

Viestintä kriisissä

Tarmo Huttunen, OH6ECF

Ilmastonmuutos on väistämätön ja me tulemme kärsimään siitä.

Tässä kirjoituksessa kriisiviestintää pohditaan sääilmiöiden aiheuttamien tilanteiden kannalta. Näkökulma on valittu koska sääkriisit ovat täysin luotettavia: niitä on ja tulee olemaan. Haluan lukijan silti tietävän, että esitetyt ajatukset pyrkivät olemaan yleispäteviä: On sanottu, että kriisin ja katastrofin ero on viestintäverkkojen toiminta tai toimimattomuus. Se on hyvin sanottu.

Tätä kirjoittaessani viimeisin suurempi sääkriisi Suomessa oli tarttuva lumi, joka aiheutti sähkökatkojen sarjan keski-Suomessa. Satoja matkapuhelintukiasemia pimeni, samoin paikallinen FM-täytelähetin ja Virve-tukiasemia. Mikä oli radioamatöörien osuus tässä kriisissä? Uutisten perusteella ei mikään.

Kriisiviestinnän ongelma on metsän näkeminen puilta. Tämän artikkelin tarkoitus on poistaa puut ja jättää metsä jäljelle. Tarkoitukseni on myös kyseenalaistaa ja ärsyttää ajattelemaan. Ilman ajattelua ei synny toimivia järjestelmiä.

Tässä artikkelissa käytetään termejä sekalaisella tavalla. Jos asialle on olemassa yleisesti käytetty lyhenne, pyrin käyttämään sitä lyhenteen alkukielestä huolimatta. Samoin vieraskielisiä termejä käytän, jos ne ovat yleisessä käytössä. Pyrin tällä välttämään kapulasuomenkielisyyden, ilmiö joka syntyy kun yleisesti käytössä olevat termit pyritään suomettamaan "oikeiksi". Kriisiviestintä, turvaviestintä ja turvallisuusradioviestintä ovat jokseenkin synonyymejä: tässä ne tarkoittavat viestintää, jolla osittain korvataan jonkin häiriön kaatamia arkipäivän viestijärjestelmiä. Kriisitilannetta hahmotetaan termillä "häiriösolu", tämä on se maantieteellinen alue jossa tavalliset viestintäverkot ovat enemmän tai vähemmän kaatuneet, erotuksena "normaalialueesta".

Tulen esittämään ehdotuksia kriisiviestinnän tekniikasta, taajuuksista, antenneista ja käytännöistä. Nämä ehdotukset ovat yrityksiä muotoilla kriisiviestinnän tekniikka tukemaan sen tarkoitusta. Olennaisia ehdotuksissa eivät ole tekniikat joita ehdotan, vaan periaatteet joita nämä tekniikat yrittävät toteuttaa.

Kriisiviestinnän kulmakiviä ovat: *tilannetietoisuus, operaattorikeskeisyys ja rajapintaymmärrys*. Näistä periaatteista nousee hahmotellun ABC-viestiverkon arkkitehtuuri.

TURVAVIESTINNÄN TEHTÄVÄ

Me olemme radisteja, radio-operaattoreita. Olemme kiinnostuneita radiosta, siitä ihmeellisestä laatikosta joka kytkee meidät näkymättömään eetterin maailmaan. Ihmiseen ja ihmisyyhteisöön verrattuna radio on yksinkertainen ja helposti ymmärrettävä laatikko. Olemme kiinnostuneita tekniikasta, emme ihmisyydestä. Kriisiviestinnän pullonkaulana ei ole puutteellinen tekniikka, vaan puutteellinen humaniikka.

“Tavalliset” kriisit ovat tilanteita joissa häiriö on maantieteellisesti rajoitettu. Näemme näitä melko usein. Tyypillisesti säätila aiheuttaa laajan sähkönjakeluverkon häiriön, joka kaataa kaupalliset matkapuhelinverkot. Kriisialueelle saadaan silloin hyvin apua normaalitilassa olevilta alueilta. Esimerkiksi alueelle pystytään kokoamaan suuri määrä sähköasentajia, koska muualla viestintäverkot toimivat edelleen täysin normaalisti.

Tavalliselle häiriötilanteelle on tyypillistä että häiriösolu ei ole yhtenäinen: taajama-alueilla verkot kaatuvat harvoin pitkiksi ajoiksi ja erilaiset johtokeskukset pystyvät enemmän tai vähemmän toimimaan. Syrjäisimmällä haja-asutusalueilla sähköjä saatetaan joutua odottamaan viikkoja.

Voidaan sanoa, että mitä käskyvaltaisempi viranomainen, sitä paremmin hänen yhteytensä on turvattu: voimme hyvällä omallatunnolla rakentaa turvajärjestelmät luottaen siihen, että viimeisenä valot sammuvat aluehälytyskeskusten näytöiltä.

Tämä tarkoittaa myös sitä, että “tavallisen” turvallisuusradioviestinnän ensisijainen tehtävä voidaan määritellä yhteyden saamiseksi alueelta, jossa viestintäverkot eivät toimi, *mihin tahansa* pisteeseen, jossa viestintäverkot toimivat normaalisti. Tästä pisteestä viestit välittyvät edelleen normaaleja reittejä varmistettuihin johtokeskuksiin *myös häiriöalueelle* ja viime kädessä esimerkiksi Virve-verkon piiriin. Toivottavasti.

Kyse on siis yhteyden *palauttamisesta* kohteesta normaaliin viestintäverkkoon.

