Viestimies

Viestiupseeriyhdistyksen julkaisu 76. vsk Numero 1 Kevät 2021

www.viestiupseeriyhdistys.fi

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Samuli Terämä
p 050 3399038
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Hanna Liitola
p 040 5930675
henkilotoimittaja@viestiupseeriyhdistys.fi

Toiminnanjohtaja
Harri Reini
p 040 514 2497
toiminnanjohtaja@viestiupseeriyhdistys.fi

Toimituskunta
Heiskanen Mikko (pj)
Blomqvist Reima
Holma Harri
Isomäki Pekka
Mikkonen Mauri
Petäjäinen Juha
Ståhlberg Mika
Suokko Harri
Valkola Eero
Wirman Kari
Yli-Äyhö Janne

Toimituksen osoite:
Päivölänrinne 7 A 1
04220 Kerava

www.viestiupseeriyhdistys.fi/viestimies
Pankkitili FI21 5780 5520 0177 44
Vuosikerta 35 €

Tilaukset ja osoitteenmuutokset
Harri Reini
p 040 514 2497
toiminnanjohtaja@viestiupseeriyhdistys.fi

Ilmoitusmyynti
Juha Halminen
p 09 873 6944, 050 592 2722
juha.halminen@kolumbus.fi

Painopaikka
Newprint Oy, Raisio
p 010 231 2600

ISSN 0357-2153

Kansikuva: Aamu sarastaa Kaunispäällä jäisen maston katveessa. (Kuva:Viestimies)

Tässä numerossa

Seuraavan numeron aineistopäivä on 10.5.2021. Lehti ilmestyy viikolla 22.

Fujitsu luo osallistavaa, kestävää ja luotettavaa tulevaisuutta

Turvallisuus syntyy luottamuksesta, osaamisesta ja vastuun kantamisesta. Fujitsu on sitoutunut edistämään ict-ratkaisuja, jotka auttavat organisaatioita ja yrityksiä rakentamaan tulevaisuutta turvallisesti ja kestävästi. Monipuolisen teknologia- ja palveluosaamisemme avulla autamme asiakkaitamme pysymään kehityksen kärjessä.

Teemme kaikkemme, jotta asiakkaamme saavat meiltä aina erinomaista palvelua riippumatta teknologiasta, hankkeen koosta tai asiakkaan tilanteesta. Tarjoamme asiakkaan luottokumppanin roolissa ict-ratkaisut tiedon saatavuuteen, integrointiin, jalostamiseen ja hyödyntämiseen, jotta yhteiskunta toimii aina – vaativissakin tilanteissa.

Lue lisää: **www.fujitsu.com/fi**

FUJITSU

Rokotetta odotellessa…

Vuosi on jälleen vaihtunut ja Viestimieslehden 76. vuosikerta lähtenyt käyntiin. Edellistä vuotta sävytti lukuisat muutokset tapahtumien järjestelyissä. Osa tapahtumista on jouduttu siirtämään ja osa peruttu tyystin. Useita tapahtumia ja tilaisuuksia siirtyi verkkoon. Suomessa tapahtuikin korona pandemian myötä merkittävä digiloikka. Esimerkiksi perinteinen TIETO-harjoitus toteutettiin täysin etäyhteyksin. Seminaarit ovat muuttuneet webinaareiksi ja Puolustusvoimien perinteiset sotilasvala- ja vakuutustilaisuudetkin on striimattu internettiin, koska koronaan liittyvät kokoontumisrajoitukset ovat estäneet yleisön paikan päälle kutsumisen. Paljon on muuttunut. Todennäköisesti päästyämme pandemian ikeestä jotain hyvääkin on tapahtunut ja tiettyjä hyviä menettelytapoja jää käytäntöön.

Vaikka korona on ollut kaikkien huulilla Suomessa ja muualla maailmalla jo kohta vuoden päivät, muutakin on tapahtunut. USA:n presidentti on vaihtunut, Myanmarissa on tapahtunut sotilasvallankaappaus, mutta hankalin on ehkä kuitenkin se, etteivät verkkorikolliset ja kyberhyökkäykset ole suinkaan laantuneet, vaan päinvastoin. Vastaamon tietomurto ja eduskuntaan kohdistunut kyberhyökkäys ovat tästä hyviä esimerkkejä. Kyberhyökkäykset ovat muuttuneet yhä uskaliaammiksi ja röyhkeämmiksi. Verkkohyökkäysten saaliita on julkaistu internetissä liki kaikkien saatavilla tai tiedolla, että ne voidaan julkaista, on kiristetty lunnaita.

Huoltovarmuuskeskus julkaisi tammikuussa tiedotteen, jossa ilmoitettiin ohjelmakokonaisuuden käynnistämisestä yhteiskunnan kyberhäiriösietoisuuden kehittämiseksi. Ohjelma on osa Suomen kansallista kyberturvallisuusstrategian toteutusta. Ohjelmalla pyritään lisäämään merkittävästi panostusta kyberturvallisuuden kehittämiseen. Sen tavoitteena on kehittää mm. kyberhäiriöihin varautumista, toimintakyvyn varmistamista häiriöiden sattuessa, lisätä yhteistyötä yhteiskunnan ja yritysmaailman toimijoiden välillä sekä tulevaisuuden ennakointia.

Ohjelmakokonaisuudessa huomioidaan myös kansainvälisen yhteistyön tuki ja osaaminen täydentämään kotimaista korkeaa tietotaitoa.

Turvallisuusympäristössämme on tapahtunut muutoksia, eivätkä kaikki todellakaan ole olleet positiiviseen suuntaan. Valtioneuvoston puolustuspoliittinen selonteko julkaistiin edellisen kerran vuonna 2017. Uutta on laadittu kiivaasti ja se onkin tarkoitus julkaista kevään kuluessa. Edellinen kesti aikaa nelisen vuotta. Sotilaallisen avun antamisen ja vastaanottamisen lait on hyväksytty, jotka mahdollistavat ulkomaisen avun vastaanottamisen, vaikka Suomi olisi kriisissä. Itämeren alueen vakaus, arktisen ulottuvuuden merkittävyyden kasvu ja erityisesti kyberulottuvuus ovat esillä ehkä suuremmassa määrin kuin aiemmin. Huolestuttava suuntaus on Venäjän suhtautuminen ydinaseiden käyttöön yhä herkemmin tilanteissa, joissa se kokee jäävänsä tappiolle mahdollisessa konfliktissa. Toisaalta Venäjän avaukset ydinaseidensa käytöstä tai pidättyvyyden vähentymisestä puolustusdoktriinin retoriikassa, ei ole uutta.

Pohjoismainen yhteistyö on tiivistynyt entisestään. Tavoitteena on yhteisoperointikyky. Tietyissä rajapinnoissa kynnys on varsin matala, mutta erityisesti johtamisjärjestelmien suhteen töitä on vielä tehtävänä. Suuria haasteita tuskin on näköpiirissä, mutta verkottuminen oikein –tietoturvallisesti, ei käy käden käänteessä. FMN-alusta tarjoaa tähän yhden ratkaisun. Pitkälle kehitettyjen kansallisten järjestelmien yhteensovittaminen ei olisi kovinkaan kustannustehokasta. On helpompi ottaa yhteinen alusta, jonka liitettävyyden perusteet ovat kaikille samat. Federated Mission Networking (FMN) kuvaa periaatteet ja määrittää rajapinnat liitettävyydelle ja palveluille. Pohjoismainen yhteistyö tulee olemaan tiivistä myös jatkossa, vaikka pandemia on rajannutkin käytännön yhteistyön minimiin. Touko-kesäkuulle suunniteltu monikansallinen Puolustusvoimien pääsotaharjoitus Arctic Lock 21 peruttiin. Sen sijaan tulevana keväänä toteutetaan pienempiä alueellisia harjoituksia.

Kaikki varmasti odottavat milloin on mahdollista saada rokote ja missä vaiheessa pandemian selkä katkeaa, jotta voisimme vähitellen palata normaalimpaan elämänrytmiin ja oloon. Yhteiskuntamme ja elämä koko maapallolla tuskin palaavat entiseen, mutta ainakin voinemme kokoontua vapaammin ja matkustaa taas – muuallekin kuin omalle takapihalle.

Yksi merkittävä muutos tapahtuu kevään kynnyksellä. Pääesikunnan Johtamisjärjestelmäpäällikkö vaihtuu. Kenraalimajuri Mikko Heiskanen luovuttaa tehtävänsä eversti Jarmo Vähätiitolle. Samalla vaihtuu myös Viestimies-lehden toimituskunnan puheenjohtaja. Viestimies-lehti ja sen toimitus haluaa kiittää väistyvää puheenjohtajaa merkittävästä ja pitkäaikaisesta panoksesta lehden kehittämisessä sekä toivottaa onnea ja menestystä uuteen tehtävään. Toivotamme uuden puheenjohtajan lämpimästi tervetulleeksi ohjaamaan lehteä ja johtamisjärjestelmäalaa.

Päätoimittaja

Samuli Terämä

Uuden ajan alku

Vuosi sitten koronavirus sai koko maailman otteeseensa ja kaiken toimeliaisuuden hiljenemään ennennäkemättömällä tavalla tunnetuin seurauksin. Varautuminen tämän kaltaiseen kriisiin todettiin kaikkialla riittämättömäksi, myös Suomessa, missä jouduttiin turvautumaan valmiuslain käyttöönottoon. Taloudelliset seuraukset kansantalouteen ja eri alojen toiminta-edellytyksiin ovat mittavia ja vaurioiden korjaaminen kestää pitkään. Vieläkään emme ole selvillä vesillä, vaikka rokotteet on jo saatu käyttöön. Meneillään on toinen peräkkäinen poikkeusvuosi.

Työnteko on monella meistä muuttunut loputtomiksi virtuaali-istunnoiksi ja sosiaalinen elämä on kutistunut lähikaupassa käymiseksi maski naamalla. Yleensä poikkeavia olosuhteita on helpompi sietää, jos tietää että ne joskus loppuvat. On kuitenkin lähes varmaa, että elämä ei palaa kaikin osin entiselleen sen enempää yhteiskunnan tasolla kuin tavallisten ihmisten arjessa, vaan meidän on mukauduttava uuteen normaaliin. Olemme joutuneet pakon edessä tekemään digiloikan nopeutetulla aikataululla ja varmasti monet uudet toimintatavat ovat tulleet jäädäkseen. Onneksi etätyövälineet ja yhteydenpidon eri muodot ovat sillä tasolla kuin ovat, kymmenen vuotta sitten tällainen kriisi olisi aiheuttanut kaaoksen.

Kaikki ei sentään ole muuttunut. Kyberrikollisuus ei ole ollut karanteenissa, eikä alamaissa vaan on entisestään vahvistunut. Voimakkaasti lisääntynyt etätyö ja etäyhteydenpito ovat lisänneet alttiutta joutua väärinkäytösten kohteeksi. Monella on kokemusta puheluista, joissa yritetään huijata käyttäjä asentamaan haittaohjelmia koneelleen. Vastaamon tietomurto on varoittava esimerkki siitä, mitä seurauksia puutteellisella tietosuojalla voi pahimmillaan olla. Erityisen haavoittuvassa asemassa olevien ihmisten tiedot ovat joutuneet vieraisiin käsiin ja ne voivat pulpahtaa esiin vielä vuosienkin päästä. Luottamus on kokenut kovan kolauksen.

Yhteiskunnan elintärkeät toiminnot eivät nekään ole suojassa rikollisilta, kuten on moneen kertaan saatu huomata. Palvelunestohyökkäykset ovat toistaiseksi aiheuttaneet rajallisesti vahinkoja, mutta suurimman uhan muodostavat vihamieliset lähestymisyritykset, joiden taustalla on luultavimmin valtiollisia resursseja.

Niiltä suojautuminen tai edes niiden havaitseminen voi olla hyvinkin työlästä.

Korona on vaikuttanut merkittävästi myös kansainväliseen politikkaan. Vielä vuosi sitten näytti todennäköiseltä, että Yhdysvaltojen istuva presidentti saisi jatkokauden virassaan. Surkeasti hoidettu pandemiatilanne muutti kuitenkin lopullisesti suunnan. Trump menetti lopulta presidentinviran lisäksi myös senaatin enemmistön, edustajainhuone oli menetetty jo aiemmin. Häviäminen on tehnyt kipeää kuten on nähty.

Tappiosta on monenlaisia seurauksia, ainakin ilmastopolitiikassa on jo tapahtunut täyskäännös. Moni salaliittoteoreetikko on myös hämmennyksen vallassa, koska ennustukset eivät tosielämässä käyneetkään toteen. Ei ihme, että erilaiset ääriliikkeet, salaliittointoilijat, ilmastodenialistit ja rokotevastaiset tahot etsivät turvaa toisistaan. Medialukutaidolle on nyt kysyntää.

Tammikuun puolivälissä lähetettiin lausuntokierrokselle ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta. Se sisältää toimeenpanosuunnitelman ja vaikuttavuusanalyysin ja se koskee vuosia 2021-2030. Kehittämisohjelman tavoitteena on synnyttää suomalainen kyberturvallisuuden ekosysteemi ja parantaa koko yhteiskunnan tieto- ja kyberturvallisuutta. Se pohjautuu hallitusohjelmassa asetettuihin tavoitteisiin.

On erinomainen asia, että kehittämisohjelmatyö on laitettu alulle. Kehittämisohjelman toimenpidesuunnitelmissa näyttää kuitenkin olevan paljon erilaisia linjauksia sen sijaan, että niissä kuvattaisiin konkreettisia etenemispolkuja kyberturvallisuusstrategian asettamiin tavoitteisiin. Toinen asia on rahoitus, joka ei esitetyllä tavalla näyttäisi riittävän uusien avauksien työstämiseen. Viestiupseeriyhdistyksen kannalta kiinnostava kysymys on vapaaehtoiskentän panoksen hyödyntäminen kehittämisohjelman toteuttamisessa. Keskustelu jatkuu.

VUY järjestää myöhemmin keväällä virtuaalitapahtuman kyberturvallisuuden kehittämisohjelman ympärille, siitä löytyy tarkempaa tietoa yhdistyksen sivuilta.

Lopuksi haluan kiittää kenraalimajuri Mikko Heiskasta vuosikymmenien mittaisesta merkittävästä työstä johtamisjärjestelmäalan suunnannäyttäjänä ja vahvasta tuesta vapaaehtoiskentän työlle. Samalla toivotan prikaatikenraali Jarmo Vähätiiton tervetulleeksi uusiin vaativiin tehtäviin. Onnea ja menestystä molemmille.

