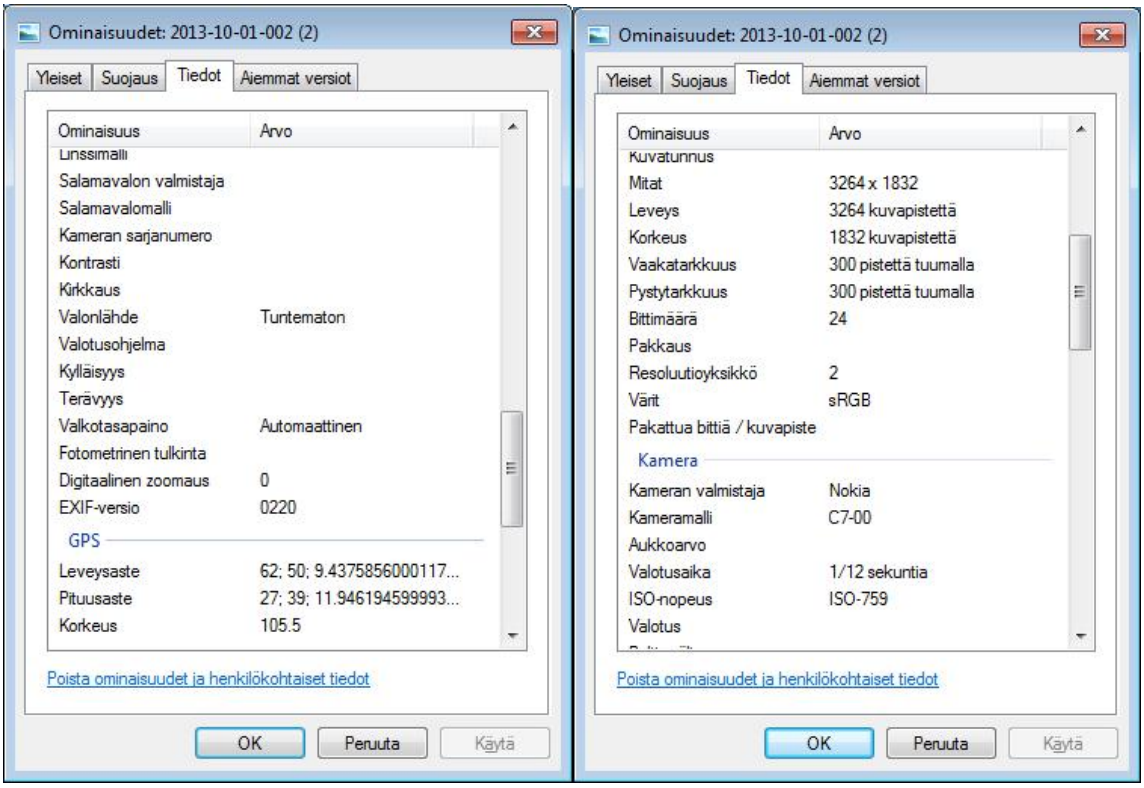
[1] Esimerkiksi iPhone -puhelimiin on saatavilla *Thermometer - Measure Temperature via the Ear Phone Jack and Arduino using FSK* -niminen sovellus, joka mittaa ympäristön lämpötilaa lisäosan avulla. ks. esim. http://schogini.com/tutorials/thermometer.

[2] NFC (Near Field Communication) -teknologia

omistaja nimetään. "Nimeä-Epäkaupallinen (CC BY-NC)" on puolestaan vastaava lisenssi, joka sallii käytön vain epäkaupallisiin tarkoituksiin. (Creative Commons 2013) Useat kaupungit ovat avanneet taloustietojaan sekä erilaisia tilastoja ulkopuolisten toimijoiden vapaaseen käyttöön. Datan avanneista tahoista esimerkiksi Jyväskylän kaupunki edellyttää, että tiedon lähde (Jyväskylän kaupunki) tulisi tietovarantoja käytettäessä mainita. Maanmittauslaitos on puolestaan avannut kaikki digitaaliset maastotietoaineistonsa kansalaisten ja yritysten vapaaseen käyttöön.

Metadata

Metadata on tietoa tiedosta (Salminen 2005). Esimerkiksi mobiililaitteella otettuun valokuvaan tallentuu teknisenä metadatana tiedoston koko, luomisaika, tiedostotyyppi, laitteen tiedot, mahdolliset käyttäjätiedot, kameran asetukset sekä usein myös sijainnin koordinaatit (kuva 4). Myös Twitterissä julkaistuissa tweeteissä on mukana runsaasti tällaista piiloon jäävää tietoa, joka kertoo muun muassa tweetin luontiajankohdan, millä sovelluksella se on lähetetty, sijaintitiedot (esimerkiksi maa ja aikavyöhyke), sekä tietoja tilin käyttäjästä (esimerkiksi julkaistujen tweettien lukumäärän, seurattavien ja seuraajien lukumäärän) (Burns & Liang 2012). Metadataa voidaan käyttää esimerkiksi tiedon järjestämiseen, luokitteluun tai hakuehtona. Hätä- ja häiriötilanteiden näkökulmasta esimerkiksi kuvien tai tweettien metadatassa olevan paikkatiedon avulla ne voidaan sijoittaa kartalle tilannekuvan hahmottamiseksi.



Kuva 4. Kännykkäkameralla otetun kuvan metadataa

4.2 Tiedon ja älypuhelinsovellusten tuottajat

Älypuhelinsovelluksen tarjoamaa tai käyttämää tietoa voivat tuottaa sovelluksen toimittaja / tuottaja, älypuhelinsovelluksen hyödyntämän palvelun tarjoaja (tai tilaaja), kolmannet osapuolet sekä loppukäyttäjä itse. Sovelluksen tietosisältö saadaan usein *palveluntarjoajalta.* Palveluntarjoaja ei välttämättä vastaa itse sovelluksen tuottamisesta, vaan se tilataan erilliseltä *toimittajalta / tuottajalta*, joka voi toimia sovelluksen teknisen toteutuksen lisäksi tiedon tuottajana. Esimerkiksi WEA-sovelluksessa tiedon, eli varoitusviestin sisällön, tuottaa toimivaltainen julkishallinnon viranomainen.

Älypuhelinsovellus voi hyödyntää myös *kolmansien osapuolten* tuottamaa tietoa, jolloin sovellus käyttää muuta kuin palveluntarjoajan tai sovelluksen tuottajan luomaa, julkisesti saatavilla olevaa tietoa: vaikkapa internet-sivuilla olevaa tietoa voidaan lukea ja jäsentää sovelluksen käyttämään muotoon automaattisesti muun muassa RSS-syötteiden avulla. Esimerkiksi Hälytyskeskus-älypuhelinsovellus hyödyntää toiminnassaan pelastustoimen PETO-mediapalvelua, joka listaa 100 viimeistä hälytyskeskuksen antamaa tehtävää. Sovellus mm. sijoittaa hälytykset Suomen kartalle tehtävätietojen perusteella.

Loppukäyttäjän tuottama tieto on sovelluksen käyttäjän syöttämää tietoa, jota voidaan jakaa sovelluksen käyttötarkoituksesta riippuen niin omalle määritellylle verkostolle kuin kaikille muille sovelluksen käyttäjille, sovelluksen ylläpitäjätaholle tai muille tahoille, kuten viranomaisille. Esimerkiksi Life360 -sovelluksen käyttäjä voi jakaa muun muassa sijaintitietoja, valokuvia ja viestejä oman lähiverkostonsa kanssa.

Moni älypuhelinsovellus kokoaa tietosisältönsä usealta taholta. Esimerkiksi UbAlert -sovelluksessa käyttäjä voi antaa sovellukseen tietoja häiriötilanteen laajuudesta, sijainnista ja vakavuudesta, ja sovellus yhdistää käyttäjien tuottamaa epävirallista tietoa virallisiin tiedotteisiin ja varoituksiin. Älypuhelinsovelluksen tiedon tuottamisen käytäntöjen yhteydessä on syytä pohtia myös tuotetun tiedon näkyvyyttä ja omistajuutta. Älypuhelinsovelluksen tietosisältöihin voidaan luoda erilaisia näkymiä, joiden tietosisällöt vaihtelevat käyttäjän roolin mukaan. Tällöin esimerkiksi sovellusta viranomaisstatuksella käyttävä näkee eri tietosisältöjä kuin kansalaiskäyttäjä. Pohjana voi olla sama tietokokonaisuus, josta eri rooleille näytetään eri osat.

Sovellukseen syötettyjen tietojen omistajuuteen liittyvät kysymykset koskevat erityisesti sovelluksen käyttäjän tuottaman tiedon omistajuutta. Mikäli sovelluksen käyttäjä ottaa valokuvan onnettomuuspaikalta ja toimittaa sen sovelluksen kautta viranomaiselle, on määriteltävä omistaako kyseisen kuvan kuvaaja itse, palveluntarjoaja eli viranomaistaho vai sovelluksen tekninen tuottaja / toimittaja. Käyttäjän sovellukseen tuottamien tietojen omistajuus voidaan ratkaista esimerkiksi jättämällä käyttäjälle itselleen oikeudet käyttää kuvaa omiin tarkoituksiinsa kuitenkin niin, että tämä luopuu mahdollisesta rahallisesta korvauksesta palveluntarjoajan saadessa oikeudet käyttää valokuvaa opetus-, kehitys- ja markkinointitarkoituksiin. Olennaista on, että omistajuuteen liittyvät ratkaisut ovat käyttäjien tiedossa.

Kansalaisilta saatava tieto voi auttaa viranomaisia tilannekuvan muodostamisessa, mutta myös haitata viranomaisten toimintaa. Esimerkiksi sosiaalisessa mediassa liikkuva tieto voi olla virheellistä tai vanhentunutta, tai tahallisesti harhaanjohtavaa. Myös älypuhelinsovelluksen avulla tuotetun tiedon kohdalla luotettavuuden arvioinnin näkökulma tulee ottaa huomioon. Luotettavuuden arvioinnissa viesteihin liittyvä data, esimerkiksi käyttäjätiedot, sijaintitiedot tai kuvien sisältämä metadata voivat lisätä niiden luotettavuutta.

Älypuhelinsovellusten tuottajat voivat olla julkisia toimijoita tai sovellustoimittajia, joilta sovelluspalvelu on tilattu tai jotka tarjoavat palvelua itsenäisesti. Lisäksi älypuhelinsovelluksia voivat tuottaa yksityiset henkilöt tai yhteisöt. Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa -hankkeen osaraportissa I tarkastelluista älypuhelinsovelluksista kartoitettiin myös niiden takana olevat palveluntarjoajat / tuottajat. (ks. Hokkanen, ym. 2013, liite 1)

5 Sovellustietomalli – Case: Wireless Emergency Alerts (WEA)

Yhdysvalloissa on käytössä kansalaisten varoittamiseen ja tiedottamiseen tarkoitettu järjestelmä Wireless Emergency Alerts (WEA). Järjestelmä tunnetaan myös nimillä Commercial Mobile Alert System (CMAS), sekä Personal Localized Alerting Network (PLAN). Järjestelmä on tarkoitettu erityisesti tilanteisiin, joissa alueellisesti kohdennetulla tiedottamisella on oleellinen merkitys ihmishenkien pelastamisessa. Esimerkiksi hurrikaani Sandyn (2012) ja Bostonin pommi-iskun (2013) aikana lähettiin WEA-viestejä. Viestit jaetaan kolmeen tyyppiin tilanteen mukaan (FEMA - Federal Emergency Management Agency 2013):

1. varoitusviesti uhkaavasta vaarasta, esimerkiksi lähestyvästä myrskystä (Imminent Threat)
2. AMBER-viesti (America's Missing: Broadcast Emergency Response) eli hälytys kadonneen lapsen tai nuoren löytämiseksi (AMBER Alert)
3. presidentin lähettämä viesti (Presidential Alert).

WEA-viestit ovat tavallisen tekstiviestin kaltaisia matkapuhelimiin lähetettäviä viestejä, jotka lähetetään maantieteellisesti rajatulle alueelle. Viestit ovat 90 merkin mittaisia tiiviitä viestejä, jonka saapuessa puhelin hälyttää normaalista poikkeavalla äänellä ja värinällä. Viestien tarkoitus on lähinnä herättää vastaanottajan huomio ja ohjeistaa heitä seuraamaan tilanteen kehittymistä esimerkiksi median välityksellä.

Kuva 5. Wireless Emergency Alert (WEA) -viesti lähetettiin Bostonin pommi-iskujen aikana (kuva: http://www.fema.gov/media-library/assets/images/34741)

WEA-viestejä voivat lähettää liittovaltion, osavaltioiden ja kuntien viranomaiset. Viestien vastaanottamisesta voi myös kieltäytyä puhelimen asetuksia muuttamalla. Poikkeuksena ovat kuitenkin Yhdysvaltain presidentin lähettämät viestit, joiden vastaanottamisesta ei voi kieltäytyä. (FEMA - Federal Emergency Management Agency 2013)

WEA-viestit ovat maksuttomia sekä viestien lähettäjille että vastaanottajille. Ne lähetetään Cell Broadcast (CB) -teknologiaa käyttäen, joka on verrattavissa matkapuhelimiin kohdistettavaan radiolähetykseen. WEA-viestiennän kanssa yhteensopiva puhelin on aina tietyllä taajuudella ja siten valmis vastaanottamaan WEA-viestejä. CB-teknologia käyttää avukseen tukiasemia tietyllä alueella lähettääkseen viestin WEA-varustettuihin puhelimiin näiden tukiasemien toimintasäteellä. CB-järjestelmän merkittävin etu on, ettei se edellytä puhelimen rekisteröintiä tai paikannusta. Järjestelmä ei myöskään käytä samoja taajuuksia kuin puhelinliikenne, jolloin järjestelmä toimii myös puhelinverkon ollessa ylikuormittunut eikä vastaavasti rasita puhelinverkkoa (Samarajiva & Waidyanatha 2009). Viestit välittyvät automaattisesti viestiä lähettävässä tukiasemasolussa oleviin puhelimiin. Älypuhelinsovelluksen kautta toteutettu vastaava viestintä onnistuisi vain jos puhelimen käyttäjä jakaa sijaintinsa.

CB-tekniikka on tunnettu Suomessa jo 1990-luvulta saakka, mutta käyttöönoton ongelmaksi ovat nousseet palvelun kustannukset. Viestintäviraston toimeksi antaman Viestintäverkkojen

tekniset viranomaisvaatimukset -ryhmän SMS/CBS-alaryhmän työryhmäraportissa "Tekstiviestijärjestelmät väestön varoittamisessa" vuodelta 2005 esitettiin suuntaa-antavia arviota CB-järjestelmän hankintakustannuksista. Kokonaishankintahintoina kolmen operaattorin osalta raportissa päädyttiin arvioon noin 4,5–6 miljoonan euron kustannuksista, joiden lisäksi huomioon tulee ottaa järjestelmään varattuna olevan radiokapasiteetin kustannukset. Työryhmän raportissa viitataan Ruotsissa tehtyyn selvitykseen CBS-järjestelmän käyttökustannuksista (ilman radiokapasiteetin kustannuksia), joiksi arvioitiin 1,5–3 miljoonaa euroa vuodessa. Verkko-operaattoreiden puolella CBS-järjestelmän käyttöönoton arvioitiin edellyttävän mm. CBC-laitteiston hankkimista, verkkoelementtien päivityksiä, yhteyksien rakentamista, hälytysalueiden määrittelyä ja henkilöstön koulutusta sekä testausta. (Viestintäverkkojen tekniset viranomaisvaatimukset -ryhmän SMS/CBS-alaryhmä 2005, 17–18)

5.1 WEA- ja CAP-tietomallit

WEA-hälytysviesti lähetetään CAP-muodossa (Common Alert Protocol), joka on avoin, vapaasti käytettävissä oleva XML-pohjainen[3] viestiformaatti hälytys- ja huomioviestien lähettämiseen. Formaatti on laajasti yhteensopiva eri järjestelmien kanssa, eikä se ole sidottu mihinkään yksittäiseen järjestelmään tai toimittajaan. Formaatin tietokokonaisuuksia ovat 1) hälytyksen tiedot (kuten osoite ja tehtävän tila), 2) tarkemmat tiedot (tapahtuman luokitus ja kuvaus sekä linkki lisätietoihin), 3) apulähteet (eli linkit ulkopuolisille sivustoille) sekä 4) sijainti (kuten koordinaatit). (Common Alerting Protocol 2010)

Vaaratiedotteen sisältö voidaan konfiguroida ennalta määritellyistä, koodattavista osista. Tällöin viestin lähettävä taho poimii varoitusviesteille luodusta tietokannasta vaihtoehdot, joiden perusteella luodaan koodattu varoitusviesti. Varoitusviesti lähetetään eteenpäin koodattuna, ja puhelin, joka vastaanottaa koodatun viestin, kääntää sen ymmärrettävään muotoon. Koodiksi pakattu viesti on kooltaan tekstipitoista viestiä pienempi, jolloin se kulkee verkossa nopeammin ja kuormittaa sitä vähemmän. Tällaisessa muodossa lähetetyt viestit ovat lisäksi eivät riipu käytetystä kielestä, sillä viestin vastaanottava sovellus voi purkaa koodatun viestin käyttäjän valitsemalle kielelle. Valmiiksi määritellyt viestiosiot mahdollistavat myös vaaratiedotteiden yhdenmukaisen rakenteen ja auttavat ehkäisemään puutteellisen tai virheellisen informaation lähettämistä. (Párraga Niebla, Muna, Grazzini & Pfeffer, 2013)

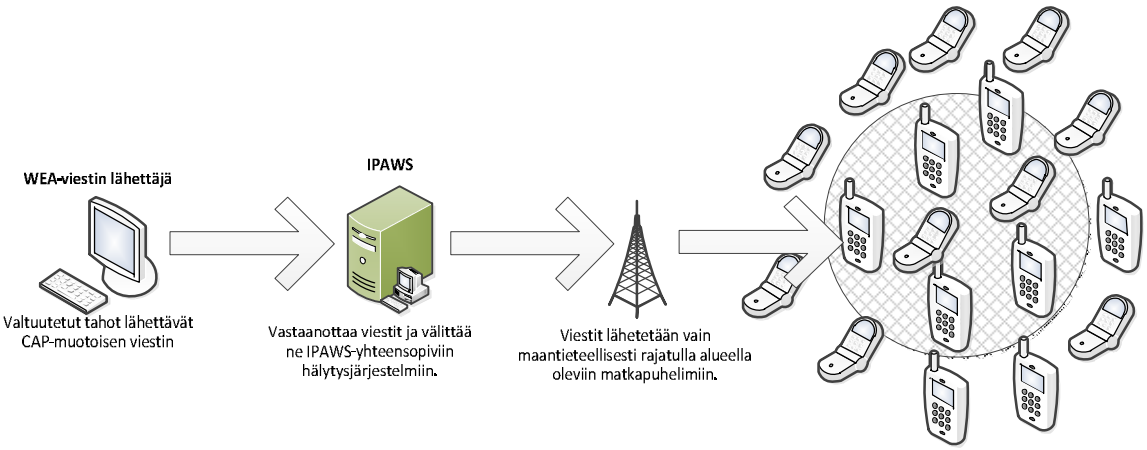
WEA-viestiin sisältyvät tiedot poimitaan huomattavasti tarkemmasta CAP-viestistä. CAP-viestistä poimitut tiedot näytetään WEA-viestissä muotoiltuina. Esimerkiksi WEA-viestin voimassaoloaika, siis aika, jonka WEA-viestin varoitus on voimassa, saadaan CAP-viestistä muodossa "2003-06-17T16:00:00-07:00", kun WEA-viestissä näytetään pelkistetysti "until 7:00 PM PDT". CAP-viestiin sisältyy useita tarkentavia tietoja, joita ei näytetä tai käytetä WEA-viestissä. Taulukossa 2 on esitetty CAP- ja WEA-viestien välinen yhteys. Liitteessä 1 on kuvattu tarkemmin CAP-viestin rakenne ja liitteessä 2 viestin luokkakaavio.