Väitän, että meidän on rakennettava turvaverkkomme ensisijaisesti palauttamaan yhteys “tavallisessa” kriisissä. Maailmanlopun ennustajat ovat olleet harvoin oikeassa. On helppo kuvitella kriisejä joissa ABC-verkko ei toimisi: vielä vaikeampi on kuvitella viestintäverkkoa, joka toimisi globaalissa kriisissä jos ei se toimi edes maakunnallisessa sähkökatkossa.

RAJAPINTAYMMÄRRYS

Viestintävälineiden käyttö on arkipäiväistä ja ihmiset ovat siihen hyvin tottuneita. Matkapuhelinverkon häiriötilanteessa useimmat työt käyvät hankaliksi. Turvaradioviestintä voi pytkiä korvaamaan oleelliset toiminnot kaatuneesta puhelinverkosta.

Tekniseltä kannalta kattava varaviestintäverkko olisi helppo ja halpa rakentaa. Jokaiseen sairaalaan, kunnantalon, paloautoon ja kyläkouluun asennettaisiin HF-radio ja NVIS-antenni. Koko Suomi olisi verkottunut radioteitse. Laitekustannus olisi pieni. Tämä on typerä ajatus.

Kansalaiset eivät osaa käyttää vanhan liiton radiota viestintärajoitana. Kansalaiset osaavat käyttää puhelinta, sähköpostia ja Facebookia. Eikä tämä muuksi muutu. Me emme pysty kouluttamaan suomalaisista radio-operaattoreita, emme varsinkaan sen jälkeen kun sähköt ovat jo poikki. Turvaradioviestinnän ensisijainen rajoitus häiriötilanteen asiakkaalle on oltava hänen oma puhelimensa tai tietokoneensa. Luit aivan oikein, hänen oma tavallinen puhelimensa ja tietokoneensa. Koska vain niitä kansalaiset osaavat käyttää. Ja siellä ovat hänen käyttämänsä sähköpostiosoitteet ja muut viestintään tarvittavat tiedot.

Ensijainen rajoitustekniikka häiriötilanteessa olisi siis wlan, wifi. Yhteys jaetaan normaalilla wlan-linkillä asiakkaille ja varsinainen yhteys normaalialueelle järjestetään Super-Um -tekniikalla, tehostetulla 3G-yhteydellä kaupalliseen matkapuhelinverkkoon, tai B-kerroksen verkon "kriisinettinä".

Ihmiset ovat myös tottuneet hoitamaan asioita puhumalla. Toinen mahdollinen rajoitus on siis puheyhteys, joko kasvokkain radio-operaattorin kanssa, tai jonkin yksinkertaisen teknisen järjestelyn kautta. Kokemukseni perusteella rivikansalainen kykenee omaksumaan PMR-radion peruskäytön lyhyellä opastuksella.

Ihmiset ovat myös tottuneet raapustelemaan asioita erilaisiin kaavakkeisiin. Kolmas mahdollinen rajoitus voisi olla jonkinlainen lippulappukirjesysteemi.

Nämä rajoituspohdinnat koskevat siis häiriöalueen asiakkaita. Normaalialueen kansalaiselle yhteys turvaviestintäverkkoon on aina järjestettävä normaalina puhelinnumerona, sähköpostiosoitteena, somena tai vastaavana tuttuuna palveluna. Viestiverkon oma nettisivu toteuttaisi parhaiten tämän rajoituksen.

Taulukko1: ABC-turvaverkon kerrokset

Ensisijainen kerros	Toiminta	Mode	Rajapinta normaalialueella	Rajapinta häiriösolussa	Baudrate	Häiriösolun kokoluokka
A	Palauttava	3G Super-Um	GSM, internet (some), SMS, email,	wifi (email,some)	“Normaali”	kunta
B	Turvaviestintä	KRH-viestiasemat, taktinen verkko	GSM, internet (some), SMS, email,	Kriisinetti, Puhe, lomake, C-tason rajapinnat	“Kohtuullinen” mutta rajoittaa käyttöä	maakunta
C	Hätäviestit, tilannetietoisuusviestit	Puhe, PskMail ym.	internet (some), email	Email: Twitter, SMS, APRS	“Edes jotain (oikeesti ihan surkea)”	valtio

Taulukko2: Kerrosten tekniikat yleistettynä

Kerros	Olennainen tekniikka	Taajuus	Modet	Huom
A: Super-Um	3G-suunta-antennit, paikallistuntemus, ajoneuvomastot, wlan-suunta-antennit, voip-puhelimet, suora yhteys taktiseen verkkoon.	900 Mhz (2.4Ghz, 800Mhz))	GSM, GPRS, 3G	GSM-verkon ajoitustekniikka rajoittaa yhteyttäisyydeksi 35 km, tätä ei voi ylittää edes tehokkaammalla antennilla. Yhteyspisteitä on kuitenkin paljon!
B: KRH-viestiasemat	Taktinen verkko: APRS, reaaliaikainen resurssinäyttö, CB, HF-NVIS, kriisinetti	Paikallisesti sopiva, esim 27 Mhz	Puhe, APRS digimodeilla (Thor, MFSK...)	Sähköverkkohäiriöt ovat yleisempiä maaseudulla, missä 27 Mhz:n CB toimii hyvin, taajuus myös etenee hyvin metsäalueella.
C: Global HF	Yhteydet eurooppalaisiin servereihin, NVIS-serveri Suomeen.	Matala, joko 10.148 Mhz tai kotimaan NVIS.	Digimodet: Thor, PSK-R, MFSK jne...,HF-APRS, NVIS-puheyhteydet.	Kotimaan NVIS-tukiasemasta olisi etua.

