EDUSKUNNAN PUOLUSTUSVALIOKUNNALLE

HYBRIDIUHAT JA KYBERTURVALLISUUS

ASIANTUNTIJALAUSUNTO

PROF MARTTI LEHTO

6.4.2017

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

Asia: VNS 3/2017 vp Valtioneuvoston puolustusselonteko

1. Kansallinen kyberalue

Puolustusselonteossa sotilaallista toimintaympäristöä on laajennettu perinteisten maa-, meri- ja ilmatoimintaympäristöjen ohella kybertoimintaympäristöön. Näissä ympäristöissä korostuvat tiedustelukyky, eri hallinnonalojen valmius toimia nopeasti kehittyvissä tilanteissa, kyky suojautua kauaskantoisten asejärjestelmien vaikutuksilta ja kyberpuolustuskyky. Kybertoimintaympäristö ei ole muista erillinen alue vaan kyberuhat ja -hyökkäykset ilmentyvät kaikissa muissa ympäristöissä. Kansallisen puolustuksen kannalta Suomen maa- ja merialue sekä ilmatila on määritelty riittävän tarkasti, mutta meiltä puuttuu tarkkarajainen määrittely kansallisesta kybertilasta. Valtion täysivaltaisuuteen kuuluu sen alueellinen koskemattomuus. Tämän tulisi koskea myös kansallista kyberaluetta.

Selonteossa viitataan Eduskunnan ulkoasiainvaliokunnan valtioneuvoston ulko- ja turvallisuuspoliittisesta selonteosta antamaan mietintöön (UaVM 9/2016), jossa todetaan, ettei Suomi salli alueensa käyttämistä vihamielisiin tarkoituksiin muita valtioita vastaan. Tämä koskee myös kansallista kyberaluetta. Kybertoimintaympäristön erityispiirre on, että hyökkäyspalvelimet voidaan sijoittaa kolmannen osapuolen maaperälle, millä halutaan salata hyökkääjän todellinen alkuperä.

2. Hybridisodankäynnistä

2000-luvun asymmetrinen sodankäynti on luonut uuden asetelman, jossa raja perinteisen ja epätavanomaisen sodankäynnin välille on hämärtynyt. Hybridisodankäyntikäsite on hankala, koska hybridisodankäynnissä toimitaan sodan ala- ja ulkopuolella. Sodankäynti sodan ulkopuolella on vaikeasti määriteltävissä, koska kansainvälinen oikeus ei määrittele tämän tyyppistä tilannetta. Toiminta perinteisin sodankäyntikäsittein sodan ja osittain fyysisen maailman ulkopuolella virtuaalisessa kybermaailmassa on haasteellista.

Hybridisodankäynnistä on esimerkkejä, jossa kineettistä sodankäyntiä on jatkettu matalan intensiteetin kineettisten ja ei-kineettisten operaatioiden avulla. Venäjän sotatoimet Ukrainassa vuonna 2014 ovat esimerkki sodankäynnistä, jossa erikoisjoukkojen rajoitetun voimankäytön, poliittisen, sotilaallisen ja taloudellisen painostuksen, strategisen kommunikaation sekä erilaisten ei-kineettisten operaatioiden avulla on luotu epävakaa Itä-Ukrainan alue, jota Venäjä hallitsee.

Kybertaistelutila ja miehittämättömyys ovat alentaneet sodankäynnin kynnystä samalla muuttaen perinteistä sota-rauha -asetelmaa. Tähän liitettiin kylmän sodan aikana käsite harmaasta vaiheesta, jolla ymmärrettiin aikaa ennen varsinaista sotaa. Hybridisodankäynti on tuonut tilan, joka voi edeltää perinteistä sotaa, ilmetä sodan aktiivisen vaiheen jälkeen tai ilman perinteistä sodankäyntiä. Uusi sodankäynnin paradigma on syrjäyttämässä perinteisen mallin sodan julistamisesta rauhan sopimukseen luomalla tilan, jossa sotaa ei julista eikä rauhaa solmita vaan hybridisodankäynnin kohde joutuu

elämään hyvinkin pitkään konfliktin ja epävakauden keskellä, jossa yhä enenevässä määrin kybertoimintaympäristö on toiminnan kohteena.