Viestiupseeriyhdistyksen puheenjohtaja
Juha Petäjäinen

TEKSTI: MIKKO HEISKANEN JA JARMO VÄHÄTIITTO
KUVAT: NUUTTI LIUKKO, RUOTUVÄKI JA JANNE JOKINEN

Johtamisjärjestelmäpäällikkö vaihtui

Kenraalimajuri Mikko Heiskanen luovutti johtamisjärjestelmäpäällikön ja kyberkomentajan tehtävät eversti Jarmo Vähätiitolle 17.2.2021. Varsinaisessa tehtävien luovutustilaisuudessa pidetyssä puheessaan Heiskanen nosti esiin kolme asiaa. Suorituskyvyn kehittämisen näkökulmasta ylitse muiden nousevat Naton operaatioverkkokonseptin (FMN) ja kyberpuolustuksen kehitystyöt. Suorituskyvyn käytön osalta hän korosti puolustusvoimien johtamisjärjestelmän kykyä elää ajassa, mikä näkyi siinä, kun Puolustusvoimat muun yhteiskunnan mukana siirtyi poikkeusoloihin viime keväänä. Johtamisjärjestelmäalan toimintamalli sai tulikasteensa ja osoittautui toimivaksi. Heiskasen toimintakaudella kehittämisen painopiste on ollut puolustushaarojen johtamisessa, mikä näkyy kaikissa puolustushaaroissa. Taktisen johtamisen valmius on rauhan ajan paras, vaikka yhteisen johtamisen kehitystäkään ei ole laiminlyöty.

Eversti Jarmo Vähätiitto korosti jatkuvuuden ja valmiuden merkitystä omalla alkavalla toimintakaudellaan. Hänen on helppo sitoutua jatkuvuuteen, koska apulaisosastopäällikön roolissa hän on johtanut johtamisen kehittämisohjelman suunnittelutyötä. Johtamisjärjestelmän valmius on koko puolustusvoimien toiminnan kannalta keskeistä, minkä vuoksi valmius on luonnollisesti johtamisjärjestelmäpäällikölle sydämen asia.

Virallisen vaihtotilaisuuden lisäksi päivän aikana pidettiin vuotuinen kausipuhuttelu koko johtamisjärjestelmäalan henkilöstölle ja tiedotustilaisuus sidosryhmille. Heiskanen korosti näissä yhdessä tekemistä ja Vähätiitto aikoi jatkaa samalla linjalla. Suomen puolustaminen edellyttää koko yhteiskunnan osallistumista. Verkostomallissa reservin, kumppaneiden, muiden viranomaisten ja yksityisen sektorin merkitys on keskeinen. Molemmat korostivat myös Puolustusvoimien ammattitaitoisen ja tehtäviinsä sitoutuneen henkilöstön omistautumista niin valmiuden ylläpidossa kuin kehittämistehtävissäkin.

Vanha ja uusi johtamisjärjestelmäpäällikkö.

Toimialan läksiäislahjana luovutettiin LV407. Luutnantti Heiskanen koulutti kyseisellä radiotyypillä sissiradisteja Jääkäriprikaatissa 1980-luvulla.

Pääesikunnan päällikkö kenraaliluutnantti Eero Pyötsiä luovutti oman muistoesineen.

Alexander Tunzelman von Adlerflugista alkanut ketju sai 25. seuraajan, kun Heiskasen kuva liitettiin joukon jatkeeksi.

Eversti Mika Seppä on Kainuun prikaatin Apulaiskomentaja

TEKSTI: MIKA SEPPÄ
KUVAT: PUOLUSTUSVOIMAT

Paikallispuolustajat jatkavat harjoittelua - väsymättä

Jos edelleen jatkuvasta ja erittäin valitettavasta COVID19 -pandemiasta on ollut jotain hyötyä, niin se on edelleen vahvistanut eri viranomaisten ja kolmannen sektorin toimijoiden yhteistä ymmärrystä varautumisen ja valmiuden tärkeydestä - olipa sitten syötteenä pandemia tai sotilaallinen uhka. Paikallispuolustusharjoituksia (PAPU) on toimeenpantu nykymuotoisena vuodesta 2017 ja ne ovat lisänneet merkittävästi eri viranomaisten yhteistoimintakykyä alueellisesti ja paikallisesti. Harjoitukset ovat olleet myös erinomaisia benchmarking -tapahtumia, jonka oppeja kukin viranomainen on voinut hyödyntää omassa toiminnassaan.

Vuoden 2021 PAPU harjoituksien suunnittelun käynnistämisessä ei ole tarvinnut motivoida ketään. COVID19 on virittänyt viranomaiskentän ja varautumisen ammattilaiset viimeistään nyt moodiin, jossa ei kysytä miksi, vaan kuinka korkealle. Myös Jääkäriprikaatin ja Kainuun prikaatin yhdessä johtamien, kevään ja syksyn PAPU 21 pohjoinen, harjoitusten tavoitteet on asetettu korkealle. Toimijoita on aiempaa useammasta puolustusvoimien yksiköstä, rajavartiolaitoksesta, poliisilaitoksesta, Tullista, pelastuslaitoksesta, sairaanhoitopiiristä tai SOTE -alueesta, hätäkeskuslaitoksesta, aluehallintovirastosta, ELY -keskuksesta, Oikeuslaitoksesta ja kuntasektorilta. Myös Huoltovarmuuskeskuksen ohjaama elinkeinoelämän varautumistoiminta on mukana ja ilmenee tilanteen mukaisena varautumistoimikunnan (ELVAR) kokouksena harjoituksen aikana. Vihdoinkin ajatus siitä, että puolustusvoimat tarjoaa paikallispuolustusharjoituksia monipuolisina kokonaisturvallisuuden harjoitusalustoina kantaa laajasti hedelmää.

Puolustusvoimat tuottaa harjoitukseen lähtökohtatilanteen ja tilanteen kehittymisen eri harjoituspäiville. Osallistuvista puolustusvoimien joukoista ja eri viranomaisista muodostettu peliorganisaatio maustaa päivittäisiä tapahtumia pelikuvauksilla, jotta halutut toiminnot saadaan liikkeelle. Peliorganisaatio kuvaa myös joukkoja ja osapuolia, joita toiminnan elävöittämiseksi tarvitaan. Valtionjohdon päätöksentekoa ja ohjausta pyritään kuvaamaan mahdollisimman totuudenmukaisesti. Näin toimintaan kytketään mukaan valtakunnallinen, alueellinen, paikallinen ja kenttätoiminnan taso mahdollisimman saumattomasti.

Johtamisen tuki mahdollistaa yhteisen tilannekuvan ja -ymmärryksen

Paikallispuolustuksen tehtävät ovat pysyneet samankaltaisina jo pitkään. Toimintaympäristön ja uhkien muutokset asettavat myös paikallispuolustajat uusien haasteiden eteen. Muutoksilla tai muutostekijöillä on aina ollut yksi yhteinen nimittäjä ja vaikutuksen kohde - johtaminen.

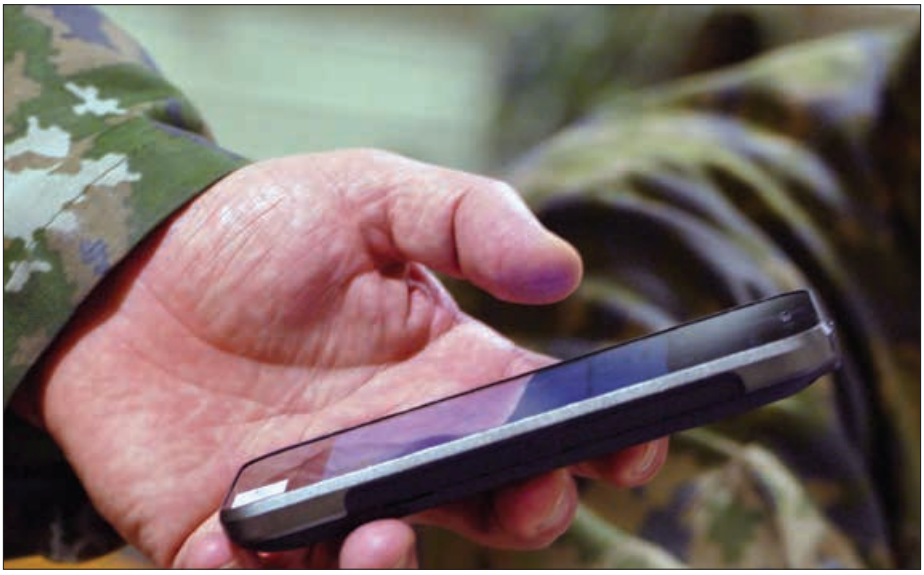
Tilannekuva ja sen tukemana muodostuva ymmärrys on johtamisen keskiössä. Ilman käsitystä vastuulla ja intressin piirissä olevasta alueesta ja sen tapahtumista, paikallispataljoonan komentajan tehtävä vaikeutuu. Pataljoona on saanut käyttöönsä lisää suorituskykyjä muun muassa alueensa valvontaan, mutta se on vahvistanut entisestään perinteistä haastettamme: miten sensorien tuottama tieto saadaan tarvitsijoille siten, että tiedon perusteella tehtävät päätökset ovat nopeampia ja oikeaan osuvampia, kuin potentiaalisen vastustajan?

Johtamisjärjestelmien kehittämisen konseptissa paikallispuolustuksen johtamisen tuen tekniset ratkaisut perustuvat niin sanottuihin arjen ratkaisuihin. Arjen ratkaisujen kehitystyössä tärkeässä roolissa ovat reserviläisemme, joilta odotetaan innovatiivisuutta ja innostunutta mukanaoloa. Miten reservimme potentiaali saataisiin hyödynnettyä?

Kainuun prikaatin vastuualueella toimii kaksi Maanpuolustuskoulutusyhdistyksen (MPK) maanpuolustuspiiriä. Yhdessä heidän kanssaan olemme pyrkineet rakentamaan toimintamallia, jossa MPK:n järjestämät sotilaallisia valmiuksia palvelevat koulutustapahtumat (SOTVA) toimisivat arjen ratkaisujen kehitysympäristöinä yhdessä puolustusvoimien vapaaehtoisten harjoitusten kanssa (PVVEH). Kehitysympäristöistä (tapah-

tumista) ratkaisut sitten siirretään tuotantoon vähintään paikallispataljoonan komentajan, mutta mieluiten alueemme johtamisjärjestelmäpäällikön päätöksellä joukon kertausharjoituksen (KH) päätteeksi. Toimintamalli tarvitsee onnistuakseen reserviläistemme merkittävän panoksen kaikissa vaiheissa. Kannustankin sinua, arvoisa reserviläisemme, tulemaan rohkeasti mukaan Viestiupseeriyhdistyksen, kiltasi tai MPK:n kautta.

Kokonaisturvallisuus on tila, jossa yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat ja riskit ovat hallittavissa. Paikallispuolustusharjoitukset ovat erinomaisia mahdollisuuksia kaikille viranomaisille ja kolmannen sektorin toimijoille testata ja kehittää yhteistä osaamistamme uhkien ja riskien hallinnassa ja erityisesti ennaltaehkäistä niitä ympäröivään yhteiskuntaan näkyvällä harjoittelemisella. Maanpuolustus on kaikkien yhteinen asia.



TEKSTI:MIKA STÅHLBERG

KUVA: F-SECURE

Kiristyksen uudet tuulet

Kirjoittaja on entinen viestiupseeri ja työskentelee F-Securella tittelillä Vice President, Detection & Response.

Kiristyshaittaohjelmat ovat viime vuosina saaneet huomattavaa näkyvyyttä ja aiheuttaneet konkreettisia vahinkoja organisaatoille. F-Securen tekemässä tutkimuksessa (F-Secure 2020 B2B Market Research, huhti-toukokuu 2020) kyberturvallisuudesta vastaavat johtajat Euroopassa ilmoittivat haittaohjelmat ja erityisesti kiristyshaittaohjelmat ykkösprioriteetikseen uhkilta suojautumisessa. Tämä oli tärkein prioriteetti kaikissa vertikaaleissa. Tosin maantieteellisesti eroja oli – pilvimyönteisissä pohjoismaissa, pilvipalveluiden suojaaminen koettiin vieläkin tärkeämmäksi.

Ensimmäinen kiristyshaittaohjelma on jo vuodelta 1989, mutta todellisen renessanssin ne kokivat noin vuoden 2013 tietämillä ja silloin myös useimmat Internet-käyttäjät tutustuivat termiin ja uhkaan. Tätä kautta useimmille kiristyshaittaohjelma tarkoittaa ohjelmaa, joka asentuu koneeseen ja asennuttuaan salaa tärkeät tiedostosi ja vaatii pienehköä lunnassummaa bitcoineina, jotta saat tiedostosi takaisin. Usein tällaista haittaohjelmaa kutsutaan lunnastroijalaiseksi. Ennen vuotta 2013 oltiin nähty jo monta evoluutioaskelta, eikä tahti ole hidastunut viime vuosinakaan, joten tämä kuva kiristyshaittaohjelmien muodostamasta uhkasta on liian suppea eikä pääskenaario, johon etenkään organisaatioiden tänä päivänä kannattaa erityisesti varautua.

Hyökkäyksen vaiheet

Kyberhyökkäykset jaetaan tyypillisesti tusinaan eri vaiheita. Tyypillisemmin käytetyt mallit ovat Lockheed Martinin Cyber Kill Chain ja Mitren Att&ck. Jos halutaan yksinkertaistaa näitä malleja entisestään voidaan ajatella, että kaikki hyökkäykset jakautuvat 1) sisään pääsemiseen ja 2) rahastamiseen. Nämä ovat usein täysin erilliset vaiheet ja eri keinoja sisään pääsemiseen voidaan käyttää hyvin erilaisissa rahastus- tai muissa hyöty-/haittatarkoituksissa.

Sisään pääsemisen tyypillisin keino on käyttäjän huiputtaminen klikkaamaan jotain sähköpostin liitetiedostoa tai -linkkiä ja sitä kautta hyväksymään koodin suoritus laitteellaan. Toisessa erittäin yleisessä hyökkäystavassa käyttäjä huiputetaan luovuttamaan salasanansa erimerkiksi väärennetyn kirjautumissivun avulla. Tätä salasanaa hyökkääjä sitten hyödyntää esimerkiksi kirjautumalla käyttäjänä yrityksen Remote Desktop (RDP)-palvelimelle.

