Monikansallinen suorituskykyjen kehittämisohjelma kyberpuolustuksen tukena

Johdanto

Tasavallan presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta päättivät 8. maaliskuuta 2011 pidetyssä yhteisistunnossaan käynnistää kansallisen kyberturvallisuusstrategian laatimisen. Vuonna 2013 julkaistun strategian mukaan Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.

Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Ilmaus on sikäli osuva, että Puolustusvoimat oli jo strategian kirjoittamisen aikaan osallisena Yhdysvaltain johtamassa monikansallisessa suorituskykyjen kehittämisohjelmassa. Kehittämisohjelman tutkimus-, kokeilu- ja kehittämistehtävien kohteena eivät ole materiaaliset kyvykkyydet vaan korostetusti käyttöperiaatteet ja toimintatapamallit.

Strategian kirjoittamisen aikaan ohjelmasta käytettiin nimitystä Multinational Experiment MNE, ja tuolloin oli käynnissä ohjelman seitsemäs kaksivuotinen toimikausi MNE-7. Ohjelman rakenteita ja käytänteitä on sittemmin päivitetty ja nykyään ohjelmasta käytetäänkin nimeä Multinational Capability Development Campaign – MCDC. Tässä artikkelissa tarkastelemme erityisesti kampanjan eri kampanjajaksojen aikana tehtyä kyberpuolustusta tukevaa tutkimus- ja kehittämistoimintaa.

Kullakin kaksivuotisella kampanjajaksolla on yleisesti ohjaava pääteema, jonka ympärille muodostetaan useampia tutkimusaiheita (objective, focus area). Vuodesta 2011 lukien yksi näistä aiheista on säännöllisesti liittynyt kyberpuolustukseen. Tutkimusaihe muodostetaan ja vahvistetaan, jos jokin osallistuvista maista suostuu ottamaan sen johdettavakseen ja aiheeseen liittyy muita maita osallistujina. Tyypillisesti tutkimusaihe toteutetaan monikansallisena ryhmätyönä, johon liittyy 2–4 fyysistä tapaamista tai työpajaa vuodessa sekä omia, itsenäisiä tutkimus- ja kirjoitustehtäviä kokousten väliaikoina. Kampanjajakson loppupuolella tuotettuja vaihtoehtoja tai toimintatapamallia tyypillisesti testataan tai koestetaan lopputuotteen laadukkuuden varmistamiseksi; tästä käytetään muun muassa nimityksiä eksperimentti tai rajattu koetoimintatapahtuma (limited objective experiment).

Vaikka osallistuminen itse tuotantovaiheeseen voidaan usein toteuttaa yhden-kahden asiantuntijan toimin, koetoiminta tapahtuman järjestämiseksi ja etenkin lopputuotteen kokeilijoiksi tarvitaan usein lopputuotteen kohderyhmäksi suunnitellun henkilöstön edustajia.

MNE-7 – Outcome 3 Cyber Domain

Vuosina 2011–2012 toteutetun MNE-7-jakson tarkastelukohteena oli monikansallisten liittoumien kyky turvata pääsy ja käytettävyys yhteiskäyttöisiin toimintaympäristöihin; tämän tarkastelun kannalta ensimmäistä kertaa mukana oli myös kybertoimintaympäristö. Tutkittavien käyttö- ja toimintaperiaatteiden kohteina olivat kansainvälinen lainsäädäntö ja kybertoimintaympäristön käytännesäännöt, uhkan ja haavoittuvuuksien arviointi, tilannetietoisuus sekä tapahtumatietojen vaihto.

Puolustusvoimien osallistuminen kampanjajakson kyberhaaraan toteutettiin Pääesikunnan johtamisjärjestelmäosaston ohjauksessa ja Verkostopuolustuksen kehittämiskeskuksen johdossa. Asiantuntijoita sekä työpanostaan kybertutkimusaiheeseen asettivat myös Puolustusministeriö, Puolustusvoimien Johtamisjärjestelmäkeskus sekä Puolustusvoimien silloinen Teknillinen tutkimuslaitos.

Tämän kampanjan kybertutkimusaihe oli tähänastisista kampanjajaksoista laajin, ja Britannian johtamassa tutkimusaiheessa oli viisi alateemaa (objectives), joista Norjan, Ruotsin, Britannian ja Italian ohella Puolustusvoimilla oli osavastuunaan tutkimusaihe kyberteknologiat yhteisen kybertilannetietoisuuden tukena.

Tässä työhaarassa tuotettiin vakioidut toimintatapamallit (Standard Operating Procedures, SOP) kyberoperaatiokeskukselle mukaan luettuna tilannekuvajärjestelyn tekniset ja toiminnalliset perusteet, jotka myös koestettiin Suomessa 6.–8.2.2012 järjestetyssä rajatussa koetoimintatapahtumassa.

