MAANPUOLUSTUSKORKEAKOULU

KYBERHYÖKKÄYKSEN VAIKUTUKSESTA

Tutkielma

Kadetti
Rami Said

98. Kadettikurssi
Maasotalinja

Maaliskuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
98. Kadettikurssi	Maavoimien johtamisjärjestelmä
Tekijä	
Kadetti Rami Said	
Tutkielman nimi	
Kyberhyökkäyksen vaikutuksesta	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka MPKK (Kurssikirjasto)
Aika maaliskuu 2014	Tekstisivuja 21

TIIVISTELMÄ

Tutkielmassani tutkin kyberhyökkäyksen vaikutuksia.

Päätutkimuskysymys on: *Mitä tapahtuu kyberhyökkäyksen aikana?*
Päätutkimuskysymystä tukevia alakysymyksiä ovat:

- *Mitä tarkoittaa kyberhyökkäys?*
- *Miten kyberhyökkäyksen vaikutuksia voi ennaltaehkäistä?*
- *Mitä kyberhyökkäyksissä on tapahtunut 2000-luvulla?*

Käytettävänä tutkimusmenetelmänä on laadullinen kirjallisuustutkimusmenetelmä. Tutkimuksen aineistona on ruotsin-, englannin- ja suomenkielistä kirjallisuutta, internetlähteitä sekä aikakauslehtiä.
Keskeisinä johtopäätöksinä havaittiin, että kyberhyökkäyksen vaikutus yhteiskunnalle voi olla merkittävän suuri ja oikeanlaisten kyberstrategisten ratkaisujen ja ennaltaehkäisyn avulla voidaan suojautua huomattavilta yhteiskunnallisilta tappioilta.

AVAINSANAT
Kybersodankäynti, kyberhyökkäys, kyberavaruus, taistelukenttä, tietoverkko, tilannekuva, elektroninen sodankäynti, elektroninen vaikuttaminen, elektroninen suojautuminen

KYBERHYÖKKÄYKSEN VAIKUTUKSESTA TAKTISELLA TASOLLA

SISÄLLYS

KYBERHYÖKKÄYKSEN VAIKUTUKSESTA

1 JOHDANTO

Viime ajat ovat osoittaneet kaikkien palveluiden olevan haavoittuvia kyberhyökkäyksiä vastaan. Jos hyökkäykselle ei ole järkevää perustetta, saattaa hyökkääjä tehdä sen huvikseen tai edistääkseen muuten omia tarkoitusperiään. Puolustautumiseen on kannattavaa panostaa, erityisesti jos vahingon määrä hyökkäyksen toteutuessa on merkittävä. [7, s. 16]

Suomen kyberturvallisuus kokonaisuutena rakentuu elinkeinoelämän varaan, koska suurin osa kriittisestä yhteiskunnan infrastruktuurista on yksityisen sektorin omistuksessa. Puolustusvoimat voi lisäksi omassa toiminnassaan hyödyntää yhteiskunnan – niin yritysten kuin yksityisten henkilöiden – osaamista.

– Aika paljon voidaan yritysten varaan laskea puolustuksessa. Tekninen osaaminen järjestelmien ja laitteiden osalta, joita yritys itse tuottaa, on paras siellä itse yrityksessä, puolustusvoimien johtamisjärjestelmäpäällikkö, prikaatikenraali Ilkka Korkiamäki toteaa.

Yksi kyrberuhkiin varautumisen tärkeä osa-alue puolustusvoimissa on harjoitustoiminta. Mittava varautumisharjoitus oli syyskuun lopulla Riihimäellä järjestetty tietojärjestelmäalan valmiusharjoitus T13TO. Tänä vuonna harjoitus pureutui toimijoiden yh-

teistyön sujuvuuteen kyberuhkatilanteissa. Korkiamäen mukaan harjoituksessa kuvattiin pelitoiminnalla tilanteita, joiden mukaan harjoitusorganisaatio toimi.