2020-luvun sodankäyntiin sekoittuu uusia elementtejä erityisesti kybertoimintaympäristössä tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Tarkoituksellisen epävakauden ylläpito ei-kineettisten operaatioiden avulla erityisesti suurvalta voi perustella läsnäoloa ja vaikuttamista tietyllä alueella. Toimintaa perustellaan rauhanturvaamisella, tasapainon säilyttämisellä, omien etujen ja kansalaisten suojaamisella tai liittolaisten tukemisella, kaikella näennäisesti hyväksyttävällä toiminnalla. Kybertoimintaympäristö on luonut uuden tilan vaikuttaa toisen valtion alueella käyttäen hyväksi erilaisia sotilaallisia ja ei-sotilaallisia painostuskeinoja poliittisten ja sotilaallisten tavoitteiden saavuttamiseksi.

3. Kybersuorituskykyjen kehittäminen
Selonteko toteaa Puolustusvoimien jatkavan ”kyberpuolustuskyvyn kehittämistä kansallisen kyberturvallisuusstrategian mukaisesti. Puolustusvoimat rakentaa kyvyn kybertilannekuvan muodostamiseen, kyberoperaatioiden suunnitteluun ja toimeenpanoon sekä omien järjestelmien suojaamiseen ja valvontaan kybertoimintaympäristössä.”

Asevoimien uudet suorituskyvyt luovat uusia mahdollisuuksia sekä kineettiseen että ei-kineettiseen voimankäyttöön kybertilassa. Tässä tilassa tulee voida integroida saumattomasti ilmassa, pinnassa, pinnan alla ja kyberavaruudessa toimivia miehitettyjä ja miehittämättömiä alustoja. Uusien järjestelmien avulla voidaan yhä tehokkaammin havaita, seurata ja identifioida maaleja sekä johtaa joukkoja ja ohjata asejärjestelmiä halutun vaikutuksen saavuttamiseksi.

Kyberuhkiin varaudutaan ja uhkia hallitaan kehittämällä ja ylläpitämällä erilaisia tiedustelu-, suojaus- ja vaikuttamiskeinoja ja lisäksi luodaan tarvittava toipumiskyky kyberhyökkäyksistä (kyberresilienssi).

Kybertiedustelu ja -valvonta
Reaaliaikaisen tilannekuvan muodostaminen ja jaetun tilannetietoisuuden aikaansaaminen tulee olla yhä nopeampaa. Johtamisprosessissa tarvitaan sisällöltään mahdollisimman tarkkaa ja oikein aikautettua informaatiota, jotta keskitetty johtaminen ja hajautettu toiminta voidaan toteuttaa sekä suojata oma toiminta kybertaistelutilassa. Perusteet resurssien käytölle pitää syntyä vastustajaa nopeammassa päätösprosessissa tilannekuvaa ja vastustajan toimintatapoja, tavoitteita ja kyvykkyyttä analysoimalla. Tilannetietoisuuden kehittäminen edellyttää tehokasta havainnointikykyä ja siksi sotilastiedustelulaki on välttämätön kybertiedustelun ja -valvonnan suorituskyvyn kehittämisen ja ennakkovaroituksen kannalta.

Kybersuojaaminen
Puolustusvoimien tulee ensisijaisesti suojata omat järjestelmänsä ja verkkonsa. Suojaamiskyky tulee mitoittaa sellaiseksi, että se mahdollisimman tehokkaasti tukee Puolustusvoimien toimintaa alueellisen koskemattomuuden turvaamiseksi ja maan puolustamiseksi. Suojaamisen kehittämisessä korostuu yhteistoiminta Puolustusvoimien,

muiden viranomaisten sekä yhteiskunnan muiden kybertoimintaympäristön toimijoiden kanssa.

Kybervaikuttaminen
Kybervaikuttamisen kehittämisessä korostuu systeeminen ajattelu. Strategisessa ajattelussa tulee huomio kohdistaa systeemivaikutuksiin eikä yksittäisiin maaleihin. Sotilaalliset operaatiot edellyttävät tarkkaa analysointia, joiden kohteina ovat vastustajan painopisteet, kriittiset rakenteet ja elintärkeät toiminnat ja niiden haavoittuvuudet. Vain tällaista kokonaisvaltaista lähestymistapaa käyttämällä voidaan strategiset tavoitteet saavuttaa kineettisillä ja ei-kineettisillä operaatioilla. Esimerkiksi liittouman hyökkäyksessä Bagdadiin vuonna 1991 ilmahyökkäyksellä tuhottiin vain 10 % sähköverkosta, mutta aiheutettiin strateginen lamautus koko kaupungissa. Nyt tällainen strateginen lamautus on mahdollinen kyberhyökkäyksen avulla.