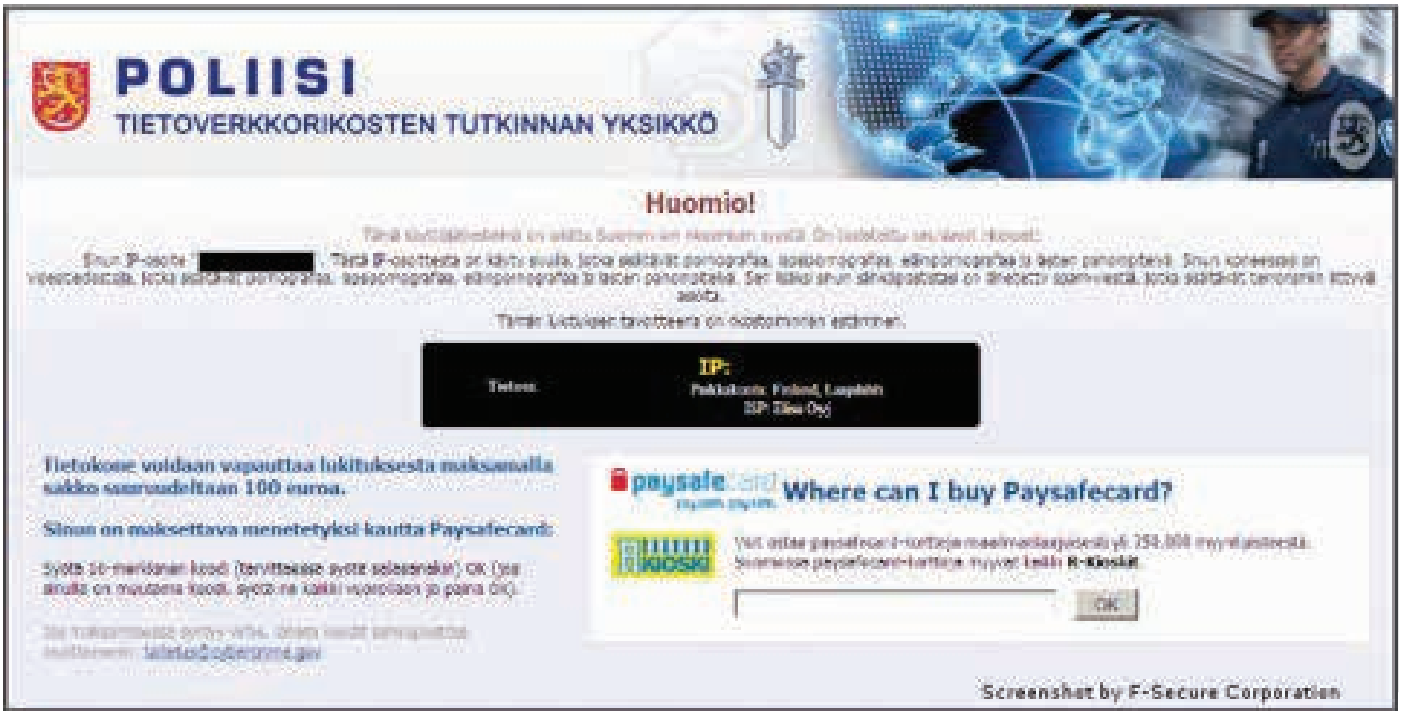
Muita yleisiä sisään pääsemisen keinoja on salasanojen arvaaminen, ohjelmistohaavoittuvuuksien hyväksikäyttö ja ns. Supply Chain (”Huoltoketju”) hyökkäykset. Supply Chain-hyökkäykset, joissa softatoimittajan kautta kohteelle päästään syöttämään haitallista koodia automaattisten päivitysten kautta, ovat saavuttaneet suurta huomiota etenkin 2017 Notpetya ja 2020 Solar Winds hyökkäysten myötä. Niiden erityisenä piirteenä on se, että uhri ei tavallaan ole tehnyt mitään virhettä, vaan toiminut juuri oikein asentaessaan tuoreimmat päivitykset heti käyttöön.

Rahastaminen

Kaikkia edellä kuvattuja tunkeutumisen keinoja voidaan käyttää myös kiristyshaittaohjelmia hyödyntävissä hyökkäyksissä. Kiristäminen on keino rahastaa. Se ei kuitenkaan ole läheskään ainoa keino, jolla kyberrikolliset ovat onnistuneet muuttamaan pääsyn tietojärjestelmiin rahaksi. Muita keinoja ovat spämmi, palveluestopalveluiden myyminen, pääsyn myyminen muille, pankkitunnusten varastaminen, mainoshuijaukset (click fraud), salaisuuksien myyminen ja moni muu.

Kiristämistäkin on monenlaista. Tiedostojen salaajat ns. lunnastroijalaiset ovat vain yksi kiristyshaittaohjelmien muoto, mutta niistä kaikki aikoinaan lähti. AIDS troijalainen vuodelta 1989 lähetettiin lerpulla kirjepostissa ja vaati lunnaana rahan maksamista Panamalaiseen postilokeroon. Siinä missä Internet mahdollisti helpon haittaohjelmien jakelun, on hyvin suurta kehitystä tapahtunut myös kiristysmaksuliikenteen osalta. Enää ei shekkejä postiteta Panamaan.

Noin 2012 suurta muotia olivat koneen pääsyn lukitsevat ”poliisitroijalaiset” (esim. Reveton) ja joitain vuosia aikaisemmin käyttäjää pelottelevat ohjelmat (esim. Winfixer). Nämä ilmiöt olivat varsin laajoja, mutta niiden Akilleen kanta-



Paysafecard.

päänä oli maksuliikenne. Pelotteluohjelmat olivat hyödyttömiä ja/tai valheellisia ohjelmistoja, joita markkinoitiin harhauttavilla taktiikoilla. Maksuvälineenä oli yleensä luottokortti. Poliisitroijalaisten kohdalla hyökkääjä yleensä väitti olevansa paikallinen poliisi, uhrin syyllistyneen johonkin rikokseen ja salaamatta tietoja lukitsi pääsyn koneelle kunnes ”sakko” oli maksettu. Näissä toki rikoskynnys ylittyi selvästi ja siksi luottokorttimaksu ei enää ollut hyökkääjille toimiva keino, joten yleinen maksuväline esim. Suomessa oli Paysafecard. Tällaisten maksuvälineiden käyttäminen oli hyökkääjille työlästä ja kiinnijäämisen riski rahaa seuraamalla on ilmeinen.

Varsinaisen mullistuksen kiristyshaittaohjelmissa toi bitcoin, joka lähti liikkeelle 2009. Bitcoin mahdollisti varsin anonyymin ja uhreille suhteellisen helposti käytettävän maksuliikenteen. Samalla kiristyshaittaohjelmat palasivat takaisin alkulähteilleen ja lunnastroijalaisista tuli yleisin vitsaus, jonka airueena toimi CryptoLocker vuonna 2013. Esimerkiksi Gpcode oli modernien lunnastroijalaisten muotoinen jo vuonna 2005, mutta ilman bitcoinin käyttöä. Tyypillisesti tällaiset lunnastroijalaiset salaavat julkisen avaimen salauksella (esim. RSA) käyttäjän tiedostohakemistosta kaikki dokumentit ja valokuvat ja näyttävät käyttäjälle lunnaslapun, jossa vaadittiin maksua bitcoinilla ja maksun saatuaan hyökkääjä lupaa toimittaa palautukseen vaaditun salasanan uhrille.

Iso osa lunnastroijalaisista oikeasti palauttaa purkusalasanan, jos lunnas maksetaan. Jos maksamalla ei saa dataansa takaisin, hajoaa hyökkääjien liiketoimintamalli heti alkuunsa: Kukaan ei maksa, jos eivät usko järkevään mahdollisuuteen, että maksaminen auttaa. Joillakin pelottelu- ja kiristyshyökkäyksillä on ollut erillinen tekninen tuki, jolla hyökkääjä varmistaa, että uhrit osaavat maksaa lunnaan ja palauttaa tietonsa. Kun palauttaminen toimii, sana siitäkin leviää ja lunnaita maksetaan entistä todennäköisemmin.

Viime vuosina painopiste on siirtynyt suuren volyymin kuluttajahyökkäysten lisäksi enemmän ja enemmän yrityksiin ja muihin organisaatioihin kohdistettuihin hyökkäyksiin. Yrityksiin kohdistuvat hyökkäykset muistuttavat usein kokonaisvaltaisuudessaan enemmän edistyneitä kohdistettuja hyökkäyksiä kuin tyypillistä virustartuntaa. Keskustelua lunnastroijalaisilta suojautumisessa on organisaatioiden tietoturvassa viime vuodet leimannut vahva varmuuskopioinnin merkityksen korostaminen. Ajatuksena on, että jos tiedoista on varmuuskopio voidaan ympäristöt nopeasti ”rakentaa” uudestaan, eikä lunnaita tarvitse maksaa. Lienee luonnollista, että hyökkääjät joutuivat muuttamaan malliaan vähentääkseen varmuuskopioimisen heidän liiketoiminnalleen aiheuttamaa uhkaa. Vuodesta 2020 alkaen on yleistynyt yrityksiin kohdistuvien lunnastroijalaisten muoto, joissa tiedostojen salaamisen lisäksi, ainakin osa niistä lähetetään hyökkääjän palvelimelle. Jos lunnasta ei makseta ajoissa, nämä tiedostot ilmestyvät julkisessa Internetissä olevalle ”wall of shame”-palvelimelle. Tällaisia perheitä ovat mm. Maze, Sodinokibi ja Ragnar Locker.

Kannattaako lunnaat maksaa?

Yleinen neuvo lunnaiden suhteen tuntuu olevan: Älä maksa. Kuitenkin jopa USA:ssa poliisilaitosten tiedetään maksaneen lunnaat ja siihen on syynsä: Maksaminen on usein halvin ja nopein tapa päästä eroon ongelmasta. Norsk Hydro kärsi kuuluisassa 2019 kohtaamisessaan LockerGoga lunnastroijalaisen kanssa, Microsoftin julkaisemien lukujen mukaan, arviolta 71 miljoonan dollarin kokonaisvahingot jätettyään lunnaat maksamatta. Toisaalta myös lunnaita maksavat organisaatiot kärsivät vahinkoja itse lunnassumman lisäksi ja niidenkin pitää usein rakentaa infrastruktuurinsa uudelleen varmistaakseen, ettei hyökkääjä pääse takaisin.

Lunnaat maksamalla yksilö tai yksittäinen organisaatio saattaa päästä helpolla, mutta koko yhteiskunnan kannalta maksaminen on vahingollista. Hyökkääjät saavat entistä enemmän motivaatiota

hyökkäyksilleen ja rahaa operaatioidensa tehostamiseen. Organisaatioille maksaminen on riski myös sikäli, että maksaja saatetaan nähdä ”helppona maalina, joka heti maksaa” ja aiheuttaa hyökkäyksiä jatkossa enemmän kuin sellaisille organisaatioille, joille tulee kitsaan tai fanaatikon maine. Samasta syystä esimerkiksi monilla valtioilla on ollut hyvin julkinen ”emme neuvottele terroristien kanssa” politiikka – vaikka käytännössä kaikki valtiot neuvottelevat joidenkin terroristeiksi määrittämiensä tahojen kanssa julkisuudelta piilossa, kuten Pohjois-Irlannin ja Espanja-ETA tulitauot osoittavat.

Lunnaiden maksamista ovat saattaneet tehdä yleisemmiksi myös jotkin kybervakuutukset, jotka kattavat tietyt lunnaskulut. On myös olemassa monia yrityksiä, jotka tarjoavat ”pankkivankineuvottelu”-palveluita lunnastroijalaisia varten. On myös epäilty, että hyökkääjät yrittävät löytää kohteita, joilla on tällainen vakuutus, jotta maksuherkkyys olisi suurempi.

Aina lunnasta ei tarvitse maksaa saadakseen tietonsa takaisin. Salaus on vaikea toteuttaa oikein. Usein luotettaviksi koetuista salaustuotteistakin löytyy isoja puutteita. Vaikka salausalgoritmit ovat kaikkien saatavissa, niiden käyttöönotto on usein haittaohjelmissa tehty amatöörimäisesti. Alkuaikoina hyökkääjät käyttivät usein symmetrisiä salausohjelmia, jolloin salausavain oli haittaohjelmassa sisällä ja sieltä kaivettavissa. Viimeiset viisitoista vuotta lähes aina hyökkäyksissä on käytetty julkisen avaimen salausta ja vahvoja algoritmeja, mutta välillä puutteellisesti. Näin ollen joihinkin lunnastroijalaisiin ja muihin kiristyshaittaohjelmiin löytyy työkaluja, joiden avulla salaus voidaan purkaa ilman lunnaiden maksamista. Europol on yrityskumppaneidensa kanssa koonnut näitä työkaluja ”No more ransom!”-palveluunsa.

Kuluttajat ja organisaatiot

Kuluttajat joutuvat yleensä uhreiksi kohdistamattomille ja automatisoiduille kiristyshaittaohjelmille. Nämä esimerkiksi saapuvat sähköpostin liitteenä ja salaavat kaikki dokumentit ja valokuvat pyytäen esim. 200 euron maksua bitcoinilla, jos käyttäjä erehtyy ajamaan liitetiedoston. Kuluttajalle summa saattaa olla suuri, mutta toisaalta jos kaikki muistosi ovat muuten mennyttä, on moni taipuvainen miettimään lunnaan maksamista.

Organisaatioissakin on töissä kuluttajia, joten yksilöiden kohtaamat uhkat saattavat aiheuttaa ongelmia tietohallinnolle. Jotkin haitakkeet myös kykenevät leviämään automaattisesti sisäverkossa, joten ongelma saattaa olla varsin iso. Esimerkkejä tällaisista lunnastroijalaisista ovat Yhdistyneiden kuningaskuntien terveydenhuollon (NHS) ongelmat WannaCry-haittaohjelman kanssa keväällä 2017 ja Maersk-yhtiön haasteet NotPetya-hyökkäyksessä myöhemmin samana vuonna. NotPetya ei tosin ollut aito lunnastroijalainen, sillä hyökkääjällä ei ilmeisestikään ollut edes tarkoitusta koskaan purkaa salausta.

Isoimmat ongelmat organisaatioille aiheuttavat kuitenkin toisenlaiset hyökkäykset, joista mm. edellä mainittu Maze-ryhmittymä on tunnettu. Näissä hyökkäyksissä käytetyt tekniikat, taktiikat ja menettelytavat ovat monipuolisempia – enemmän käsityönä tehtyä ”hakkerointia” kuin automaattisia haittaohjelmia muistuttavia – ja hyökkääjät määrätietoisempia. Usein kyseessä ovat kohdistetut hyökkäykset, joissa hyökkääjä pyrkii pääsemään sisään maksukykyisiin ja oletettavasti maksuhaluisiin organisaatioihin. Hyökkääjä erimerkiksi tunkeutuu yhdelle työasemalle lähettämällä työntekijälle sähköpostin liitteenä takaportin. Tätä takaporttia hyväksikäyttäen hyökkääjä levittäytyy laajemmalle organisaatiossa ja hankkii pääsyn isoon osaan tietojärjestelmistä. Näihin tietojärjestelmiin sitten asennetaan varsinainen salaava työkalu/troijalainen, joka käynnistetään jollakin sopivalla ajanhetkellä: Esimerkiksi silloin kun hyökkääjä pelkää menneensä liian pitkälle ja paljastuvansa pian.

Organisaatioihin kohdistuvissa kiristystapauksissa hyökkääjät eivät tyydy sadan euron lunnaisiin vaan summat saattavat liikkua miljoonissa. Tammikuussa 2021 AdvIntel ja HYAS julkaisivat tutkimuksen, jossa he olivat seuranneet yrityksiin kohdistettuja lunnastrojalaishyökkäyksiä tehtailevan Ryuk-ryhmän bitcoin-osoitteita ja päättelivät Ryukin muuttaneen n. 150 miljoonan dollarin arvosta bitcoineja perinteisemmiksi valuutoiksi. Tyypillisimmät Ryukin keräämät yksittäiset lunnaat ovat satoja tuhansia dollareita.

Miten suojautua?

Kiristyshaittaohjelmilta suojautuminen ei poikkea erityisen paljon muilta tietoturvauhkilta suojautumisesta.