– Pyrimme saamaan harjoitukseen vastavuoroisuutta. Tietyllä tavalla tämä oli casetoimintaa, mutta kyseessä oli jatkuva tilanne, johon organisaation toimenpiteillä oli vaikutusta. Pelikuvaus kesti noin puolitoista vuorokautta yhtä mittaa, Korkiamäki sanoo. Harjoitukseen osallistui yli sata organisaatiota ja yli 200 henkilöä. Ministeriöiden ja virastojen ohella mukana oli yrityksiä ja yhteisöjä esimerkiksi tietotekniikan, liikenteen, terveydenhuollon ja logistiikan alalta. [12, s. 3]

1.1 Tutkimuksen tausta, aiempi tutkimus aiheesta, tutkimuskysymykset ja päämäärä

Tutkimuksen taustana on johtamisjärjestelmäopintosuunnan valintaa seurannut looginen sotatekniikan pääainevalinta. Tästä edelleen seurasi mielenkiinto uutta aihetta kohtaan, jota ei Suomessa ole paljon tutkittu. Aiheesta löytyi lähinnä englanninkielisiä verkkojulkaisuita ja joitakin niteitä. Tutkimuksen valintaan vaikutti myös tutkijan suppea käsitys aihealueesta ja halu kehittää omaa tietämystä.

Päätutkimuskysymys on:

- *Mitä tapahtuu kyberhyökkäyksen aikana?*

Päätutkimuskysymystä tukevia alakysymyksiä ovat:

  - *Mitä tarkoittaa kyberhyökkäys?*
  - *Miten kyberhyökkäyksen vaikutuksia voi ennaltaehkäistä?*
  - *Mitä kyberhyökkäyksissä on tapahtunut 2000-luvulla?*

Tutkimuksen tavoitteena on laajentaa näkemystä kybersodankäynnistä yleisellä tasolla. Tavoitteena on etsiä vastauksia tutkimuskysymyksiin ja koota johdonmukaiset päätelmät tutkielman loppuun.

1.2 Tutkimusmenetelmä ja tutkimuksen rakenne

Tutkimuksessa käytettävä tutkimusmenetelmä on laadullinen kirjallisuustutkimusmenetelmä.

Tutkimus alkaa johdannolla, jossa käsitellään tausta ja päämäärä sekä kerrotaan päätutkimuskysymys ja tutkimuskysymykset. Johdannossa kerrotaan käytettävä tutkimusmenetelmä ja avataan tärkeimmät käsitteet. Johdannon lopussa rajataan aihe.

Toisessa luvussa puretaan kyberhyökkäyksen määritelmä ja erotellaan se elektronisesta sodankäynnistä. Kolmannessa luvussa analysoidaan kyberhyökkäyksen aikana tapahtuvia asioita ja paneudutaan kyberhyökkäyksen ennaltaehkäisyyn sekä torjumiseen ja siltä suojautumiseen. Neljännessä luvussa esitellään esimerkkejä tapahtuneista tunnetuista kyberhyökkäyksistä maailmalla 1900- ja 2000-luvulla. Lopuksi kootaan johdonmukaiset päätelmät johtopäätöksiin.

1.3 Tärkeimmät käsitteet

Tutkimuksen keskeisimmät käsitteet ovat kybersodankäynti, kyberhyökkäys, kyberavaruus, taistelukenttä, tietoverkko, tilannekuva, elektroninen sodankäynti, elektroninen vaikuttaminen, elektroninen suojautuminen. Alla esitellään käsitteet lyhyesti.

Kybersodankäynti:

Kybersodankäynti on jatkuvasti kehittyvä sodankäynnin ala. Useiden eri kyberhyökkäysten muodostama kokonaisuus vaihdellen sisäisistä hyökkäyksistä valtionjohtoa vastaan ulkoisiin hyökkäyksiin, joiden tavoitteena voi olla strategisen tason internetsivujen käytön estäminen. Ulkoisten hyökkäysten taustalla voi olla jopa kokonaisia valtioita. [1, s. 39]

Kybersodankäynnin tavoitteena on häiritä, estää käyttöä tai tuhota tietoa sisältäviä tietokoneita tai tietokoneverkkoja. Kyberavaruudessa käytävä sodankäynti on kilpailijan tiedon ja tietojärjestelmien muokkaamista jälkiä jättämättä. [2, s. 29]