[3] XML-kieltä (Extensible Markup Language, laajennettava merkintäkieli) käytetään pääasiassa rakenteisten dokumenttien luomiseen. XML-kieli ei ole ohjelmointikieli, pikemminkin datan rakentumista kuvaava järjestelmä, joka helpottaa tiedon esittämistä jonkin muun sovelluksen kautta. (Nykänen 2003)

Taulukko 2. WEA- ja CAP-viestien yhteydet (mukaillen FEMA 2012)

CAP-viesti		WEA-viesti	
CAP-viestin osa	CAP-esimerkki	WEA-viestin osa	WEA-esimerkki
Tapahtumakoodi (Event Code)	FFW	Tapahtuman nimi	Flash Flood Warning
Sijaintikoodi (Location Code)	6109	Alue	in this area
Päättyminen (Expires)	2003-06-17T16:00:00-07:00	Voimassaolo	until 7:00 PM PDT
ToiminnanTyyppi (Response Type)	Avoid	Lyhyt kuvaus	Avoid hazard
Lähettäjä (Sender ID)	NWS	Lähettäjä	NWS

Viestit välitetään IPAWS-Open (Integrated Public Alert and Warning System Open Platform for Emergency Networks) alustan kautta. IPAWS-alusta vastaanottaa ja varmentaa viestit, ja välittää ne IPAWS-yhteensopiviin hälytysjärjestelmiin, kuten WEA-järjestelmään. [4]



Kuva 6. WEA-järjestelmä yksinkertaistaen

WEA-muotoiseen viestiin sisältyy taulukon 3 mukaan tilanteen nimi, viestin voimassaoloaika sekä lyhyt kuvaus tilanteesta, sekä viestin lähettäjä. Viesti kertoo vastaanottajalle tämän olevan hätä- tai häiriötilanteen vaikutusalueella. Hätä- tai häiriötilanteen vaikutusaluetta ei kuvata tarkemmin, koska ilmoitukset lähetetään maantieteellisesti kohdennettuna. Tilanteen jälkeen voidaan lähettää vielä varmistusviesti, jossa erikseen ilmoitetaan tilanteen olevan ohitse. Taulukossa 4 on esitetty muutama esimerkki WEA-viesteistä.

[4] WEA -järjestelmän rinnalla Yhdysvalloissa on käytössä Emergency Alert System (EAS) -varoitusjärjestelmä, jonka viestit kulkevat myös IPAWS-alustan kautta. EAS on kansallinen varoitusjärjestelmä, joka edellyttää mm. televisio- ja radiolähetysten, kaapelitelevisiojärjestelmien ja satelliittilähetysten tarjoajat mahdollistamaan Yhdysvaltain presidentille viestintävalmiudet kansalaisten tavoittamiseen kymmenen minuutin sisällä kansallisesta hätätilanteesta.

Taulukko 3. WEA-viestin perusrakenne

Tapahtuman nimi	Tapahtumaa kuvaava otsikko
Alue	Alueen rajoitus, eli ilmoitus "tapahtuma on alueellasi".
Voimassaolo	Aika, johon asti viesti on voimassa.
Lyhyt kuvaus	Lyhyt kuvaus tai toimintaohjeet tilanteeseen.
Lähettäjä	Viestin lähettäjän nimi tai sen lyhenne

Palvelun kautta voidaan välittää varoitusten lisäksi myös muita kansalaisia koskevia viestejä. Esimerkiksi AMBER-viestit voivat koskea muun muassa katoamisilmoituksia, silminnäkijähavaintoja tai muita tärkeitä tiedotteita, joissa pyydetään seuraamaan paikallista mediaa tärkeiden ilmoitusten osalta tai kuvataan etsintäkuulutetun ajoneuvon tuntomerkkejä. AMBER-viestit voivat myös erota edellä esitetystä WEA-viestin perusrakenteesta (AWARE 2013).

Taulukko 4. Esimerkkejä WEA-viesteistä (lähde: Ready.gov 2013; 6abc.com 2013; AWARE 2013)

Tapahtuman nimi	Alue	Voimassaolo	Lyhyt kuvaus	Lähettäjä
Tornadovaroitus	tällä alueella	kello 18:30 saakka.	Hakeudu suojaan. Seuraa paikallista mediaa.	- NWS
AMBER-hälytys on annettu	alueellasi		seuraa paikallista mediaa.	
AMBER-hälytys:			seuraa paikallista mediaa. LIC/B27504V (WA) 1998 Black Ford F-150	
AMBER-hälytys	alueellasi		on ohi.	

6 Mahdollisuuksia tietomalleiksi

Tässä luvussa esitetään mahdollisia tietomalleja erilaisten sovellusten ja niiden käyttötarkoitusten mukaan. Seuraavassa on hahmoteltu tietomalleja onnettomuuden elinkaaren eri vaiheissa aktivoituihin sovelluksiin.

6.1 Ennalta ehkäisevä viestintä

Ennaltaehkäisevässä viestinnässä käytettävät sovellukset voivat käyttää tiedon lähteenä jo olemassa olevia materiaaleja, kuten kirjoja tai oppaita (esim. Pelastustoimen turvaopas) tai verkkoaineistoja (esim. Terveysportti). Tällaiset tiedot ovat luonteeltaan staattisia, ja ne voidaan saattaa älypuhelinsovelluksen käyttämään muotoon manuaalisesti tai erilaisia teknisiä ratkaisuja käyttäen. Varsinaisen tekstin lisäksi mukaan voidaan liittää myös kuvia, videoita ja linkkejä lisätietoihin. Sovellusten käyttötarkoitus on antaa vinkkejä ja ohjeita oikeista toimintatavoista, joilla onnettomuusriskiä voidaan vähentää.

Taulukko 5. Mahdollinen tietomalli ennaltaehkäisevään viestintään (sisältölähde: Sisäasiainministeriön pelastusosaston ja Suomen Pelastusalan keskusjärjestön Kodin turvaopas)

Otsikko	Vältä sähköpalot	Käytä grilliä oikein
Ennaltaehkäisevät toimenpiteet	1. tarkista sähköjohdot 2. älä peitä pattereita 3. jätä ilmatilaa 4. käytä oikeatehoista lamppua	1. sytytä grilli oikein 2. sammuta grilli huolella 3. kaasu- ja sähkögrillit
Tarkempi toimintaohje	1.1. Huonokuntoiset sähköjohdot pitää vaihdattaa ehjiin. Määräajoin tehtävä sähköasennusten kuntotarkastus on hyvä keino estää sähkön aiheuttamat vahingot. 1.2. Korjaukset ja asennukset on aina teetettävä ammattilaisella. 1.3. Testauslaitoksen merkki sähkölaitteessa (esim. FI-tunnus) tarkoittaa, että puolueeton testauslaboratorio on todennut laitemallin turvalliseksi.	1.1 Sytytä grilli takkatikuilla tai grillisytyttimellä. 1.2 Siirrä tulentekovälineet ja sytytysaineet pois lämmönlähteen, avotulen ja lasten lähettyviltä. 1.3 Bensiiniä tai spriitä ei saa käyttää sytyttämiseen. 1.4 Leimahdusvaaran välttämiseksi anna sytytysnesteen ensin riittävästi imeytyä hiiliin ja sytytä vasta sitten. 1.5 Käytä suojakäsineitä grillatessa, äläkä työnnä kasvoja liian lähelle.
Liite	1.1.1. Kuva	1.1.1. Web: Lisätietoja www.xxx.fi
Lähde	Pelastustoimen turvaopas	Pelastustoimen turvaopas

6.2 Vaaratiedotteen uusi tietomalli

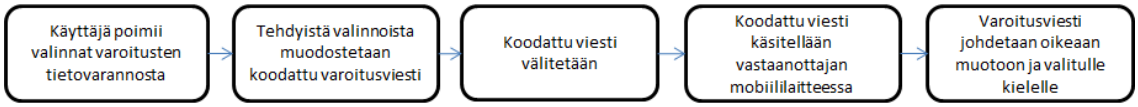
Nykyinen vaaratiedote koostuu kuudesta eritellystä tietoelementistä: otsikosta, paikka- tai aluetiedosta, päivämäärästä ja kellonajasta, vaaratilanteen kuvauksesta, toimintaohjeista, sekä tiedot tiedottavasta viranomaisesta. Lisäksi vaaratiedoteoppaaseen on liitetty fraasiluettelo, jota vaaratiedotteen lähettävä viranomainen voi käyttää apuna tiedotteen kirjoittamisessa.

Näiden ominaisuuksien pohjalta olisi mahdollista luoda järjestelmä, jossa vaaratiedote rakennetaan valmiiksi määritellyistä vaihtoehdoista valitsemalla.

Taulukko 6. Vaaratiedotteen muodostaminen valmiiksi määritellyistä osista

Vaaran tyyppi	Paikka	Aika	Toimintaohje	Lähde
1. Kemikaalivuoto 2. Maastopalo 3. Mellakka 4. Räjähdysvaara 5. Säävaroitus 6. Tulipalo . . .	Lääni A Maakunta A.1. Kunta A.1.A Alue A.1.A.1	PP/KK/VVVV hh/mm/sek.	1. Pysy sisällä 2. Sulje ikkunat 3. Mene suojaan 4. Poistu alueelta 5. Vältä aluetta . . .	Viranomainen A Pelastuslaitos A.1 . . .

Näin muodostettu viesti olisi mahdollista lähettää eteenpäin koodattuna siten, että vastaanottajan puhelin avaa kodin luettavassa muodossa – ja valitulla kielellä.



Kuva 7. Koodatun viestin lähetys ja vastaanotto (mukaillen Párraga Niebla & al, 2013)

Valmiista "rakennuspalikoista" koostettu varoitusviesti on rakenteeltaan ja sisällöltään selkeä ja määritellyt viestin osat ehkäisevät puutteellisen informaation eteenpäin lähettämistä. Viestin koostaminen valituista paloista voi myös tapahtua nopeammin kuin sen kirjoittaminen alusta loppuun.

6.3 Vaaratilanteen aikainen viestintä

Hätä- ja häiriötilanteen kohdatessa sen vaikutuspiiriin kuuluvien henkilöiden, kuten onnettomuuden uhrien ja heidän omaistensa, tiedontarve korostuu. Erityisesti toivotaan tietoa ja toimintaohjeita pelastustoimia ohjaavilta viranomaisilta. (Huhtala & Hakala 2007, 17) Taulukossa 7. on kuvattu vaaratilanteen aikaisen sovelluksen tietomalli viranomaisen ja kansalaisen väliseen viestintään silloin, kun vaaratilanteesta on jo varoitettu. Tällaiset häiriötilanteen aikana aktivoituvat sovellukset voidaan ladata puhelimeen jo ennen hätä- ja häiriötilanteen käynnistymistä, tai ne voidaan ottaa käyttöön sellaisen kohdatessa.

Sovelluksen kautta älypuhelimiin toimitettavan viestin sisältö voisi olla käytettävissä myös muissa järjestelmissä, esimerkiksi internet-sivuilla. Esimerkiksi CAP-viesti toimitetaan useaan järjestelmään, joissa hyödynnetään viestin eri osia.

Taulukko 7. Mahdollinen tietomalli vaaratilanteen aikaiseen viestintään

Otsikko	Toimintaohje	Toimintaohje	Toimintaohje
Hätä-, häiriö- tai vaaratilanne	Räjähdysvaara Vihtavuoressa	Räjähdysvaara Vihtavuoressa	Räjähdysvaara Vihtavuoressa
Pvm ja kellonaika	12.7.2013 klo 10.00	12.7.2013 klo 17.15	12.7.2013 klo 21.30
Tilannepäivitys	Räjähdysvaara kasvanut.	Räjähdysvaara jatkuu	Räjähdysvaara ohi.
Toimintaohje	Vihtavuoren alue evakuoidaan välittömästi Sydän-Laukaan koululle. Ota mukaan välttämättömät lääkkeet.	Vihtavuoren alue evakuoitu, älä liiku alueella.	Evakuointikäsky purettu, vaara ohi.
Liite	Web: Lisätiedot: www.xxx.fi	Web: Lisätiedot: www.xxx.fi	
Tiedottava viranomainen	Keski-Suomen pelastuslaitos	Keski-Suomen pelastuslaitos	Keski-Suomen pelastuslaitos

6.4 Kansalaisen viestintä viranomaiselle

Hätä- ja häiriötilanteen aikana käytettävä sovellus voisi mahdollistaa onnettomuusalueella tai tilanteen vaikutuspiirissä olevien toimimisen tiedonlähteinä niin viranomaisille kuin muille kansalaisille. Älypuhelinsovellukseen syötettävät tiedot voitaisiin luokitella tietomallin mukaisesti, jolloin käyttäjien syöttämä tieto olisi rakenteeltaan yhdenmukaista ja helpommin jäsennettävää kuin rakenteeltaan vapaamuotoinen teksti. Tiedon tuotannon luotettavuutta voidaan pyrkiä lisäämään edellyttämällä käyttäjää jakamaan esimerkiksi sijaintietonsa.

Taulukko 8. Mahdollinen tietomalli kansalaisten viestintään

Otsikko	Tieto alueelta	Kuva alueelta
Hätä-, häiriö- tai vaaratilanne	Asta-myrsky	Asta-myrsky
Pvm ja kellonaika	30.7. 2010 klo 14.00	30.7. 2010 klo 17.15
Raportti / tieto	Tie 69 poikki Istunmäen kohdalta.	Puita kaatunut sähkölinjoille, kuva.
Lähettäjä	L. Hokkanen	P. Paananen
Paikkatieto	N 6948608 E 475655	N 6984167 E 411983
Liite	----	Kuva

6.5 Tietomallien toteutuksesta

Tietomallien voidaan ajatella ilmenevän älypuhelin- tai muiden sovellusten kautta: näiden avulla niin kansalainen kuin viranomainen voivat tuottaa, jakaa ja vastaanottaa tietoa, joka jäsentyy järjestelmän sisällä tietomallin mukaisesti. Kansalaisen käyttämän varsinaisen älypuhelinsovelluksen tai WEA-tyyppisen järjestelmän lisäksi viranomaiset tarvitsevat käyttöönsä sovelluksen, jolla kokonaisuutta hallitaan. Oleellista on, että sovellukset ovat selkeitä ja helppokäyttöisiä – niin yksinkertaisia, että niitä voi käyttää ilman ennakkoon perehtymistä. Toisaalta viranomaisen sovelluksen tulee tukea hektistä toimintaa tilanteen

aikana ja ehkäistä esimerkiksi sovelluksen kautta lähetettävän hätätiedotteen lähettäminen vahingossa tai väärälle kohdeyleisölle.

Tietojen lähettäminen älypuhelinsovelluksesta taustalla toimivaan tietovarastoon voi tapahtua erilaisin keinoin verkkoyhteyden tai Cell Broadcast (CB) -teknologian avulla. Tiedot voidaan lähettää esimerkiksi WEA-järjestelmän tapaan XLM-rakenteisena, joka mahdollistaa myös järjestelmän kehittämisen sekä laajentamisen. Jyväskylän yliopiston tietotekniikan laitoksen

Sapporo -hankkeessa on hiljattain kehitetty älypuhelimia hyödyntävä kriisiviestinnän järjestelmä, jonka avulla voidaan lähettää kohdennettuja varoitusviestejä yksityisten ihmisten matkapuhelimiin sekä suurten organisaatioiden ja yhteisöjen henkilöstölle. Hälytyksiä voidaan vastaanottaa sekä tavallisilla että älypuhelimilla, ja järjestelmän käyttäjät voivat lähettää sen avulla myös hätäkutsuja. Matkapuhelinten lisäksi hälytykset voidaan lähettää useille muunlaisille päätelaitteille kuten työasemille ja tablettitietokoneille, sähköisille ilmoitustauluille, sosiaaliseen mediaan ja tiedotusvälineille. (Jyväskylän yliopisto 2013) Järjestelmä perustuu satelliittipaikannukseen. Järjestelmä toimii kaikissa verkoissa - mikäli matkapuhelinyhteydet ovat poikki, se toimii langattomien lähiverkkojen kautta. Sovellus mahdollistaa myös kaksisuuntaisen viestinnän. Ohjelmisto on kehitetty Android-alustalle, mutta hätäviestit välittyvät myös muihin uusiin ja vanhoihin matkapuhelimiin tekstiviesteinä (Kuula 2013). Järjestelmää on testattu mm. poliisin valmiusryhmien sisäisenä testauksena sekä poliisin suorittamana sisältö-/väestötestauksena. Testien perusteella poliisin lähettämien hälytysviestien alueellista kohdentamista pidettiin hyvänä. Testauskokemusten johtopäätöksenä todettiin, että älypuhelinviestien personointia ja sisältöjä sekä kohdennetun mobiiliviestinnän hälytyskynnystä viranomaiskäytössä pitäisi pohtia lisää ennen laajamittaisen hälytysviestinnän aloittamista suoraan väestölle. Lisäksi haasteeksi nähtiin se, ettei organisaatioiden nykyisissä toimintaohjeissa ei ole ohjeistusta vuorovaikutteisten mobiilihälytysten ja tilannekuvajärjestelmien käytölle, esimerkiksi liittyen siihen, kuka/mikä organisaatio voi varoitusviestejä lähettää. (Kuula 2013) Järjestelmän laajamittaisempi kokeilu viranomaisten viestinnässä voisi olla yksi suunta varoitusviestinnän kehittämisessä. Valittavasta teknologiasta riippumatta sovellusten toiminnan tulee olla mahdollisimman alustariippumatonta, jotta se ei jatkossa sido liikaa tiettyihin toimittajiin tai tekniikoihin.

Paitsi viranomaisviestinnässä, viranomaisten tuottamaa tietoa voidaan hyödyntää myös kaupallisessa toiminnassa. Suomi on liittynyt maailmanlaajuiseen Open Government Partnership (OGP) -aloitteeseen, jonka tavoitteena on entistä läpinäkyvämmän, tuloksellisemman ja tilivelvollisemman hallinnon kehittäminen. Osana aloitteeseen liittyvää Avoimen tiedon ohjelmaa selvitetään asiakirjamuotoisen tiedon avaamista rakenteellisena. Avoimen tiedon ohjelma käynnistetään yhtäaikaisesti Avoimen hallinnon toimintasuunnitelman toimeenpanon kanssa. Toimintasuunnitelman ensimmäisenä vuonna kootaan tietoa julkisen hallinnon tietovarannoista ja niiden sisältämistä tiedoista. (Valtiovarainministeriö 2013, 4–5)

Julkishallinnon tietovarantojen avautuessa data, jota voi käyttää erilaisten sovellusten pohjana, lisääntyy entisestään. Sovellukset voivat yhdistää eri lähteistä tulevaa dataa tiedoksi varsin innovatiivisillakin tavoilla ja vastata siten mitä erilaisimpiin tarpeisiin. Esimerkiksi Sisäasiainministeriön pelastusosaston ja Suomen Pelastusalan keskusjärjestön Kodin turvaoppaan[5] tietosisältö mahdollistaisi wikiHow: How to and DIY Survival Kit -sovelluksen[6] kaltaisen mobiilioppaan luomisen.