Tietoturvallisuus on klassisen määritelmän mukaan jaettu kolmeen kontrolliryhmään: Estäviin, havaitseviin ja palauttaviin kontrolleihin. Mikään näistä kontrolleista ei koskaan yksinään riitä, vaan tarvitaan tasapaino näiden välillä. Sopiva tasapaino ja investointitasot riippuvat uhkista ja riskinottokyvystä.

Estäminen ei koskaan ole satavarmaa, mutta se ei onnistuessaan aiheuta jatkotoimenpiteitä kuten GDPR-ilmoituksia, hankalia keskusteluja lehdistön edustajien ja asiakkaiden kanssa sekä järjestelmien uudelleenasennuksia, joten sitä ei kannata väheksyä. Estäviä kontrolleja ovat mm. pääsynhallinta, vahva tunnistautuminen, antivirus, palomuurit, yms. Koska sähköposti on tänä päivänä hyökkäyksen ensimmäinen askel yli puolessa kiristyshaittaohjelmatapauksista, kannattaa sähköpostin turvaan, turvalliseen käyttöön ja työasemien suojaukseen liitetiedostoja ja webbilinkkejä vastaan panostaa. Avointen RDP (Windowsin Remote Desktop) porttien käyttö on yksittäisenä vektorina myös ollut merkittävä, ja koska ei pitäisi olla mitään syytä pitää RDP-portteja avoimina suoraan julkisessa Internetissä, kannattaa myös varmistaa, että RDP on suojattu.

Havaitsevat kontrollit tunnistavat, kun estäminen epäonnistui. Kiristyshaittaohjelmien torjunnassa on tärkeää virittää kontrollit havaitsemaan hyökkäyksen vaiheet ennen varsinaista tiedostojen salaamista tai kopiointia. Havaitsevia kontrolleja ovat mm. lokien seuranta ja Endpoint Detection & Response (EDR)-tuotteet. Siinä missä tyypillinen kuluttajakäyttäjään kohdistettu lunnastroijalainen yleensä salaa koneen tiedostot lähes välittömästi, saattaa yritykseen kohdistuvan hyökkäyksen valmistelu ja siihen liittyvä poikittainen siirtyminen organisaatiossa kestää päiviä tai jopa kuukausia, joten aikaa vastata ajoissa usein jää, kunhan hyökkäys havaitaan ajoissa.

Palauttavat kontrollit tarkoittavat fyysisen maailman palokuntaa vastaavia järjestelyjä. Mitä tehdään, jos hyökkäys havaitaan? Kiristyshaittaohjelmien osal-

ta kannattaa valmistella palauttavat kontrollit sekä tilanteeseen, jossa hyökkäys havaitaan ennen varsinaista aktivoitumista ja tilanteeseen, jossa tiedot on salattu ja/tai hyökkääjän hallussa. Palauttaviin kontrolleihin lukeutuvat mm. varmuuskopiointijärjestelyt ja tietoturvayritysten tarjoamat incident response-palvelut. Myös pilvipalvelut voivat mm. versionhallinnan ja SaaS-mallin kautta auttaa vähentämään palautumisen haasteita. Varmuuskopiointi toki kannattaa ja palautumista kannattaa harjoitella. Varastettujen tietojen vuotamisella kiristämistä varmuuskopiointi ei estä ja hyökkääjän pääsy varmuuskopioihin käsiksi pitää estää. Jos hyökkäys on havaittu ennen varsinaisen kiristystoiminnan aloittamista, on tärkeää tehdä vaste tavalla, jossa hyökkääjä ei ehdi aktivoimaan sitä, eikä siirtämään herkkiä tietoja ulos organisaatiosta.

Evoluutio jatkuu

Lunnashyökkäykset ovat vuodesta 1989 kehittyneet usean välivaiheen kautta. Muutokset teknologiassa, yhteiskunnassa ja suojauskeinoissa synnyttävät uusia tapoja hyökätä. Kyseessä on jatkuva asevarustelun kierre. Maailma on myös kyberuhkien osalta osittain syklinen: Välillä hyökkäystekniikka poistuu, koska se ei ole enää tehokas, mutta ympäristön muutosten myötä tai muiden hyökkäysten heikentyessä se saattaa taas kohta olla, ehkä jonkin mutaation kautta, tehokkain. Tämä on nähty esimerkiksi makrovirusten, kiristyshaittaohjelmien ja haitallisten skriptien tullessa uudelleen suosioon.

Kiristyshyökkäykset juuri nyt kehittyvät, vuonna 2020 julki tulleen, Vastaamo-murronkin (jossa ei tosin ollut kyse lunnastroijalaisesta) osoittamalla tiellä. Ei niin, että välttämättä juuri terveystiedot olisivat kohteena, mutta yritysten ja yksilöiden oppiessa varmuuskopioimaan arvokkaimman tietonsa, käyttämään pilvipalveluita ja palauttamaan järjestelmänsä nopeammin alkutilaan, täytyy hyökkääjien keksiä uusia keinoja kannustaa uhreja maksamaan. On todennäköistä, että lunnastroijalaishyökkäykset enenevässä määrin tiedon salaamisen lisäksi myös kopioivat ainakin osan siitä hyökkääjälle julkistamista odottamaan. Jokaisella yksilöllä ja organisaatiolla on, jos ei varsinaisia synkkiä salaisuuksia, niin kuitenkin sähköposteja, taloustietoja, lääkärintodistuksia, valokuvia, yms. , joita he eivät haluaisi kaiken maailman nähtäväksi – ja myös GDPR vähentää yritysten halua nähdä sisäiset tietonsa julkisessa jakelussa. Eli, jokaista on mahdollista kiristää. Ja lunnaat maksamalla kierre jatkuu.

Kirjoittaja on johtava järjestelmäarkkitehti Fujitsu Finland Oy:ssä. Hänellä on pitkä kokemus it-alalta, joista viimeiset 14 vuotta pääasiassa turvallisuus- ja puolustussektorilla, ja jossa hänen yksi roolinsa on CDS-järjestelmien tuotepäällikkö.

TEKSTI JA KUVA: TIMO SEPPÄLÄ

Yksi työasema riittää - haavetta vai todellisuutta

Tapahtuu suuronnettomuus tai terrori-isku. Hetken kuluttua sosiaalinen media tulvii siihen liittyviä videoita ja uutisia. V iranomaistoiminta käynnistyy nopeasti. Kenttäjohtajalla on käytössään korkean tietoturvallisuuden työasema operatiiviseen toimintaan, mutta hänen pitäisi nähdä tapahtumasta otettuja silminnäkijöiden youtube-videoita ja liittää tärkeimmät tilannekuvaan. Hän joutuu katsomaan ne joko toiselta työasemalta tai mahdollisesti omalta puhelimeltaan. Videoiden linkit lähetetään sähköpostilla tai pikaviestimellä operaatiokeskukseen, jossa sitä analysoidaan ensin ei-operatiivisella työasemalla. Samalla käynnistyy manuaalinen tiedonsiirto- ja haittaohjelmien tarkistusprosessi turvalliselle operatiiviselle puolelle.

Moni puolustus- ja turvallisuussektorilla toimiva viranomainen kohtaa työssään tilanteita, jossa usean eri tietoturvaluokan päätelaitteen välillä pitää välittää tietoa. Tiedon selaaminen ja lataaminen niiden välillä on usein monimutkaista ja vaatii hidasta manuaalisesti tehtävää työtä.

Arkaluonteisen informaation tietoturva aiheuttaa lukuisia käytännön pulmatilanteita. Suomessa viranomaisten ohjeet ja määräykset luovat perusteet turvalliselle tietojen käsittelylle. KATAKRI- ja VAHTI-ohjeissa määritetään tietoturvavaatimukset työskentelyvälineille ja paikoille, joissa tietoa voidaan käsitellä.

Yksi haaste on ollut esimerkiksi julkisesta verkosta ladatun tiedon siirtäminen turvalliselle puolelle. Tällöin tieto on haettu ns. internet- tai muulla alemman tason työasemalla, jonka jälkeen se on siirretty erillisten haittaohjelmatarkistusten – ja prosessien kautta korkeamman tietoturvaluokan välineisiin.

Tiedon suorakäyttö korkealta tietoturvatasolta julkiverkkoihin on kuitenkin mahdollista. Esimerkiksi Iso-Britannian turvallisuusviranomaisilla on käytössään ratkaisu, jolla korkean tietoturvallisuuden työasemalla pystyy selaamaan nettisivuja, katsomaan videoita ja siirtämään dokumentteja julkisen verkon ympäristöstä salaiseksi luokiteltuun ympäristöön.

Security Domain

Tietoturvavyöhyke tai -alue on tietojärjestelmien muodostama kokonaisuus eli ympäristö, joka on luotu tietoturvasäännöstöjen määrittämien ohjeiden ja luokitusten mukaan. Ympäristössä tieto tallennetaan ja käsitellään niin, että salassa pidettävä tieto pysyy suojattuna. Tahaton tai tahallinen tiedon väärinkäyttö tai siirtäminen voidaan estää. Näistä tietoturva-alueista käytetään useasti englanninkielistä nimitystä enclave.

Suomessa viranomaisten luokiteltuja ympäristöjä on kolme tasoa: TL II – SALAINEN, TL III – LUOTTAMUKSELLINEN ja TL IV – KÄYTTÖ RAJOITETTU. Ne on tehty yleensä itsenäisiksi, eristetyiksi tietoturvavyöhykkeiksi. TL II -taso on niistä suojatuin ja eristetyin.

Cross Domain Solutions (CDS) -mallit ja järjestelmät on kehitetty eri turvallisuusvyöhykkeiden välisten tiedon saanti- ja siirtotarpeiden ratkaisemiseen.

Cross Domain Solutions

CDS-järjestelmät tarkoittavat tietoturvallista, tiedon, järjestelmien ja prosessien kautta tapahtuvaa tiedon saantia, siirtoa ja käsittelyä eri tietoturvatasojen ja/tai organisaatioiden välillä.

CDS-käyttötapauksia on useita. Kuvaan tässä jutussa kahden CDS-tyypin: Access CDS browse down (selaus alemmalle tasolle) ja Transfer CDS uni-directional (yhdensuuntainen tiedonsiirto) käyttötapaustyyppejä varten suunniteltuja tuotteita ja ratkaisuja.

Selaus alemmalle tasolle tarkoittaa esimerkiksi nettisivun selaamista ylemmältä tasolta turvallisen puolen työskentelyvälineellä. Yhdensuuntainen tiedonsiirto on tiedon siirtoa alemmalta tasolta ylemmälle. Kahdensuuntainen, bi-directional, tai tiedon siirto alemmalle tasolle, vaativat lisäksi vähintään tiedon tietoturvaluokittelua ja sidontaa sekä niitä tukevia Gateway-toteutuksia.

Selaus alemmalle tasolle

CDS-tyypin toteutus mahdollistaa alemman tietoturvaluokan tietojen selaamisen ja käsittelyn ylemmältä tasolta. Tätä tyyppiä voi käyttää myös saman tietotur-

valuokan järjestelmiin, jos ne ovat esimerkiksi eri organisaatioiden palveluja.

Sen suurin hyöty on se, että päätelaitteiden lukumäärää voidaan vähentää, koska esim. netin selaaminen mahdollistetaan.

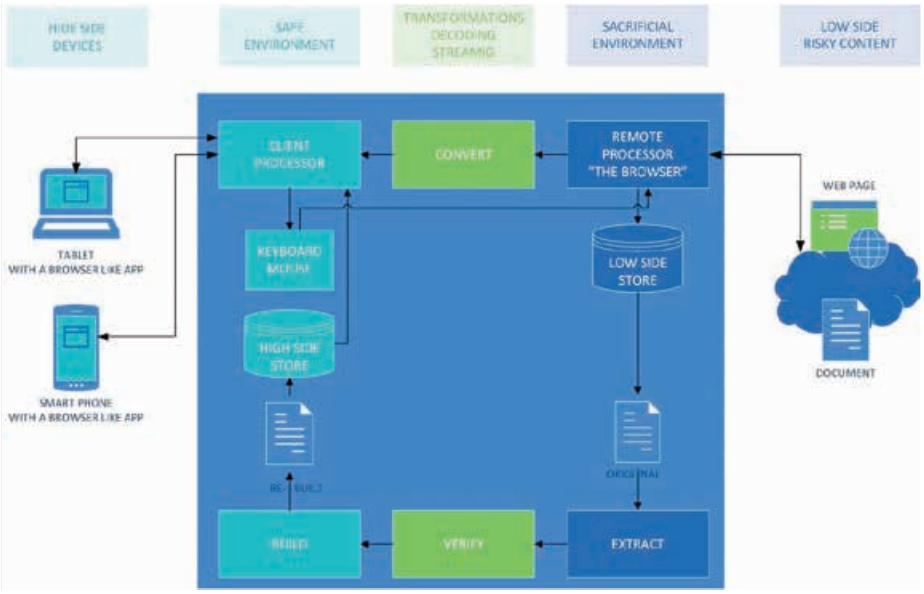
Yhdensuuntainen tiedonsiirto

Ratkaisu koostuu yhdensuuntaisesta datavirtauksen ohjauksesta, jota ympäröivät erikoistuneet tietojenkäsittelykomponentit.

Manuaaliset haittaohjelmistojen tarkistusprosessit voidaan jättää pois eikä tietoa ei tarvitse kirjoittaa uudestaan. Siirtynyt sisältö on myös puhdasta.

Tekninen integroitu ratkaisu

Viereisessä kuvassa.



Cross Domain Solutions periaatekuva.

Turvallinen selausteknologia

Turvallista selausta varten tehty erillinen laitteisto, jossa on jokaiselle käyttäjälle varattu kaksi prosessoria, jotka muodostavat noodin. Selaus perustuu eristämiseen (isolaatioon) ja eheyden varmistamiseen (verification), jossa uhrautuvan, alemman puolen prosessori suorittaa sivun, toimii käytännössä selaimena ja tekee sivusta tietovirran, joka dekoodataan Puhtaalle, ylemmälle puolelle saatu tietovirta prosessoidaan puhtaan puolen prosessorilla ja kompressoidaan laitteistopohjaisella, sisäänrakennetulla videopakkauksella. Se lähetetään työasemassa tai esimerkiksi Android-laitteessa olevaan selainsovellukseen. Sama toimenpide tapahtuu myös äänelle.

Paluukanava, eli hiiren ja näppäimistön painallus, on yksisuuntainen ja eristetty käytettävään laitteistoon. Kun käyttäjän istunto päättyy, prosessin noodi pyyhitään laitteistosta.

Myös videoita voi toistaa vastaavasti. Video tuodaan käyttäjälle turvallisella pikselivirralla, joka on raakapakattu bittikartta. Vaikka alemman puoleinen siru vaarantuisi, suoratoistoon päätyy vain video siitä, mitä alemman puolen siru näkee. Tällöin virukset tai haittaohjelmat eivät voi siirtyä alemmalta puolelta ylemmälle.