Kyberhyökkäys:

Kyberhyökkäys tarkoittaa tietokoneiden, tietoverkkojen tai niiden sisältämän tiedon käytön häiritsemiseen, estämiseen, laitteiden hajottamiseen tai tuhoamiseen tähtäävää toimintaa. [2, s. 170]

Kyberavaruus:

Tietoverkon sähköinen tietotila, jossa eri tietojärjestelmien välinen viestintä on mahdollista. Kyberavaruutta kuvaillaan myös keinotekoisesti ja tietokoneellisesti luoduksi todellisuudeksi. [6, s. 17]

Taistelukenttä:

Historiassa taistelukenttä on vastannut käytännössä maata ja merta. Uusia ulottuvuuksia ovat ilma, fyysinen avaruus ja kyberavaruus [10, s. 26-29]. Tutkielmassa taistelukentällä ei tarkoiteta ainoastaan tilaa, jossa ihmisen on fyysisesti mahdollista liikkua, vaan myös aluetta, jossa tieto liikkuu.

Tietoverkko:

Tietoverkko on tietokoneita ja laitteita yhdistävä kanava tiedonjakoa ja tiedon varastointia varten. Yksi tunnetuimmista tietoverkoista on internet. [3, s. 22]

Tilannekuva:

Nykyaikaisen taistelun voittamisen perusedellytys, joka muodostuu omien ja vastustajan joukkojen tilanteesta, ympäristöstä ja muista osapuolista. Tilannetietoisuus edellyttää viimeisintä, korrektia ja kattavaa tilannekuvaa eri johtoportaissa. Tilannekuvan on perustuttava kaikkialla samaan tietoon. Tämän edellytyksenä ovat reaaliaikaiset viestiyhteydet. [5, s. 215]

Elektroninen sodankäynti:

Hyökkääminen vihollista vastaan tai elektromagneettisten kohteiden hallitseminen hyödyntäen elektromagneettista energiaa jollain sotilastoimella. Pääalalajit ovat elektroninen vaikuttaminen (ELVA), elektroninen suojautuminen (ELSU) ja elektroninen tuki (ELTU). [2, s. 172]

Elektroninen vaikuttaminen:

Elektroninen vaikuttaminen on elektronisen sodankäynnin osa-alue. Siinä käytetään hyväksi elektromagneettista, kohdistettua energiaa tai hakeutuvia aseita henkilöstöä, rakennettuja kohteita tai varusteita vastaan tarkoituksena hajottaa, lamauttaa tai tuhota vihollisen kyky käydä taistelua. Lyhennetään ELVA. Elektroninen vaikuttaminen sisältää keinot vihollisen elektromagneettisen spektrin tehokkaan käytön estämiseksi tai vaikeuttamiseksi sekä elektromagneettista tai kohdistettua energiaa ensisijaisena tuhoavana koneistonaan käyttävien aseiden kuten lasereiden, radioaaltoaseiden ja hakeutuvien aseiden käytön. [2, s. 172]

Elektroninen suojautuminen:

Elektroninen suojautuminen sisältää keinot henkilöstön, rakennettujen kohteiden ja varusteiden suojaamiseksi ulkopuolisen tahon elektronista sodankäyntiä vastaan tämän pyrkiessä hajaannuttamaan, lamaannuttamaan tai tuhoamaan oman taistelukyvyn. Lyhennetään ELSU. [2, s. 172]

1.4 Aiheen rajaus

Aihe rajautuu kyberhyökkäyksen vaikutuksiin yleisellä tasolla. Tutkimuksessa ei syvennytä yksittäisiin laitteisiin tai johtamisjärjestelmäsovelluksiin, vaan pysytellään yleisellä tasolla. Tutkielmassa painottuu laajemman tukirakenteita vastaan tehdyn kyberhyökkäyksen vaikutus yhteiskuntaa vastaan sekä ennalta ehkäisevä toiminta strategisella tasolla yleisten toimintamahdollisuuksien takaamiseksi. Elektroninen sodankäynti sisältäen elektroninen vaikuttaminen ja suojautuminen käsitellään lyhyesti.

