EDUSKUNNAN PUOLUSTUSVALIOKUNNALLE

KYBERMAAILMA JA TIEDUSTELU

ASIANTUNTIJALAUSUNTO

PROF MARTTI LEHTO

20.2.2018

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

Asia: HE 198/2017 vp, HE 199/2017 vp, HE 202/2017 vp, HE 203/2017 vp

1. TURVALLISUUSYMPÄRISTÖN MUUTOS

Euroopan komissio analysoi pohdinta-asiakirjassaan kesällä 2017 tulevaisuuden uhkamaailmaa. Sen mukaan teknologian kehitys muuttaa merkittävästi niin turvallisuuden kuin maanpuolustuksen luonnetta. Big data, pilviteknologia, miehittämättömät alustat ja tekoäly mullistavat puolustussektoria vahvistaen myös siviiliteknologian merkitystä puolustusalalla. Tämän verrattain helposti saatavilla olevan uuden teknologian käyttö mahdollistaa epätavanomaisten, valtioiden rajat ylittävien ja epäsymmetristen uhkien nopean kasvun. Näitä ovat muun muassa hybridi- ja kyberuhat, terrorismi sekä kemialliset, biologiset ja radiologiset iskut.

Hallituksen esityksessä (HE 203/2017 vp) on selkeästi esitetty nykytila ja toimintaympäristön muutos. Kybertoimintaympäristössä tietoverkossa toteutettavia hyökkäyksiä voidaan käyttää myös poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella. Esimerkit maailmalla osoittavat, että kybermaailmasta voidaan ei-kineettisin hyökkäyksin vaikuttaa fyysiseen toimintaympäristöön. Uhkien kansainvälisestä luonteesta seuraa, että niiden taustalla olevat tahot ovat verkostoituneet eri maiden alueelle ja osalliset kommunikoivat yli valtiorajojen.

2. HYBRIDISODANKÄYNNISTÄ

2000-luvun asymmetrinen sodankäynti on luonut uuden asetelman, jossa raja perinteisen ja epätavanomaisen sodankäynnin välille on hämärtynyt. Hybridisodankäynnistä on esimerkkejä, jossa kineettistä sodankäyntiä on jatkettu matalan intensiteetin kineettisten ja ei-kineettisten operaatioiden avulla. Venäjän sotatoimet Ukrainassa 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.

Kybertoimintaympäristö on luonut uuden tilan vaikuttaa toisen valtion alueella käyttäen hyväksi erilaisia sotilaallisia ja ei-sotilaallisia painostuskeinoja poliittisten ja sotilaallisten tavoitteiden saavuttamiseksi.

3. KYBERTAISTELUYMPÄRISTÖ

Valtioiden kybersodankäynnin kyvykkyydet tulevat edelleen kehittymään sekä hyökkäysten laajuudessa että edistyksellisyydessä. Valtioiden tekemät kyberhyökkäykset tulevat vaikuttamaan poliittisiin suhteisiin sekä valtarakennelmiin ympäri maailmaa. Lisäksi valtiollisten toimijoiden käyttämät kybertyökalut valuvat jollakin aikavälillä myös kyberrikollisryhmien käyttöön.

Kyberoperaatioissa korostuu vaatimus toiminnan nopeudesta, laajuudesta ja vaikuttavuudesta. Kybersodankäynnissä ei ole näkyviä rintamalinjoja vaan sodankäynti tapahtuu kaikkialla kybertilassa. Kyberhyökkäykset ja hyökkäysvektoreiden muutokset ovat

hyvin nopeita ja toiminnassa on siirrytty päivä- ja tuntiluokasta minuutteihin ja sekunteihin.

Tulevaisuudessa kybertaisteluista voi tulla merkittävämpiä kuin taisteluista fyysisessä maailmassa. Joka tapauksessa raja rauhan ja sodan välillä hämärtyy toimittaessa kybertoimintaympäristössä. Digitalisaation vahvistuessa ja yhteiskuntien riippuvuuden kasvaessa kriittisestä infrastruktuurista kyberhyökkäysten kohteena kehittyy keskeinen tekijä tulevissa konflikteissa ja sodankäynnissä. Älykkyyden kehittyessä osaava toimija voi pienilläkin resursseilla luoda huipputason kyvykkyyttä kybertaistelukentälle.

Useat valtiot kehittävät kykyään toteuttaa operaatioita kyberavaruudessa maan, meren, ilman ja avaruuden lisäksi osana sotilaallista voimankäyttöä. Suorituskyky perustuu **tiedusteluun ja vaikuttamiseen**. Tiedustelulla pyritään selvittämään kohteen järjestelmien ja verkkojen kokoonpanoa ja haavoittuvuuksia sekä vastapuolen kykyä suorittaa kyberoperaatioita. Vaikuttamisen tavoitteena on saada aikaan haluttu poliittinen ja/tai sotilaallinen vaikutus vastapuolen järjestelmien ja verkkojen kautta.