Jos selaimessa olisi tietoturva-aukko, isolaation ansiosta kyseinen selausprosessi pyörii vain alemman, uhrautuvan puolen sirulla eikä ylempi, puhdas puoli saastu. Työasemassa oleva selainta muistuttava sovellus vastaanottaa vain data- tai videovirtaa, eikä siis esimerkiksi suoritettavaa HTML5-koodia.

Jos uhrautuva puolen noodi saastuu, on yhden käyttäjän sivun tai kuvan laatu on huono.

Turvallinen latausteknologia ja –prosessi

Lataustuotteiden avulla tiedostoja voi ladata turvallisesti selauslaitteiston alemman puolen kautta ylemmälle tasolle, aina työasemaan saakka. Tätä varten selauslaitteistoon on tehty integraatio-ohjelmisto ja työasemaan asennettava integraatiokirjasto, jotka osallistuvat tiedostojen siirto- ja puhdistusprosessiin (extract-verify-build, EVB).

Kun käyttäjä selaa turvallisella selauksella esimerkiksi nettisivuja ja käynnistää latauksen (download), se onnistuu samoin kuin normaalilla selaimella. Alemman puolen vastaanottava tiedonsiirtopalvelin (receiver) vastaanottaa tiedostoja laajennuksen avulla selauslaitteesta ja käynnistää extract-vaiheen prosessista. Kyseinen palvelin purkaa informaation tiedostosta ja muuntaa sen sisäiseen transformaatiorakenteeseen. Jos tiedostoon olisi piilotettu haittaohjelma, se putoaa pois, koska odottamattomasta tiedoston sisällön rakenteesta ei haeta informaatiota. Tässä vaiheessa myös poistetaan tietorakenteissa olevat mahdolliset haittaohjelmat jäsentämällä rakenteet alimmalle tasolle ja ottamalla siirrettäväksi vain tiedoston uudelleenrakentamiseen tarvittava informaatio.

Transformoitu tiedosto välitetään tarkistuslaitteistolle (verifier), jossa se varmennetaan ennen siirtämistä ylemmän tietoturvaluokan välittävälle palvelimelle (transmitter). Verify-vaiheessa tarkistetaan, että tiedoston sisäinen esitys on oikein jäsennelty ja että siirtämiseen käytettyä protokollaa noudatetaan. Tarkistuslaitteisto sisältää elektroniset diodit tietovirran ohjaamiseksi. Logiikkaykksikkö tekee itsenäisen vahvistusvaiheen, joka estää hyökkääjiä kohdistamasta haavoittuvuuksia mm. verkkoliitännän laiteohjelmistoihin, protokollapinoon tai sisältöön.

Välittävä palvelin rakentaa build-vaiheessa esimerkiksi word- tai pdf-tiedoston uudelleen niiden määritysten(skeeman) mukaan transformoidusta tietovirrasta, ja siirtää tiedonvaihtopalvelimen kautta uudelleenrakennetun tiedoston käyttäjän tallennettavaksi työasemaan asennetun integraatiokirjaston avulla.

Kaikkia alemman puolen tiedostoja pi-

detään ”saastuneina” eikä puhdaskaan tiedosto siirry ylemmälle puolelle ilman EVB-prosessia. Tuettuja tiedostomuotoja on kymmeniä, mukaan lukien yleisimmät kuvatiedostomuodot. Latausteknologian kautta voidaan välittää myös XML- ja json-stuktuureja, kun niille on tehty skeema. Tuntematon tiedostomuoto, jolla ei ole aktiivista käsittelijää, ei siirry. Siitä saadaan ilmoitus käyttäjälle kuten myös niissä tapauksissa, joissa tiedosto oli niin saastunut, että sitä ei voitu siirtää prosessin läpi.

Helppokäyttöinen ja turvallinen – ratkaistu dilemma

Korkeammalle tietoturvatasolle tietoa voidaan siirtää ilman, että tieto on luokiteltua, mikä tekee niiden käyttöönotosta yksinkertaisempaa. Tiedoston lataus alemmalta tasolta voidaan käynnistää vastaavasti kuten normaalilla selaimella, joten käyttö on helppoa, vaikka tekniikka on hienostunutta.

CDS päätelaitteessa tarjoaa helppokäyttöisen ja korkean tietoturvan ratkaisun loppukäyttäjille ilman erillistä koulutustarvetta. Ainoa osaamisvaatimus on selaimen käyttö. Työasemaan tai älypuhelimeen asennetaan oma selain, mutta ilman selaimen haavoittuvuusrajapintaa, koska varsinainen selainprosessi pyörii uhrautuvassa, alemman puolen prosessorissa. Jokaiselle käyttäjälle on varattu kaksi prosessoria, joten tehokkuus pyysyy vakiona käytön lisääntymisestä huolimatta. Prosessoreina käytetään mobiilipuhelimista tuttuja siruja. Vaikka selauslaitteisto sisältää satoja prosessoreja, on sen rakentaminen kustannustehokasta.

Transformaatioiden, eristämisen, siirtorakenteiden ja tarvittavien kontrollien käyttö teknisessä ratkaisussa huomioi myös nollapäivähaavoittuvuudet. Nollapäivähaavoittuvuus tarkoittaa tietoturva-aukkoa, jolle tuotteen valmistaja ei ole tehnyt korjausta. Integroidun CDS:n ratkaisun turvallisuus on rauta-, ohjelmisto- ja arkkitehtuuripohjaista, eikä niitä ole mahdollista ohittaa.

Tuloksena on ratkaistu dilemma.

Yksi työasema riittää

Suurin hyöty CDS:n käytöstä saadaan TL II- ja TL III-tasoilla, koska niissä eri turvallisuusalueiden tiedon selaamisella, käytölle ja lataamiselle on korkeat vaatimukset, jotta salassa pidettävä tieto pysyy suojattuna. Kuvatut CDS tyypit on kehitetty mahdollistamaan helppokäyttöisempi tapa turvalliselle tiedonvaihdolle ja vähentämään tapauksissa käytettyjä eri tietoturvaluokkien päätelaitteita. Päätelaitteiden lukumäärää vähentämällä saavutetaan merkittäviä kustannussäästöjä.

Todellisuutta jo nyt

Teknologia on koeteltua ja käytössä olevaa, teknologian hyväksyntäprosessi kansalliselle tasolle on alkanut. Yksi yhden työaseman käytön mahdollistajista on todellisuutta Suomessa vuonna 2021 – ja toteutuu monivyöhyketyöasemassa, Single Secure Desktopissa (SSD). Pian on mahdollista suorakäyttää ja siirtää julkisesta verkosta ladattua tietoa korkean tietoturvallisuuden työasemaan.

TEKSTI: VKL:N PUHEENJOHTAJA JUKKA-PEKKA VIRTANEN
KUVAT: JUKKA-PEKKA VIRTANEN, ETELÄ-HÄMEEN VIESTIKILTA RY

Viestikiltojen liitto vuonna 2021

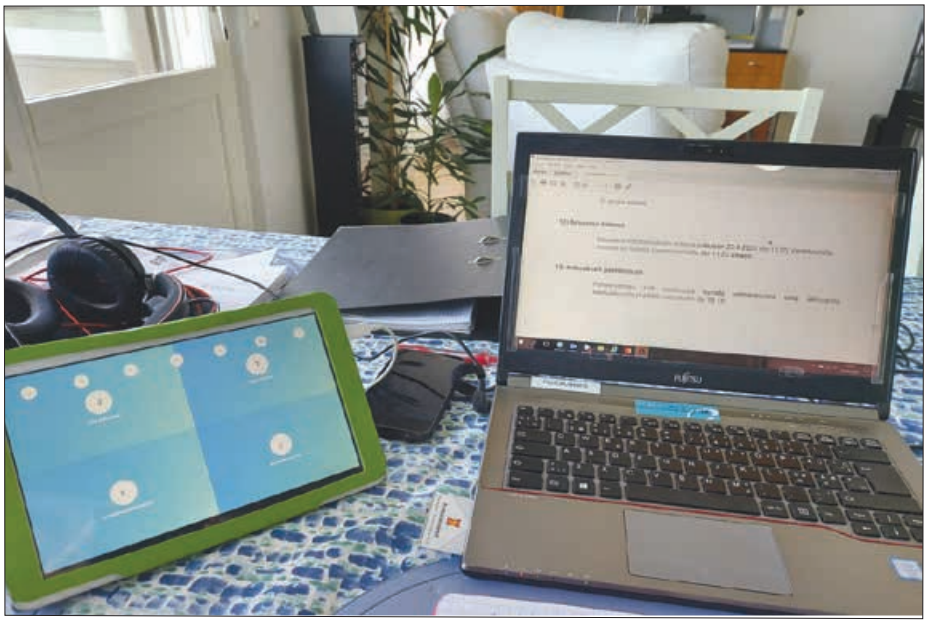
- Koronapandemia kurimuksesta toimintamuotoja kehittämällä uuteen normaaliin

Maaliskuussa 2020 alkanut koronapandemian värittämä ajanjakso piirtyy Viestikiltojen Liiton ja koko viestiaselajin vapaaehtoiskentän historiankirjoihin hyvin haasteellisena. Maaliskuiset Museo Militariassa järjestetyt vuosipäiväjuhlallisuudet kevätkokouksineen saatiin pidettyä, mutta seuraava merkintä onnistuneesta tapahtumasta onkin vasta syyskuun lopulta, jolloin pidettiin järjestyksessään neljäs valtakunnallinen A.R. Saarmaa -seminaari. Onnistumisen iloa koettiin vielä syyskokouksen yhteydessä Kaarinassa järjestetyissä juhlatilaisuuksissa, joiden yhteydessä palkastettiin Viestipataljoona 33:n muistolaatta. Kaikessa haasteellisuudessaan vuosi pakotti meitä pohtimaan ja osin myös toteuttamaan vanhojen hyväksi koettujen toimintamallien rinnalla uusia verkossa toimeenpantavia tapahtumia.

Viestikiltojen tukeminen toiminnan keskiössä

Haasteellisista olosuhteista huolimatta Viestikiltojen Liitto on lähtenyt rakentamaan vuoden 2021 toimintaa hyvin kunnianhimoisin tavoittein. Halumme edelleenkin kehittyä aktiivisena, ammattitaitoisena ja kiinnostavana viestialan perinteiden vaalijana, viestialan kouluttajana ja poikkeusolojen kansallisen johtamisvalmiuden kehittäjänä. Toiminnan keskiössä ovat alueelliset viestikillat, joiden toiminta turvataan nyt ja tulevaisuudessa.

Liiton kehittämisprojekteissa laadittu Viestikiltojen toiminnan kehittämissuunnitelma tarjoaa yhdessä toimintasuunnitelman kanssa tavoitteiden toteuttamisen tueksi käyttökelpoisia työkaluja. Viestikiltojen Liiton toimintakalenteri muodostaa tänäkin vuonna oivallisen



Koronapandemia osoitti Liittohallituksen vakiokäytänteiksi muodostuneet verkkokokousjärjestelyt erittäin toimiviksi. Perinteisten ja hyväksi koeteltujen toimintamallien rinnalla onkin tunnistettu tarve viedä toimintaa yhä enemmin verkkoihin.

tapahtumarungon killoille, jota niiden on mahdollista täydentää joustavasti oman aktiivisuuden ja resurssien mukaan. Toimintamallien ja yhteisten tapahtumien lisäksi Liitto tukee aktiivisia kiltoja taloudellisin resurssein sekä tuottamalla jäsenhankintaa tukevaa aineistoa.

Viestikillat jatkavat yhteistoimintajoukkojen edustajien rekrytoimista hallituksiin, tehtävänään tukea Viestikiltoja puolustusvoimien kanssa tehtävässä yhteistyössä ja erilaisten tilaisuuksien järjestämisessä. Myös tapahtumakalentereiden vakioiminen jatkuu. Vuosisuunnitelmaan pyritään sisällyttämään tutustuminen tai osallistuminen paikallispuolustusharjoituksiin, vierailut yhteistoimintajoukossa, alan yrityksissä, oppilaitoksissa ja sotahistoriallisissa kohteissa, ajankohtaisseminaari tai -esitelmä sekä varautumiskoulutustapahtuma.

Paikallispuolustuksen johtamisen kärkiosaajaksi

Liiton koulutustavoitteissa korostuu profiloituminen paikallispuolustuksen viestitoiminnan osaajana ja kehittäjänä. Viestikiltojen Liitto jatkaakin yhteistoiminnassa Viestikiltojen kanssa Maapuolustuskoulutusyhdistyksen johtamisjärjestelmä- ja viestikoulutusohjelman toimeenpanoa, joka edellyttää koulutuspäälliköiltä aktiivisuutta ja kiinteää yhteistoimintaa. Tähän kytkeytyy myös viestikiltojen kärkihanke - Paikallispuolustuksen viestitoiminta -koulutustapahtuma. Viestikillat toimeenpanevat joko yksin tai yhteistoiminnassa alueen maanpuolustusjärjestöjen kanssa paikallispuolustuksen viestitoimintaan keskittyvän koulutustapahtuman.

Mielenkiintoinen hanke onnistuessaan on myös ”Viestipataljoonat jatkosodassa”. Vuoden 2021 kesällä tulee kuluneeksi 80 vuotta siitä, kun 26 viestipataljoonaa lähti puutteellisesti koulutettuina ja varustettuina jatkosotaan. Viestikillat tuottavat teemalla ”Viestipataljoonat jatkosodassa” esitelmätilaisuuden tai näyttelyn ja siihen liittyvän artikkelin, jolla lisätään samalla kiltojen medianäkyvyyttä.

Koronan vaikutus vapaaehtoiskentän toimintaan on korostanut uudella tavalla

Museo Militarian johtajalle Miia-Leena Tiilille luovutettiin Viestiaselajin vuosipäiväjuhlan yhteydessä 5.3.2020 Viestiristi tunnustuksena merkittävästä viestiaselajin eteen tehdystä työstä.

Viestikiltojen Liitto osallistuu Etelä-Hämeen viestikillan toimenpitein Viestikoulun luokkarakennuksessa sijaitsevan Viestirykmentin perinnehuoneen ylläpitoon ja kehittämiseen. Kuvassa Pertti Parkki (vas.) ja Ari Haikarainen.

verkkotiedottamisen sekä sähköisten toimintamallien ja tapahtumien kehittämisen tärkeyttä. Viestikillat kehittävätkin omia Internet-sivujaan ja huolehtivat entistäkin aktiivisemmin niiden ajantasaisuudesta. Resurssien puitteissa lisätään sähköisiä toimintamalleja ja tapahtumia. Esimerkkinä näistä ovat paikallispataljoonan johtamista ja johtamisvälineistöä käsittelevät kurssit, ”Viestivisakisat”, sähköiset jäsenlehdet, webinaarit - unohtamatta erilaisten sosiaalisen mediakanavien monipuolista hyödyntämistä. Tässä tukeudumme mahdollisuuksien mukaan Maanpuolustuskiltojen liiton hankkeeseen, jonka tavoitteena on tuottaa alusta jäsenkiltojen verkkotuetulle toiminnalle.