2 KYBERHYÖKKÄYKSEN MÄÄRITELMÄ

Inhimillinen tekijä vaikuttaa merkittävästi erityisesti taktisella tasolla. Informaatioylivoima tarkoittaa koko taistelutilassa olevan tiedon hallitsemista. Perinteisen elektronisen sodankäynnin kenttä on laajentumassa kyberavaruutta laajempaa informaatioavaruutta kohti. Informaatioylivoiman saavuttamiseksi on hallinnoitava taistelutilassa olevaa tietoa. Informaatiorakenteet on suunniteltava tukemaan viestitaktiikkaa. Tiedosta on tullut hallitsemisen arvoinen resurssi, jota voi käyttää aseena. Tulevaisuuden taistelukentällä tavoitteena on joukkojen tuhoamisen sijaan johtamisjärjestelmien tuhoaminen. [5]

Kun molemmilla taistelevilla osapuolilla on kolme tietoverkkojen suomaa etua, tilannetieto, paikannuskyky ja kyky johtaa hajautettuja joukkoja yhtenäisesti, ratkaisevaa taistelussa on löytää ja tuhota vastapuolen fyysinen voima. Käytännössä hyökkäämisen pitäisi muodostua tärkeämmäksi kuin suojautuminen hajauttamalla. Jos näin olisi, molemmat verkottuneet osapuolet olisivat haavoittuvaisempia verrattuna taisteluun ilman kybertukea. Paremmalla kybertuella varustautuneella joukolla on paremmat mahdollisuudet löytää ja tuhota vastapuoli, mutta ensimmäinen olisi haavoittuvampi ja heikompi, jos sitä vastassa olisi kybertuella varustautumaton vihollinen.

Nopean päätöksenteon merkitys taktisella tasolla tulee korostumaan. Ajan ja tiedon hallinta on elintärkeää voiton sekä nerokkaan taktisen ajattelun ja päätöksenteon

kannalta. Voitto lankeaa sille, jolla on paras yhdistelmä onnea, yllätyksellisyyttä, virheenhallintaa ja korkealle koulutettu henkilöstö [10, s. 62-63].

2.1 Elektroninen sodankäynti vs kybersodankäynti

Kybersodankäynti on informaatiosodankäyntiä kyberavaruudessa. Kyberavaruus viittaa tietokonejärjestelmiin, tietoverkkoihin, viestintäjärjestelmiin ja kaikkiin niiden tukemiin rakenteisiin ja toimenpiteisiin. Sillä vaikutetaan tietojärjestelmiin, tiedonsiirtoon tai tietoon itseensä sekä suojataan omaa tietoa, tietojärjestelmiä ja tiedonsiirtoa. [3, s. 13]

Elektroninen sodankäynti on tiedon valvomista ja keräämistä elektronista säteilyä käyttävistä tai lähettävistä järjestelmistä, näihin järjestelmiin vaikuttamista tai järjestelmien suojaamista. [3, s. 12-13]

2.2 Elektroninen vaikuttaminen ja suojautuminen

Taistelun alkamista edeltää usein tehokas viestijärjestelmien tiedusteleminen sekä häirintä-, harhautus- ja tuli-iskuyritykset. [5, s. 133]

Jokaisen viestivälineen käyttäjän tulee osata omat suojautumismenetelmänsä. Yksittäisistä elementeistä koostuva kokonaisuus on vain siten suojattavissa oikealla hetkellä. Muistettavia perusasioita ovat:

1. Toimintaympäristö
2. Käytettävän viestintäjärjestelmän suorituskyky
3. Vastustajan suorituskyky
4. Vastustajan päätöksenteon ja johtamisen ennakointi
5. Viestijärjestelmän rakenteen salaaminen
6. Viestijärjestelmän muutosten salaaminen
7. Viestijärjestelmän osien määrän salaaminen
8. Aikautuksen salaaminen
9. Liikkeellä tai linnoittautumisella suojautuminen