[5] Kodin turvaopas on saatavilla verkosta osoitteesta http://turvaopas.pelastustoimi.fi.

Yleisesti sovellustuotannon kannalta hedelmällinen kehittämisen suunta voisi olla viranomaistietoihin perustuvien CAP-muotoisten "informaatiopakettien" lähettäminen. Tieto – vaikkapa onnettomuudesta tai muusta hätätilanteesta – voitaisiin lähettää yhteisellä, rakenteeltaan avoimella ja ilmaisella formaatilla, joka olisi eri toimijoiden käytettävissä ja edelleen sovellettavissa, mukaan lukien viranomaiset itse. Kuten CAP-viesteissä, tämä formaatti voisi pitää sisällään rakenteista julkista tietoa, jota voitaisiin automaattisesti jakaa ja josta olisi jalostettavissa WEA-viestien tapaan kansalaisille toimitettavaa tietoa.

[6] WikiHow: How to and DIY Survival Kit on ilmainen iPhone-, iPad-, ja iPod-alustoille saatavilla oleva sovellus. Sovellus sisältää wikiHow-sivustolta löytyviä ohjeita, mm. ensiapuohjeita sekä muita ohjeita luonnononnettomuuksien, kolarien ja kodin tapaturmien varalle. Lisäksi sovelluksesta löytyy viihteellistä sisältöä, kuten ohjeita juhliin.

7 Yhteenveto

Älypuhelinsovellusten avulla on mahdollista paitsi jakaa ennalta ehkäisevää, luonteeltaan staattista viranomaistietoa esimerkiksi opassovellusten muodossa, myös reaaliaikaista ohjeistusta hätä- tai häiriötilanteen vaikutuspiiriin kuuluville henkilöille. Viranomaisten lisäksi myös kansalaiset voivat toimia tiedon tuottajina – sovellusten avulla tätä tietoa voidaan johtaa viranomaisten, ja muiden kansalaisten, käyttöön. Älypuhelinsovellukset voivatkin hyödyntää ja yhdistää toiminnassaan moninaista tietoa, jota voivat tuottaa niin teknologiset sensorit kuin sovellusta käyttävät henkilöt. Kehitettäessä sovelluksia viranomaisten viestintään hätä- ja häiriötilanteissa ja ennaltaehkäisevässä viestinnässä on oleellista, että sovellukset, niiden toiminta ja tietosisällöt ovat luotettavia. Kansalaisten ja kolmansien osapuolten tuottaman tiedon luotettavuutta voidaan parantaa hyödyntäen esimerkiksi välitettyyn tietoon liittyvää metadataa (esimerkiksi käyttäjän tiedot, sijaintitiedot).

Tässä osiossa avattiin tarkemmin erityisesti varoitusviestinnän tietomalleja sekä tarkasteltiin tiedon tuotannon eri näkökulmia. Viranomaisten vaaratiedottamisessa viestinnän monikanavaisuus on olennaista. Älypuhelimien (ja niihin liittyvien älypuhelinsovellusten) nopeasti kasvava määrä tarjoaa uuden kanavan muun muassa nopealle varoitusviestinnälle. Nykyistä vaaratiedotejärjestelmää on kritisoitu siitä, ettei se mahdollista alueellista tai paikallista vaaratiedottamista. Älypuhelimien ja niihin luotujen sovellusten avulla varoitusviesti voitaisiin lähettää vaara-alueella oleville henkilöille kohdennetusti esimerkiksi Cell broadcasting -järjestelmän avulla. Push-muotoisena viestinä toimitettavien varoitusten lähettämiseen vaadittavaa teknologiaa ja sen käyttöönottoon liittyviä kustannuskysymyksiä tulisikin jatkossa selvittää.

Jo nyt hätäkeskuksen tietojärjestelmästä lähetetään hätäilmoituksen tekijän antamiin tietoihin pohjautuvat julkiset ensitiedotteet automaattisesti: tätä tietoa johdetaan edelleen erilaisille internetsivuille (esim. Tilannehuone.fi) ja älypuhelinsovelluksiin (esim. Hälytyskeskus). Viestintäprosesseja ja -teknologioita tarkastelemalla voitaneen löytää nykyisiin käytäntöihin niveltyviä uusia tapoja hyödyntää sosiaalista mediaa ja mobiiliteknologiaa viranomaisviestinnässä. Viranomaisten viestintäprosesseja tarkastellaan raportin seuraavassa osiossa.

Osa II – Palveluntuotanto ja viestintä sosiaalisessa mediassa

8 Johdanto

Sosiaalisen median hyödyntämismahdollisuuksia pohdittaessa on otettava huomioon palveluiden ominaisuuksien, rajoitusten, ja mahdollisuuksien ohella myös palveluntarjoajien rooli sekä näiden asettamat rajoitukset ja mahdollisuudet. Tässä osiossa selvennetään sosiaalisen median palveluiden tuottamiseen ja käyttämiseen liittyviä reunaehtoja sekä pohditaan sosiaalisen median soveltamista hätä- ja häiriötilanneviestinnässä. Sosiaalisella medialla viitataan tässä yhteydessä yleisesti välineeseen, sillä se käsittää terminä paremmin ne kaikkien eri palveluiden tarjoamat mahdollisuudet välittömän, ajantasaisen, sisällöltään monimuotoisen, paikasta ja ajasta riippumattoman sekä tasavertaisen viestinnän erilaatuisten ja kokoisten yleisöjen välillä. Sen sijaan sosiaalisen median asettuminen terminä muun muassa tietoverkkojen, niitä ylläpitävien palvelimien, käytettävien laitteiden sekä näiden laitteiden fyysisten sijaintien alaisuuteen edellyttää teeman pilkkomista pienempiin osiin (Pesonen 2013). Selvennämme siten lyhyesti lukijalle sosiaalisen median toimintaperiaatteita sekä teknisestä että palvelun käyttämisen näkökulmasta menemättä kuitenkaan syvemmälle esimerkiksi ohjelmointi-infrastruktuuriin.

Myös sosiaalisen median palveluiden käyttämiseen liittyvät oikeussuhteet vaativat selventämistä, sillä ne liittyvät keskeisesti palvelun käyttämiseen. Sosiaalisen median palveluiden toimintaperiaatteiden pohjalta muodostuu monitahoisia asiakkuus- ja sopimussuhteita. Tyypillisimpiä muotoja ovat sosiaalisen median palveluntarjoajien ja käyttäjien välinen suhde, käyttäjien väliset keskinäiset suhteet, sekä palveluntarjoajan ja kolmannen osapuolen – kuten mainostajan tai palvelun ja sen käyttäjien suhde ulkopuoliseen tahoon. Pohdimme seuraavassa lyhyesti näitä suhteita muun muassa rekisteröitymisen, käyttämisen, tiedonhallinnan sekä lainsäädännön osalta.

Tarkastelemme lopuksi myös sosiaalisen median palveluiden tuomaa muutosta viestinnälliseen toimintaan ja toimintakenttään. Keskitymme erityisesti pohtimaan sosiaalisen median uusia viestintäprosesseja suhteessa perinteiseen viranomaisviestintään liittyviin viestintäprosesseihin. Tarkastelemme viestintäprosesseja viestintävälineiden, viestintätapojen sekä viestinnällisten näkemysten muutoksen pohjalta, sekä esittelemme mahdollisuuksia uudenlaisten viestintätapojen ja välineiden hyödyntämiselle hätä- ja häiriötilanneviestinnässä.

9 Sosiaalinen media palvelutarjoajien, käyttäjien sekä tiedonhallinnan näkökulmista

Sosiaalinen media perustuu vuorovaikutteisen verkon sekä sen rakentumiseen liittyvien teknisten laitteiden ja järjestelmien kokonaisuuteen, jonka pohjalle luodut erilaiset verkkopohjaiset palvelut ja sovellukset tarjoavat käyttäjilleen mahdollisuuden sisällöntuottamiseen ja -jakamiseen. Sosiaaliseksi mediaksi voidaan periaatteessa lukea kaikki laitteet, sovellukset, alustat ja palvelut, jotka tarjoavat käyttäjälle mahdollisuuden informaation virtuaaliseen luomiseen, hakemiseen, saamiseen ja jakamiseen toisten kanssa. Terminä sosiaalinen media korostaa verkon ja sen käyttäjien sosiaalista ja kulttuurista muutosta viestinnän osalta. (Laaksonen, Matikainen & Tikka 2013, 13–14; Kaplan & Haenlein 2010; Gupta & Brooks 2013, 18)

Sosiaalisen median käsitettä ei useinkaan ole määritelty selkeästi. Seuraavassa esittelemme esimerkkejä tyypillisten sosiaalisen median palveluiden käytön edellytyksistä ja reunaehdoista. Keskitymme sosiaalisen median tarkastelussa sellaisiin palveluihin, jotka perustuvat lähtökohtaisesti avoimeen verkkoon ja ovat vapaasti kaikkien verkon käyttäjien ulottuvilla.

9.1 Lähtökohdat sosiaalisen median palveluiden käytölle

Sosiaalisen median käyttäminen edellyttää päätelaitetta, kuten mobiililaitetta tai tietokonetta, joka on mahdollista yhdistää tietoverkkoon, ts. internetiin. Internet on itsessään maailmanlaajuinen tietoverkko, joka koostuu pienemmistä tietoverkoista, toisiinsa kytketyistä tietokoneista, sekä näiden välisistä standardoiduista yhteyksistä. (ks. Oxford Dictionary) Päätelaitteen yhdistäminen tietoverkkoon on mahdollista monissa julkisissa tiloissa, kuten kirjastoissa, kahviloissa, yms., mutta esimerkiksi älypuhelimen yhdistäminen tietoverkkoon puhelinverkon kautta tai tietokoneen yhdistäminen tietoverkkoon kotona sijaitsevan tietoliikennekaapelin kautta vaatii tietoverkkoyhteyssopimusta asianomaisen palveluntarjoajan kanssa. Sopimuksen pohjalta käyttäjä voi muodostaa yhteyden viestintäverkkoon, jonka sisältö on edelleen erilaisten palveluntarjoajien hallinnoima. Päätelaitteen ja tietoverkkoyhteyden lisäksi käyttäjä tarvitsee verkkoyhteysohjelman, kuten esimerkiksi verkkoselaimen, joka mahdollistaa internetin sisällön ja palveluiden käytön. Yhdistettyään päätelaitteen viestintäverkkoon käyttäjä voi rekisteröityä haluamansa sosiaalisen median palvelun käyttäjäksi. (Pesonen 2013)

Tietoverkon käyttöä säädellään sähköisen viestinnän tietosuojalain puitteissa, joka määrittelee toisiinsa liitetyistä laitteista muodostuvan, viestien siirtoon ja jakeluun tarkoitetun verkoston viestintäverkoksi. Jokaisella tietoverkkoon yhdistävällä päätelaitteella on oma IP-osoite (Internet Protocol), joka toimii verkossa tunnisteena kyseiselle laitteelle. Kulloisellakin laitteella toteutetusta verkkoliikenteestä syntyy lokimerkintä vähintään palvelimelle johon tallentuu tiedot yhteydenottokohteesta ja ajankohdasta. Verkkoliikenne voi olla yhteydestä tai palvelusta riippuen suojattua tai suojaamatonta. Tiedot, jotka tallentuvat verkkoliikenteestä palvelimelle tai päätelaitteelle, asettuvat sähköisen viestinnän tietosuojalain mukaisten tunnistamistietojen alaisuuteen, sillä niistä on useimmiten tunnistettavissa esimerkiksi lähetettyjen viestien vastaanottaja tai yhteyskone. Näin ollen esimerkiksi teleyritys ei saa paljastaa palvelimilleen tallentuneita tietoja ulkopuoliselle, eikä niitä ulkopuolinen saa seurata. (Pesonen 2013, 136–137)

Sosiaalisen median palvelun käyttäminen edellyttää sopimusta kyseisen palvelun tarjoajan kanssa. Sosiaalisen median palveluun rekisteröityminen edellyttää useimmiten tunnistautumiseen liittyvien yhteystietojen tallentamista sosiaalisen median palveluntarjoajan tietokantaan. Useimmiten tällaisia tunnisteyhteystietoja ovat rekisteröity sähköpostiosoite tai matkapuhelinnumero. Päästäkseen palveluun on käyttäjän näin ollen myös tehtävä sopimus sähköpostipalveluntarjoajan tai teleoperaattorin kanssa. Palveluntarjoaja tekee tarjolla olevan teknologian puitteissa palvelun, johon käyttäjät saavat käyttöoikeuden sitoutumalla käyttöehtoihin. Palvelua voi käyttää millä tahansa tietokoneella, joka on yhteydessä tietoverkkoon, jossa on palvelua tukeva verkkoselain, tai vaihtoehtoisesti mobiililaitteella, jonka verkkoselain tukee palvelun käyttämistä tai sisältää palvelun käyttämiseen soveltuvan älypuhelinsovelluksen. Sosiaalisen median palveluiden käyttäminen mobiililaitteilla on yleistynyt viime vuosina merkittävästi (Hokkanen ym. 2013, 26–28). Useimmiten palveluiden käyttämiseen on tarjolla palveluntarjoajan oma älypuhelinsovellus, joka on optimoitu kääntämään palvelun ominaisuudet käytettäväksi mobiililaitteella sekä hyödyntämään älypuhelinten teknisiä ominaisuuksia, kuten esimerkiksi GPS-paikannusta tai kameraa. Älypuhelimella sosiaalista mediaa käytetään usein palveluntarjoajien itsensä tuottamien sovellusten kautta, sillä ne vastaavat usein parhaiten palvelun keskeisten ominaisuuksien hyödyntämistä myös muilla päätelaitteilla. Sitä vastoin esimerkiksi valtaosa osaraportissa I esittelemistämme sosiaalista mediaa hyödyntävistä älypuhelinsovelluksista toimii rajatun yksisuuntaisesti joko tuottaen käyttäjälleen tietoa tai keräämällä käyttäjien tuottamaa dataa. Näissä sovelluksissa sosiaalinen media on huomioitu lähinnä sovelluksen tietojen jakamismahdollisuuksissa; tietoja voi jakaa esimerkiksi sosiaalisen median kautta eteenpäin omille verkostoilleen. (Hokkanen, ym. 2013, 42) Sen sijaan sosiaalisen median hyödyntäminen vuorovaikutukseen sovellusten käyttäjien kanssa jää pintapuoliseksi. Näkemystä tukee myös se, että esimerkiksi Facebookin ja Twitterin hyödyntämisestä ennaltaehkäisevässä turvallisuusviestinnässä ja hätä- ja häiriötilanneviestinnässä on kokemusta ja tutkittua tietoa enemmän kuin tähän tarkoitukseen liittyvistä älypuhelinsovelluksista. Osaltaan tähän vaikuttanee myös se, että suosituimmilla sosiaalisen median palveluilla, kuten esimerkiksi Facebookilla ja Twitterillä on usein kapasiteettia kestää suuriakin käyttäjävolyymeja. Tällöin yhteisöpalveluja voidaan käyttää apuna viestien välittämisessä myös laajamittaisissa hätä- ja häiriötilanteissa (Bird, Ling & Haynes 2012, 27).

Sosiaalisen median palveluita tuottavat pääasiassa yksityiset yritykset sekä henkilöt, ja niiden perustuminen avoimeen verkkoon tekee niistä pääsääntöisesti alusta lähtien kansainvälisiä palveluita. Palvelut ja niiden markkinat ovat kuitenkin usein yrityksen alkutaipaleella paikallisia: esimerkiksi yhteisöpalvelu Facebook aloitti toimintansa Harvardin yliopiston sisäisessä käytössä, mutta levisi pian maailmanlaajuiseen käyttöön. Sosiaalisen median palveluiden paikallisuus voi perustua esimerkiksi rekisteröitymisrajoituksiin, joissa palveluun voi rekisteröityä vain tietyllä sähköpostiverkkotunnuksella (kuten esimerkiksi koulutusorganisaatiot), mutta useimmiten paikallisuus juontuu niiden vaihtelevasta suosiosta. Sosiaalisen median palveluiden suosion voidaan nähdä perustuvan niissä muodostettaviin sosiaalisiin verkostoihin sekä niiden väliseen vuorovaikutukseen. Paikallisesti suositussa palvelussa kyseisen alueen käyttäjien verkostot ovat hyvin edustettuina, jolloin palvelu voi näyttäytyä kyseisellä alueella oleville relevanttina ja houkuttelevana. Mikäli taas käyttäjän olemassa olevat sosiaaliset verkostot eivät ole palvelussa edustettuina, ei se välttämättä palvele tarkoitustaan sosiaalisen vuorovaikutuksen kanavana. Palveluiden suosio kasvaakin usein monien paikallisten sosiaalisten verkostojen välisten yhteyksien lisääntymisen seurauksena.

Sosiaalisen median kenttä on kuitenkin nopea muuntautumaan, ja uusia kilpailevia palveluja julkaistaan jatkuvasti. Sosiaalisen median palveluiden käyttäjämäärien kasvu on usein ennalta arvaamatonta. Siksi sosiaalisen median palveluja tarjoavat yritykset joutuvat kehittämään

palvelujaan kestämään suuria käyttäjävolyymeja sekä sietämään erilaisia häiriöitä. Suosituimmat sosiaalisen median palvelut ovatkin kehittäneet infrastruktuuriaan kestämään suuria käyttäjämääriä kerralla. Vastaavasti kuin palvelun tuottamisessa, on viranomaisviestinnässä huomioitava käytettävien palvelujen oletettu suosio tai käytettävyys. Esimerkiksi hätä- ja häiriötilanteissa suositaan tutkitusti sellaisia palveluja, joita on arkipäiväisessä toiminnassa totuttu käyttämään. (Vihalem, Kiisel & Harro-Loit 2012) Ennalta tuttujen palvelujen etuna on viestinnän perustuminen jo olemassa oleviin verkostoihin sekä niiden hyödyntämiseen. Näkemystä tukevat myös tutkimustulokset, joissa varoitusviestinnän on todettu olevan vaikuttavampaa silloin kun viestijän tai viestintäkanavan käsitetään olevan "lähellä" vastaanottajan omaa elämänpiiriä. (ks. esim. Taylor, Wells, Howell & Raphael 2012, Austin, Fisher & Yan 2012)

Sosiaalisen median palvelut vaativat lähes aina rekisteröitymisen. Palveluiden käyttäminen edellyttää usein myös profiilin luomista itseään koskevilla tiedoilla, jolloin käyttäjä yksilöidään palvelun käyttäjäksi. Profiileja ja rekisteröitymistä varten tallennetut henkilötiedot muodostavat sosiaalisen median palvelun henkilörekisterin (Pesonen 2013, 243). Käyttäjän näkökulmasta rekisteröityminen helpottaa palveluun palaamista. Käyttäjän ei tarvitse syöttää tietoja tai etsiä verkostoja uudelleen, vaan ne on tallennettu palveluntarjoajan palvelimelle ja ne latautuvat automaattisesti käyttäjän nähtäväksi ja käytettäväksi hänen kirjautuessaan palveluun. Palveluntuottajan näkökulmasta rekisteröityminen on paras tapa tunnistaa käyttäjä, pitää käyttäjäkunta ja julkaistu sisältö järjestelmällisessä muodossa ja näin myös helpottaa palvelun ylläpitoa sekä käyttäjän toimimista palvelussa. Sosiaalisen median palveluun rekisteröityminen edellyttää useimmiten tunnistautumiseen liittyvien yhteystietojen tallentamista sosiaalisen median palveluntarjoajan tietokantaan. Koska väärillä profiileilla esiintyminen on helppoa sosiaalisessa mediassa, vaatii lähes jokainen sosiaalisen median palvelu rekisteröitymisen tunnisteyhteystiedoksi vähintään rekisteröidyn sähköpostiosoitteen tai matkapuhelinnumeron. (Pesonen 2013, 242–243) Palveluun rekisteröityminen ja sen käyttäminen on yleensä ilmaista, mutta edellyttää palveluntarjoajan palvelulle asettamien käyttö- ja sopimusehtojen hyväksymisen. Nämä käyttö- ja sopimusehdot takaavat palveluntuottajalle muun muassa ylläpitovaltuudet esimerkiksi poistaa laitonta tai asiatonta sisältöä, mutta myös toteuttaa aktiivista valvontaa esimerkiksi käyttöehtosopimuksen noudattamisen sekä käyttäjien palvelussa toimimisen osalta mutta myös aktiivisesti valvoa esimerkiksi käyttöehtosopimuksen noudattamista sekä käyttäjien toimimista palvelussa. (Haasio 2013, Wrenn 2012, Achohido 2011) Aihetta esitellään tarkemmin luvussa 2.3 *Sopimussuhteet ja tiedonhallinta sosiaalisen median palveluissa*.