OPERAATTORIKESKEISYYS

Suomessa (ja maailmassa) on valtava joukko toimivia radioasemia ja taitavia operaattoreita. Koska tämä on tosiasia, sitä ei tarvitse todistaa.

Tästä resurssista huolimatta, viestintäyhteydet Suomessa voivat mennä totaalisesti poikki. Tämä on nähty suurten sähkökatkosten yhteydessä. Miksi tämä resurssi ei ole käytettävissä silloin kun sitä tarvitaan?

Jos viestintävälineistöä on, mutta se ei ole käytettävissä, jokin muu kuin välineistö on pullonkaulana. Tässä se on operaattorien puute. Miksi?

Yleensä radio-operaattori on muutakin kuin operaattori: Isä tai äiti, työntekijä, opiskelija...tai unessa, saunassa tai katsomassa Salkkareita.

Se keskimääräinen osa vuorokaudesta, jonka radio-asemat ovat käytössä, on häviävän pieni. Jos kaikki Suomen turvaviestintään sopivat radiolaitteet (ilman matkapuhelimia) ynnättäisiin yhteen, saataisiin valtava luku. Sanotaan vaikka 100 000. Kun tämä luku kerrotaan käyttöasteella, saadaan pieni luku. Se voi olla luokkaa 100. Suuri resurssi onkin todellisuudessa pieni. Pullonkaulana on operaattorien lukumäärä ja sitä kautta radioasemien käyttöaika.

Kannattaa myös ymmärtää POH-periaate (Paska Omissa Housuissa): Siellä missä sähköt ovat poikki, operaattoreilla on muuta tekemistä kuin harrastaa radioita. Esimerkiksi kirjoittajalla on radioasema ja aggregaatti. Meillä on ollut usein sähkökatkoja, pitkiäkin. En ole koskaan kokeillut käyttää asemaani generaattorilla. Sähkökatkon aikaan minulla on muuta tekemistä.

Johtopäätös on yksinkertainen: Turvallisuusradioviestinnän pullonkaula ei ole laitteissa, vaan ihmisissä. Siksi operaattori on asetettava tekniikan edelle.

Me emme pysty rakentamaan valtakunnallista ja ketterää verkkoa, jos määrittelemme millaisia verkon asemien pitää olla ja odotamme sitten että 1000 operaattoria alkaisi varustaa asemaansa hätaviestintää varten.

Kriisiviestintäverkkoa suunniteltaessa ei pidä miettiä millaisia verkossa toimivien asemien pitäisi olla, vaan miten nykyiset asemat voisivat toimia tehokkaana verkkona.

Verkon rakenne on suunniteltava niin, että se mahdollistaa tavallisen aseman toimisen verkossa: Tavallisen aseman resurssit ovat: jokin radiolaitte, tietokone ja puhelin. Joten näillä mennään.

Johtopäätös: Turvaviestintäverkkoa suunniteltaessa on mietittävä millaisia radioasemat ovat: ei millaisia niiden pitäisi olla.

Johtopäätös: Turvallisuusradioviestintää ei pidä supistaa "radioamatööri-toiminnaksi" koska silloin suuri määrä operaattoreita on pelistä pois.

Johtopäätös: POH-periaate: Kriisialueen viestintään on pyrittävä käyttämään mahdollisimman paljon normaalialueen resursseja, normaalialueen asemia.

Ehdotus: "KRH-viestiasema mode", taktisen viestiverkon perustaminen.

TILANNETIETOISUUS

Termi “tilannetietoisuus” (situation awareness, SA), voidaan käsittää ymmärrykseksi jonkin tilanteen olosuhteista ja käytettävissä olevista resursseista. Kun tilannetietoisuus on hyvällä mallilla, kyetään tilanteessa tekemään järkeviä päätöksiä, käyttämään resursseja tehokkaasti.

Kriisiviestinnän näkökulmasta oleellista on tietoisuus käytettävissä olevista resursseista, nimenomaan asiakkaan näkökannalta. Jos asiakas ei tiedä eikä tunne viestintäresurssia, se ei tule käytetyksi eikä hyödyksi.

Radio-operaattorin kannalta resurssien käyttäjät voidaan ajatella “tiimeiksi”. Kriisitilanteen toimintaa voidaan ajatella eri tiimien (pelastuslaitos, kotisairaanhoido, tieverkon ylläpito, sähköverkon korjaustiimit...) toimintana ja yhteistoimintana.

Tilannetietoisuuden puute on olennainen ongelma kriiseissä. Esimerkiksi poikkeuksellisissa keliolosuhteissa tieverkon ylläpitäjän olisi hyvä ymmärtää sähköverkon korjaustiimien tarpeita. Eri tiimien tarpeet ovat kuitenkin monimutkainen kokonaisuus. Samoin käytettävissä olevat resurssit ovat vaikeasti hahmotettava ja hajanainen kokonaisuus.

Siksi varaviestintäresurssi on “paketoitava” helposti käytettäväksi ja omaksuttavaksi.

Viestintäresurssin käyttö ei saa aiheuttaa lisää päänvaivaa muutenkin hankalassa tilanteessa.

Kuten todettu, kriisiviestinnän pullonkaulana on operaattoreiden vähyys. Siksi tiimeihin ei voida lisätä “tiimi-operaattoreita”, näitä lukuisia operaattoreita ei ole eikä tule koskaan olemaankaan. Turvaviestinnän varsinainen resurssi, osaava operaattori, pitää jakaa tehokkaammalla tavalla.