MCDC1314 CICOA (Cyber Implications for Combined Operational Access)

Kampanjajakson 2013–2014 pääteemana oli monikansallinen operatiivinen käytettävyys. Monikansallisen operaation suunnittelu edellyttää myös kybertoimintaympäristön tuntemista. Erityisesti monikansallisissa operaatioissa haasteena on se, että jaetun monikansallisen kybertoimintaympäristön tilanneymmärrys puuttuu eikä kybertoimintaympäristön huomioon ottavia prosesseja ollut tuolloin vielä käytettävissä.

Kampanjan kyberaiheisena tutkimustehtävänä oli Italian johdossa tunnistaa työkalut kybertoimintaympäristön tiedustelemiseksi sekä Norjan johdossa muodostaa ohjeistus kybertoimintojen huomioon ottamiseksi operatiivisessa suunnitteluprosessissa (Naton COPD-prosessi). Kybertutkimustehtävään osallistuivat tällä jaksolla Puolustusministeriö, Pääesikunnan johtamisjärjestelmäosasto, Puolustusvoimien johtamisjärjestelmäkeskus sekä Puolustusvoimien tutkimuslaitos.

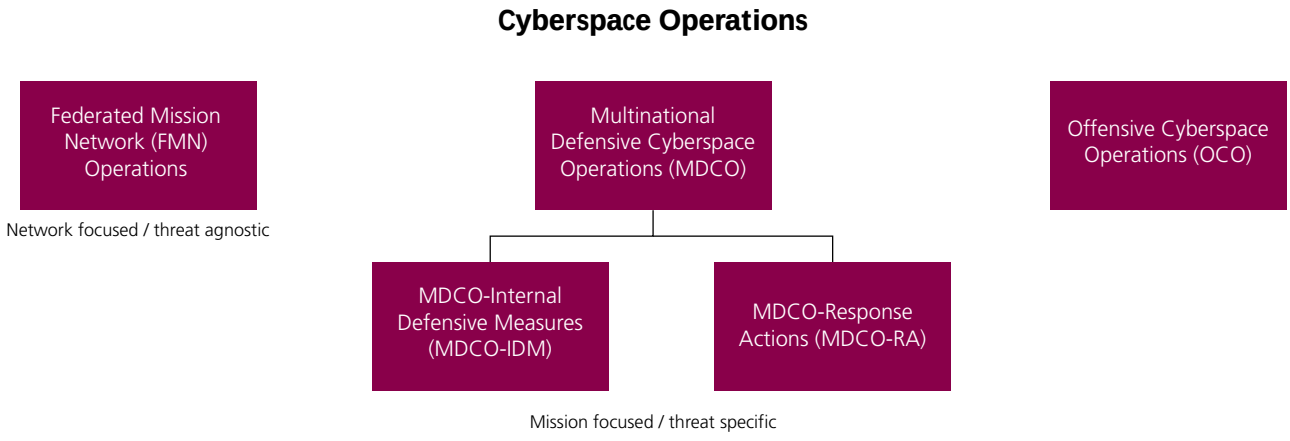
Tutkimustehtävän huipentumana voidaan pitää elokuussa 2014 Espanjan johdolla järjestettyä mittavaa ”esikuntaharjoitusta” (92 osallistujaa), jossa kaksi operaatioesikunnan ydintä (joint operational planning group, JOPG) käyttivät laadittua kyberoperaatiosuunnittelun käsikirjaa oman suunnitteluprosessinsa tukena. Harjoituskuvaus pohjautui Euroopan unionin sotilasesikunnan omaan aikaisempaan harjoitukseen, joka Euroopan puolustusviraston, EDAn, tukemana oli sovitettu kyberoperaatiosuunnittelun tarpeita tukevaksi. Esimerkkinä nostettakoon lukijoillemme EU-johtoisen operaation skenaario, jossa sotilaallisen kriisinhallintaoperaation päätavoite ja tehtävä oli turvata kuvitteellisen kriisikohteen siirtyminen demokraattiseen hallintoon. Tällöin kriisikohteen julkiset tiedotusvälineet, väestötietojärjestelmät sekä sähköinen vaalijärjestelmä muodostuvat operaation komentajalle ja operaatiolle keskeisiksi suojattaviksi kohteiksi – eikä tämä toteudu pelkästään kineettisin sotilaallisin keinoin.

MCDC1516 MDCO (Multinational Defensive Cyberspace Operations)

Monikansallisissa operaatioissa eri osallistuvilla mailla on hyvinkin erilaiset kansalliset rajoitteet osallistumiselle kyberoperaatioihin. Samalla osallistuvien maiden tekniset kyvykkyydet sekä joukkokokoonpanot ja osallistuvan henkilöstön osaaminen on hyvinkin erilaista. Näiden vuoksi operaatioon sisältyvien puolustuksellisten kyberoperaatioiden suunnittelu, johtaminen ja toimeenpano on hyvinkin haasteellista ja altista virheille.