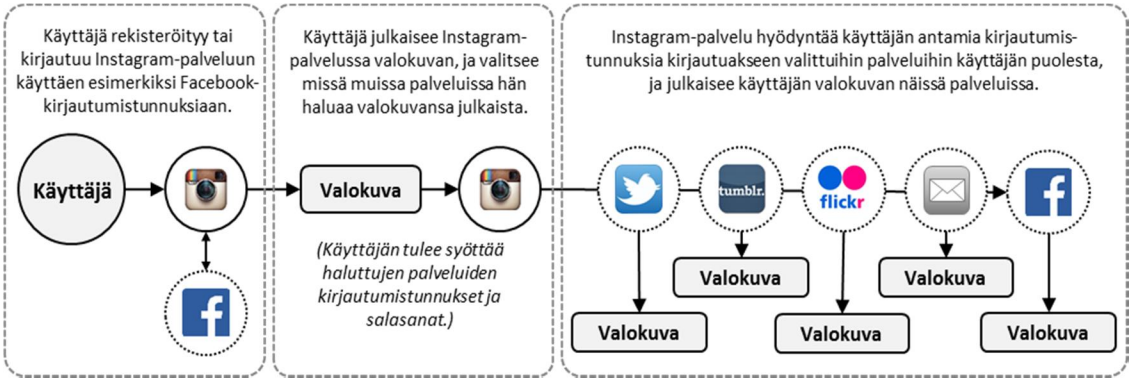
9.2 Sosiaalisen median palveluiden rajapinnat sekä ominaisuuksien yhdentyminen

Sosiaalisen median palvelut perustuvat useimmiten jonkin tietyn ominaisuuden tai tietynlaatuisen sisällön julkaisemiseen ja tarjoamiseen sekä tämän pohjalle rakentuviin sosiaalisiin verkostoihin. Palvelun jokin erityinen ominaisuus toimii yleensä palvelun keskeisenä kilpailutekijänä, sekä on syynä sen suosioon. Kilpailuedun säilyttäminen voi kuitenkin olla haastavaa, sillä palveluiden ominaisuuksien kopioiminen tai sisällyttäminen muihin palveluihin on osaavalle palveluntarjoajalle helppoa. Palvelun käyttäjämäärien lisääntyessä palveluntarjoajilla onkin tapana lisätä palveluun erilaisia ominaisuuksia, jotka helpottavat palvelun käyttämistä, sekä mahdollisesti tekevät muiden palveluiden välillä navigoimisesta vaivattomampaa. Tämä on johtanut sosiaalisen median palveluiden ominaisuuksien yhdentymiseen. Esimerkiksi Google on ottanut mallia Facebookin tilapäivitys- ja tykkäämistoiminnosta, Twitterin hashtag-asiasanamerkinnästä sekä Foursquaren

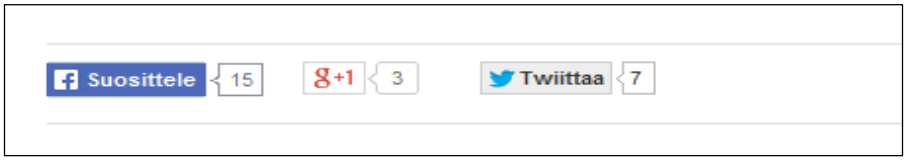
paikkakirjautumisesta, ja tuonut kaikki nämä ominaisuudet käytettäväksi omassa Google+-yhteisöpalvelussaan. Ominaisuuksien lisäämisellä pyritään luonnollisesti kehittämään palvelua sellaiseksi, että se pitää mahdollisimman hyvin jo saadut asiakkaat palvelun käyttäjinä.

Sosiaalisen median palvelut ovat kuitenkin monelta osin hyvin erilaisia. Niiden käyttötarkoitukset, niissä luodut verkostot ja niissä julkaistut sisällöt voivat näyttäytyä käyttäjälle hyvin erilaisilla tavoilla. Esimerkiksi LinkedIn-yhteisöpalvelu keskittyy pääosin ammatilliseen verkostoitumiseen, ja Twitter-mikroblogipalvelu taas erityisesti keskusteluun ja kommentointiin. Koska sosiaalisen median palveluiden toimintaperiaatteet vaihtelevat suuresti sekä sisällöiltään että ominaisuuksiltaan, on yhdellä henkilöllä usein profiili useammassa kuin yhdessä sosiaalisen median palvelussa. Helpottaakseen useiden profiilien hallintaa monet sosiaalisen median palvelut ja sovellukset tarjoavat käytettäväksi *Cross-platform-accessibility* -ominaisuuden, jossa yhden SoMe-palvelun kirjautumistunnuksia voidaan hyödyntää muihin palveluihin rekisteröitymisessä. Esimerkiksi Foursquare-paikkatietopalveluun rekisteröitymisessä voidaan käyttää Facebook- tai Google+-kirjautumistunnuksia, jolloin Foursquare-palvelu hakee kaikki kirjautumiseen tarvitsemansa tiedot käyttäjän Facebook- tai Google+-profiilista. Myös siirtyminen eri palveluiden välillä voi olla työlästä, mikäli esimerkiksi sama sisältö halutaan julkaista useissa eri palveluissa. Siksi monet palvelut tarjoavatkin mahdollisuuden sisällön ristikkäisjulkaisemiselle. Tällöin käyttäjä antaa yhdelle sosiaalisen median palvelulle myös muiden sosiaalisen median palveluiden kirjautumistunnukset, ja näin antaa tälle luvan julkaista sisältöä samanaikaisesti myös muissa palveluissa, mikäli nämä palvelut tukevat kyseisen sisällön julkaisemista. Esimerkiksi Instagramissa julkaistun kuvan voi muutamalla klikkauksella tai sormenliikkeellä julkaista myös Twitterissä, Facebookissa, Tumblrissa, Flickrissä tai sähköpostitse. Kuvassa 8. on havainnollistettu tyypillinen esimerkki ristikkäiskirjautumisen ja -julkaisemisen toimintaperiaatteesta Instagram-valokuvapalvelussa.

Ristikkäiskirjautumis- ja -julkaisemisominaisuutta hyödyntävät laajimmin uudet ja käyttäjämääriltään pienet palvelut, kun taas tarjoavat suurimmat palvelut, kuten Facebook, Twitter ja Google. Taulukoissa 9. ja 10. on listattu esimerkiksi tunnetuimpien sosiaalisen median palveluiden mahdollisuudet rajapintojen ylittämiselle.



Kuva 8. Esimerkki ristikkäiskirjautumisen ja -julkaisemisen toimintaperiaatteesta Instagram-valokuvapalvelussa



Kuva 9. Esimerkki sosiaalisen median jakamispainikkeista verkkosivulla

Taulukko 9. Ristikkäiskirjautuminen muutamissa tunnetuissa sosiaalisen palveluissa

CROSS-PLATFORM ACCESSIBILITY / Palveluiden ristikkäiskirjautumismahdollisuudet				
Palvelut, joiden kirjautumistunnuksilla voidaan kirjautua myös muihin palveluihin	Palvelut, joihin sisältöä voidaan rekisteröityä ristikkäiskirjautumisella			
	Facebook	Twitter	Youtube	Google+
Facebook				
Twitter				
Youtube				X
Google+			X	
LinkedIn	X			
Instagram	X			
Foursquare	X			X

Taulukko 10. Ristikkäisjulkaiseminen muutamissa tunnetuissa sosiaalisen palveluissa

CROSS-PLATFORM PUBLISHING / Palveluiden ristikkäisjulkaisemismahdollisuudet					
Palvelu, josta alkuperäinen julkaiseminen tapahtuu	Palvelut, joihin sisältöä voidaan julkaista ristikkäiskirjautumisella				
	Facebook	Twitter	Youtube	Google+	LinkedIn
Facebook		tilapäivitykset, linkit, valokuvat, videot, tapahtumat, paikkatiedot			
Twitter	tilapäivitykset, valokuvat, linkit, videot				
Youtube	videot	videot		videot	videot
Google+			videot		
LinkedIn		valokuvat, videot, teksti			
Instagram	valokuvat, videot	valokuvat, videot			
Foursquare	paikkatiedot, valokuvat, tykkäämiset, kommentit	paikkatiedot, valokuvat, tykkäämiset, kommentit			

Sosiaalisen median palvelut ovat pyrkineet madaltamaan myös käyttäjiensä muun verkossa toimimisen sekä palveluiden käyttämisen rajapintoja. Esimerkiksi erinäisillä verkkosivuille sijoitettavilla jakamispainikkeilla on pyritty helpottamaan sisällön julkaisemista palvelussa,

jotta käyttäjän ei tarvitse poistua varsinaiselta verkkosivulta (ks. kuva 9). Jakamispainikkeita on perusteltu muun muassa käyttäjän toiminnan helpottamisella, tiedon leviämisellä sekä yritysten verkkosivujen näkyvyyden kasvamisella (Mainstreethost 2012). Sosiaalisen median palveluiden ristikkäisjulkaisemisominaisuutta tarjoavat myös monet kolmannen osapuolen sovellukset. Esimerkiksi IFTTT-palvelu (*If this then that*) perustuu pelkästään käyttäjien toimintojen yhdistämiseen eri verkkopalveluissa. IFTTT-palvelussa käyttäjä voi luoda "resepteiksi" kutsuttuja toimintoprosesseja eri palveluiden välille antamalla IFTTT-palvelulle luvan käyttää tämän kirjautumistunnuksia eri palveluihin. Nämä toimintoprosessit muistuttavat suurelta osin ristikkäisjulkaisemisominaisuuksia, mutta ne voivat olla monimuotoisempia kuin itse palveluntarjoajan vaihtoehdot, sekä sisältää useampia palveluita, joiden välille prosesseja voidaan tehdä. Julkaistaessa esimerkiksi valokuva Instagramissa, voidaan IFTTT määrittää tallentamaan kyseinen valokuva Dropbox-pilvipalveluun.

Ristikkäiskirjautumista ja -julkaisemista hyödyntävät myös useat älypuhelin- ja käyttöjärjestelmävalmistajat. Esimerkiksi Applen iPhone-älypuhelimessa on sisäänrakennettu mahdollisuus tallentaa käyttäjän Twitter, Facebook, Flickr ja Vimeo-tunnukset puhelimeen, jolloin käyttäjä voi vaivattomammin jakaa sisältöä suoraan puhelimesta kyseisiin palveluihin, ilman tarvetta ladata sovellusta tai kirjautua palveluun. Vastaavia ominaisuuksia on myös olemassa WindowsPhonella sekä Googlen Android-käyttöjärjestelmässä. Palveluiden käyttämiseen on tarjolla paljon erilaisia sovelluksia, jotka hyödyntävät sosiaalisen median palveluja ristikkäiskirjautumisen kautta. Käyttäjän syöttäessä kirjautumistiedot sovellukseen, sovellus pystyy kirjautumaan palveluun ja toteuttamaan käyttäjän sovelluksessa tekemät toimenpiteet sosiaalisen median palvelussa. Ristikkäisjulkaisemisominaisuutta käyttävien sovellusten kohdalla on kuitenkin olemassa mahdollisuus, että sovellus voi halutessaan esimerkiksi julkaista käyttäjän sosiaalisen median profiilissa myös jotakin muuta sisältöä. Esimerkiksi kaupalliset sovellukset voivat hyödyntää käyttäjän sosiaalisen median profiilia mainosten levittämiseen tai verkostojen analysoimiseen. (Steel ja Fowler 2010) Älypuhelinsovellusten suunnittelu ja koodaaminen toteuttamaan erilaisia toimenpiteitä on riippuvainen älypuhelimen tai sen käyttöjärjestelmän tuottajan tarjoamista mahdollisuuksista. Esimerkiksi mobiilikäyttöjärjestelmien (iOS, Android, BB10 ja Windows) lähdekoodin avoimuus vaihtelee paljon tuottajien välillä, joka myös vaikuttaa niille tehtyjen sovellusten tarjontaan (Wilson 2013).

Erilaiset ristikkäisjulkaisemisen ja -kirjautumisen mahdollisuudet ovat tehneet useiden sosiaalisen median palveluiden seuraamisesta sekä niissä julkaisemisesta nopeampaa ja helpompaa. Se voi myös moninkertaistaa viestin tavoittavuuden. Hätä- ja häiriötilanneviestinnän näkökulmasta ristikkäiskirjautuminen ja -julkaiseminen voisivat helpottaa monikanavaisen viestinnän toteuttamista sosiaalisessa mediassa sekä lisätä mielikuvaa viranomaisen läsnäolosta sosiaalisessa mediassa. Mahdollisen sovelluksen tai palvelun tuottamisen näkökulmasta ristikkäiskirjautuminen tarjoaisi myös mahdollisuuden tunnistaa palvelun käyttäjä helposti esimerkiksi sosiaalisen median profiilin perustella.

9.3 Sopimussuhteet ja tiedonhallinta sosiaalisen median palveluissa

Sosiaalisen median palveluiden toiminta perustuu yleensä palveluntarjoajien liiketoimintaperiaatteisiin. Näin ollen ryhtyessään sopimussuhteeseen sosiaalisen median palveluntarjoajan kanssa käyttäjän tulee useimmiten hyväksyä sopimus palveluun tallentamiensa tietojen säilyttämisestä palveluntarjoajan rekistereissä, sekä antaa suostumus palveluun ladatun tiedon tallentamisesta ja käyttämisestä. Viranomaisten näkökulmasta sosiaalisen median palveluiden käyttäminen voikin olla monimutkaista, sillä palveluiden

käyttämiseen edellytettävät sopimusehdot ovat suostumukseen perustuvia ja samat kaikille käyttäjille, oli kyseessä viranomainen tai ei. Näin ollen palveluntarjoajilla on valta luoda edellytykset myös viranomaisen sosiaalisen median käytölle. Esimerkiksi yhteisöpalvelut tallentavat kaiken käyttäjistä suoraan tai epäsuorasti saamansa informaation, sillä niiden toiminta perustuu näiden tietojen kokoamiseen, tallentamiseen ja jatkokäsittelyyn. (Pesonen 2013, 245) Muun muassa tiedot siitä, missä tilapäivitykset on tehty, millä koneilla palveluja on käytetty ja missä palveluun ladatut valokuvat on otettu, tallentuvat palvelujen palvelimille määrittämättömän pitkäksi ajaksi (Haasio 2013).

Palveluntarjoajilla on myös mahdollisuus systemaattisesti valvoa toimintaa sosiaalisessa mediassa. Somessa julkaistaankin paljon sellaista informaatiota, joka ei välttämättä ole käyttäjän tietoisesti jakamaa. Koska valtaosa sosiaalisen median palveluista saa liiketulonsa suoramarkkinoinnista ja mainostuloista, palveluntarjoajat seuraavat käyttäjän käyttäytymistä somessa sekä hyödyntävät näitä tietoja markkinointitutkimuksissa. Tapoja seurataan muun muassa erilaisen metatason informaation kautta, jolloin käyttäjälle pyritään näiden pohjalta luodun profiilin mukaisesti tarjoamaan mainoksia häntä kiinnostavista tuotteista. (Pesonen 2013, 245) Monet sosiaalisen median palvelut tarjoavat käyttäjistä keräämäänsä tietoa myös ulkopuolisten käytettäväksi. Esimerkiksi Twitter tarjoaa palvelustaan ja käyttäjistään laajasti tietoa API-informaation (*Application Programming Interface*) muodossa, jota ulkopuoliset sovellus- ja palvelukehittäjät voivat hyödyntää muun muassa omien Twitteriä käyttävien palveluiden tai sovellusten kehittämisessä (Twitter, Inc. 2013a).

Palveluntarjoajien käyttämien tekniikoiden avulla käyttäjiä on mahdollista seurata tarkasti muiltakin osin, usein lakien ja käyttöehtojen rajapintoja hipoen. Useat sosiaalisen median palvelut seuraavat myös käyttäjän verkkoselaimen toimintaa, ja näin muodostavat profiileja käyttäjistä, heidän mielenkiinnon kohteistaan, elämäntapahtumistaan, asuinpaikoistaan ja liikkumisistaan. Sosiaalisen median palveluista ainakin Facebook tiettävästi seuraa, tallentaa ja analysoi käyttäjiensä palvelun ulkopuolista verkon käyttöä. Käytännössä tämä seuranta tapahtuu evästeiden (*cookies*) avulla, jolloin käyttäjän toiminta kyseisessä verkkoselaimessa tallentuu Facebookin käytettäväksi (Achohido 2011). Palveluihin ladatut tiedot sekä niissä julkaistut viestit voivat muodostaa valtavia henkilötietopankkeja, joita kansainväliset yhtiöt hallinnoivat ja määrittelevät. jotka ovat kulloistenkin kansainvälisten yhtiöiden hallinnoimia ja määrittämiä. (Pesonen 2013, 41) Facebook on myös kertonut käyttävänsä ohjelmaa, joka systemaattisesti skannaa tilapäivityksiä, yksityisviestejä sekä valokuvia rikollisen toiminnan havaitsemiseksi (Wrenn 2012). Palvelun käyttäjän suostumuksen pyytäminen tällaiseen valvontaan ei kuitenkaan ilmene esimerkiksi Facebookin käyttöehdoista. Sosiaalisen median palvelujen tarjoajat saattavat siis käyttää oikeusjärjestelmän näkökulmasta ylimitoitettuja keinoja rikollisen toiminnan kitkemisessä, sillä esimerkiksi Suomen lakien mukaan vain poliisi ja tulli voivat rikostutkinnassa lain suomien edellytyksin tutkia tietokoneita tai niiden sisältämiä viestejä. (Pesonen 2013, 105) Muun muassa näistä syistä esimerkiksi viranomaisen ja kansalaisen välisen viestinnän luottamuksellisuutta ei ole mahdollista taata sosiaalisessa mediassa.