Liiton 60-vuotishistoriikin kirjoitustyö käynnistyy

Liiton edeltäjän Viestikilta ry:n perustamisesta tulee 3.3.2023 kuluneeksi 60 vuotta. Vuoden 2021 aikana käynnistetään 60-vuotishistoriikin kirjoitustyö siten, että historiikki voidaan julkaista Viestijoukkojen vuosipäivänä 5.3.2023. Projektin vastuuhenkilöksi on lupautunut Pekka Wallenstjerna. Parhaillaan kootaan projektiryhmää, jossa kaikkia asian omaksi tuntevia kannustetaan aktivoitumaan. Viestiaselajin muistolaattaprojektia jatketaan yhteistoiminnassa Viestikiltojen kanssa. Muistolaatat on tarkoitus paljastaa Oulussa 1951-89 toimineelle 1.ErVK:lle yhteistoiminnassa Pohjan Viestikillan kanssa ja Karkussa toimineelle Viestikoulutuskeskukselle yhteistoiminnassa Pirkanmaan Viestikillan kanssa. Museo Militaria -päivä järjestetään 15.5.2021, jolloin tehdään talkoilla museon toimintaa tukevia kunnostus- ja parannustöitä.

Viides valtakunnallinen A.R. Saarmaa -seminaari järjestetään verkkotuettuna Riihimäellä perjantaina 24.9.2021 yhteistoiminnassa puolustusvoimien, Viestiupseeriyhdistyksen ja Maanpuolustuskoulutusyhdistyksen kanssa. Vuoden Viestikilta -kilpailua jatketaan uudistetuilla arviointiperusteilla. Viestikiltojen Liiton kotirata-ammunnat järjestetään tällä kertaa kesäkuusta lokakuuhun ulottuvalla aikajaksolla, jotta ammuntoja voisi suorittaa myös ulkoradoilla ja näin kaikki viestikillat saataisiin mukaan. Lisäksi osallistutaan erikseen päätettäviin Maanpuolustuskoulutusyhdistyksen ja muiden alan toimijoiden järjestämiin valtakunnallista valmiutta ja varautumista kehittäviin koulutustapahtumiin, johon liittyen parannetaan MPK:n koulutuskalenterin seurantaa ja Viestikilloille soveltuvien tilaisuuksien ennakoivaa kartoittamista ja niistä tiedottamista.

Viestikiltojen Liiton koulutustavoitteissa korostuu paikallispuolustuksen viestitoiminta. Liiton johdolla syyskuussa toimeenpantua paikallispuolustuksen johtamiseen keskittynyttä neljännen A.R. Seminaarin sisältöjä kiiteltiin jälleen kerran ajankohtaisuudestaan. Esiintymisvuorossa VKL:n koulutuspäällikkö Juha Peltomäki.

Viestikiltojen Liiton muistolaattaprojekti jatkui Piikkiössä, jossa syyskokouksen yhteydessä paljastettiin Viestipataljoona 33:n muistolaatta. Juhlaesitelmän VP33:n sodanaikaisista vaiheista piti FM Riku Kauhanen. Tilaisuutta isännöi Varsinais-Suomen Viestikilta.

Viestiristejä myönnetään perinteiseen tapaan viestiaselajin vuosipäivänä 5.3.2021 ja eversti A.R. Saarmaan syntymän vuosipäivänä 23.9.2021.

Viestiaselajin vuosipäiväjuhlallisuudet pyritään järjestämään osana Viestikoulun 80-vuotisjuhlallisuuksia. Mikäli tilaisuus perutaan koronasta johtuen, pidetään Liiton oma tilaisuus pienimuotoisena kevätkokouksen yhteydessä Museo Militariassa Hämeenlinnassa. Viestimiespäivät järjestetään Eteläisessä Suomessa 20.-22.8.2021. Järjestelyistä vastaa Uudenmaan Viestikilta. VKL:n hallitus aloittaa yhteistyössä Kymen Viestikillan kanssa infotilaisuuksien pitämisen viestiaselajin reserviupseerikurssille Haminassa. Vies-

tikillat järjestävät vastaavanlaisia rekrytointitilaisuuksia myös kotiutuville viestiaselajin varusmiehille. Vuonna 2020 Varsinais-Suomen Viestikilta täytti 50 vuotta (24.11.2020) ja Kaakkois-Suomen Viestikilta 40 vuotta. Tilaisuudet jouduttiin perumaan koronatilanteesta johtuen, mutta pyritään järjestämään vuoden 2021 aikana.

Kaikki hyvin - vain onko sittenkään?

Tiedottamisen ajankohtaisuuteen on tarve kiinnittää erityistä huomiota myös kuluvana vuonna. Internetsivujen ja sähköpostien lisäksi tietoa tapahtumista ja toiminnasta jaetaan Liiton facebook-ryhmässä, johon kiltalaisia ja muitakin alan vapaaehtoistoiminnasta kiinnostuneita kannustetaan liittymään. Hallituksen verkkokokoukset ovat vakiintuneet normaaleiksi käytännöiksi ja niiden rinnalla aktiivista vuoropuhelua käydään liitto- ja kiltajohdon yhteisessä WhatsApp-ryhmässä. Toki sähköisen viestinnän ohella hyödynnämme aktiivisesti Viestimies-lehteä, johon vuoden aikana laaditaan tämän toimintakatsauksen lisäksi artikkelit mm. Viestimiespäivistä, A.R. Saarmaa -seminaarista ja valitusta Viestikillasta esimerkkinä kiltakentän toiminnasta.

Viestikiltojen Liiton taloudellinen tilanne on hyvä ja antaa vahvan perustan menestyksekkäälle toiminnalle. Tulot perustuvat ensisijaisesti viestiristituottoihin ja jäsenmaksuihin, joka on jo pitkään ollut kolme euroa jäseneltä. Menoista tärkeimmät syntyvät Museo Militarian jäsenmaksusta, Viestiristien, levykkeiden ja muiden palkitsemisesineiden hankinnasta sekä Liiton ja Kiltojen tapahtumien järjestelyistä ja tukemisesta. Talouden puolella tapahtui uuden vuoden alkajaisiksi henkilövaihdos, kun pitkäaikainen tehtävän hoitajan Kai Lagerström luovutti tehtävät Harri Reinille.

Liittohallituksen puheenjohtajana näen Viestikiltojen Liiton tulevaisuuden valoisana. Perinteisen toiminnan rinnalla kehitämme rohkeasti uusia toimintamuotoja. Haluan kannustaa ja tukea Viestikiltojen johtoa tässä tärkeässä maanpuolustustyössä ymmärtäen hyvin toiminnan haasteellisuuden. Aktiivisen ja kehityshakuisen kiltajohdon merkitys korostuu näissä korona-ajan haasteissa entistäkin vahvemmin, jossa yhteistoiminta puolustusvoimien, Maanpuolustuskoulutusyhdistyksen, reserviläisjärjestöjen ja muiden alalla toimivien kumppaneiden kanssa on äärimmäisen tärkeää. Maanpuolustustahdon ylläpitämisen ohella on killoissa tehtävällä työllä yhä tärkeämpi merkitys myös kansallisen valmiuden ja varautumisen kehittämisessä. Toivonkin tämän työn käytännön toimeenpanolle johtamisjärjestelmäalan ja viestiaselajin johdolta, komentajilta, päälliköiltä ja koko henkilökunnalta kaiken mahdollisen tuen. Puheiden ja lämpimien ajatuksen sijasta tarvitaan tekoja. Yksin emme pärjää, mutta yhdessä olemme moninkertaisesti vahvempia!

TEKSTI: SEPPO URO
KUVAT: SA-KUVA

Jääkärieversti Perttu Pertamo

- radioteollisuutemme uranuurtaja

Jääkärieversti, diplomi-insinööri Perttu Pertamo (vuoteen 1935 Bertel Petrelius) toimi lähes kaksi vuosikymmentä puolustusvoimien radioalan keskeisenä kehittäjänä ja sotiemme aikana viestihuollon ylimpänä käytännön johtajana. Hän ei koskaan palvellut varsinaisissa viestijoukoissa, minkä vuoksi hän lienee jäänyt nykyiselle viestimiespolvelle varsin vieraaksi.

Bertel Abraham Petrelius syntyi Helsingissä 26.1.1892. Hänen vanhempansa olivat arkkitehti Albert Petrelius ja hänen puolisonsa Agnes os. Rönnqvist. Bertelin lisäksi perheen neljästä pojasta myös kaksi nuorempaa antautui sotilasuralle. Bertel kirjoitti ylioppilaaksi Helsingin suomalaisesta normaalilyseosta vuonna 1910, liittyi Eteläsuomalaiseen osakuntaan ja opiskeli tämän jälkeen Teknillisen korkeakoulun koneinsinööriosastossa vuosina 1910-15. Tieto jääkäriliikkeestä levisi myös teekkareiden keskuuteen ja vuoden 1915 lopulla Petreliuskin päätti lähteä mukaan. Myös hänen nuorempi veljensä Väinö Armas Petrelius (s. 1897) päätti lähteä jääkäriksi ja molemmat ilmoittautuivat Lockstedtin leirillä Saksassa 15.12.1915. Heidät sijoitettiin koulutusjoukon konekivääriкomppaniaan. Tässä molemmat palvelivatkin lähes koko jääkärikautensa ajan osallistuen myös jääkäripataljoonan mukana rintamapalvelukseen Missejoella ja Riianlahdella vuonna 1916 ja Bertel myös Aajoen talvitaisteluihin seuraavana talvena. Bertel ylennettiin Hilfsgruppenführeriksi 1.10.1916 ja Gruppenführeriksi 20.7.1917, Väinö Hilfsgruppenführeriksi 11.11.1916.

Syksyllä 1917 jääkäreitä ryhdyttiin lähettämään pienissä erissä Suomeen tekemään valmisteluja mahdollisesti puhkeavia sotatoimia varten. Joulukuun alussa Bertel määrättiin noin 20 jääkäriä käsittäneeseen etukomennuskuntaan, joka suuren aselastin kanssa kuljetettiin aselaiva Equityllä Suomeen. Aselasti oli suunniteltu purettavaksi Merikarvialla, mutta vain osa aseista saatiin maihin paikallisten kalastajien kieltäydyttyä avustamasta operaatiossa. Lastina oli myös kaksi suurta akkua, jotka saatiin maihin ja joukossa mukana ollut jääkäri Karl Nyström kuljetti ne Vaasassa olleelle jääkäri Arthur Stenholmin (Saarmaan) perustamalle salaiselle radioasemalle. Vuoden 1917 lopulla yhteiskunnallinen tilanne Suomessa oli kireä ja sekä punaisten että valkoisten puolella tehtiin valmisteluja mahdollisten yhteenottojen varalta. Suojeluskunnat vahvistuivat pääkaupunkiseudulla huolimatta punaisten ylivallasta. Korkeakouluopiskelijat olivat perustaneet ylioppilassuojeluskunnan, jolta kuitenkin puuttui johtajia. Tällaisten kouluttamiseksi järjestettiin Vimpelissä Pohjanmaalla runsaan kahden viikon pituinen kurssi, jonka vahvuus oli noin 200 oppilasta. Kurssi jaettiin kahteen komppaniaan, joiden kouluttajiksi määrättiin toistakymmentä aselaiva Equityn mukana tullutta jääkäriä. Heidän joukossaan oli myös Bertel Petelius, joka joulukuun lopulla 1917 määrättiin Vimpelin sotakoulun Pokelan komppanian (1.K) apulaispäälliköksi ja konekivääriкouluttajaksi. Hänen veljensä Väinö Petrelius oli jo aikaisemmin siirtynyt Saksasta Ruotsiin, josta myös hänet joulukuun lopulla lähetettiin kouluttajaksi samaan komppaniaan. Vimpelin kurssia pidetään itsenäisen Suomen ensimmäisenä upseerikurssina.

Tammikuun lopulla 1918 Bertel Petrelius määrättiin Vöyriin perustetun sotakoulun johtajaksi ja Väinö sen konekivääriкouluttajaksi. Myös tällä kurssilla oli tarkoituksena kouluttaa suojeluskuntiin sotilasohjaajia. Kurssin koulutus katkesi kuitenkin vapaussodan alkaessa ja sen kouluttajat ja toista tuhatta oppilasta joutuivat osallistumaan venäläisten aseistariisuntaan Vähässäkyrössä ja taisteluihin Oulussa. Taistelujen tauottua kurssin koulutus jatkui kestäen yhteensä noin kuusi viikkoa. Tätä kurssia pidetään puolustusvoimien ensimmäisenä aliupseerikurssina. Maaliskuussa Bertel Petrelius osallistui Vöyrin sotakoulupataljoonan mukana mm. Kurun, Teiskon ja Tampereen taisteluihin. Hänet ylennettiin luutnantiksi helmikuussa ja kapteeniksi jo huhtikuussa 1918. Väinö Petrelius toimi helmikuussa Sipoossa muodostetun ns. Vihreän Pataljoonan komentajana osallistuen mm. Keravan, Sipoon ja Pellingin seuduilla käytyihin taisteluihin. Hän joutui punakaartilaisten vangiksi ja surmattiin Helsingissä 13.2.1918.

Vapaussodan päätyttyä Bertel Petrelius palveli lyhyen aikaa mm. konekivääriкomppanian päällikkönä Itämeren Jalkaväkirykmentissä 1918, opettajana Viipurin Markovillan upseerikokelaskursseilla 1918-19 sekä suojeluskuntien yliesikunnan koulutusosaston päällikkönä 1919-20. Sen jälkeen hänelle myönnettiin opintolomaa kesken jääneiden opintojen loppuun saattamiseksi. Vuonna 1921 hän suoritti pikkudiplomin Helsingissä ja jatkoi sen jälkeen opintoja Saksassa Karlsruhen teknillisessä korkeakoulussa valmistuen siellä diplomi-insinööriksi vuonna 1923. Palattuaan Suomeen hän toimi suojeluskuntien yliesikunnan radioupseerina vuosina 1924-25.

Vuonna 1925 puolustusvoimien radioalan kehittämistä varten perustettiin Puolustusministeriön radiolaboratorio, jonka johtajaksi Petrelius nimitettiin. Laboratorioon liitettiin myös Radiopataljoonan radiopaja. Vuonna 1927 radiolaboratoriota laajennettiin muodostamalla siitä Puolustusministeriön Sähkölaboratorio. Kapteeni Petrelius jatkoi myös sen johdossa. Laboratoriolla oli toimitiloja mm. Katajanokalla, Santahaminassa ja Suomenlinnassa. Laitoksessa palveli 1920- ja 1930-luvuilla useita tunnettuja radioalan kehittäjiä, kuten mm. Elias Hellberg ja Georg Sallavuori, yhteensä useita kymmeniä henkilöitä. Radiolaboratorio ja Sähkölaboratorio kehittivät ja valmistivat ennen sotia pääosan puolustusvoimien radiokalustosta. Jo Radiopataljoonan radiopajalla aloitettiin

ensimmäisten kenttäradioiden kehittäminen ja vuonna 1925 valmistui ns. molekyyliradio, C-radion prototyyppi. Vuosina 1927-32 valmistuivat Sähkölaboratoriossa sarjatuotantona talvisodassa käytetyt C-, D- ja B-radiot. Näistä C-radio oli pataljoonaradio, D-tykistöradio ja B-radio rykmenttiradio. Vuonna 1937 valmistui ylempien johtoportaiden käyttöön tarkoitettu AB-radio, ns Anna-Bella. Noin vuodesta 1927 alkaen Sähkölaboratoriossa kehitettiin myös ilmavoimien eri lentokonetyypeille omat radionsa samoin kuin huomattava määrä kiinteitä lähettimiä ilmailuliikenteen ja merenkulun palvelukseen. Petrelius (vuodesta 1935 Pertamo) ylennettiin majuriksi vuonna 1925, everstiluutnantiksi vuonna 1928 ja everstiksi vuonna 1938. Vuonna 1924 hän julkaisi tiettävästi ensimmäisen suomenkielisen radiotekniikkaa käsittelevän kirjan "Elektroniputki ja sen käytäntö radiotekniikassa" ja toimi vuosina 1925-26 radiotekniikan opettajana Sotakorkeakoulussa.