Kybersodankäynnin strategisen tason kyberoperaatioissa valtio pyrkii vaikuttamaan toisen valtion sekä toimintaan että toimintakykyyn. Operatiivisella ja taktisella tasolla kyberoperaatioita suoritetaan osana muuta sotilaallista voimankäyttöä. Tavoitteena voi esimerkiksi olla sotilaallisen johtamisen häiritseminen, lamauttaminen tai harhauttaminen tai sotilaallisen voimankäytön estäminen tai viivästyttäminen.

Viimeisen yli kymmenen vuoden aikana kyberoperaatiot ovat olleet ja ovat edelleen osa valtioiden välisiä kriisejä ja konflikteja. Tunnetuimmat esimerkit ovat ja Viron (2007), Georgian (2008) ja Ukrainan (2014) tietojärjestelmiin kohdistetut verkkohyökkäykset, joiden taustalla arvioidaan olleen valtiollisia toimijoita tai niihin läheisesti liittyviä tahoja. Näiden lisäksi kaikki paikalliset ja alueelliset konfliktit sisältävät kyberelementin mm. Israelin ja Palestiinan sekä sitä tukevien maiden välillä, Koreoiden välillä, Syyriassa jne.

Tällä hetkellä kyberhyökkäysten monimutkaisuus, tehokkuus ja kyvykkyys kasvavat nopeammin kuin puolustuskyky. Kybertaistelutila, uudet teknologiat ja miehittämättömyys ovat alentaneet sodankäynnin kynnystä muuttaen siten koko toimintaympäristön luonnetta.

4. KYBERTIEDUSTELUN MAAILMA

Tiedustelun siirtyminen verkkoon on tapahtunut samassa tahdissa yhteiskuntien digitalisaation kanssa. Kybertiedustelun voimakkaan kasvun alku ajoittuu 2000-luvun puoliväliin. Kehittyneimmille vakoiluohjelmille on ollut tyypillistä, että ne on havaittu vasta vuosia operaation alkamisesta.

Vuonna 2011 havaittiin siihen saakka merkittävin verkkovakoiluoperaatio. Operaatiossa Shady RAT onnistuttiin tunkeutumaan 72 järjestön, yrityksen ja hallituksen järjestelmiin pääasiassa länsimaissa. Toiminta oli jatkunut jo viiden vuoden ajan.

Samana vuonna havaittiin verkossa Duqu-haittaohjelma, joka keräsi tietoa teollisuuslaitoksista kyberhyökkäysten valmistelemiseksi. Duqun arvioitiin toimeen verkossa neljä vuotta.

Vuonna 2012 löydettiin Flame-haittaohjelma, joka hyvin monipuolisesti kykeni käyttämään saastuttamansa tietokoneen resursseja. Se oli ensimmäinen usean megatavun kokoinen haittaohjelma, kun aikaisemmin ohjelmat ovat olleet kooltaan satoja kilotavuja. Haittaohjelmatartunnat keskittyivät Lähi-Itään. Tämän ohjelman arvioitiin toimineen verkossa viisi vuotta.

Vuonna 2013 raportoitiin NetTraveler-haittaohjelmasta, joka oli ollut toiminnassa vuodesta 2004. Tässä ainakin vuoteen 2016 jatkuneessa operaatiossa kohteena on ollut yli 350 organisaatiota 40 maasta. Hyökkäyskohteita ovat olleet avaruus-, nano, energia-, ydin-, laser- ja tietoliikenneteknologian sekä farmasian tietovarannot.

Vuonna 2014 havaittiin Regin-haittaohjelma, joka oli ollut käytössä jo vuodesta 2008 asti. Regin on enemmän ohjelmisto kuin yksittäinen ohjelma ja se oli tuolloin historian kehittynein ja monipuolisin. Tämä monitasoinen vakoiluohjelma kykeni hallitsemaan kohdettaan täydellisesti ja leviämään tehokkaasti. Kohteita oli ainakin 14 maassa.

Vuonna 2015 Yhdysvaltain Office of Personnel Management (OPM) ilmoitti, että se oli joutunut tietomurron kohteeksi, jossa siltä anastettiin noin 21,5 miljoonan liittovaltion työntekijän (nykyisiä ja entisiä) henkilörekisteritietoja kuten sosiaaliturvatunnus, nimi, syntymäaika ja -paikka sekä osoite.

Vuonna 2016 raportoitiin Remsec-haittaohjelma-alustasta (ProjectSauron). Sen arvioidaan toimineen vuodesta 2011. Kohteita sillä on ollut ainakin 30 useassa maassa ja se kykenee asentamaan takaovia, varastamaan tietoja ja tallentamaan näppäimistön käyttöä.