Sosiaalisen median käyttäjien seuraaminen sekä tallennettujen tietojen käyttäminen palveluntarjoajien toimesta on noussut keskeiseksi aiheeksi kansalaisten tietosuojaan liittyvässä keskustelussa. Palvelut eivät esimerkiksi takaa käyttäjilleen tiedollista itsemääräämisoikeutta esimerkiksi siinä määrin kuin eurooppalainen tietosuoja edellyttäisi. Yhteisöpalveluiden käyttö edellyttää joidenkin henkilötietojen tallentamista palveluntarjoajan asiakasrekistereihin. Koska menettely perustuu useimmiten palveluntarjoajan sopimusehtojen hyväksymiseen, on käyttäjän myönnettävä palveluntarjoajalle oikeus kaiken itsestään palveluun tallentaman tiedon saatavuuteen määrittämättömän pitkäksi ajaksi. Vaikka näitä tietoja poistettaisiin tai muutettaisiin käyttäjän toimesta, jäävät aikaisemmat tiedot

useimmiten palveluntarjoajan käyttöön. Mikäli käyttäjä haluaa käyttää kyseistä palvelua, on hänen sitouduttava noudattamaan palvelun käyttäjäehtoja, jotka ristiriitatilanteessa ratkaistaan palveluntarjoajan noudattaman järjestelmän mukaisesti. (Pesonen 2013, 67) Sosiaalisen median palvelut myös muuttavat käyttöehtojaan usein, jolloin niiden seuraaminen on erittäin hankalaa. Esimerkiksi Facebook hyväksyttää muuttuneet käyttö- ja sopimusehdot automaattisesti käyttäjillä heidän kirjautuessaan palveluun. Mikäli käyttäjä ei halua hyväksyä muutoksia, tulee hänen sulkea käyttäjätilinsä. (Haasio 2013)

Yksittäisen käyttäjän mahdollisuudet valvoa omien oikeuksien noudattamista sosiaalisessa mediassa ovat siis lähes olemattomat, sillä palveluiden tarjoajat ovat pääasiassa kansainvälisiä yrityksiä (Pesonen 2013, 67). Oikeudet sosiaalisen median palvelujen osalta ovat myös sikäli ongelmallisia, että mitään yleistä oikeutta käyttää tiettyä sosiaalisen median palvelua ei ole. Palveluntarjoajilla on omistusoikeuden johdosta oikeus valita käyttäjänsä. Tämä ei kuitenkaan yksinomaan tarkoita, että yksilön tulisi luopua kaikista perusoikeuksistaan vain käyttääkseen sosiaalisen median palveluja. Vaikka palvelun käyttö perustuukin suostumukseen, ja palvelun käyttämät tekniikat ja käyttöehdot muuttuvat usein, pyrkii kansainvälinen oikeusyhteisö valvomaan, että esimerkiksi ihmisoikeudet ovat voimassa ja toimivat myös uusissa ja uusiutuvissa palveluissa. Esimerkiksi Euroopan henkilötietojen suojajärjestelmän periaatteen mukaan palvelut saavat kerätä vain toiminnalle tarpeellisia ja virheettömiä henkilötietoja, ja vanhentuneet tiedot tulee poistaa. (Mt. 67, 244) Palveluntarjoajat toimivat kuitenkin useimmiten maailmanlaajuisesti, ja niiden kotipaikka on Suomen ja jopa Euroopan ulkopuolella. Tästä syystä niiden toiminnalle esimerkiksi EU:ssa asetetut sisämarkkinoiden edellyttämät juridiset vaatimukset eivät aina yllä koskemaan sosiaalisen median palveluja. Käyttäjän ja palveluntarjoajan välinen oikeussuhde ei myöskään ole verrattavissa esimerkiksi tyypilliseen kuluttajan ja palveluntarjoajan sopimukseen, jossa keskinäiset oikeudet ja velvollisuudet olisivat selkeitä henkilötietolain tai kuluttajansuojalain soveltamisen osalta. Sosiaalisen median palvelujen käyttäjien tuottamasta sisällöstä muodostuvat valtavat henkilötietopankit ovat siten käyttöehtojen osalta kansainvälisten yhtiöiden hallittavana. Vaikka palvelut toimivat maailmanlaajuisesti, voidaan EU-maiden tietosuojalainsäädäntöä ja sen direktiivejä soveltaa, mikäli palvelujen käyttö tapahtuu EU:n alueella. Useiden palvelujen käyttö edellyttääkin, että käyttäjä hyväksyy evästeiden käytön laitteessaan. Evästeiden avulla laite voidaan tunnistaa sijaitsemaan tietyssä maassa, jolloin käyttämiseen sovelletaan sen EU-maan lainsäädäntöä, jossa laitetta käytetään. (Mt. 244)

Sosiaalisen median palvelut pyrkivät kuitenkin olemaan rajoittamatta palvelun käyttämistä sekä käyttäjien toimintaa palveluissa. Palvelun käyttäminen edellyttää palveluntarjoajan esittämien sopimusehtojen hyväksymistä, mutta esimerkiksi palveluun tuotetun sisällön oikeellisuuden ja todenperäisyyden vastuu on aina viestin lähettäjällä ja vastaanottajalla. Käyttäjä on siis vapaa käyttämään palvelua haluamiinsa tarkoituksiin kantaen kuitenkin vastuun julkaisemastaan sisällöstä. (Pesonen 2013, 67) Sosiaalisessa mediassa julkaistun sisällön osalta haasteita kuitenkin asettavat informaation avoimuus sekä sosiaaliselle medialle ominainen nopea julkaiseminen ja reagoiminen. Kynnys tiedon julkaisemiselle ja jakamiselle sosiaalisessa mediassa on matala ja tietoa voi julkaista kuka tahansa, lähes mistä ja milloin tahansa. Nopea julkaiseminen ja reagointi voivat johtaa harkitsemattomien ja virheellisten tietojen julkaisemiseen internetissä, ja niiden poistaminen tai korjaaminen voi osoittautua hankalaksi ellei mahdottomaksi (Mt. 30). Esimerkiksi Bostonin 2013 Maratonin pommi-iskun tekijöiden kiinniottamisen yhteydessä poliisi joutui pyytämään ihmisiä olemaan julkaisematta näkemäänsä poliisitoimintaa Twitterissä, jotta tämä ei haittaisi taktista toimintaa (Hokkanen, ym. 2013, 22).

Sosiaalisen median kautta välitetyn informaation keskeinen ominaisuus on myös sen muuntuvuus ja polveutuvuus. Eri tavat olla vuorovaikutuksessa ihmisten ja julkaistun

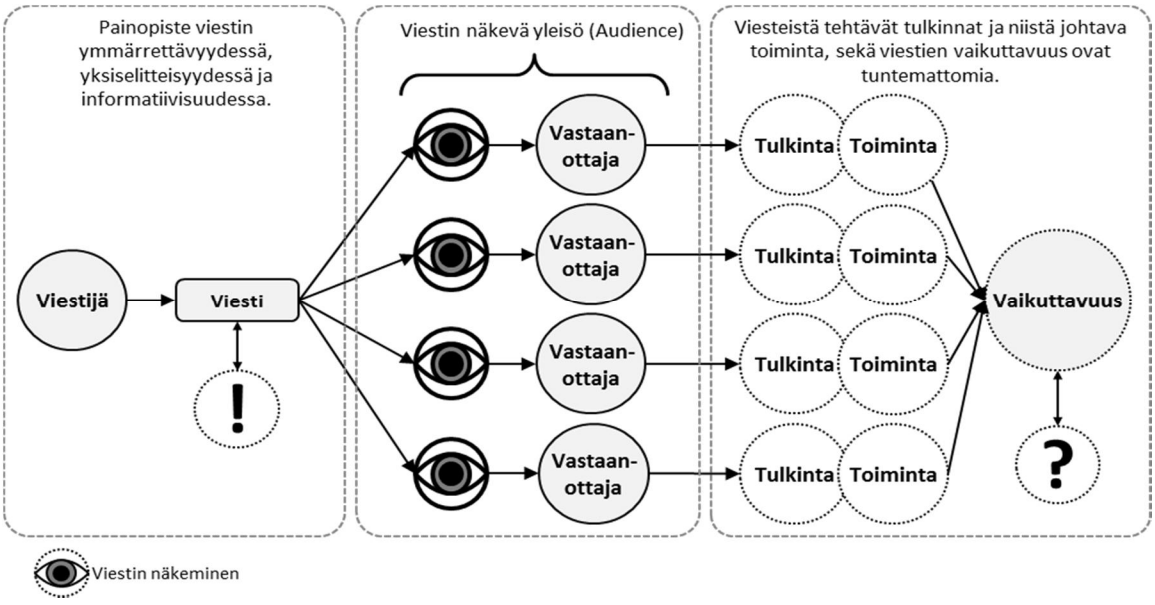
tietosisällön kanssa saattavat irrottaa tai muuttaa informaation alkuperäisestä kontekstistaan ja merkityksestään, kun se esitetään uudessa yhteydessä (Pesonen 2013, 243). Alkuperäisen informaation sisältö voi hetkessä muuntua tai täydentyä kommenttien, jakamisen, muokkaamisen, yms. toiminnan johdosta. Tietoa kuitenkin halutaan aiempaa nopeammin ja hidas reagointi esimerkiksi viranomaisten taholta voidaan nähdä negatiivisesti (Tirkkonen & Luoma-Aho 2011). Sosiaalisen median palveluntarjoajien ja viranomaisten yhteistyö voi myös osoittautua hankalaksi julkaistujen sisältöjen hallinnan osalta. Esimerkiksi onnettomuuspaikoilta julkaistujen kuvamateriaalien käyttäminen voidaan nähdä ongelmallisena sekä palveluntarjoajan että palvelun käyttäjien näkökulmasta. Kärsivien ja loukkaantuneiden ihmisten kuvaaminen voidaan kokea hyvin negatiivisesti, ellei taustalla oleva käyttötarkoitus ole selvä. (Landgren & Bergstrand 2010, 29)

Tyypillisesti palveluntarjoaja poistaa esimerkiksi palvelun käyttäjien tai palveluntarjoajan itsensä kyseenalaiseksi arvioiman sisällön näkyvistä. Yhteistyö palveluntarjoajan ja palvelun käyttäjien välillä voi muodostua ongelmalliseksi tilanteessa, jossa poistettavaksi pyydettävä materiaali koskee esimerkiksi viranomaisen tekemää väkivaltaa ja sisällön loukkaavaksi esittänyt taho on viranomainen. Myös viranomaisten tekemät tietopyynnöt käyttäjistä nähdään usein hankalina. Palveluntarjoaja joutuu tällöin kyseenalaiseen vastuuseen tiedon levittämisen arvottamisesta sekä käyttäjiensä suojelemisessa. Sosiaalisen median palveluntarjoajat ovatkin tehneet linjauksia ja toimintaohjeita, joiden kautta he pyrkivät määrittämään mitkä ovat riittäviä perusteita luovuttaa käyttäjien tietoja viranomaisille. (ks. esim. Facebook 2013, Twitter, Inc. 2013b) Sosiaalisen media käyttäminen osana viranomaisviestintää haastaa viranomaiset erityisesti tietoturvan ja yksityisyydensuojan kannalta, mutta se myös asettaa paineita nopeammalle reagoimiselle hätä- ja häiriötilanneviestinnässä. Viranomaisten toiminta sosiaalisen median eri palveluissa tulisikin suunnitella siten, että viranomaiset pystyvät toimimaan tehokkaasti, mutta tiedonhallinnan, tietoturvan ja luottamuksellisuuden kannalta järkevästi.

10 Sosiaalinen media ja uudenlaiset viestintäprosessit

Perinteinen organisaatiolähtöinen viestintä on perustunut suurelta osin sisällön, yleisyyden, ajoituksen ja välineen kontrolliin. Viestintä on nähty lineaarisena prosessina, sillä perinteisen median viestinnälliset mahdollisuudet ovat rajoittuneet pääosin yksisuuntaiseen viestintään joukkoviestintävälineiden kautta. Esimerkiksi hätä- ja häiriötilanneviestinnässä perinteiset joukkoviestintävälineet ovat olleet tarvittaessa viranomaisten käytettävissä. Organisaation rajojen ulkopuolisen informaation leviäminen on rajoittunut suurelta osin henkilökohtaiseen ja suulliseen vuorovaikutukseen yksittäisten kansalaisten välillä ja näin ollen nähty tiedon leviämisen kannalta minimaalisena. (Mangold & Faulds 2009; Mayzlin 2006) Hätä- ja häiriötilanteissa viestinnän kohde tai viestien vastaanottaja on nähty useimmiten ennalta tuntemattomana, jonkin tietyn ryhmän edustajana. Viestinnän onnistuminen on riippunut kohteiden ja viestittäjien tulkinnoista, joihin ovat vaikuttaneet fyysiset ja kulttuuriset tilanne- ja toimijatekijät. Viestinnän tärkeimpinä aspekteina onkin korostunut viestittävän asian viestiksi pukeminen ja tulkitseminen; ei niinkään tämän puitteissa tapahtuva vuorovaikutus. Viestinnän sijasta onkin käytetty yleisesti termiä "tiedottaminen" tai "vaaratiedottaminen" (Sisäasiainministeriö, 2013).

Kuvassa 10. on karkeasti hahmoteltu tiedottava ja yksisuuntainen viestintäprosessi sekä oletus kohderyhmästä, eli *yleisöstä (audience).* Viestijän välittämä viesti on viestintävälinettä käyttävien henkilöiden nähtävillä, mutta viestin ymmärrettävyys, siitä tehtävät tulkinnat ja vaikuttavuus jäävät yksisuuntaisessa viestinnässä tuntemattomiksi. Painopisteeksi nousee tällöin itse viesti, jonka tarkka muodostaminen on ainoa tapa varmistaa viestin vaikuttavuus. Toisin sanoen, viestin ymmärrettävyys ja yksiselitteisyys ovat keskeisessä asemassa, jotta siitä tehdään haluttuja tulkintoja, jotka edelleen johtavat haluttuun toimintaan.



Kuva 10. Yksisuuntainen / tiedottava viestintä

Sosiaalisen median aikakautena perinteisen viestinnän valta-asema on murentunut ja rinnalle on noussut monia muita viestinnän välineitä (Mangold & Faulds 2009). Viestintäprosessin on

huomattu olevan luonteeltaan dynaaminen, sillä viestinnän tapahtuma eri vaiheineen vaikuttaa lopputulokseen, ja viestinnän vastaanottaja voi olla passiivinen kohde tai aktiivinen toimija (Napoli 2008). Mediakonvergenssin seurauksena verkosta on tullut keskeinen tiedonlähde ja viestinnän kanava erilaisissa hätä- ja häiriötilanteissa; sosiaalisen median kautta tieto ja siitä käytävä keskustelu leviää laajalti. Esimerkiksi vuonna 2008 Yhdysvalloissa riehuneiden Gustav ja Ike -hurrikaanien aikana Twitterissä julkaistiin arviolta 100 000 aiheeseen liittyvää viestiä, eli *twiittiä*. Vuoden 2010 Haitin maanjäristyksen aikana vastaavia twiittauksia tehtiin arviolta 4,2 miljoonaa kappaletta ja 2012 Sandy-hirmumyrskyn aikana julkaistiin jo noin 20 miljoonaa twiittiä. (Palen 2013) Itsenäiset ja riippumattomat palveluntarjoajat ovat tuoneet tarjolle välineen, jonka kautta organisaation rajojen ulkopuolisen informaation levittäminen on kaikkien ulottuvilla. Lisäksi se mahdollistaa useampien yksilöiden ja yhteisöjen välisen kommunikoinnin. (Mangold & Faulds 2009; Li & Bernhoff 2008) Vuorovaikutteiset joukkoviestintävälineet ovat myös mahdollistaneet palautteen saamisen lineaarisen viestintäprosessin yksisuuntaisuuden lisäksi, jonka seurauksena on ollut merkitysten yhteinen rakentaminen. (Starbird & Palen 2012; Starbird & Palen 2011, De Choudhury, Sundaram, John & Duncan Seligmann 2010) Toimiva viestintäprosessi edesauttaa merkitysten muodostumista ja parhaimmassa tapauksessa aikaansaa dialogia viestijän ja kohderyhmän välille. Hätä- ja häiriötilanneviestinnän näkökulmasta tätä kuvannee parhaiten Lontoon 2011 mellakoiden aikaista viranomaisten ja kansalaisten välistä Twitter-aktiivisuutta tarkastellut tutkimus, jossa havaittiin, että keskusteleva ja vuorovaikutteinen viestintätapa sai aikaan inhimillisen ja luottamuksellisen suhteen yleisöön, joka edelleen lisäsi seuraajien määrää, ja paransi viestinnän tavoittavuutta. Sen sijaan etäinen ja yksisuuntainen tiedottava viestintä – vaikkakin viestinnän hallittavuuden kannalta helpompi – ei luonut yhtä merkittävää sidettä kansalaisten ja viranomaisten välille, ja näin vaikeutti viestinnän saavuttavuutta. (Denef, Bayerl & Kaptein, 2013)

Sosiaalisen median ja mobiiliteknologian kehittymisen myötä käyttäjät ovat aiempaa useammin viestintäprosessien käynnistäjiä. Julkaisemalla viestin käyttäjä käynnistää viestintäprosessin, jossa viestin lukija voi edelleen käynnistää uuden viestintäprosessin aiempaan viestiin vastaamalla tai viestiä välittämällä. Viestintäprosesseista on tullut eräänlaisia julkisia oikeuksia, jossa kaikki osallistujat ovat tasavertaisia viestintäprosessin osallisia, ja joihin ei liity minkäänlaisia erityisiä tuotanto- tai jakeluprosesseja. Tästä syystä myös näkemykset viestinnän osapuolista ovat laajentuneet koskemaan yksittäistä henkilöä, ryhmää, kohderyhmää tai suurta yleisöä. Keskusteluun ovat nousseet käsitteet *yleisöstä (audience)* sekä *julkisosta (public)*, joista ensimmäinen käsittää viestimiä ja viestisisältöjä lähinnä kuluttavien yksilöiden kokonaisuuden, ja jälkimmäinen tietoa jakavien ja tuottavien sekä niistä keskustelevien yksilöiden käyttäjäkunnan. (Pietilä & Ridell 2008)

Sosiaalisen median palvelut rakentuvat useimmiten käyttäjien jakaman sisällön tai heidän fyysisen maailmansa sosiaalisten kontaktien ympärille. Tietoa ja sisältöä tuotetaan sekä arkipäiväisiä tilanteita tallentamalla että kommentoimalla, tykkäämällä ja välittämällä muiden julkaisemaa tai välittämää tietoa. Sosiaalisen median käyttämistä leimaa myös trendi huomion tavoittelusta ja tilannetietoisuudesta. Yhteisöpalveluissa tapahtuva vuorovaikutus on usein välitöntä, lyhytjänteistä ja sidottua johonkin tiettyyn sisältöartefaktiin (Pesonen 2013, 34, 243). Viestittävä informaatio voi vaihdella verkon sosiaalisissa verkostoissa kutsuina tapahtumiin, työpaikkailmoituksina, verkkokirjamerkkeinä, valokuvina, videoina, kirjallisuutena ja monina muina muotoina. Vuorovaikutuksen keskiössä voivat siis olla informaatiosisällöt tai ne voivat vaihtoehtoisesti perustua sosiaalisiin verkostoihimme, joita muodostamme päivittäin arkielämässämme. Sosiaalisen median palveluissa tapahtuva vuorovaikutus rakentuukin usein jonkin tietyn mediasisällön pohjalle, mutta keskittyy itse vuorovaikutukseen.