Ensimmäisenä on suojauduttava tiedustelulta, sitten tuhoutumiselta ja kolmanneksi häirinnältä. Ajan merkitys on huomioitava. Nopeampi osapuoli taistelussa säilyttää todennäköisemmin johtamiskykynsä. [5, s. 133-134]

3 KYBERHYÖKKÄYS

Kyberhyökkäys voidaan jakaa kahteen osaan: hyökkäyksiin infrastruktuuria vastaan ja hyökkäyksiin tietolähteitä vastaan. [6, s. 51]

Yhdysvallat määrittelee kyberhyökkäyksen tavoitteiksi tietokoneen, tietoverkon tai niissä olevan tiedon häiritsemisen, estämisen, muokkaamisen tai tuhoamisen. Tämän taka-ajatuksena on sotilaallisen tai poliittisen päätöksenteon vaikeuttaminen hyökkäyksin tietolähteitä vastaan [9, s. 27].

3.1 Kyberhyökkäyksen aikana

Hyökkäys sotilaallisia tietoverkkoja vastaan voi vaikeuttaa puolustusvoimien kykyä kohdata vihollinen tehokkaasti. Hyökkäys siviiliyhteiskuntaa vastaan kuten hyökkäys viestintä- tai sähköverkkoja vastaan, saattaa huomattavasti vahingoittaa sotilaallisen organisaation kykyä toteuttaa tehtävänsä. Tämä korostuu nykypäivän puolustusvoimissa, jotka ovat äärimmäisen riippuvia useista siviiliyhteiskunnan järjestelmistä.

Kyberhyökkäyksen tekninen vaikutus näkyy järjestelmän tai sen osan menetettynä kykynä suorittaa oma tehtävänsä sille tarkoitetulla tavalla: esimerkkinä järjestelmän tai sen osan ylikuormittuminen tai tuhoutuminen. Kyseinen järjestelmä voi sotilassovellutuksissa tarkoittaa johtamisjärjestelmää, joka mahdollistaa tehokkaan päätöksenteon sekä käskyjen välittämisen. Lisäksi siviiliyhteiskunnan kriittinen infrastruktuuri, joka mahdollistaisi taistelutilanteessa tehokkaan huollon kuten täydennykset ja muonitukset, on riippuvainen tietoverkkopohjaisista järjestelmistä. Nämä järjestelmät on rakennettu avoimiin tietoverkkoihin, koska ne ovat riippuvaisia ulkopuolelta tulevista käyttäjistä.

Myös suljetuilla ja puoliavoimilla tietoverkoilla on haavoittuvat kohtansa. Vaikka järjestelmä olisi rajattu sotilaskäyttöön, sen komponentit todennäköisesti tarvitsevat

ajoittaisia päivityksiä siviilipuolelta. Hyvänä esimerkkinä on suljettu sotilaallinen ilmavalvontajärjestelmä. Täten sekin on haavoittuvainen mahdolliselle kyberhyökkäykselle. [6, s. 33-34]

Kyberhyökkäyksessä voidaan käyttää hyväksi bottiverkkoja. Botilla tai robotilla tarkoitetaan tässä yhteydessä ohjelmaa joka joko suorittaa irrallaan pieniä toistuvia tehtäviä tai toimii välittäjänä, jota itse hyökkääjä hallitsee ja käskee suoraan. Kun tällainen botti on jollakin tavalla latautunut tietokoneelle, esimerkiksi sähköpostin tai muun tiedoston liitteenä, voi hyökkääjä käskeä sitä suorittamaan toimintoja täysin tietokoneen käyttäjän huomaamattomissa. Kun sama botti on tarttunut useaan tietokoneeseen, puhutaan bottiverkosta. Yhtä tällaisen verkon tietokonetta voidaan kutsua zombieksi. [16, s. 40-41]

3.2 Vastareaktio kyberhyökkäykseen

Tärkein vastareaktio kyberhyökkäykselle on riskien arviointi ja ennaltaehkäiseminen. On kyettävä varautumaan uhkakuvaan laaja-alaisesti. Jotta ennaltaehkäiseminen on tehokkaasti mahdollista, on katsottava tilannetta mahdollisen hyökkääjän silmin.