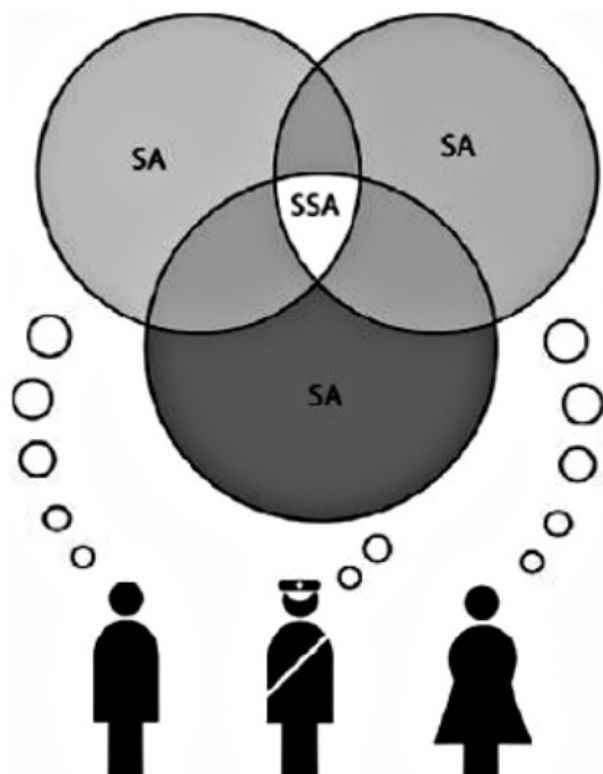
Miten turvaviestinnän resurssi saadaan jaettua eri tiimien käyttöön ja tilannetietoisuuteen? Ennalta ei voida edes tietää, mitkä tiimit pystyvät parhaiten resurssia käyttämään.

Kun yhteen suuntaan kumartaa, toiseen pyllistää. Jos operaattori toimii osana sähköverkon korjaustiimiä, hän ei voi samalla hoitaa kotisairaanhoidon viestintää. Turvaviestintä tarvitsee kuitenkin pitkäjänteistä suunnittelua ja harjoittelua. Ilman olemassaolevaa, todellista asiakasta, harjoittelu on kuvittelua.

Ihanteellista olisi, jos turvaviestinnän resurssi voitaisiin antaa kaikille olennaisille tiimeille. Mutta miten yksi radio-operaattori voisi olla osa *jokaista* tiimiä? Helposti.

Kuva 1: Kansalaisten tilannetietoisuus (situation awareness, SA) yhdessä muodostavat tiimien jaetun tilannetietoisuuden (shared situation awareness, SSA). Kuva on julkaisusta “Situation awareness for critical infrastructure protection” (toim. Jouko Vankka, Maanpuolustuskorkeakoulun julkaisu). Kuva on irrotettu tässä varsinaisesta asiayhteydestään mutta selventää kauniisti ajatusta, että kansalaisten tilannetietoisuus yhdessä muodostuu osaksi tiimien tilannetietoisuutta.

Jokainen tiimi koostuu ihmisistä, kansalaisista. Kun turvaviestinnän



resurssi jaetaan suoraan kansalaisille, se on kaikkien tiimien käytössä. Jokainen poliisi, palomies ja hätäkeskusvirkailija on kansalainen. Siksi resurssi jaetaan nimenomaan kansalaisille, ei jollekin ennalta päätetylle toimijalle.

Johtopäätös: Turvaviestinnän resurssia ei pidä kohdentaa erityisesti viranomaisille. Olennaista on järjestää avoin kansalaisrajapinta turvaviestintäverkkoon. Ennalta ei pidä rajata, kuka resurssia tarvitsee.

Ehdotus: Avoin “taktinen nettisivu”, joka toimii rajapintana normaalialueen kansalaisille, rajapintana eri viestintäkeinojen kesken ja tilannenäyttönä operaattoreille.

ABC-VERKON RAKENNE

Lyhyesti:

ABC = “Always Best Connected”

A-kerros: Super-Um: “etä-3G”

B-kerros: Viestiasemat: “taktisen nettisivun” avulla yhteen toimivat asemat.

C-kerros: HF-yhteydet, kotimaan NVIS ja datayhteydet ulkomaisiin asemiin.

Artikkelin seuraavassa osiossa on ehdotus kriisiviestintäverkon arkkitehtuuriksi. Kuten alkuun totesin, olennaista ehdotuksessa eivät ole tekniikat joita esitän vaan periaatteet joita ne yrittävät toteuttaa: tilannetietoisuus, operaattorikeskeisyys ja rajapintaymmärrys

Verkon “kerrokset” on suunniteltu häiriösolun kokoluokan mukaan: A-kerroksen toiminta on pyritty optimoimaan kunnan kokoluokkaa olevan häiriösolun kannalta, B-kerros maakunnan kokoisen ja C-kerros valtion kokoluokkaa olevan häiriön varalta. Esitys on tietysti yksinkertaistus: ei ole mitään syytä miksi C-kerrosta ei voisi käyttää maantieteellisesti pienessä häiriössä.

ABC, Always Best Connected, eli “Paras yhteys” voidaan ymmärtää kunkin tilanteen parhaaksi mahdolliseksi kaistanleveydeksi. Mitä lievempi kriisi ja lyhyempi etäisyys normaalialueeseen, sitä suurempi kaistanleveys voidaan saavuttaa. Paras kaistanleveys saavutetaan Super-Um yhteydellä.

A-kerros: Super-Um

A-kerros on ajateltu kunnan kokoluokkaa olevan häiriösolun operointiin.