Vuorovaikutusta ylläpitäviksi tekijöiksi voidaan nähdä aiheen mielenkiintoisuus, yhteisössä tunnettujen tai muusta yhteydestä tunnetun käyttäjän kommenttien kiinnostavuus, sekä muiden käyttäjien keskustelun dynamiikan kiinnostavuus. Mielenkiintoisen ja houkuttelevan keskustelun tulee myös osoittaa jonkinlaista jatkuvuutta kyseisessä yhteisössä. Tällaiseksi jatkuvuudeksi nähdään esimerkiksi käyttäjän osallistuminen myös muihin aiheesta käytäviin keskusteluihin, vastaavanlaisten keskustelujen etsiminen, sekä käytyjen keskusteluteemojen välittyminen ja leviäminen muihin keskusteluihin. (De Choudhury ym. 2010) Näin nähtynä sisältöön liittyvä kommunikaatio houkuttaa käyttäjät palaamaan julkaistun mediasisällön äärelle, mutta myös seuraamaan tai jatkamaan vuorovaikutusta muissa yhteyksissä. Ilmiö on nähtävissä myös sosiaalisen median palveluiden sekä älypuhelinten ominaisuuksissa. Käyttäjät voivat halutessaan saada sosiaalisen median palvelulta ilmoituksen muiden käyttäjien toiminnasta. Älypuhelinten push-teknologia mahdollistaa ilmoitusten saamisen lähes reaaliajassa, jolloin myös vuorovaikutus on ajantasaista (Hokkanen ym. 2013). Vuorovaikutus sosiaalisessa mediassa on siten entistä vahvemmin ajasta ja paikasta riippumatonta, sekä keskittyy jatkuvaan läsnäoloon ja osallistumiseen.

Hätä- ja häiriötilanneviestinnän näkökulmasta sosiaalisen median hyödyntäminen näyttäisi edellyttävän täysin uudenalaisia toimintatapoja yksisuuntaisen tiedottavan viestinnän rinnalle. Hätä- ja häiriötilanteiden aikaisesta sosiaalisessa mediassa käydystä viranomaisviestinnästä tehdyissä tutkimuksissa alleviivataan läsnäolon merkitystä nimenomaan viranomaisten näkökulmasta, sillä hätä- tai häiriötilanteessa osallisena olemisen nähdään kasvattavan tiedon tarvetta, ja korostavan vaatimuksia viestinnän nopeudelle, saavuttavuudelle ja ajantasaisuudelle. Viranomaisen läsnäolo verkossa nähdään myös keskeiseksi tekijäksi luottamuksen ja dialogin aikaansaamisessa. Esimerkiksi luottamuksen rakentumisen ei välttämättä nähdä perustuvan pelkästään turvallisuus- ja pelastusviranomaisen substanssiosaamiseen, vaan viranomaisilta odotetaan myös inhimillistä suhtautumista, empatiakykyä sekä avoimuutta päätösten tekemisen ja vaihtoehtojen perustelemisessa (Palttala, Boane, Lund & Ragnhild 2012). Huomioita tukevat muun muassa varoitusviestinnän vaikuttavuuteen keskittyneet tutkimukset, joissa varoitusviestinnän todetaan olevan vaikuttavampaa, kun viestijä tai viestintäkanava nähdään olevan "lähellä" vastaanottajan omaa elämänpiiriä (Vihalem ym. 2012, 14). Myös Lontoon 2011 mellakoiden yhteydessä tehdyssä tutkimuksessa korostettiin viranomaisten vuorovaikutteista viestintää sekä läsnäolon merkitystä viestinnän tavoittavuuden ja vaikuttavuuden osalta (Denef ym. 2013). Vastaavia havaintoja tehtiin myös Suomen poliisin ja Helsingin poliisilaitoksen Facebook-sivujen aktiivisuutta tarkastelleessa selvityksessä, jossa korostettiin vuorovaikutuksellista viestinnän ja monimuotoisen sisällön käyttämisen merkitystä pyrittäessä käyttäjien näkökulmasta mielenkiintoiseen viestintään. Mielenkiintoisella sisällöllä sekä osallistavalla viestinnällä saadaan aikaan mielikuva läsnä olevasta viranomaisesta sekä houkutellaan käyttäjiä vuorovaikutukseen. Tavoittavuuden lisäämiseksi nähtiin tärkeäksi keskittyä läsnäolon aikaansaamiseen keskustelunomaisuutta ja viestien julkaisemistiheyttä lisäämällä. Inhimillinen ja ihmisläheinen tapa viestiä käyttäjien kanssa sekä yllätyksellisyys ja luovuus on viestinnässä tärkeää, mikäli käyttäjien halutaan osallistuvan viestintään. (Ezy Insights 2013) Sen sijaan viranomaisen puuttuminen hätä- ja häiriötilanteen aikana käytävästä keskustelusta on nähty johtavan helposti negatiiviseen suhtautumiseen viranomaisia kohtaan sekä vaikeuttavan viestinnän toteuttamista myöhemmissä vaiheissa. Esimerkiksi hitaan reagoinnin ja osallistumisen keskusteluun on nähty vaikeuttavan dialogin muodostamista jo aktiivisten somen käyttäjien kanssa, sekä myötävaikuttavan negatiivisten asenteiden muodostumiseen. (Tirkkonen & Luoma-Aho 2011; Palttala, ym. 2012)

Sosiaalisen median käyttäminen vuorovaikutuksen ja läsnäolon aikaansaamiseksi edellyttää kuitenkin siihen liittyvien viestintätapojen ymmärtämistä. Keskeistä onkin huomioida esimerkiksi monimuotoisen sisällön merkitys vuorovaikutuksen ja läsnäolon aikaansaamisessa.

Monimuotoinen sisältö voi auttaa vuorovaikutuksen aikaansaamisessa, mutta myös viestien leviämisessä ja viestinnän tavoittavuudessa. (De Choudhury, ym. 2010) Lisäksi se voi lisätä yleistä tietoutta onnettomuuksien ehkäisemisestä ja vaikuttaa kansalaisten asenteisiin, uhkiin varautumiseen ja toimintakykyyn hätä- tai häiriötilanteessa. Olennaista sosiaalisessa mediassa käytävän hätä- ja häiriötilanneviestinnän kehittämisessä onkin uusien välineiden käyttöönoton ohella vuorovaikutustapoihin liittyvien havaintojen tekeminen sekä niiden hyödyntäminen.

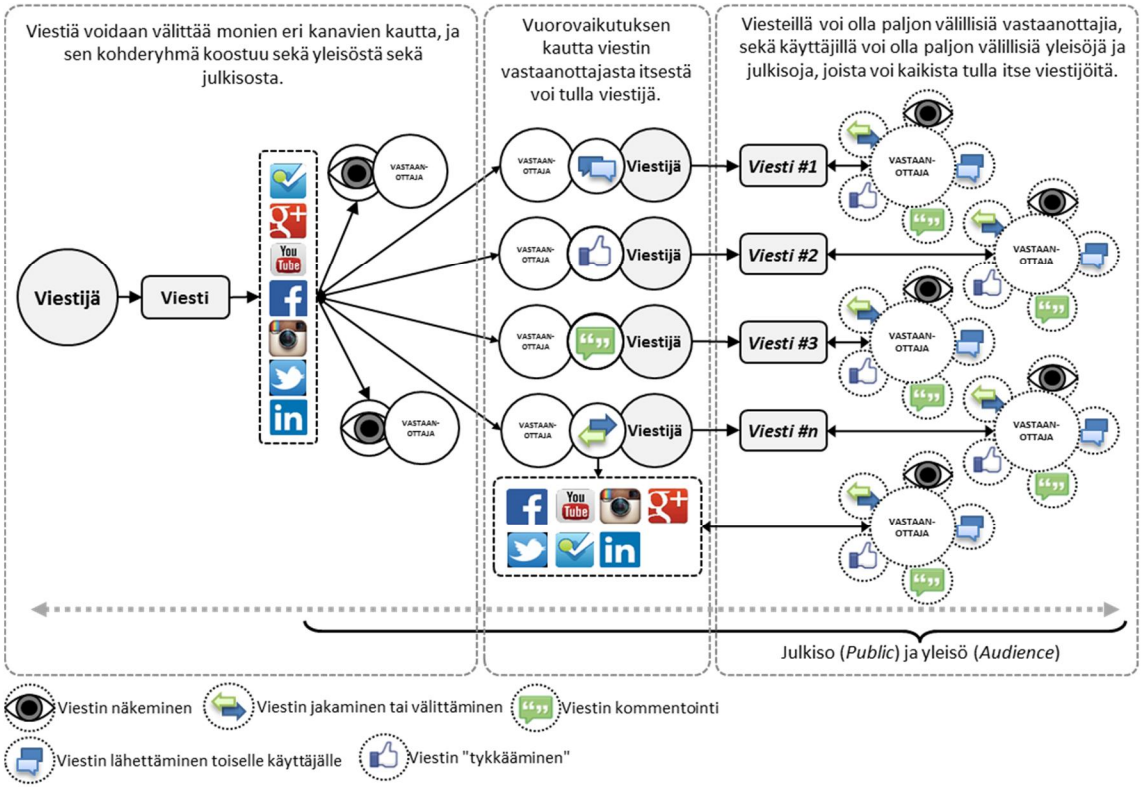
Pohdittaessa näitä aspekteja hätä- ja häiriötilanne- tai viranomaisviestinnän näkökulmasta ylipäänsä on tunnistettava uudet vuorovaikutuksen tavat, niiden vaihtelevuus, sekä tekniset ominaisuudet. Sosiaalinen media on tuonut viestintään uuden ulottuvuuden, joka järkevästi hyödynnettynä tavoittaa entistä suuremman määrän ihmisiä. Keskeisenä eroavaisuutena aiempiin viestintäprosesseihin on mahdollisuus monimuotoiselle vuorovaikutukselle. Sosiaalisen median vuorovaikutuksen muotoja voidaan jaotella koskemaan tyypillisimpiä tapoja viestiä sosiaalisen median palveluissa. Näitä ovat De Choudhuryn, ym. (2010) mukaan muun muassa:

1. Viestit. Tyypillisesti lyhyet, tietylle käyttäjälle tai tietylle käyttäjäryhmälle osoitetut viestit, joiden julkisuus voi vaihdella yksityisistä viesteistä kaikille näkyviin viesteihin.
2. Kommentit ja vastaamiset. Julkaistun sisällön kommentoiminen tai kommentteihin vastaaminen, joka luo mahdollisuuden sisältöön keskittyvälle vuorovaikutukselle, esimerkiksi keskustelun tai mielipiteen ilmaisun ominaisuudessa. Erilaisen sisällön julkaisemiseen liittyvää kommentointia tai sisältöön vastaamista voidaan pitää tarkoituksenmukaisena vastauksena tiettyyn edeltävään viestiin.
3. Mediasisällön ympärille rakentuva keskustelu. Eroavaisuutena edellä mainittuun kommentointiin ja vastaamiseen voidaan erottaa jonkin tietyn mediasisällön, kuten uutisen, videon, valokuvan, blogikirjoituksen, tms. ympärille muodostuva keskustelu, jota voidaan käydä muissakin yhteisöissä kuin vain itse julkaisun, palvelun tai tiedon julkaisijan oman verkoston sisällä.
4. Tykkäämiset. Tykkääminen, suositteleminen tai äänestäminen on noussut yhdeksi keskeiseksi viestinnän välineeksi sosiaalisen median palveluissa. Verrattavissa esimerkiksi viestin valtuuttamiseen, kuittaamiseen tai "digitaaliseen nyökkäämiseen", joka ilmentää viestityn sisällön hyväksyntää, tunnistamista tai kiinnostusta sitä kohtaan.
5. Mikrobloggaus. Lyhyiden mikroblogi-merkintöjen tai tilapäivitysten julkaiseminen, niistä keskusteleminen sekä niiden jakaminen on tullut yhdeksi keskeisimmäksi sosiaalisen median toiminnoksi, sillä se mahdollistaa julkisen viestinnän ohjaamisen tietylle yhteisölle, keskustelulle, käyttäjälle. Lisäksi se mahdollistaa viestinnän sisältöjen välittämisen ja välittymisen aiheesta kiinnostuneille, sekä vuorovaikutuksen ja palautteen saamisen sisällöistä. (De Choudhury, ym. 2010)

Edellä mainittujen vuorovaikutustapojen myötä joudutaan tulkitsemaan aiempaa monimutkaisempia vuorovaikutuksen muotoja, mutta toisaalta vuorovaikutukseen voidaan käyttää useampia välineitä, jolloin viestintä saavuttaa useammat ja on aktiivisempaa. Esimerkiksi viestistä tykkäämiseen tai edelleen välittämiseen vaadittu kynnys on matalampi kuin esimerkiksi viestiin vastaamisessa tai keskustelun aloittamisessa. Siten myös kynnys vuorovaikutukselle voi olla pienempi. Sosiaalisessa mediassa käytävään viestintään ei myöskään oletuksellisesti sisälly harkittua viestisisältöä. Monimuotoisten viestisisältöjen rinnalle on tullut ennennäkemättömiä vuorovaikutuksen ja viestinnän tapoja, joissa viestintä voi edellä kuvatulla tavalla perustua pelkästään toisen viestistä tai valokuvasta tykkäämiseen tai tämän jakamiseen. Vuorovaikutus ei siten vaadi sanallista kontribuutiota keskusteluun. Valokuvasta, viesteistä tai puheenvuoroista tykkääminen, kuvan tai keskustelun jakaminen tai sen upottaminen toiseen sosiaalisen median palveluun, on yhtälailla mahdollinen

vuorovaikutuksen muoto sosiaalisessa mediassa. Tällaisen vuorovaikutuksen arvo sosiaaliseen mediaan liittyvässä viestinnässä, on sosiaalisen median palveluiden algoritmien toiminta. Sosiaalisen median palveluissa algoritmit määrittävät julkaisujen tärkeys- tai uutisarvoa niihin kohdistuneiden vuorovaikutustoimien pohjalta. Mitä enemmän käyttäjät tykkäävät julkaisusta, osallistuvat keskusteluun julkaisusta tai jakavat sitä edelleen, sitä korkeammaksi nousee tämän kyseisen julkaisun julkisuusarvo. Toisin sanoen, mitä useammat painavat julkaisun kohdalla tykkää-painiketta, kommentoivat julkaisua tai jakavat sitä edelleen, sitä useammalle kyseinen julkaisu myös näkyy.

Viimeaikaisen tutkimuksen mukaan sosiaalisen median käyttäjät ovat myös taipuvaisia "tykkäämään" sellaisista julkaisuista, joista muutkin pitävät (Muchnik, Aral & Taylor 2013). Ilmiö toisin sanoen ruokkii itseään. Näin ollen esimerkiksi viestien tavoittavuutta kehitettäessä olisi tärkeää huomioida viestinnän vuorovaikutukseen houkuttelevuus sekä sen jatkuvuus. Vastaavasti kohdennettaessa viestintää sekä julkisolle että yleisölle, tulee ymmärtää että sosiaalisen median vapaassa julkaisemisessa myös palveluiden käyttäjillä on itsellään yleisöjä ja julkisoja. Esimerkiksi jakaessaan julkaisun omalle verkostolleen käyttäjä voi aloittaa uuden viestintäprosessin, jossa hänen verkostonsa (*yleisönsä* ja *julkisonsa*) voivat edelleen välittää informaatiota tai aloittaa viestintäprosessin (ks. kuva 11). Vuorovaikutuksen aikaansaaminen sekä aktiivisten toimijoiden tavoittaminen voi olla keskeinen tekijä hätä- ja häiriötilanneviestinnän tavoittavuuden kannalta.



Kuva 11. Viestintäprosessi sosiaalisessa mediassa

11 Yhteenveto

Sosiaalisen median käyttämiseen liittyy monenlaisia tiedonhallintaan sekä käyttöoikeuksiin liittyviä haasteita. Käyttäjän oikeus julkaista viestejään toteutuu verkkoympäristöissä oikeutena päästä tietoverkkoihin. Yleistä oikeutta käyttää tiettyä palvelua ei kuitenkaan ole, sillä operaattoreilla ja ylläpitäjillä on omistusoikeuden vuoksi oikeus valita asiakkaansa. (Pesonen 2013, 29–30) Useimmissa palveluissa käyttäjäksi rekisteröityminen edellyttää jonkin tunnistettavan yhteystiedon, kuten rekisteröidyn sähköpostiosoitteen tai puhelinnumeron tallentamista palveluntarjoajan rekisteriin. Rekisteröityminen edellyttää myös käyttöehtosopimuksen solmimista palveluntarjoajan kanssa. (Mt. 39) Mahdollisuus esimerkiksi käyttäjien ihmisoikeuksien suojan ja noudattamisen valvontaan sosiaalisessa mediassa on käytännössä olematon sillä palveluyksiköt ovat maailmanlaajuisia ja kasvottomia ja asia on juridisestikin ongelmallinen. Palveluntarjoajien käyttämät tekniikat ja käyttöehdot muuttuvat usein, ja palveluja tarjoavien yritysten tarkoitus on kaupallinen. Siihen sisältyy tavoite käyttää yksityisten ihmisten tietoja laajasti hyväksi yritystoiminnan kulloinkin edellyttämällä tavalla. Palveluihin syötettyjä tietoja on tallennettuna useissa eri palveluissa monien eri käyttö- ja sopimusehtojen alaisuudessa. Näin myös tietosuojastamme on tullut aiempaa ongelmallisempi käsite. Sosiaalisen median hyödyntäminen viranomaisviestinnässä haastaakin viranomaiset erityisesti tietoturvan ja yksityisyydensuojan kannalta, sillä palveluiden käyttämiseen edellytettävät sopimusehdot ovat suostumukseen perustuvia ja samat niin viranomaisille kuin kansalaisillekin. Näin ollen palveluntarjoajilla on valta luoda edellytykset myös viranomaisen sosiaalisen median käytölle.