4. Yhteiskunnan elintärkeät toiminnat ja kyberhuoltovarmuus
Kyberhyökkäysten kohteena eivät ole vain asevoimat vaan yhteiskunnan elintärkeät toiminnat. Yhteiskunnan elintärkeät toiminnat on pystyttävä turvaamaan kaikissa tilanteissa. Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja siksi kriittisen infrastruktuurin kyberympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella. Näin kansallisesta kyberpuolustuksesta muodostuu kiinteä osa kokonaismaanpuolustusta.

Suomella on hyvä perinne huoltovarmuuden järjestämisessä. Kyberhuoltovarmuutta ja -omavaraisuutta tulee kehittää osana tätä työtä. Kyberhuoltovarmuuden ja -omavaraisuuden avulla luodaan kyky ylläpitää yhteiskunnan elintärkeitä perustoimintoja väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen toiminnan turvaamiseksi vakavissa häiriötilanteissa ja poikkeusoloissa. Kyberhuoltovarmuus- ja omavaraisuus edellyttävät ensisijaisesti riittävän kyberosaamisen turvaamista sekä Puolustusvoimissa että koko yhteiskunnassa. Riittävä määrä huippuosaajia tarvitaan luomaan tehokasta kansallista kyvykkyyttä. Samalla mahdollistetaan kansainvälisistä toimijoista riippumaton kyberturvallisuustuotteiden ja -palveluiden suunnittelu-, kehittämis- ja tuotantokyky Suomessa erityisesti turvallisuustoimijoiden käyttöön.

5.Kansallinen kyberpolitiikka
Kansainvälisessä politiikassa painottuu nykyisin kyberasioiden poliittinen luonne (cyberpolitics), mikä kuvaa kybertoimintaympäristön ensisijaista ymmärrystä nimenomaan poliittisena toimintaympäristönä. Kyberturvallisuuden asiat ovat esillä yhä laajemmin ja vahvemmalla painoarvolla kansainvälisillä foorumeilla ja järjestöissä, kuten ETYJ:ssä, EU:ssa, NATO:ssa, OECD:ssä ja Eurooppa-neuvostossa. Kansainvälisillä yhteistyöfoorumeilla ja valtioiden kahdenvälisissä suhteissa vaikuttaminen on yksi keskeinen keino edistää Suomen kyberturvallisuuden kannalta myönteisiä asioita.

Suurvallat ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin. Toistaiseksi kyberoperaatiot on tulkittu niin sanotuiksi

pehmeiksi toimiksi, minkä vuoksi niiden käyttökynnys on alempi kuin perinteisten sotilasoperaatioiden.

Kybertoimintaympäristö onkin muuttanut perinteisiä kansainvälisiä valta-asetelmia. Se antaa pienillekin valtioille ja ei-valtiollisille toimijoille mahdollisuuden toimia tehokkaasti. Kybermaailmassa suuruus ja massa eivät enää ole hallitsevia, vaan osaaminen. Kybertoimintaympäristössä tapahtuva kansainvälinen kehitys lisää uusien uhkien mahdollisuutta meitä vastaan. Julkishallintoon ja elinkeinoelämään kohdistuu jatkuvia järjestelmähaavoittuvuuksien hyväksikäyttö- tai murtoyrityksiä. Hyökkäyksissä korostuu ammattimaisuus, mikä näkyy hyökkäysmenetelmien tehokkuudessa ja kohdistuksessa.

Kybermaailman avoimuus mahdollistaa hyökkäykset eri puolilta maailmaa käyttäen hyväksi järjestelmien haavoittuvuuksia, joita on niin ihmisten toiminnassa, organisaatioiden toimintaprosesseissa kuin käytettävässä informaatioteknologiassa. Monimutkaisia ja kehittyneitä haittaohjelmia vastaan on vaikea suojautua. Hyökkääjiä on vaikea tunnistaa tai löytää heidän todellista identiteettiä. Kyberturvallisuuden tuottaminen alkaakin Suomen ulkopuolelta, joten kansainvälinen yhteistyö on olennaisen tärkeää.

Professori, ST Martti Lehto
Informaatioteknologian tiedekunta
Jyväskylän yliopisto
martti.lehto@jyu.fi