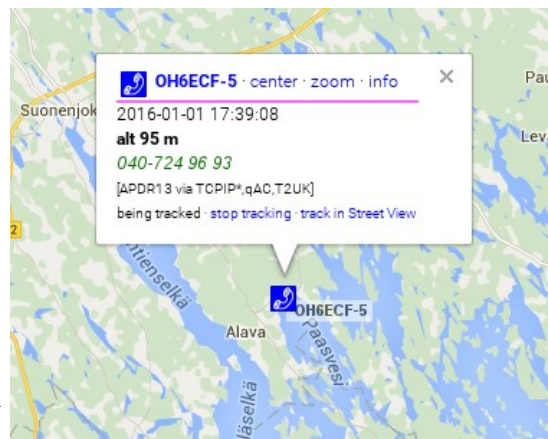
Matkapuhelimen ja tukiaseman välistä yhteyttä kutsutaan Um-rajapinnaksi. Super-Um on yksinkertaisesti “superpuhelin”, puhelin jonka yhteydenpitokykyä on parannettu radikaalilla antenniratkaisulla. Antenniratkaisu voi olla esimerkiksi ajoneuvoon rakennettu teleskooppimasto, jossa on 900 Mhz:n diboli, moxon tai yagi-antenni. Asema raportoi itsensä taktisen verkon kartalle matkapuhelinverkon kautta, vaikkapa APRSdroid-ohjelmalla. Super-Um asema pystyy myös päivittämään taktisen verkon sivua häiriösolusta käsin manuaalisesti tavallisella selaimella.

Kuva 2: Matkapuhelimet on suunniteltu hyvin myytäviksi, ei hyvin kuuluviksi. Jo tällainen yksinkertainen 900 Mhz:n diboli parantaa yhteyttä hämmästyttävästi. Super-Um-linkiksi voidaan sanoa ajoneuvoon rakennettua radikaalia matkapuhelinverkon antenniratkaisua. Saavutettu datayhteys jaetaan häiriöalueen asiakkaille, ehkä parhaiten wlan-tukiasemana. (Kuva-kirjoittajan kokeiluja)



Kuva 3: Normaali alueen rajapintana Super-Um asemaan olisi kartalla näkyvä puhelimen kuva ja numero – siis toimiva puhelin alueella jossa matkapuhelinverkko on kaatunut. (Kuva-kirjoittajan kokeiluja)

Parhaassa tapauksessa Super-Um-yhteys voitaisiin jakaa häiriöalueen asiakkaille tehokkaalla wlan-tukiasemalla. Wlan-tukiasema voidaan varustaa suunta-antennilla ja saavuttaa satojen metrien jakoetäisyys. Tämä antaa mahdollisuuden sijoittaa Super-Um edulliseen kohtaan maastossa. Asiakas näkisi yhteyden omalla puhelimellaan tai tietokoneella wlan-verkkona, jolla voi käyttää sähköpostia, somea ja olennaisia internetin palveluja.

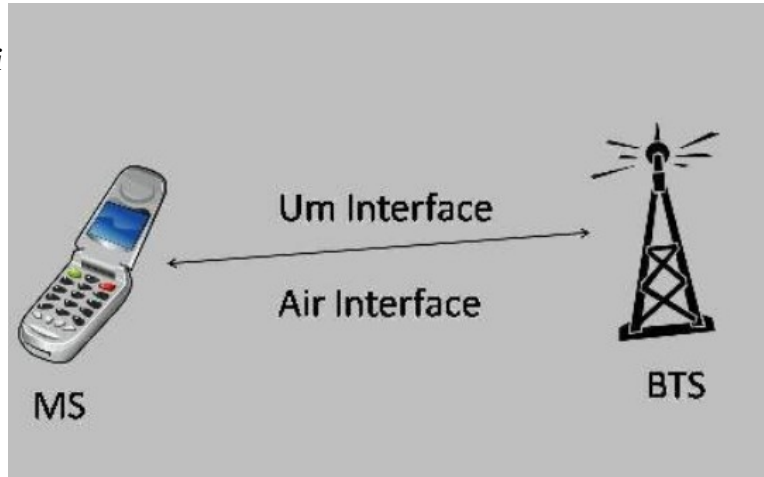


Super-Um on kaistanleveydeltään ylivoimainen muihin turvallisuusradioviestinnän keinoihin verrattuna. Lisäksi tämä voidaan saavuttaa vain yhden operaattorin toiminnalla, ja palauttaa häiriösolun asiakkaille osa normaalista tutusta viestintärajapinnasta. Häiriösolun sisällä asiakkaat voisivat viestiä normaaleja kanavia pitkin eri Super-Um-ajoneuvoasemien muodostamien viestintäsolujen välillä. Näiden mahdollisuuksien hylkääminen turvaradioverkosta vain koska kyse ei ole “oikeasta radioamatööri-toiminnasta” olisi silkkää tyhmyyttä.

Super-Um “moden” perusongelma on että, radio-operaattorit eivät useinkaan tunne matkapuhelintekniikkaa. Ihan totta. Sitä ei koeta kiinnostavaksi. Toinen kummallinen ongelma on matkapuhelinverkkojen kattavuus: Super-Um-järjestelmiä on vaikea testata normaalioloissa, koska riittävän hankalat testiolosuhteet ovat harvassa.

Ehdotus: Super-Um-tietoa aletaan kerätä taktisen netin yhteyteen.

Kuva 4: Um-rajapinta mahtuu puhelimeen, Super-Um -rajapinnan voisi toteuttaa ajoneuvomastolla.