Esimerkkinä Naton ensisijainen tavoite kyberpuolustukselle (2012) on varmistaa esteetön kyberympäristön käyttö ja järjestelmien koskemattomuus. Tämä tehokas suojautuminen vaatii nopeita päätöksiä ylätasolla ja niiden nopeaa välittämistä taktiselle tasolle [8, s. 20].

Tähänkin pätee sanonta ”tilaisuus tekee varkaan”. Esimerkiksi DDoS-hyökkäyksen vuokraaminen tunniksi maksaa kymmenen ja päiväksi 50 yhdysvaltain dollaria, 1000 tietokoneen tartuttaminen haavoittavilla koodeilla noin 50 yhdysvaltain dollaria Euroopassa ja 160 Yhdysvalloissa [6, s. 58].

Ensiarvoisen tärkeää on palvelun valvonta hyökkäyksen havaitsemiseksi. Jos järjestelmät on mitoitettu palautumaan hyökkäyksistä ja toimintahäiriöstä riittävän nopealla palautumisajalla, hyökkäyksen teho jää vähäiseksi. [7, s. 5; 6, s. 37]

Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden kärkimaaksi. Meillä on vahva osaamisperusta sekä pitkät perinteet tiivistä ja luottamuksellisesta yksityisen ja julkisen sektorin yhteistyöstä sekä hallinnon alojen välisestä yhteistyöstä.

Nykyisessä kybersodankäynnissä hyökkäykset ovat sillä tasolla, etteivät ne välttämättä rajoitu tietojärjestelmiin, vaan kykenevät vaikuttamaan myös fyysiselle tasolle kuten esimerkiksi jonkin tietokoneohjatun laitteen tai esineen toimintaan. Kyberhyökkäys on erityisen helposti toteutettavissa, mikäli kohteen tietoturva ei ole riittävällä tasolla. Myös internetistä eristettyihin verkkoihin on mahdollista murtautua vaikkapa fyysisten tallennusvälineiden avulla. Tämä korostaa tietoturvasta huolehtimisen merkityksellisyyttä muun muassa henkilöstön koulutuksen tasolla sekä ohjelmistojen ja fyysisten laitteiden tasolla. Tietoturvan merkitystä ei kuitenkaan tulisi korostaa liikaa. Tällöin tietoturvasta voi syntyä päinvastoin jokapäiväistä työskentelyä rasittavaa, kun tietoturvan rajat saattavat hämärtyä yksittäisten työntekijöiden silmissä. [14, s. 23]

3.3 Suomen strategiset linjaukset kybertuvallisuudesta

Suomen kyberturvallisuuden visiona on, että:

• Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.
• Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.
• Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa. [13 s. 3]

1. Viranomaisten ja muiden toimijoiden välinen tehokas yhteistyömalli

Aktiivisella yhteistoiminnalla eri toimijoiden välillä edistetään jaettua tilannetietoisuutta ja tehokasta uhkien torjuntaa. Eri toimialojen toimintaa häiriötilanteissa harjoitellaan määräajoin sekä kansallisessa että kansainvälisessä mittakaavassa. Kansainvälisissä harjoituksissa saatua kokemusta jaetaan tehostetulla tiedonvaihdolla ja koordinoinnilla. Tavoitteena on oman toiminnan ja järjestelmien haavoittuvuuksien löytäminen, suorituskyvyn kehittäminen sekä henkilöstön harjoituttaminen. [13, s. 7]