Sosiaalisen median ominaispiirre on nopea ja monipuolinen julkaiseminen. Julkaisut ovat useimmiten ajankohtaisia ja ajantasaisia, sillä niiden julkaiseminen ei vaadi mitään erillistä tuotanto- tai jakeluprosessia. Sosiaalinen media on myös tuonut verkon käyttäjien ulottuville laajan määrän alustoja ja jaettuja tiloja, jotka kannustavat käyttäjien väliseen kommunikaatioon, ja joiden myötä perinteisen tiedottavan joukkoviestinnän kontrolli on murentunut. (Mangold & Faulds 2009) Tieto- ja viestintäteknologian kehittyminen on tuonut viestintään uusia sisältöjä sekä uusia vuorovaikutuksen muotoja. Sosiaalisen median myötä käyttäjät voivat olla viestintäprosessien käynnistäjiä, ja viestinnän keskiössä voivat olla monimuotoiset informaatiosisällöt, kuten videot, valokuvat, blogikirjoitukset, uutiset, sosiaaliset verkostomme, yms. Myös vuorovaikutuksen tavat ovat moninaiset. Tykkäämiset, jakamiset, kommentoinnit, yms. ominaisuudet sekä mukana kulkevat mobiililaitteet tekevät osallistumisesta vaivatonta ja nopeaa, sekä mahdollisesti madaltavat kynnystä osallistua vuorovaikutukseen. Vuorovaikutuksen nähdään myös olevan tekijä, joka houkuttaa käyttäjiä palaamaan julkaistun mediasisällön äärelle. (De Choudhury, ym. 2010) Pelkästään vuorovaikutteisuuden lisäämisellä on mahdollista tavoittaa suurempia määriä käyttäjiä. Näin ollen esimerkiksi sosiaaliseen mediaan keskittyvässä hätä- ja häiriötilanneviestinnässä tulisi huomioida ja hyödyntää mahdollisuudet edellä mainitun vuorovaikutuksen aikaansaamiselle sekä siitä saatavalle hyödylle. Esimerkiksi viranomaisen läsnäolon ja vuorovaikutteisen toiminnan verkossa on todettu parantavan viestinnän tavoittavuutta, sekä lisäävän luotettavuutta. Monimuotoisen tietosisällön houkuttelevuus vuorovaikutukseen sekä sen pohjalta aikaansaatava jatkuvuus voisi tarjota myös mahdollisuuden seurata ja kartoittaa kansalaisten, median ja sidosryhmien viestintätapoja, sekä riskitietoutta ja mielikuvia yhteiskunnassa. Myös viestinnän tavoittavuuden sekä esimerkiksi huhujen ja väärien tai harhaanjohtavien tietojen korjaaminen on helpompaa. Vuorovaikutusta aikaansaava viestintä voi varoittamisen osalta tarjota myös työvälineen viestinnän tavoittavuuden sekä reaktioiden seuraamiseen. Esimerkiksi ensireaktiot ja kysymykset varoitukseen liittyen voivat olla olennaisia viestiin liittyvien väärinymmärrysten tai epäkohtien huomioimisessa. Sosiaalisen

median vuorovaikutteiset ominaisuudet voivat myös edesauttaa viestinnän laajempaa leviämistä ja tavoittavuutta. Vastaavasti sosiaalisessa mediassa tapahtuvan vuorovaikutuksen kautta saatava palaute palvelee osaltaan myös toiminnan arviointia ja seuraamista.

Myös sosiaalisessa mediassa hätä- ja häiriötilanneviestinnän tehokkuus tulee monikanavaisuudesta. Sosiaalinen media on laaja palveluiden verkosto, joissa käyttäjien osallisuus vaihtelee. Ohjelmointirajapintojen lisääntymisen myötä sosiaalisen median palveluiden sekä niitä käyttävien laitteiden ja sovellusten myötä sisällön julkaisemisesta sekä sosiaalisen median käyttäjyydestä on tullut universaalimpaa. Tehokkaan ja tavoittavan viestinnän tarjoaminen edellyttää siten viranomaisen läsnäoloa mahdollisimman monessa palvelussa. Keskeistä esimerkiksi viestintäprosessien arvioimisessa ei ole teknologian mahdollistamien ominaisuuksien kartoittaminen, vaan käyttäjien käyttämien palvelujen sekä niiden tarjoamien mahdollisuuksien hyödyntäminen käyttäjien näkökulmasta. Ihmiset ovat luovia keksimään vaihtoehtoisia kommunikointivälineitä hätätilanteissa, ja useimmiten he ajautuvat tarkistamaan uusimpia tietoja ensimmäiseksi verkosta. Palveluiden ohjelmointirajapintojen ansiosta mahdollisuus ristikkäiskirjautumiselle sekä ristikkäisjulkaisemiselle tekee monikanavaisesta some-viestinnästä sekä sen hallinnasta helpompaa, mutta se myös lisää tietoisuutta viranomaisten läsnäolosta sosiaalisessa mediassa. Esimerkiksi valokuvapalvelussa julkaistu, ja sittemmin ristikkäisjulkaisemisominaisuuden keinoin toiseen sosiaalisen median palveluun tuotu sisältö, tarjoaa käyttäjälle mahdollisuuden löytää sisällön julkaisseen käyttäjän myös valokuvapalvelusta. Vaikka edellä mainittu esimerkki korostaakin erityisesti tiettyjen ominaisuuksien käytön opettelua monikanavaisen viestinnän aikaansaamisessa, ei tarkoituksemme ole painottaa erityisten taitojen tai palvelujen yksityiskohtaista opettelua, vaan korostaa tarvetta sosiaalisen median taitojen kokonaisvaltaisuudelle. Tämä mahdollistaisi taitojen siirtämisen ja hyödyntämisen alati muuttuvalla viestinnän kentällä.

Vaikka viestintäprosessit ovat muuttuneet sosiaalisen median myötä sisällöltään ja viestinnän muodoiltaan monimuotoisemmiksi sekä tavoittavuudeltaan osittain kattavammiksi, on muistettava että sosiaalinen media ei vielä tavoita kaikkia kansalaisia. Onkin huomioitava, ettei perinteinen yksisuuntainen tiedottaminen ole yksinomaan huono tapa viestiä sosiaalisessa mediassa, vaan pikemminkin yksi tapa muiden rinnalla. Aiemmat käytännöt hätä- ja häiriötilanneviestinnässä ovat osoittautuneet toimiviksi, eikä niitä tulisi hylätä uuden edessä. Tärkeämpää olisi huomioida, että sosiaalisen median aktiiviset käyttäjät voivat olla tehokkaita toimijoita tiedon levittämisessä, tiedotettavan informaation rakentamisessa sekä palautteen saamisessa. Tämän resurssin hyödyntäminen ei kuitenkaan ole mahdollista ilman sitoutumista vuorovaikutukseen sosiaalisen median käyttäjien kanssa.

Lähdeluettelo

6abc News. (15. 1 2013). 6abc.com. Haettu 28. 10 2013 osoitteesta http://abclocal.go.com/wpvi/story?section=news/local&id=8954738

Achohido, B. (16. 12.2011). Facebook tracking is under scrutiny – USA Today; Tech. Haettu 14. 11 2013 osoitteesta: usatoday30.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1?csp=34money

Austin, L., Fisher, B. & Jin, Y. (2012). How Audiences Seek Out Crisis Information: Exploring the Social-Mediated Crisis Comunication Model. Journal of Applied Communication Research, 40(2), 188–207.

AWARE: Alerts, Warnings & Response to Emergencies. (30.1.2013). AWARE Forum. Haettu 28.10.2013 osoitteesta: http://www.awareforum.org/2013/01/cmas-replaces-popular-wireless-amber-alert-program-for-child-abduction-alerts/

Bird, D., Ling, M. & Haynes, K. (2012). Flooding Facebook - the use of social media during the Queensland and Victorian Floods. The Australian Journal of Emergency Management, 27(1), 27–33.

Burns, A. & Liang, Y. E. (2012). Tools and methods for capturing Twitter data during natural disasters. First Monday, 17, (4–2).

Common Alerting Protocol. (1.7.2010). Haettu 9.10.2013 osoitteesta: http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf

Creative Commons. (2013). creativecommons.org. Haettu 2.10.2013 osoitteesta: http://creativecommons.org/licenses/?lang=fi

De Choudhury, M., Sundaram, H., John, A. & Duncan Seligmann, D. (2010). Analyzing the Dynamics of Communication in Online Social Networks. Handbook of Social Network Technologies and Applications, 59–94.

Denef, S., Bayerl, P. & Kaptein, N. (2013). Social Median and the Police – Tweeting Practices of British Police Forces during the August 2011 Riots. CHI '13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 3471–3480.

FEMA - Federal Emergency Management Agency. (17.5.2012.) Emergency Management Institute. Haettu 20.10.2013 osoitteesta: http://emilms.fema.gov/IS247a/lesson3/L3_Print.htm

Ezy Insights. (2013). Yleiskatsaus: Helsingin poliisilaitos and Suomen poliisi Facebook Pages. Ezy Insights.

Facebook. (2013). Facebook: Turvallisuuskeskus: Turvallisuus ja sinä: Tietoja lainvalvontaviranomaisille. Haettu 26. 11 2013 osoitteesta http://www.facebook.com/safety/groups/law/guidelines

FEMA - Federal Emergency Management Agency. (2013). Wireless Emergency Alerts Fact Sheet. Haettu 10. 9.2013 osoitteesta http://www.fema.gov/media-library-data/20130726-1911-25045-3639/wea_fact_sheet.pdf

Gupta, R., & Brooks, H. (2013). Using Social Media for Global Security. Indianapolis: John Wiley & Sons, Inc.

Haasio, A. (2013). Netin pimeä puoli. Helsinki: Suomalaisen kirjallisuuden seura.

Helsinki Region Infoshare. (2013). Helsinki Region Infoshare. Haettu 24.10.2013 osoitteesta http://www.hri.fi/fi/mita-on-avoin-data

Hokkanen, L., Pylväs, K., Kankaanranta, T., Sihvonen, H.-M., Paananen, P. & Honkavuo, H. (2013). Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa. Osaraportti I - Sosiaalisen median ja älypuhelinsovellusten käyttö viranomaisten toiminnassa. Helsinki: Sisäasiainministeriön julkaisu 28/2013.

Huhtala, H. & Hakala, S. (2007). Kriisi ja viestintä. Yhteiskunnallisten kriisien johtaminen julkisuudessa. Helsinki: Gaudeamus.

Jaakohuhta, H. (1999). Suuri tietotekniikan tietosanakirja. Jyväskylä: Suomen Atk-kustannus Oy.

Julkisen hallinnon tietohallinnon neuvottelukunta - JUHTA. (5.10.2012). JHS-suositukset - JHS 162 Paikkatietojen mallintaminen tiedonsiirtoa varten. Haettu 15.8.2013 osoitteesta: http://www.jhs-suositukset.fi/suomi/jhs162

Jyväskylän yliopisto. (10 2013). Jyväskylän yliopisto: Ajankohtaista: Arkisto: 2013: 10/2013: Jyväskylän yliopisto kaupallistaa kehittämänsä kriisiviestintäsovelluksen. Haettu 12. 1. 2014 osoitteesta https://www.jyu.fi/ajankohtaista/arkisto/2013/10/tiedote-2013-10-11-13-58-16-293781

Järvelä, E. & Puusaari, E. (2005). UML-käsikirja. Kokkola: Chydenius-instituutin selvityksiä 1/2005.

Kaleva. (29.7.2013). Vaaratiedotteet aivan liian laajassa jakelussa. Kaleva.fi. Haettu 29.10.2013 osoitteesta: http://www.kaleva.fi/mielipide/paakirjoitukset/vaaratiedotteet-aivan-liian-laajassa-jakelussa/637287/

Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59–68.

Kuula, J. (12.11.2013) Uusi älypuhelinsovellus kriisiviestintään ja kevyen tilannekuvan muodostamiseen vaaratilanteesta. Haettu 10. 1.2014 osoitteesta http://www.sppl.fi/files/2159/Kuula_-_Uusi_alypuhelinsovellus_kriisiviestintaa.pdf.

Laaksonen, S.-M., Matikainen, J. & Tikka, M. (2013). Tutkimusotteita verkosta. Teoksessa S.-M. Laaksonen, J. Matikainen & M. Tikka, Otteita verkosta (9–34). Tampere: Vastapaino.

Landgren, J. & Bergstrand, F. (2010). Mobile Live Video in Emergency Response: Its Use and Consequences. Bulletin of the American Society for Information Science and Technology, 36(5), 27–29.

Laki vaaratiedotteesta. 2012. 466/2012.

Li, C. & Bernhoff, J. (2008). Groundswell: Winning in a World Transformed by Social Technologies. Boston: Harvard University Press.

Mangold, G. & Faulds, D. (2009). Social media: The new hybrid element of the promotion mix. Business Horizons, 52(4), 357–365.

Marketvisio. (5.9.2012). Älypuhelimien osuus kipuamassa lähes 70 prosenttiin myydyistä puhelimista. Marketvisio.fi. Haettu 23. 10 2013 osoitteesta: http://www.marketvisio.fi/fi/ajankohtaista/uutiset-marketvisio/1430-lypuhelimien-osuus-kipuamassa-l-hes-70-prosenttiin-myydyist-puhelimista

Mayzlin, D. (2006). Promotional chat on the Internet. Marketing Science, 155–163.

Muchnik, L., Aral, S.& Taylor, S. (2013). Social Influence Bias: A Randomized Experiment. Science, 341(6146), 647–651.

Nykänen, O. (28.8.2003). XML 10 kohdan tiivistelmä. Haettu 23.8.2013 osoitteesta: http://www.w3c.tut.fi/translations/xml/xmlin10pts/

Oxford Dictionaries (2014). Haettu 11.2.2014 osoitteesta: http://www.oxforddictionaries.com/definition/american_english-thesaurus/data

Palen, L. (14.3.2013). How Social Media Might Help You Survive the Next Big Disaster. Santa Fe Institute. [luentotaltiointi] Haettu 10.10.2013 osoitteesta: http://www.youtube.com/watch?v=7SNFbPA-96o

Palttala, P., Boane, C., Lund, R. & Vos, M. (2012). Communication Gaps in Disaster Management: Perceptions by Experts from Governmental and Non-Gevernmental Organizations. Journal of Contingencies and Crisis Management, 20(1), 3–12.

Párraga Niebla, C., Muna, J., Grazzini, S. & Pfeffer, R. (2013). A complete communication framework for public alert: the Alert4All approach. TIEMS Berlin Conference 2013. TIEMS.

Pesonen, P. (2013). Sosiaalisen median lait. Helsinki: Lakimiesliiton kustannus.

Pietilä, V. & Ridell, S. (2008). Verkkomedia toimijuuden alustana : yleisö, yhteisö, julkiso ja YouTube. Lähikuva(2), 27–43.

Ready.gov. (10.9.2013). Emergency Alerts. Ready.gov. Haettu 28.10.2013 osoitteesta: http://www.ready.gov/alerts

Saari, M. (2006). Moniarvoisen relevanssin hyödyntäminen XML-tiedonhakujen evaluoinnissa. Tampere: Tampereen yliopisto.

Salminen, A. (2005). Metatiedot organisaatioiden sisällönhallinnassa. Helsinki: Eduskunnan kanslia.

Samarajiva , R. & Waidyanatha, N. (2009). Two complementary mobile technologies for disaster warning. info, 11(2), 58–65.

Sanastokeskus TSK ry (2014). Sanastokeskus TSK:n termipankki. Haettu 11.2.2014 osoitteesta: http://www.tsk.fi/tepa/

Sisäasiainministeriö. (2013). Vaaratiedoteopas. Sisäasiainministeriön julkaisu 1/2013.

Starbird, K.& Palen, L. (2011). "Voluntweeters": Self-Organizing by Digital Volunteers in Times of Crisis. CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1071–1080.

Starbird, K.& Palen, L. (2012). (How) will the revolution be retweeted?: information diffusion and the 2011 Egyptian uprising. CSCW '12 Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work. New York: ACM, 7–16

Suurla, R. (2001). Helmiä kalastamassa - Avauksia tietämuksen hallintaan. Teknologian arviointeja. Loppuraportti. Helsinki: Eduskunnan kanslia.

Suomen virallinen tilasto (SVT) (7.11.2012). Etusivu: Tilastot: Tiede, teknologia ja tietoyhteiskunta: Väestön tieto- ja viestintätekniikan käyttö: 2012: 3. Internetin käyttö muualla kuin kotona tai työpaikalla. (Tilastokeskus, Toimittaja) Haettu 8.8.2013 osoitteesta Tilastokeskus: http://www.stat.fi/til/sutivi/2012/sutivi_2012_2012-11-07_kat_003_fi.html

Taylor, M., Wells, G., Howell G. & Raphael, B. (2012). The Role Of Social Media as Psychological First Aid as a Support to Community Resilience Building. A Facebook Study from "Cyclone Yasi Update". Australian Journal of Emergency Management, 27(1), 20–26.

Tirkkonen, P. & Luoma-Aho, V. (2011). Online authority communication during an epidemic: A Finnish example. Public Relations Review, 2011(37), 172–174.

Twitter, Inc. (2013a). Twitter: Developers. Haettu 5. 11 2013 osoitteesta https://dev.twitter.com/

Twitter, Inc. (2013b). Twitter: Ohjekeskus: Guidelines for Law Enforcement. Haettu 26. 11 2013 osoitteesta http://support.twitter.com/articles/41949

Valtioneuvoston kanslia. (2013). Valtionhallinnon viestintä häiriötilanteissa ja poikkeusoloissa. Helsinki: Valtioneuvoston kanslia.

Valtiovarainministeriö. (n.d.) ”Suomen avoimen hallinnon toimintaohjelma.” Haettu 24.10.2013 osoitteesta: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/Avoin_hallinto_toimintasuunnitelma.pdf

Viestintäverkkojen tekniset viranomaisvaatimukset -ryhmän SMS/CBS-alaryhmä. (2005). Työryhmäraportti 7/2005 Tekstiviestijärjestelmät väestön varoittamisessa. Viestintävirasto.

Vihalem, T., Kiisel, M. & Harro-Loit, H. (2012). Citizen's Response Patterns to Warning Messages. Journal of Contingencies and Crisis Management, 20(1), 13–25.