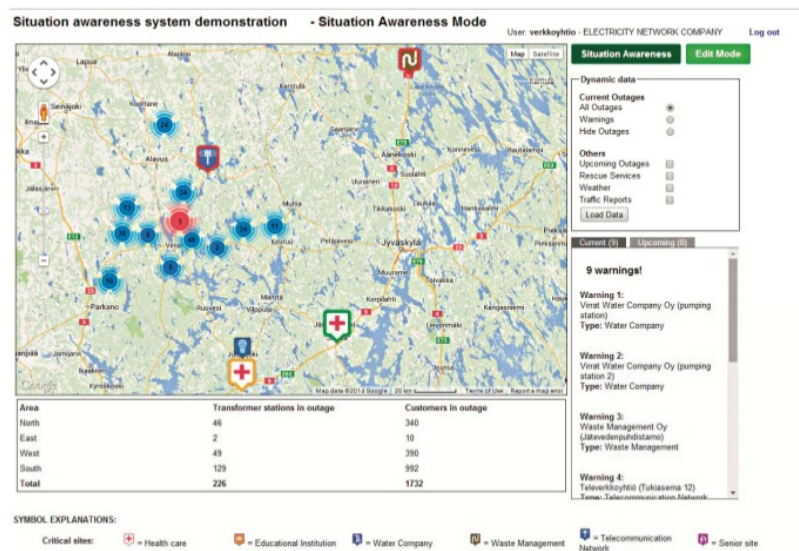
B-kerros: KRH-viestiasemat

Nimitän B-kerroksen asemia “KRH-viestiasemiksi”. B-kerros on suunniteltu maakunnan tasoiseen toimintaan ja perustuu “oikeaan” radioverkkoon lisättynä avoimella normaalialueen rajapinnalla, “taktisella verkkosivulla”.

Taktisen verkon nettisivulla rajapinnat näkyvät puhelinnumeroina, sähköpostiosoitteina sekä avoimena some-palveluina. Normaalialueen asemat “isännöivät” taktisen verkon nettisivua, päivittäen tilannenäkymää ja välittäen sanomia häiriösolun asemille ja häiriösolusta taktisen verkon sivulle, someen, sähköpostiin, viranomaisille jne.

Tämä isännöinti on kollektiivista viestiasemien toimintaa. Isännöinti tapahtuu maantieteellisesti ja ajallisesti hajautettuna. Näin saadaan lisättyä toimintaan pystyvien operaattoreiden määrää. Koska sivu on toteutettu eri palvelujen avulla (aprs.fi, facebook, twitter, häiriöinfo.fi ...), sisältö on hajautettu eri servereille. Esimerkiksi taktisen kartan palvelimen kaatuessa, tilannetta voidaan auttaa facebook-päivityksillä jne...

Kuva 5: Esimerkki taktisesta kartasta. Vastaava järjestelmä voidaan toteuttaa olemassa olevia palveluita järkevästi soveltamalla. Olennaista on, että järjestelmän kautta sekä operaattori että kansalainen näkevät, mitä kautta yhteyden voi saada: Kuva on julkaisusta “Situation awareness for critical infrastructure protection” (toim. Jouko Vankka, Maanpuolustuskorkeakoulun julkaisu).



B-kerroksen arkkitehtuuri ei määrittele mitä taajuuksia tai modeja radioyhteyksiin on käytettävä, päinvastoin. Yhteystaajuuksien moninaisuus lisää toimintavarmuutta ja mukana olevien asemien määrää. ABC-verkon asemat ovat itsenäisiä ja päättävät itse millä keinoin toteuttavat yhteytensä. Asemien käyttämä ja isännöimä taktinen nettisivu mahdollistaa tämän.

Operaattorikeskeisyyden kannalta on järkevää rohkaista CB-asemia toimimaan viestiasemina vaikka esimerkiksi 10 metrin amatöörialue voisi olla teknisesti parempi. Tekninen paremmuus ei kuitenkaan auta jos vasta-asemaa ei ole. Mikään ei estä amatööriasemia käyttämästä toistimia, NVIS-yhteyksiä, sähkötystä tai vaikka RTTY-sanomia jos siltä tuntuu ja verkossa on normaalialueen vasta-asema olemassa.

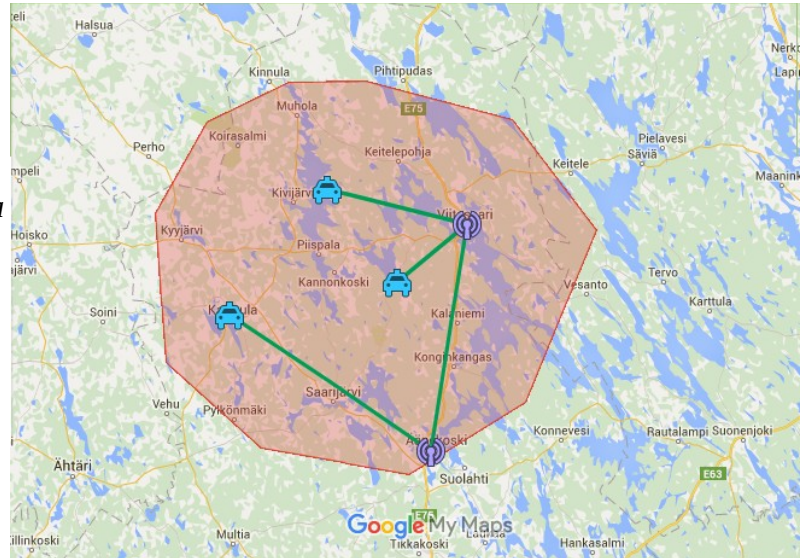
B-kerroksessa häiriösolun sisäiseen viestintään käytetään ajoneuvoasemia viestiverkon normaalialueen asemien koordinoimina. Kyseessä ei ole enää normaalin viestintäraajapinnan palauttaminen, vaan turvallisuusradioviestintä jossa vain oleellinen on tärkeää.