Talvisodan ja välirauhan aikana Pertamo toimi edelleen Puolustusministeriön Sähkölaboratorion johtajana. Laitoksen toiminta siirrettiin joksikin aikaa pommitusten vuoksi ensin Hämeenkyröön ja myöhemmin Kokkolaan. Jatkosodan aikana Pertamo toimi ensin Päämajan viestiosasto I:n korjaamotoimiston päällikkönä ja vuodesta 1943 lähtien Päämajan viestiosasto III:n päällikkönä. Hänen johdossaan olivat Päämajan alaiset neljä ja alajohtoportaiden alaiset 22 viestikorjaamoa. Niissä työskenteli yhteensä noin 300 viestiasentajaa. Viestiosasto III:n tehtävänä oli myös viestikaluston kehitystyö yhteistoiminnassa kotimaisen teollisuuden kanssa.

Sotien päätyttyä kaikki puolustusvoimien viestikorjaamot lakkautettiin keväällä 1945. Niiden työn jatkajaksi perustettiin Valtion Sähköpaja Oy ja eversti Pertamo toimi lyhyen aikaa sen toimitusjohtajana. Uusi yhtiö sai toimitilat pääasiassa Espoon Mäkkylästä. 1940-luvun lopulla Santahaminassa toimineista entisistä Sähkölaboratorion korjaamoista muodostettiin Puolustuslaitoksen Santahaminan Tehdas. Se ryhtyi tuottamaan pääasiassa erilaisia moottorikäyttöisiä ja hydraulisia työkoneita, kuten tiehöyliä, salaojien kaivinkoneita, traktorikaivureita ja viljankuivaajia. Eversti Pertamo valittiin tämän tehtaan toimitusjohtajaksi ja hän toimi virassa kuolemaansa saakka vuoteen 1956.

Kolmas arkkitehti Petreliuksen neljästä pojasta, Eero Albert Pertamo syntyi vuonna 1902, suoritti varusmiespalveluksensa Radiojoukoissa ja kävi Kadettikoulun vuosina 1923-25. Hän palveli nuorempana upseerina ja lentueen päällikkönä 1.Merilentolaivueessa 1925-32, sen jälkeen Ilmavoimien esikunnan viestiupseerina, tiedustelu-upseerina ja toimistopäällikkönä 1934-39 sekä huoltopäällikkönä 1940-41. Talvisodan aikana 1939-40 hän toimi ilmavoimien viestikomentajana, jatkosodassa vuosina 1941-44 Viestipataljoona 11:n ja VP 26:n komentajana. Sodan jälkeen hän toimi lyhyen aikaa Puolustusvoimien Pääesikunnan radio-osaston päällikkönä 1944-45 ja siirryttyään siviiliin pankkialalla parikymmentä vuotta. Majuri Pertamo kuoli vuonna 1980.

Analysaattori

Verkkokapinaa ja valkoista kohinaa

Se sitten Trumppi lähti kuten toivottiinkin, mutta ei ihan suosiolla kuten arvattiinkin. Hän järjesti kunnon läksiäiset Capitolin kukkulalla vannoutuneiden kannattajiensa avustuksella tavalla, joka meni kerrasta Yhdysvaltain historiaan eikä siis mitenkään hyvässä mielessä. Uutisoinnissa puhuttiin, kuinka maailman vanhin demokratia oli vaarassa. Tuosta väittämästä olisin kyllä heti vähän eri mieltä, sillä demokratiaa jossain olomuodossa oli jo Antiikin Kreikassakin. Kotisohvalta tätä pelleilyä tiiviisti seurannut Analysaattori täällä hämmästelee edelleen selkkauksen digitaalista ulottuvuutta. Twitterin ja muidenkin sosiaalisten medioiden osuus on niin merkittävä, että pitäisi oikeastaan esittää kysymys, miten se on edes mahdollista.

Kun Capitolin kapinanpoikasen jälkeen Twitter sulki Trumpin tilit pysyvästi, otti tämä media tavallaan osaa poliittiseen päätöksentekoon. Twitter perustelee tätä aika rankkaa toimenpidettä sillä, että heidän tavoitteenaan on, että käyttäjät voivat kuulla suoraan esim. poliitikkojen ja maailman johtajien oman äänen. Palvelua ei kuitenkaan saisi käyttää väkivaltaan yllyttämiseen, joten mahdollisia jatkorähinöitä estääkseen pistetiin tämä tuulitukkainen hiukan huonompi häviäjä sitten digitaalisesti pakkaseen. Muutkin sosiaalisen median palvelut blokkasivat Trumpin melko nopeasti, mutta Twitterin rooli oli kyllä se merkittävin tekijä. Jo pitkään ennen vaalejakin ryhtyi Twitter sensuroimaan Trumpin väittämiä eli omia totuuksia, joita yleisesti myös valheiksi kutsutaan.

Näin jälkeen päin, kun tarkastelee Trumpin twiittejä syntyy tunne, että olisikohan jotain vastaavaa pitänyt tehdä jo paljon aikaisemmin. The New York Times julkaisi nimittäin sähköisen luettelon kaikista Trumpin twiiteistä vuosilta 2015-2021. *(The Complete List of Trump's Twitter Insults (2015-2021)*. Luettelo on helppolukuinen ja aakkosjärjestyksessä sen mukaan kehen loukkaus on aina kulloinkin kohdistunut. Loukkauksista on nimenomaan kyse ja ne kohdistuivat noin 850 yksittäiseen henkilöön kokonaismäärän ollessa jotain lähempänä kymmentä tuhatta. Aika helpolla pääsi mm. Venäjän presidentti Putin, joka sai vain yhden twiitin Syyrian presidentin Assadin tukemisesta. Pohjois-Korean "Pieni Rakettimies" Kim Jong Un sai sentään kymmenkunta osumaa. Nyt istuva USA:n presidentti Joe Biden oli itsestään selvä listaykkönen useilla sadoilla törkeillä loukkauksilla. Kyse oli sellaisista viesteistä, joilla uskoisin Suomessa joutuvan nopeasti raastupaan, mutta rapakon takana se tuntuu kuuluvan olennaisena osana päivän politiikkaa. Suomalaisiin osuvia törkeyksiä en itse ainakaan tuosta listalta löytänyt. Ainoa joka periaatteessa saattaisi koskea välillisesti meitäkin on Lockheed Martin F35-ohjelman saama tölväisy "*out of control*".

Samaan aikaan kun muu maailma yrittää aktiivisesti unohtaa Trumpin on myös virkaveli Venäjällä ajautumassa hankaluuksiin. Aleksei Navalnyin pieleen mennyt myrkytys ja miehen hullunrohkea paluu kotiin vangittavaksi on juuri tätä kirjoitettaessa aiheuttanut jo toisena viikonloppuna peräkkäin kymmenien tuhansien ihmisten mielenosoituksia ympäri Venäjää. En nyt sanoisi, että Vladimirin valtaistuin välttämättä edes heilahtaa, mutta toisaalta juuri näinhän ne monet diktaattorit on ennenkin kaadettu. Putinin vastaisessa operaatiossa onkin sitten merkittävimmäksi digitaaliseksi alustaksi noussut Twitterin ja Instagramin ohessa kiinalainen Tik Tok. Kyseessä on siis nuorison suosima media, jossa tyypillisesti leviää hauskoja haasteita ja tanssivideoita. Nyt siellä leviää kutsuja myös Navalnyin tukimielenosoituksiin. Vahva huhu kertoo, että näitä kutsuja leviäisi myös Tinderissä. Siinäpä muuten olisikin varmasti mieleenpainuvat treffit. *"Tunnistat minut kaasunaamarista, jossa on kukka"*. Joskus sitten myöhemmin voisi vaikka kertoa lapsenlapsille, kuinka hauskasti mummu ja vaari saivat pampusta samana päivänä, kun tapasivat ensi kerran.

Putinin ongelmat alkoivat myös kasaantua verkkovälitteisesti, sillä Navalnyin tukijoukot julkaisivat melkein kaksituntisen videon YouTubessa, jossa esiteltiin Putinille verovaroilla rakennettu kesämökki Mustan meren rannalla. Video keräsi hetkessä yli 100 miljoonaa katselukertaa. Kyseessä on siis vaatimaton 1,2 miljardin euron arvoinen n. 17 000 neliömetrin kokoinen palatsi. Pelkästään makuuhuone on kooltaan n. 260 neliötä ja ostereita kasvatetaan omassa rannassa. Kiinteistöön kuuluu myös kylpylä, elokuvateatteri, viinikellari, teatteri, kasino, tankotanssilava, ja oma kirkko.

Putin tietenkin kiistää, että hänellä tai perheellään olisi mitään tekemistä sen kanssa. Kohun kasvaessa omistajaksi riensi ilmoittautumaan Putinin kaveri, meillekin kovin tuttu Jokereiden entinen omistaja Arkadi Rotenberg, joten on entistäkin selvempää, kenen omaisuudesta on siis kysymys. Mutta jos se palatsi nyt sitten sattuisikin todella olemaan Arkadin omaisuutta, niin sinnehän olisi kiva viedä vanha lätkäjoukkuekin rentoutumaan. Kuuluuhan kiinteistöön myös maanalainen jäähalli. Siihen sisältyisi tiettyä symboliikkaakin, jos narripaidat siellä höntsäilisivät tämän Arkadin kanssa, joka samalla tekee itsestäänkin tässä juuri narrin. Rikkaan sellaisen, mutta kuitenkin.

Tuolta sosiaalisen median verkostoista pongasin myös mielenkiintoisen aiheeseen löysästi liittyvän filosofisen kysymyksen. Mitäs jos Venäjän viranomaiset tarjoaisivat Aleksei Navalnyille koronarokotusta. Ottaisikohan Aleksei sen vai mahtaako hän olla nykyään sellainen rokotevastainen henkilö?

Tässä samalla kun kirjoittelen tätä, katselen suoraa lähetystä verkosta Moskovasta näistä mielenosoituksista. HD-tasoista kuvaa, jota voi siis seurata kuka tahansa missä vaan. Eipä olisi tullut 70-luvulla mieleenkään, että näinkin voi joskus tapahtua. Vaikuttaa myös siltä, että Putinin esikunnassa on ymmärretty varoa

sosiaalisen median vaikutusvaltaa, sillä Moskovassa on kaikkia avoinna olevia kahviloita kehotettu sulkemaan avoimet langattomat verkkonsa. Tämä selkkaus itärajamme takana ei luultavasti vielä ole edes kunnolla alkanutkaan, joten pitäkää selaimenne päivitettyinä, jatkoa seuraa kyllä.

Kaikki maailman johtajat seuraavat varmasti näitä tapahtumia tarkkaan, sillä eihän sitä koskaan tiedä miten nopeasti kansa nousee barrikaadeille, jos vaikka joku toisinajattelija jääkin vahingossa henkiin ja alkaa verkkokapinoimaan. Eräs yksinvaltias tuskin kuitenkaan pelkää Twitteriä eikä varmaan Tinderiäkään. Pohjois-Korean Kim Jong Un, Taivaasta laskeutunut, Paektuvuoren perillinen. Kim pitää omaa kesähoviaan Wonsanin alueella. Siellä sijaitsee hänen kesäpalatsinsa ja sitä ei ole salaa rakennettu verovaroilla. Se on rakennettu ihan suunnitelmallisesti ja julkisesti. Kim on myös kätevästi yhdistänyt huvin ja hyödyn sillä hän on ampunut kymmeniä ohjuksia sieltä huvilansa alueelta. Virkamatkat johtamaan tärkeitä ohjuskokeita ovat näin merkittävästi lyhyempiä ja rahaakin säästyy. Kimin ei tarvitse varsinaisesti pelätä sosiaalista mediaa johtuen astetta kovemmista rajoituksista kansalaistensa sometuksen osalta. Vainoharhainen hän kyllä on valtansa suhteen ja hoitelee järjestelmällisesti päiviltä kaikki, jotka vähänkin alkavat saavuttaa liian suurta suosiota. Eräs turhamaisuutensa osoitus on myös hänen oman nimensä suojaaminen. Pohjois-Koreassa on käytössä varsin rajallinen määrä erilaisia nimiä. Valtaan päästyään hän kielsi Kim Jong Un nimen antamisen vastasyntyneille lapsille. Ja ikään kuin varmistaakseen, ettei sekaannuksia pääse syntymään hän kielsi sen myös jo niiltä henkilöiltä, joille se oli joskus jo ehditty antamaan. En tiedä mutta vahvasti epäilen, että Pohjois-Korean paikallinen Digi-ja Väestötietovirasto toteutti nämä kumulatiiviset massaristiäiset ripeästi ja tarkasti kuuntelematta vastalauseita. Tuskin niitä kyllä tulikaan, on siellä sen verran opittu olemaan kiltisti hiljaa, kun on sellainen aika. Ja yleensä on.

Löysänä aasinsiltana uusiin nimiin liittyen ilmoitan täten juhlallisesti, että Analysaattorikin on saanut sellaisen. Nyt saa kutsua Vaariksi. Ensimmäinen lapsenlapsemme näki päivänvalon loppuvuodesta ja onhan tässä opittu taas uudelleen asioita, jotka olivat jo kivasti päässeet unohtumaan. Paljon on tapahtunut kehitystä varsinkin vauvaikäisten lasten kasvatuksessa ja käsittelyssä. Eikä liene yllätys, että digitaalisuuskin on tullut mukaan. Eräs hienoimmista apuvälineistä, joka tässä on tullut vastaan, on digitaalinen jänis. Tämä pupu on ikään kuin unikaveri, joka sijoitetaan sinne piltin kaveriksi kehtoon. Hänen muhkea vatsansa vaihtaa väriä ja jänis myös ääntelee. Ei tosin laula eikä soita pimpelipom-musiikkia vaan toistaa sen sijaan puhdasta valkoista kohinaa. White Noise, sillä se vauva sitten rauhoittuu. Samaa tavaraa löytyy ilman jänistä myös Spotifystä. Saatavana on esimerkiksi 11 tuntia pitkä White Noise soittolista. Sen verran tuota jänistä on nyt testattu, että se kohina nukuttaa kyllä helposti vähän varttuneemmankin henkilön. Jota siis nykyään Vaariksi kutsutaan.