Wilson, R. (11.1.2013). OSS Watch: App Stores And Openness. Haettu 25. 11.2013 osoitteesta http://oss-watch.ac.uk./resources/appstores

Wrenn, E. (13.7.2012). Right or wrong? Facebook monitors chat conversations and informs the police of anything suspicious - but the privacy breach does catch paedophiles. The DailyMail Online: Science & Tech. Haettu 11.11. 2013 osoitteesta: http://www.dailymail.co.uk/sciencetech/article-2173081/Right-wrong-Facebook-monitors-chat-conversations-informs-police-suspicious--privacy-breach-does-catch-paedophiles.html

YLE. (28 6.2013). Uudet vaaratiedotteet hämmentävät ja ärsyttävät - määrä yllätti myös viranomaiset. Yle Uutiset. Haettu 22.10.2013 osoitteesta: http://yle.fi/uutiset/uudet_vaaratiedotteet_hammentavat_ja_arsyttavat_-_maara_yllatti_myos_viranomaiset/6709779

YLE. (12.7.2013). Lukuisat vaaratiedotteet ärsyttävät kansalaisia. Yle Uutiset. Haettu 8.8.2013 osoitteesta: http://yle.fi/uutiset/lukuisat_vaaratiedotteet_arsyttavat_kansalaisia/6731801

Liitteet

Liite 1: CAP-tietomalli
Liite 2: CAP-viestin luokkakaavio

CAP - Common Alerting Protocol Version 1.2 x = WEA-järjestelmässä näkyvä tieto							Vaade: onko tieto pakollinen (P) vai vapaaehtoinen (V).
Luokka	Tieto	Alkup.termi	Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
Hälytys		Alert			-		Sisältää hälytyskomponentin osat
	Tunniste	Message ID (identifier)	P	Lähettäjän määrittämä tunniste, joka yksilöi viestin.	Identi-fioija	Kokonaisluku tai teksti	Ei pilkkuja, välejä tai "<"- tai "&"-merkkejä. Lähettäjän määrittämä.
x	Lähettäjä	Sender ID (sender)	P	Viestin alkuperäisen lähettäjän yksilöivä tunniste (ID). Maailmanlaajuisesti yksilöllinen tunniste, esim. verkkotunnus (domain name).	Identi-fioija		Ei pilkkuja, välejä tai "<"- tai "&"-merkkejä.
	LähetysAika	Sent Date/Time (sent)	P	Kellonaika ja päiväys, jolloin alkuperäinen viesti on lähetetty.	Aika	DateTime Data Type	"2002-05-24T16:49:00-07:00" (24.5.2002 klo 16:49 PDT) aikavyöhyke. UTC -aikavyöhyke tulee esittää "-00:00". Aakkosellista aikavyöhyke-esitystä kuten Z ei tule käyttää.
	ViestinTila	Message Status (status)	P	Koodi, joka määrittää hälytysviestin asianmukaisen käsittelyn. Harjoituksen yksilöinti merkinnällä <note> .	Koodi	Valmiit vaihtoehdot	* Tosi - edellyttää kaikilta vastaanottajilta toimia * Harjoitus - edellyttää toimia vain harjoitukseen osallistujilta * Järjestelmä * Testi - vain tekniseen testaukseen, kaikki voivat jättää huomiotta * Luonnos - pohjustava malli tai luonnos, ei edellytä toimia tässä muodossa

Luokka	Tieto	Alkup.termi	Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
	ViestinTyyppi	Message Type (msgType)	P	Ilmaisee viestin tyypin / luonteen.	Koodi	Valmiit vaihtoehdot	* Hälytys - esitiedon mukaan vaatii vastaanottajan huomiota * Päivitys - päivittää aiempaa viestiä, joka määritetty kohdassa <Viittaukset> * Peruutus - kumoaa aiemman viesti, joka määritetty kohdassa <Viittaukset> * Virhe - ilmaisee viestin hylkäämisen, lisätietoja kohdassa <Huomautus>
	Lähde	Source (source)	V	Hälytyksen erityinen lähde.	Identi-fioija	Teksti	
	Jakelu	Scope (scope)	P	Tarkentaa aiottua jakelua.	Koodi	Vaihtoehdot	* julkinen - yleiseen levitykseen rajoittamattomalle yleisölle * rajoitettu - levittäminen vain henkilöille tietyille henkilöille (täsmennetty kohdassa <JakelunTarkennus>) * luottamuksellinen - levitetään vain tietyihin osoitteisiin (täsmennetty kohdassa <Osoitteet>)
	JakelunTar-kennus	Restriction (restriction)	V	Käytetään, kun kohdan <Jakelu> arvona on "rajoitettu". Kuvaa viestin jakelun rajoittamisen säännön.	Teksti	Teksti	
	Osoitteet	Addresses (addresses)	*	Listaa tarkoitetut viestin vastaanottajat.	Ryhmä	Teksti	Vaadittu, kun <Jakelu> on luottamuksellinen, muuten vapaaehtoinen. Jokainen vastaanottaja tulee yksilöidä tunnisteella tai osoitteella. Monta osoitetta voidaan erottaa välilyönnein, jolloin osoitteet mukaanlukien välilyönnit tulee laittaa lainausmerkkien sisälle.
	KäsittelyKoodi	Handling Code (code)	V	Tarkentaa erityisen viestin käsittelyn.	Koodi		

Luokka			Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
	Tieto	Alkup.termi					
	Huomautus	Note (note)	V	Kuvaa viestin tarkoitusta tai merkitystä.	Teksti	Teksti	Tarkoitettu pääasiassa käytettäväksi, kun <tila> on harjoitus tai <tyyppi> on virhe.
	Viittaukset	Reference IDs (references)	V	Ilmoittaa mahdolliset aiemmat viestit, joihin tämä viesti liittyy.	Ryhmä	<Lähettäjä>, <Tunniste> ja <Lähetysaika>	Mikäli viesti liittyy useaan aikaisempaan viestiin, ne erotetaan välilyönnein.
	MuutTapauk-setID	Incident IDs (incidents)	V	Liittää yhteen useat viestit, jotka liittyvät eri aspekteilta samaan tilanteeseen.	Ryhmä	Identifioija	Mikäli viitataan useaan viestiin, ne erotetaan tosistaan välilyönnein. Tällöin myös tapahtumien nimet mukaan lukien välilyönnit erotetaan lainausmerkein.
Info			V		Ryhmä		Sisältää kaikki info -alaelementin komponentit.
	Kieli	Language (language)	V	Määrittää hälytysivestin info-alaelementin kielen.	Koodi	Natural language identifier [RFC 3066] tai "en-US" .	Mikäli jätetään täyttämättä, se tulkitaan 'en-US'.

Luokka			Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
	Tieto	Alkup.termi					
	Kategoria	Event Category (category)	P	Koodi ilmoittaa viestin ilmoituksen aiheen kategorian. Aiheesta voi olla useita ilmentymiä.	Koodi	Valinta	* Geo - Geofysikaalinen (esim. maanvyörymä) * Met - Meteorologinen (esim. tulva) * Turvallisuus - Yleisin hätätilanteisiin ja turvallisuuteen liittyen * Yleinen järjestys - Lain toimeenpano, asevoimat, kotimaa ja paikallinen/kunnallinen / yksityinen security) * Pelastus - Pelastus ja elpyminen * Tuli - Tulen sammuttaminen ja pelastaminen * Terveys - Lääketieteellinen ja julkinen terveys * Ympäristö - Saastuminen ja muut ympäristönsuojelu * Kuljetus - Julkinen ja yksityinen kuljetus * Infra - sähkö, teleliikenne, muu ei-kuljetuksellinen infrastruktuuri * CBRNE - Kemikaali, biologinen, radioaktiivinen, ydin- tai korkean luokituksen herkästi räjähtävä uhka tai hyökkäys * Muu - Muut tapahtumat
	Tapahtuma	Event Type (event)	P	Koodi ilmoittaa viestin ilmoituksen aiheen.	text	Teksti	

Luokka	Tieto	Alkup.termi	Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
x	Toiminnan-Tyyppi	Response Type (responseType)	V	Koodi määrittää toiminnan tyypin hälytysiviestin vastaanottajille.	code	Valinta	* Suoja - Mene suojaan <Ohje> mukaan * Evakuointi - siirry turvaan <Ohje> mukaan * Valmistaudu - Valmistaudu <Ohje> mukaan * Toimi - Toimi ennalta <Ohje> mukaan. * Vältä - Vältä tilanteen aiheuttajaa <Ohje> mukaan * Tarkkaile - Tarkkaile eri (tiedon)lähteitä kuten <Ohje> neuvottu. * Arvioi - Arvoi tämän viestin sisältöä (Tätä ei käytetä julkisissa varoitussovelluksissa). * Kaikki kunnossa - Tilanne ei enää aseta uhkaa tai huolta ja kaikki jatkotoimet ovat <Ohje> -kohdassa. * Ei suositella toimintaa
	Kiireellisyys	Urgency (urgency)	P	Määrittää hälytysiviestin kiireellisyyden.	Koodi	Valinta	* Välitön - Viestiin tulee reagoida välittömästi. * Odotettu - Viestiin tulee reagoida pian (tunnin sisällä). * Tulevaisuus - Viestiin tulee reagoida lähiaikoina. * Menneisyys - Toimia ei enää vaadita. * Tuntematon - Kiireellisyyttä ei tiedetä.
	Ankaruus	Severity (severity)	P	Osoittaa viestin aiheen ankaruuden.	Koodi	Valinta	* Äärimmäinen - Erikoislaatuinen uhka ihmisille tai omaisuudelle. * Ankara - Merkittävä uhka ihmisille tai omaisuudelle. * Kohtalainen - Mahdollinen uhka ihmiselle tai omaisuudelle. * Vähäinen * Tuntematon

Luokka	Tieto	Alkup.termi	Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
	Varmuus	Certainty (certainty)	P	Kertoo viestin aiheen varmuuden tietyllä asteikolla.	Koodi	Valinta	* Havaittu * Potentiaalinen * Mahdollinen * Epätodennäköinen * Tuntematon
	Vastaanottajat	Audience (audience)	V	Kuvaa viestin tarkoitetut vastaanottajat.	Teksti		
x	Tapahtuma-koodi	Event Code (eventCode)	V	Järjestelmäspesifi koodi, joka yksilöi viestin tapahtuman tyypin.	Koodi	<eventCode> <valueName> valueName </valueName> <value>value</value> </eventCode>	Voivat sisältää numeroita ja kirjaimia. Esim. valueName = "SAME" ja value = "CEM". Arvot kirjoitettava isoilla kirjaimilla ilman pisteitä (pediod? piste?)
	Vaikutusaika	Effective Date/Time (effective)	V	Aika, jonka viesti on voimassa. Tänä aikana viesti lähetetään viiden minuutin välein alueella sijaitseviin yhteensopiviin puhelimiin, mutta ne näyttävät viestin vain kerran*.	Aika	DateTime Data Type	"2002-05-24T16:49:00-07:00" (24.5.2002 klo 16:49 PDT).
	Alkaminen	Onset Date/Time (onset)	V	Odotettu aika, jolloin viestin ilmoittama aihe (varoituksen aihe) alkaa.	Aika	DateTime Data Type	"2002-05-24T16:49:00-07:00" (24.5.2002 klo 16:49 PDT).
x	Päättyminen	Expiration Date/Time (expires)	V	Aika, jolloin viestin ilmoittama aihe (varoituksen aihe) päättyy.	Aika	DateTime Data Type	"2002-05-24T16:49:00-07:00" (24.5.2002 klo 16:49 PDT).
	LähettäjäNimi	Sender Name (senderName)	V	Nimeää viestin alkupeäisen lähettäjän.	Teksti		
	Otsikko	Headline (headline)	V	Viestin otsikko.	Teksti	Teksti	Huom! Jotkut laitteet näyttävät viestistä vain tämän otsikon: siksi tämän tulisi olla mahdollisimman yksinkertainen ja selkeä.

Luokka	Tieto	Alkup.termi	Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
	Kuvaus	Event Description (description)	V	Viestin kuvaus: kuvaa viestin aiheen (eli varoituksen syyn).	Teksti		
	Ohje	Instructions (instruction)	V	Kuvaa suositellut toimenpiteet, joita viesti vaatii vastaanottajiltaan.	Teksti		Ohjeet ihmiselle hyvin luettevissa olevassa muodossa. Mikäli erilaisia ohjeita on tarkoitettu eri vastaanottajille, ne esitetään eri <info> -kokonaisuuksissa.
	Web	Information URL (web)	V	Lisätietoja viestin aiheesta antavan linkin tunniste.	Identi-fioija.		
	Yhteystieto	Contact Info (contact)	V	Kertoo, mihin ottaa yhteyttä seuratakseen tilannetta tai vahvistaakseen viestin tiedot.	teksti		
	Parametri	Parameter (parameter)	V	Järjestelmäspesifi hälytysviestiin liittyvä parametri.	Koodi	<parameter> <valueName> valueName </valueName> <value>value</value> </parameter>	Voivat sisältää numeroita ja kirjaimia. Esim. valueName = "SAME" ja value = "CEM". Arvot kirjoitettava isoilla kirjaimilla. Yhteen <Info> -kokonaisuuteen voi liittyä useita parametereja.
Resurssi		Resource	V		Ryhmä		
	resKuvaus	Description (resourceDesc)	P	Resurssin kuvaus.	Teksti	Teksti	Ihmiselle luettavissa olevassa muodossa esitetty kuvaus resurssin tyypistä ja sisällöstä.
	mimeTyyppi	MIME Type (mimeType)	P		Identi-fioija		[RFC 2046], www.iana.org/assignments/media-types
	Koko	File Size (size)	V	Resurssitiedoston koko.	Luku	Kokonaisluku	Tiedoston arvioitu koko tavuina.
	www	URI (uri)	V		Identi-fioija		Absoluuttinen verkko-osoite tai suhteellinen osoite.
	derefUri	Dereferenced URI (derefUri)	V		Data		
	Tiiviste	Digest (digest)	V		Koodi		Tiedon salaukseen liittyvä tunniste.

Luokka			Vaade	Määritelmä	Esitys	Tietotyyppi	Tarkennus
	Tieto	Alkup.termi					
Alue		Area	V		Ryhmä		
	Kuvaus	Area Description (areaDesc)	V		text	Teksti	Alueen sanallinen kuvaus.
	Monikulmio	Area Polygon (polygon)	V		group		
	Kehä	Area Circle (circle)			group		
x	Sijaintikoodi	Area Geocode (geocode)	V		code		
	Korkeus	Altitude (altitude)	V		quantity		
	maksimiKor-keus	Ceiling (ceiling)	V		quantity		

Taulukko pohjautuu Common Alerting Protocol Version 1.2 -dokumenttiin, joka on saatavilla verkosta osoitteesta http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf.

Hakasulkeilla viitataan toiseen tässä taulukossa esiintyvään luokkaan tai tietoon.

Liite 2. CAP-viestin luokkakaavio

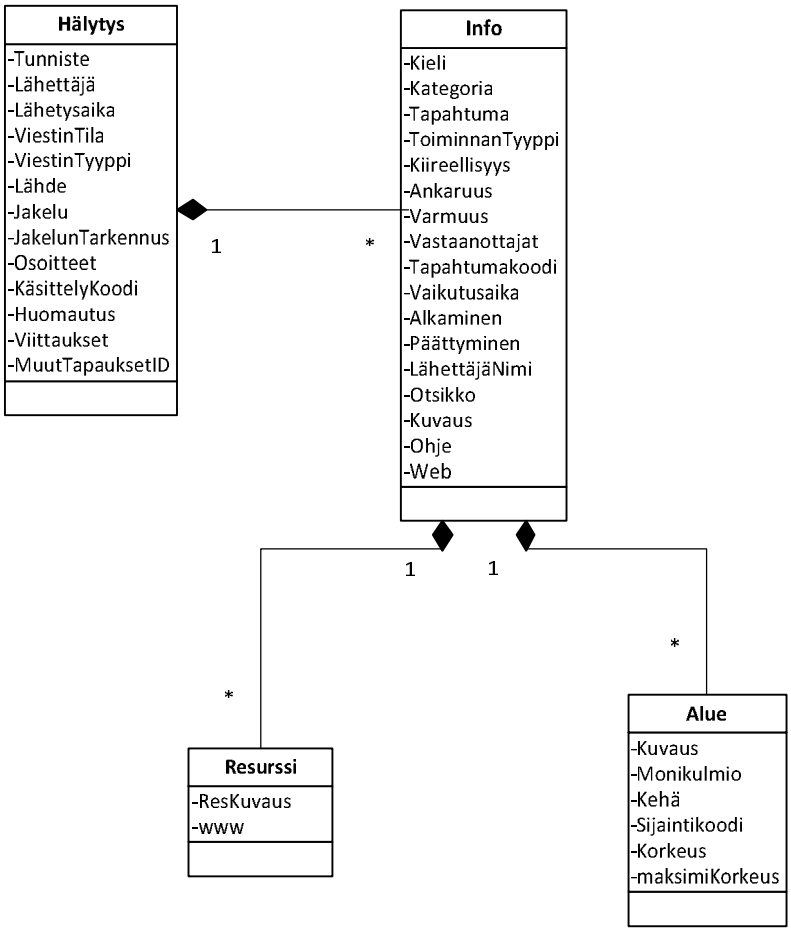
Luokkakaavio (class diagram) on staattinen mallinnustyyppi, joka kuvaa järjestelmän pysyvät rakenteet luokkien ja niiden välisten suhteiden avulla. Luokkakaavion luokat voidaan toteuttaa suoraan luokkarakennetta tukevalla olio-ohjelmointikielellä. Luokan rakenne koostuu luokan nimestä, attribuuteista (eli tiedoista) ja operaatioista (toimia, joilla tietoa käsitellään). (Järvelä ja Puusaari 2005, 18-19)

Alla olevassa kuvassa on esitetty tiivistetty CAP-viestin luokkakaavio. Luokkakaaviossa esitetään loogisella tasolla oleellisimmat tiedot, jotka kuuluvat CAP-viestiin. Luokkakaavio koostuu luokista, eli laatikoista, jotka sisältävät attribuutteja, eli tietoja, joita CAP-viesti sisältää. Kuten aiemmin mainittiin, CAP-viesti koostuu tietokokonaisuuksista (Common Alerting Protocol 2010):

1. hälytyksen tiedot (kuten osoite ja tehtävän tila)
2. tarkemmat tiedot (tapahtuman luokitus ja kuvaus sekä linkki lisätietoihin)
3. apulähteet (eli linkit ulkopuolisille sivustoille)
4. sijainti (kuten koordinaatit).

Nämä tietokokonaisuudet ilmenevät luokkakaaviossa luokkina Hälytys, Info, Resurssi ja Alue. *Hälytys*-luokassa yksittäisen hälytyksen perustiedot: hälytyksen yksilöivä tunniste, hälytyksen lähettäjän nimi ja lähetysaika, viestin tilaan ja jakeluun liittyviä määritteitä sekä tapahtumapaikan osoite. *Info*-luokassa esitetään tarkempia tietoja kyseisestä hälytyksestä: mihin kategoriaan tapahtuma liittyy, mikä on tapahtuman aiheuttaja, millaista toimintaa hälytys edellyttää vastaanottajalta ja mikä on tapahtuman kiireellisyys ja voimakkuus. Lisäksi viestille voidaan asettaa tapahtuman alkamis- ja päättymisajat.

Info-luokkaa edelleen täsmentävät Resurssi- ja Alue-luokat. *Resurssi*-luokka määrittelee lähinnä verkosta löytyvää lisätietoa tapahtuneesta. Resurssista ilmoitetaankin sen kuvaus ja verkko-osoite. *Alue*-luokalla puolestaan rajataan maantieteellistä aluetta, jolla hälytyksen aiheuttama tapahtuma vaikuttaa.



Kuva 1. CAP-viestin luokkakaavio.

Viivat eri luokkien välillä kuvaavat luokkien välisiä yhteyksiä. Luokat voivat liittyä toisiinsa eri tavoin: yhteen luokkaan voi kuulua toisen luokan kaksi eri ilmentymää. Tätä kuvataan viivan yhteydessä olevilla numeroilla ja tähti-merkeillä (*): numerolla osoitetaan, montako kyseisen luokan ilmentymää liittyy toiseen luokkaan. Tähti-merkintä tarkoittaa, että rajoittamattoman monta. Hälytys-luokan esitetään liittyvän Info-luokkaan. Numero yksi Hälytys-luokan ja tähti-merkki Info-luokan puolella tarkoittavat, että yhteen hälytykseen voi liittyä yksi tai useampi Info-luokka, siis Info-luokan tiedot. Suomen kontekstissa voitaisiin ajatella, että yksi Info-luokan ilmentymä eli yksilöllinen kokonaisuus sisältää kielenä Suomen ja toinen Ruotsin: kummallakin näistä ovat mm. samat kategoriat, vaikutusajat sekä ilmoituksen alkamis- ja päättymisajat, mutta eri kuvaus ja otsikko. Kuvaus ja otsikko olisivat tässä tapauksessa siis eri kielillä.

Yhteen Info-luokkaan voi liittyä vastaavasti yksi tai useampi Resurssi- tai Alue-luokan ilmentymä. Info-luokkaan voi siis sisältyä esimerkiksi useampi internet-linkki tai alueen kuvaus.