Taktisen verkon merkitys rajapintana

Viestiasemien isännöimä taktinen verkko mahdollistaa joustavien yhteysratkaisujen käytön.

Taktisen verkon ja “perinteisen” kriisialueen radioverkon ero on esitetty tässä kahdella kuvalla. Lienee syytä korostaa, että kyseessä on yksinkertaistus, palikkamalli. Taktinen verkko ei ole rajoitus viestintäkeinoihin vaan *lisäys* niihin. Taktinen verkko on ennenkaikkea *rajapinta* eri viestintäkeinojen välillä.

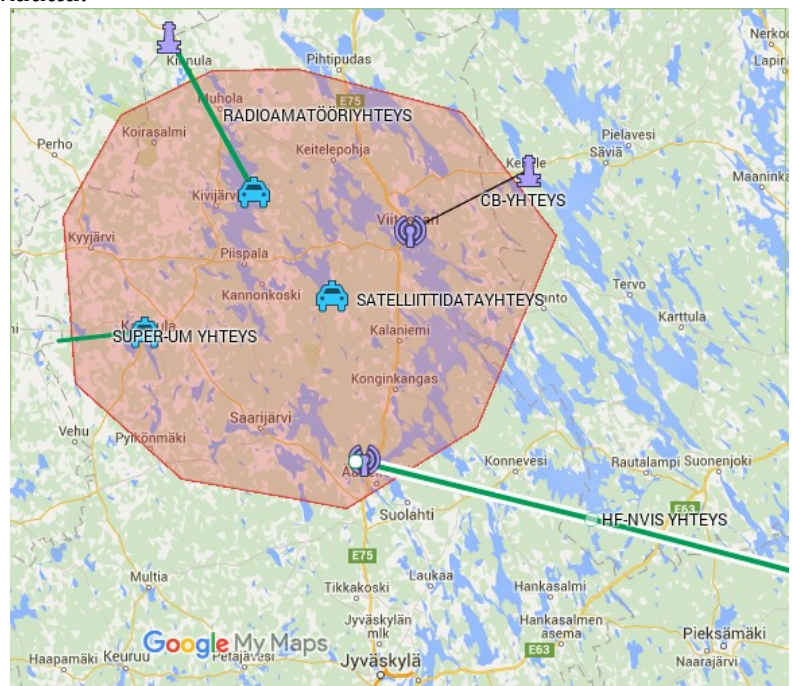
Kuva 6: Perinteinen malli kriisivialueen viestintään. Häiriösoluun rakennetaan radioverkko. Verkon asemat toteuttavat verkon sisäisiä standardeja: taajuuksia, modulaatiota ja yhteyskäytäntöjä. Asemien on oltava teknisesti yhteensopivia. Asemien ensisijainen tehtävä on saada yhteys johonkin toiseen verkon asemaan.



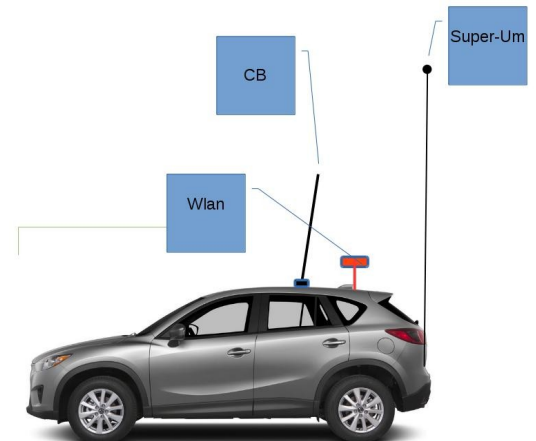
Kuva 7: Taktisen verkon avulla toteutettu viestintäverkko. Huomaa että kuvan asemat ovat yhteydessä **keskenään** taktisen verkon kautta.

Häiriösolun asemien ensisijainen tehtävä on muodostaa yhteys normaaliin viestintäverkkoon. Rajapintana voi toimia jokin taktisen verkon normaalialueen asema, Super-Um yhteys tai vaikka satelliittidatayhteys. Taktinen verkko toimii manuaalisena **rajapintana** eri viestintäkeinojen välillä: Näin esimerkiksi HF-NVIS yhteyttä verkossa operaiva asema voi viestiä CB-aseman kanssa, tai vastaanottaa kansalaisen lähettämän Twitter-sanoman.

Taktisen verkon avulla toteutetussa viestinnässä asemien ei tarvitse toteuttaa samoja standardeja. Ne voivat valita itselleen parhaiten sopivat yhteyskeinot. Ainoa tekninen “standardi” on selainohjelma.



Kuva 8: Liikkuva KRH-viestiasema voisi näyttää jotakuinkin tältä. Piirroksessa voisi olla myös HF-alueen antenni, mutta jätin tarkoituksella pois kaikki amatöörisenssin vaativat laitteet. Silti tämä esimerkki toteuttaa A- ja B-kerrokset.



Ongelma: B-kerroksen rajapinta häiriösolussa

Häiriöalueen rajapinnan toiminta on B-tasolla jo huomattavan ankeaa.