KUTSU VIESTIUPSEERIYHDISTYKSEN KEVÄTKOKOUKSEEN

Viestiupseeriyhdistyksen hallitus kutsuu yhdistyksen jäsenet kevätkokoukseen torstaina 15.4.2018 klo 15.00 alkaen verkkokokouksena. Yhteyksien testaus ja joustavan kokoustamisen valmistelut aloitetaan klo 14.30.

Kokouksessa käsitellään sääntöjen 5 §:ssä kevätkokouksessa käsiteltäväksi mainitut asiat:

1) Kokouksen puheenjohtajan valinta

2) Kokouksen sihteerin valinta

3) Kokouksen kahden pöytäkirjan tarkastajan ja ääntenlaskijan valinta

4) Kokouksen laillisuuden ja päätösvaltaisuuden toteaminen

5) Kokouksen työjärjestyksestä päättäminen

6) Yhdistyksen toimintakertomuksen ja tilinpäätöksen käsittely

7) Toiminnantarkastajan kertomuksen käsittely

8) Toimintakertomuksesta päättäminen ja tilinpäätöksen vahvistaminen

9) Hallituksen vastuuvapaudesta päättäminen

10) Muut asiat

Kokous järjestetään koronatilanteesta johtuen verkkokokouksena. Verkkokokouksen perusteet lähetetään ilmoittautuneiden sähköpostiin viimeistään päivää ennen kokousta.

Ilmoittautumiset pe 9.4.2021 mennessä www.viestiupseeriyhdistys.fi (toivottavin tapa), sähköpostitse toiminnanjohtaja@viestiupseeriyhdistys.fi tai puhelimitse 040 514 2497.

Tervetuloa kevätkokoukseen!

Viestiupseeriyhdistys ry:n hallitus

Kirjoittanut: Reino Tamminen

Datasiirron nykyisistä ja tulevista käyttömahdollisuuksista

Datasiirtoon puhelinverkossa tarvittavat tekniset perusteet ovat yleisesti tunnetut. Puhelinmiehen kannalta on merkittävin osa modem, jota voidaan kutsua osuvasti myös tietokoneen puhelimeksi. Modemin tehtävänähän on muuttaa tasavirtamuodossa oleva data puhelinverkossa etenemään sopivaksi äänisignaaliksi.

Nopeusvaatimus ulottuu yhä lähemmäksi jokaista meistä elämässämme. Tämän vaatimuksen toteuttamiseksi on esimerkiksi datasiirto tulossa vaikuttamaan tapoihimme ja tottumuksiimme. Teemmepä mitä tahansa, ajamme kolarin tai menemme naimisiin, voimme olla vakuuttuneita siitä, että muutamien aikojen kuluttua se rekisteröidään jossakin keskitetyssä tietopankissa tai vastaavassa. Toivoa vain sopii, että tiedon siirtäminen aina onnistuisi, sillä tietokonehan on niin yksinkertainen, ettei se osaa tunnustaa tekemiään virheitä saatikka sitten korjata niitä.

Tietokoneteollisuus on kasvanut ja kehittynyt miltei räjähdyksenomaisesti. Noin kahdeksassa vuodessa tietokoneiden määrä on kasvanut 10 000:sta yli 100 000:ksi. Määrän mukana on myös tietojenkäsittelykapasiteetti noussut moninkertaiseksi. Tietokoneet on pidettävä täystyöllistettyinä. Käsiteltävien asioiden määrää on lisättävä ja tulokset palautettava nopeasti. Tämä vaatii datansiirtoa. Laitekohtaiseen datansiirron standardisointiin on vaikea päästä. On todennäköisimmin odotettavissa, että laitevalikoima kirjavoituu jatkuvasti teknisen kehityksen edetessä nopeasti. Puhelinlaitoksen kannalta

on huomioonotettavaa, että modem rakennettaneen – ellei sitä hallinnollisin pakkotoimin estetä – päätelaitteen kiinteäksi osaksi. Puhelinlaitoksen osuudeksi jää tällöin pääasiassa hyvien ja riittävien yhteyksien tarjoaminen telekommunikaation kolmiulotteisessa ääntä, dataa ja kuvaa siirtävässä maailmassa.

Näppäinpuhelimen käyttö datansiirtolaitteena yleistynee päätelaitteiden yleistyessä. Näppäinpuhelimella lähetettävän datan tulisi oltava dekaadisiksi numeroiksi muunnettua. Kirjaintenkin lähettäminen on mahdollista, mutta se vaatii kahden näppäimen peräkkäistä painallusta kirjainta kohti ja mielellään 16- osaisen näppäimistön. Näppäinpuhelimesta tuskin kehittyy kirjeiden välittäjää, mutta se sen sijaan saattaa soveltua esim. tilintarkastuksiin, tietojen keräilyyn ja poissaoloilmoitusten laatimiseen. Puhelimitse tapahtuvien rahansiirtojen suurimpana pulmana ovat henkilön identiteetin varmistaminen ja mahdolliset käyttöoikeuskategoriat.

Pienoisreikäkortti tai vastaava lähetin, jonka näppäimistöön voi yhdistää tuo mukaan uusia sovellutuksia. Tulevaisuudessa 200 bit/s datapäätelaite on likimain puhelimen kokoinen ja yhtä yksinkertainen kytkeä puhelinverkkoon kuin puhelinkin. Tähän ryhmään voitaneen lukea myös osoituskäyttö ja tietopankit. Tietopankkihan tarkoittaa, että tietokoneen avulla muistiin sijoitettuja tietoja voidaan poimia sieltä haluttuna yhdistelmänä ja saada ne tavalla tai toisella näkyvään muotoon. Tietopankit voivat tulevaisuudessa muodostua esim. monista eri rekistereistä. Lähiaikoina lähes kaikki inhimillisen toiminnan muodot ovat siirtymässä keskitettyihin muisteihin, joista niitä sitten halutulla tavalla ryhmitettynä saadaan poimituksi esille.

Datasiirrossa ei voi paljon puhua nykyisyydestä ja tulevaisuudesta erikseen, sillä muutokset ovat niin nopeita, että painomuste ei aina ehdi kuivua, kun ollaan jo sovittamassa käyttöön uusia menetelmiä. Paitsi sitä, että datasiirron mahdollisuudet aletaan tunnistaa, kuuluu muotiin puhua automaattisesta tietojenkäsittelystä. Tätä meidän puhelinmiesten kannattaa tukea sekä olla aina valmiina puhumaan datasiirron puolesta ja osoittaa asiakkaillemme puhelinverkon monipuoliset, tehokkaat ja ennen kaikkea halvat käyttömahdollisuudet.

Artikkelin kirjoittaja: Veli-Matti Pesola

In Memoriam Olli-Matti Virva 1930-2021

Monipuolisen upseerinuran tehnyt ye-everstiluutnantti Olli-Matti Virva kuoli Espoossa 5.2.2021. Hän oli 90-vuotias, syntynyt Helsingissä 22.6.1930. Virva vietti lapsuus- ja nuoruusvuotensa Riihimäen varuskunnassa, jossa hänen isänsä, everstiluutnantti Veli Matti Virva toimi Viestikoulun johtajana vuodesta 1946 aina vuonna 1951 tapahtuneeseen varhaiseen kuolemaansa saakka. Olli-Matti kirjoitti ylioppilaaksi Riihimäen lyseosta vuonna 1950 ja suoritti varusmiespalveluksensa 2. Erillisessä Viestikomppaniassa Hämeenlinnassa vuonna 1951. Kotitausta ja lapsuusvuosien kokemukset lienevät vaikuttaneet siihen, että hän valitsi elämäntehtäväkseen upseerin uran. Riihimäeltä löytyi myös aviopuoliso, evp-upseerin tytär Eeva Jukomaa.

Olli-Matti Virva kävi Kadettikoulun vuosina 1951-53 sekä suoritti yleisesikuntaupseerin tutkinnon Sotakorkeakoulun teknisellä opintosuunnalla v 1964 ja yleisellä opintosuunnalla v 1967. Hän palveli aluksi nuorempana upseerina 2.ErVK:ssa Hämeenlinnassa vuosina 1953-56, sen jälkeen Panssarikoulun viestilinjan johtajana 1956-59 sekä komppanianpäällikkönä ja toimistopäällikkönä Viestirykmentissä Riihimäellä 1960-64. Sotakorkeakoulun jälkeen hänet määrättiin Kouvolaan ensin toimistoupseeriksi 3.Divisioonan esikuntaan ja vuodesta 1967 viestitoimiston päälliköksi Kaakkois-Suomen Sotilaslääninn esikuntaan. Vuonna 1970 hän siirtyi jälleen Riihimäelle, ensin Viestikoulun koulutusupseeriksi ja kapteenikurssin johtajaksi ja sen jälkeen Viestirykmenttiin pataljoonan komentajaksi. Vuosina 1973-74 hän palveli viestitoimiston päällikkönä Pääesikunnan viestiosastossa, jonka jälkeen hänet määrättiin Viestikoulun johtajaksi Riihimäelle. Tässä tehtävässä hän toimi aina vuoteen 1981 saakka, jolloin erosi puolustusvoimien palveluksesta. Vuosina 1981-94 hän toimi Valtion Teknillisen Tutkimuskeskuksen turvallisuuspäällikkönä.

Olli-Matti Virva oli monin tavoin mukana myös Viestiupseeriyhdistyksen toiminnassa. Hän oli yhdistyksen hallituksen jäsen vuosina 1973-77, joista kaksi viimeistä vuotta hallituksen varapuheenjohtajana. Kuten hänen isänsä 1940-luvun lopulla myös Olli-Matti toimi myös Viestimies-lehden päätoimittajana vuosina 1973-78 ja oli sen jälkeen vielä lehden toimituskunnan jäsenenä vuodet 1978-81. Päätoimittajana hän kehitti lehteä monin tavoin. Lehden painopaikka muutettiin hänen kaudellaan Mikkelistä Hyvinkään Kirjapainoon, jonka nykyaikainen tekniikka helpotti kuvitusta ja laajensi typografisia mahdollisuuksia. Hän aloitti käytännön, että lähes jokaisessa lehdessä oli myös päätoimittajan itsensä tai yhdistyksen puheenjohtajan laatima pääkirjoitus. Lehti saikin tunnustusta uudistuneesta ulkonäöstään ja sisällöstään. Monet viestiupseeripolvet muistavat Olli-Matti Virvan monipuolisena ja aikaansaavana kolleegana ja esimiehenä.

Seppo Uro, eversti evp

Olli-Matin oppilas, alainen ja ystävä

Viestiupseeriyhdistyksen webinaari 20.5.2021

”Vapaaehtoinen maanpuolustus kyberturvallisuuden kansallisessa kehittämisessä”

Viestiupseeriyhdistys ry järjestää torstaina 20.5.2021 webinaarin teemana ”Vapaaehtoinen maanpuolustus kyberturvallisuuden kansallisessa kehittämisessä”.

Tilaisuudessa käsitellään valmisteilla olevaa kansallisen kyberturvallisuuden kehittämisohjelmaa ja vapaaehtoisen maanpuolustuskentän roolia tämän ohjelman toimeenpanossa.

Webinaarin alustajina ovat kyberturvallisuusjohtaja Rauli Paananen liikenne- ja viestintäministeriöstä, prikaatikenraali Jarmo Vähätiitto Pääesikunnasta ja tutkimusjohtaja Mikko Hyppönen F-Securesta. Paneelikeskusteluun osallistuu alustajien lisäksi koulutusjohtaja Timo Mustaniemi Maanpuolustuskoulutus – MPK:sta.

Webinaari on tarkoitettu organisaatioiden tietoverkkojen toimintavarmuudesta, suunnittelusta, ja tietoturvallisuudesta kiinnostuneille.

Tilaisuus on osallistujille maksuton. Webinaariin osallistumisen perusteet lähetetään ilmoittautuneille sähköpostiin viimeistään päivää ennen tilaisuutta.

Ilmoittautumiset 10.5.2021 alla olevalla lomakkeella tai spostilla seminaari@viestiupseeriyhdistys.fi.

Lisätietoja antaa Harri Reini, puh. 040 514 2497 tai seminaari@viestiupseeriyhdistys.fi

OHJELMA: Torstai 20.5.2021

12.30 - 13.00	Yhteyksien muodostaminen ja testaus
13.00 - 13.10	Webinaarin avaus, VUY:n puheenjohtaja Juha Petäjäinen
13.10 - 13.40	”Kehittämisohjelma kyberturvallisuuden kokonaistilan parantamiseksi”, Rauli Paananen, kyberturvalli suusjohtaja, Liikenne-ja viestintäministeriö.
13.40 - 14.10	”Puolustusvoimat osana kansallista kyberturvallisuutta”, prkenr Jarmo Vähätiitto, johtamisjärjestelmä päällikkö, Pääesikunta
14.10 - 14.40	”Näkökulmia kansalliseen kyberturvallisuuteen”, tutkimusjohtaja Mikko Hyppönen, F-Secure Oyj.
14.40 - 14.45	TAUKO, valmistautuminen paneeliin
14.45 - 15.30	Paneelin teema: ” Vapaaehtoisen maanpuolustuskentän rooli yhteiskunnan digitaalisen turvallisuuden kehittämisessä”. Paneelin osallistujat: Rauli Paananen, Jarmo Vähätiitto, Mikko Hyppönen ja Timo Mustaniemi Moderaattori: Juha Petäjäinen
15.30 - 15.45	Tilaisuuden päättäminen, Juha Petäjäinen, VUY

Henkilöasiat:

Viestimies lehti ei julkaise puolustusvoimien henkilökunnan siirtoja ja tehtävään määräämisiä henkilösuojalain rajoitusten vuoksi.

Ylennykset 6.12.2020

Everstiksi

- everstiluutnantti **Jari Riihimäki**

Majuriksi

- kapteeni **Juha-Matti Hirvonsalo**
- kapteeni **Heikki Lähteenmäki**

Ylennykset reservissä 6.12.2020

Kapteeniksi

- yliluutnantti **Laitinen Mikko**
- yliluutnantti **Matturi Mika**

Patria 100

Patria vuodesta 1921

Sata vuotta on vahva perusta yhdessä tekemiselle ja menestymiselle.
Se on perusta turvalliselle tulevaisuudelle.

Tutustu sataan tarinaan osoitteessa
patriagroup.com

Yhteydet maastoon Nestorin tuotteilla

Nestor Cablesin valikoimasta löytyvät vaativaan kenttäkäyttöön soveltuvat valokaapelit väliaikaisten verkkojen rakentamiseen. Kaapelit ovat saatavilla erilaisilla liitinvaihtoehdoilla, ja niiden lisäksi valikoimassa ovat myös asennuslaitteistot sekä huolto-tarvikkeet. Kenttäkaapelituotteita voidaan hyödyntää myös erilaisissa siviilitapahtumissa.

nestor cables

www.nestorcables.fi
info@nestorcables.fi
Puh. 020 791 2770

Mittarikuja 5,
90620 Oulu
PL 276, 90101 Oulu