Kampanjajakson 2015–2016 kyberaiheena oli täydentää ja syventää edellisellä jaksolla laaditun kyberoperaatiosuunnittelun ohjetta. ”Monikansallinen puolustuksellisten kyberoperaatioiden suunnitteluohje” kokoaa, mitä seikkoja operaatiosuunnittelussa tulee ottaa huomioon osana esikunnan suunnitteluprosessia valmiine lomakkeineen ja tehtävä- ja tarkistuslistoineen.

Tutkimustehtävän johti ensimmäistä kertaa Yhdysvallat, ja Puolustusvoimista osallistui tällä kertaa Puolustusvoimien tutkimuslaitos ja Puolustusvoimien johtamisjärjestelmäkeskus.



Kuva 1. Monikansallisten puolustuksellisten kyberoperaatioiden suunnitteluohjeessa käytetyt keskeiset käsitteet. (Kuva: Multinational Defensive Cyberspace Operations -ohje)

MCDC1718 ICOPC (International Cyberspace Operations Planning Curricula)

Kansainväliseen operaatioon osallistuvilta mailta puuttuvat kattavat, vakioidut ja yhteensopivat koulutusjärjestelyt, jotta kyberoperaatiosuunnittelun ripeä käynnistäminen ja tehokas toteuttaminen on mahdollista monikansallisissa operaatioesikunnissa. Kampanjajaksolle 2017–2018 kehittämisen kohteeksi valikoitui kansainvälinen kyberoperaation suunnittelun standardoitu opetusohjelma. Tavoitetilassa käytössä olisivat turvaluokittelemattomat, vakioidut ja yhteensopivat koulutukselliset tavoitteet, moduulit ja kurssit sekä yhteinen ymmärrys keskeisistä oppisisällöistä kyberoperaatiosuunnittelijoiden koulutuksen toteuttamiseksi kansallisesti.

Myös tämän kampanjan johtovastuu on ollut Yhdysvalloilla, mutta mielenkiintoista kylläkin, keskeinen pedagoginen ja opetussuunnitteluun liittyvä osaaminen saatiin sekä Kanadalta että Tanskalta. Suomesta tämän kampanjajakson tähän tutkimusaiheeseen osallistuivat Puolustusvoimien tutkimuslaitoksen lisäksi Pääesikunnan johtamisjärjestelmäosasto, Maanpuolustuskorkeakoulu sekä Jyväskylän yliopisto. Luonnosteltua opetusohjelmaa testattiin Euroopan puolustusviraston ja Itävallan yhteisesti toimeenpanemassa Cyber Phalax 2018 -koetoimintatapahtumassa toukokuussa 2018 sekä kansallisesti Maanpuolustuskorkeakoulun toimeenpanemassa kansallisessa kyberoperaatiosuunnittelun opetustapahtumassa elokuussa 2018. Opetusohjelman viimeistelemiseksi ja laadukkuuden toteuttamiseksi toteutettiin viimeinen ns. Critical Review -seminaari Jyväskylän yliopistolla syyskuussa 2018.

Kuva 2. MCDC1718 ICOPC Critical Review -seminaarin osallistujat 19.9.2018 Jyväskylän yliopistolla.
(Kuva: Jasmin Suikki / Jyväskylän yliopisto)

Pohdinta

Osallistumalla monikansallisiin suorituskykyjen kehittämiskampanjan tutkimusaiheisiin Puolustusvoimat on saanut edullisin panostuksin laadukkaita ja oikea-aikaisia suorituskykyjen kehittämistä tukevia tuotteita käyttöönsä. Toisaalta kehitys kyberpuolustussektorilla on viimeisen seitsemän vuoden ajan ollut ripeää. Onkin ilmeistä, että MNE-7-kampanjan aikana laaditut tuotteet ovat osin jo vanhentuneet. Kyberoperaatioiden kansainvälisoikeudellisen analyysikehikon on korvannut Naton kyberpuolustuksen erikoisosaamiskeskuksen CCDCOE:n toimittamat Tallinn Manual -käsikirjat (osat 1 ja 2). Tilannekuvajärjestelyjä saa tänä päivänä hankittua kaupallisesti niin palveluina kuin tuotteinakin. Sen sijaan kyberoperaatiosuunnittelun käsikirja (MCDC1314) ja sitä täydentävä puolustuksellisten kyberoperaatioiden ohjekin (MCDC1516) ovat ajankohtaisia ja käyttökelpoisia. Tätä kirjoitettaessa valmistumassa oleva opetusohjelma (MCDC1718) tukee edellisten viemistä käytäntöön Maanpuolustuskorkeakoulun opetustyön kautta. Näin tutkittu tieto saadaan siirrettyä Puolustusvoimien kokonaisvaltaisen kyberpuolustuskyvyn osaksi.

Kirjoittaja:

Yleisesikuntakomentaja Topi Tuukkanen toimii tutkimusalajohtajana Puolustusvoimien tutkimuslaitoksen informaatiotekniikkaosastossa tietoverkkosodankäynnin tutkimusalalla.