Perinteisiä rajapintakeinoja ovat esimerkiksi lomakkeille kirjoitetut viestit, joita voidaan välittää radioteitse, samoin voidaan ajatella jonkinlaista PMR-radioihin (tai wlan-verkossa toimiviin sisäisiin puheluihin) perustuvaa lähiverkkoa. Liikkuva viestiasema päivystää tätä lähiverkkoa ja lähettämää ulkopuolelle tarkoitettuja viestit eteenpäin.

Oletan, että viestinnän pullonkaulana B-kerroksessa on häiriösolun asiakasrajapinta. Mielenkiintoinen mahdollisuus olisi "kriisinetti". Teknisesti kyse olisi wlan-verkosta joka jaetaan viestiverkon ajoneuvosta tai siirrettävästä tukiasemasta. Asemalla olisi oma "nettiserveri" joka jakaisi taktisen netin sivua tässä paikallisverkossa. Operoiva radioasema päivittäisi tätä "kriisisivua" manuaalisesti tiedoilla, joita saa esimerkiksi puheyhteydellä normaalialueen asemiin, jakaen tiedotuksia, viestejä ym. Alueen asukkaat voisivat lähettää sanomia operoivalle asemalla tämän "kriisinetin" kautta omalla puhelimellaan tai tietokoneella, välitettäväksi normaalialueelle tai muihin kriisiverkon radioasemiin. Sivu olisi optimoitava mobiilikäyttöön, koska sähkökatkossa pääsääntöisesti puhelimia voidaan ladata autolatureilla, mutta tietokoneet sammuvat nopeasti.

Mobiililaitteisiin on vuosien mittaan alkanut ilmestyä wlan verkossa "mesh" -periaatteella toimivia viestiapletteja, kuten FireChat tai Serval Mesh. Ehkä olisi mahdollista hyödyntää näitä B-kerroksen häiriösolun viestintärajapinnan maantieteelliseen laajentamiseen tiheästi asutulla alueella. Mesh-networking -periaatteella toimivat appletit "hyppäyttävät" viestit puhelimen muodostaman verkon kautta, laitteelta laitteelle kunnes ne saapuvat vastaanottajalle. Mesh-tekniikan ansiosta viestiverkon viestit voisivat liikkua myös viestiaseman wlan-verkon kantamatkan ulkopuolella.

Kuva 9: Liikkuvan viestiaseman perusvarustus on radiolaite ja puhelin tai tablet-kone. Näiden pohjalle voidaan toteuttaa sekä Super-Um että B-tason viestiasematoiminta. Kuvan yhdistelmällä on testattu myös halpaa rtl-sdr "tv-tikku" vastaanottoon perustuvaa aprs-systeemiä CB-alueella, ja todettu toimivaksi. Kokeilussa käytettiin PskMail järjestelmää, jolla APRS-tiedon lähetykseen voidaan käyttää "oikeita" digimodeja, kuten virheenkorjauksen sisältävää THOR-modea. (Kuva: Kirjoittajan kokeiluja.)



C-kerros, maailmanlopun odottajien ja amatööripreppareiden alue.

Sivuutan C-kerroksen lyhyellä maininnalla, ensiksikin koska en pidä sitä tässä yhteydessä kovin olennaisena ja toiseksi koska C-kerroksen toimintaa ei ole tarpeen samalla tavalla yhtenäistää kuten B-kerrosta. Kukin asema pystyy luomaan omanlaisensa C-kerroksen jos katsoo sen tarpeelliseksi. ABC-verkon toiminnan kannalta asemien ei tarvitse pystyä C-luokan toimintaan (Lue: amatöörilisenssi ei ole välttämätön, mutta se antaa mielenkiintoisia mahdollisuuksia).

Olosuhteissa, joissa ABC-verkko sinänsä toimii, mutta häiriösolussa toimivalla asemalla on vaikeuksia saada yhteys, voisi C-kerroksen tekniikoista olla apua. Esimerkiksi jos CB-alue on kovin häiriöinen, voisi kotimaan NVIS-yhteys toimia. On makuasia katsotaanko kotimaan NVIS-yhteys B- vai C-kerroksen toiminnaksi.

C-kerrosta voidaan katsoa samoilla silmillä kuin muitakin: Rajapintaymmärrys, operaattorikeskeisyys ja tilannetietoisuus. C-kerroksessakin on mahdollista toteuttaa esimerkiksi sähköpostin lähettämistä ja vastaanottamista. Tilannetietoisuuden kannalta HF-radion kautta voi lähettää myös somepäivityksiä ulkomaisten servereiden kautta. Operaattorikeskeisyys tarkoittaa, että turvaverkko on rakennettava hyödyntämään jo olemassa ja käytössä olevia asemia ja viestintämuotoja.

Olosuhteissa, joissa ABC-verkko voi toimia enää C-tasolla, eli "koko internetti" on saavuttamaton koko verkon alueella... jokainen asema voi itse harkita onko sillä sijaintinsa puolesta mitään tärkeitä viestintätehtäviä, ja miten sen voisi toteuttaa.

Kuvat 10-12: Myös C-kerroksen viestinnässä voi pyrkiä yhteyteen ensisijaisesti normaalin viestintäverkon kanssa. Esimerkissä on salkkuun asennettu HF-asema, "peräkonttikoon PskMail-magneettilooppi" ja lopputulos: PskMail-verkon kautta lähetetty Twitter-päivitys, joka siirtyy "automaattisesti" myös Facebook-päivitykseksi. Viesti on lähetty Suomesta Itävallassa sijaitsevan OE5RTL-serveriaseman kautta.(Kuvat:Kirjoittajan kokeiluja.)



Tarmo Huttunen

9. tammikuuta kello 10:47 · Twitter ·

Power shortage test...running pure battery power

Tykkää

Kommentoi

Jaa