Vuonna 2017 kiristyshaittaohjelma WannaCry:tä seurannut haittaohjelma Petya levisi nopeasti ympäri maailmaa ja lamautti IT-järjestelmiä erityisesti Ukrainassa, mutta myös kymmenet yritykset ympäri maailmaa joutuivat kohteeksi. Petya naamioitiin kiristyshaittaohjelmaksi, mutta lunnaiden vaatiminen oli vain savuverho. Hyökkäyksen todellinen tarkoitus oli lamauttaa yhteiskunnan kriittisiä toimintoja ja aikaansaada poliittista epävakautta tai ainakin testata hyökkäysoperaation toimivuutta. Tämä valtiollisen toimijan toteuttama monivaiheinen hyökkäys oli myös osoitus hyökkääjän kyvykkyydestä – tuotettiin pelotevaikutusta.

Keskeistä kybertiedustelun kehitykselle on ollut haittaohjelmien monimutkaisuuden ja kyvykkyyden kasvu samalla kun niiden havaitseminen on käynyt yhä vaikeammaksi.

5.KANSALLINEN KYBERPOLITIIKKA

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 identiteettiään ja motivaatiotaan. Tämä kehityskulku edellyttää kansallista strategisen tason analysointikyvykkyyttä, jotta meihin kohdistuva toiminta voidaan aikaisessa vaiheessa luotettavasti havaita ja sekä toiminta että toimijat identifioida.

Kyberturvallisuuden tuottaminen alkaa Suomen ulkopuolelta, joten kansainvälinen yhteistyö on olennaisen tärkeää myös tiedustelutoiminnassa.

KYBERTIEDUSTELU JA -VALVONTA – TILANNEYMMÄRRYKSEN PERUSTA

Uhat kybertoimintaympäristössä tulee nähdä osana hybridivaikuttamista ja siltä suojatumista. Tämä edellyttää valtioilta vahvaa ja keskitettyä havainnointi-tilannekuva-johtaminen -kyvykkyyttä.

Reaaliaikaisen kybertilannekuvan 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 vastatoimenpiteiden käytölle pitää syntyä vastustajaa nopeammassa päätösprosessissa omaa tilannekuvaa ja vastustajan toimintatapoja, tavoitteita ja kyvykkyyttä analysoimalla. **Tilannetietoisuus on kaiken toiminnan perusta** ja sen kehittäminen edellyttää tehokasta havainnointikykyä ja siksi sotilastiedustelulaki on välttämätön kybertiedustelun ja -valvonnan suorituskyvyn kehittämisen ja ennakkovaroituksen kannalta.

Sotilastiedustelu perustuu Puolustusvoimien lakisääteiseen tehtävään puolustaa valtakunnan itsenäisyyttä ja alueellista koskemattomuutta. Sotilastiedustelu kohdistuu Suomen ulkopuoliseen toimintaympäristöön ja sieltä lähtöisin olevaan uhkaan. Sotilastiedustelun tehtävänä on muodostaa ja ylläpitää sotilaallisen päätöksenteon edellyttämää sotilasstrategista tilannekuvaa.

Sotilastiedustelulaki antaa selkeät ja riittävän tarkkarajaiset perusteet em. toimintaan. Laki määrittää riittävällä tarkkuudella sotilastiedustelun kohteet ja tiedusteluun liittyvän suhteellisuusperiaatteen, jossa keskeisenä periaatteena on kansalliseen turvallisuuteen kohdistuva uhka. Tarkkarajaisuutta osoittaa mm. se, että tietoliikennetiedustelussa tiedustelu kohdennettaisiin tuomioistuimen luvassa määrättyihin viestintäverkon osiin, kuten Suomen rajan ylittävän valokaapelin sisältämään yksittäiseen kuituun, kuitupariin tai aallonpituuteen (kanavaan) ja vain pieni osa liikenteestä seulotaan tuomioistuimen myöntämien hakuehtojen perusteella.

Laissa on määritelty tiedustelumenetelmien käytön yleiset edellytykset. Lain mukaan tiedustelumenetelmiä käytetään, kun niillä voidaan perustellusti olettaa saatavan tietoa tiedustelutehtävän kannalta ja lisäksi menetelmien käytölle on asetettu ajallisia rajoituksia (keräyslupa myönnetään vain rajoitetuksi ajaksi, 6 kk).

Laissa on kuvattu seikkaperäisesti eri tiedustelumenetelmät, päätöksentekoprosessi ja toimintaan liittyvä laillisuusvalvonta. Suomalaisen kansalaisyhteiskunnan kannalta laki antaa riittävän turvan kansalaisten yksityisyydelle. Tiedusteluviranomaisten lainmukainen pääsy tietoliikenteeseen ei vaaranna kansalaisen yksityisyyden suojaa. Kohdennettu valvonta on tehokkainta tiedustelutehtävien tavoitteiden saavuttamisen kannalta.

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