2. Keskeisten toimijoiden tilannetietoisuuden parantaminen

Toimijoiden tilannetietoisuutta parannetaan tarjoamalla päivitettyä, koottua ja jalostettua tietoa häiriöistä, haavoittuvuuksista ja niiden vaikutuksista. Tilannekuvassa näkyvät arviot ja ennusteet aiheutuvista uhkista. Kyberuhkien ennaltaehkäisy vaatii poliittisen, sosiaalisen, teknisen, kulttuurisen, teknologisen ja taloudellisen tilanteen arvioinnin. Viestintäviraston osana toimiva Kyberturvallisuuskeskus luodaan tämän tilannekuvan tuottamiseksi ja ylläpitämiseksi. Kyberturvallisuuskeskus kerää ja välittää tietoa kyberuhista. Tiedon saaja puntaroi oman toimialansa ja vasuunsa kannalta tietoa. Eri toimijat tuottavat analyysejä, jotka lähetetään takaisin Kyberturvallisuuskeskukseen. Kyberturvallisuuskeskuksessa ne edelleen liitetään yhteiseksi päätöksenteon pohjaksi eri toimijoille. Valtioneuvoston tilannekeskuksella on käytettävissään päivitetty ja monipuolinen kyberturvallisuuden kokonaistilannearvio. Sen osina ovat Kyberturvallisuuskeskuksen yhdistetty tilannekuvaus ja hallinnonalojen arvio kybertapahtumien vaikutuksista elintärkeille tahoille. [13, s. 7]

3. Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta olennaisten yritysten ja organisaatioiden kyberhavainnointikyvyn ylläpito ja kehittäminen

Yhteiskunnan elintärkeiden toimintojen kannalta keskiössä olevat yritykset ja organisaatiot ottavat kattavasti huomioon kyberuhkatekijät turvallisuus- ja valmiussuunnittelussaan sekä pitävät yllä suojautumiskykyä. Tavoitteena on mahdollisten häiriöiden tunnistaminen, havainnointi ja reagointi pienimmillä mahdollisilla haittavaikutuksilla. Olennaista on sietokyvyn kehittäminen sekä varatoimintojen suunnittelu ja harjoittelu sille tasolle, että kyberhyökkäyksen alla kyetään toimimaan.

4. Poliisin toimintamahdollisuuksien takaaminen kyberhyökkäyksien ennaltaehkäisyssä

Poliisi on kyberrikollisuutta sekä kybertoimintaympäristöä koskevan laittoman toiminnan esitutkintaviranomainen. Lisäksi poliisi on yksi tärkeimmistä kohdan kaksi keskeisistä toimijoista ja muodostaa oman analyysinsä Kyberturvallisuuskeskuksen yhdistettyä kyberturvallisuuden tilannekuvaa varten. Poliisin toimivaltuuksista, resursseista sekä osaavasta ja motivoituneesta henkilöstöstä huolehtiminen on tärkeä osa kybertoimintaympäristöön kohdistuvan rikollisuuden ennaltaehkäisyä. Poliisin kansainvälistä operatiivista työtä jatketaan ja syvennetään vastaavien toimijoiden kuten Europolin ja Euroopan Unionin maiden muiden lainvalvontaviranomaisten kanssa. [13, s. 8]

5. Puolustusvoimat takaa kyberpuolustuskyvyn

Sotilaallinen kyberpuolustuskyky on tiedustelua, vaikuttamista ja suojautumista. Puolustusvoimat suojautuu kyberuhilta niin, että kykenee suoriutumaan lakisääteisistä tehtävistään; kokonaismaanpuolustuksesta, muiden viranomaisten tukemisesta sekä kansainväliseen kriisinhallintaan osallistumisesta. Tämän suorituskyvyn varmistamiseksi kybertoimintaympäristössä kehitetään tiedustelu- ja vaikuttamiskykyä muun sotilaallisen toiminnan kehittämisen rinnalla. Puolustusministeriön johdolla laaditaan toimivaltuussäännöstö, joka helpottaa edellä mainittujen tehtävien täyttämistä. Tässä säännöstössä tunnistetut puutteet korjataan lainsäädännön toimenpitein. Viranomaiset harjoittelevat ja kehittävät yhteistoiminnassa kyberpuolustusta kansallisella ja kansainvälisellä sekä strategisella että taktisella tasolla. [13, s. 8]

6. Kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan osallistuminen

Kansainvälisen yhteistyön tavoitteena on parhaiden käytäntöjen jakaminen ja oppiminen sekä soveltaminen kansallisen kyberturvallisuuden tason nostamiseksi. Jokainen viranomainen toimii yhteistyössä niiden omalla toimialallaan niiden valtioiden ja organisaatioiden kanssa, jotka ovat kansainvälisesti edelläkävijöitä kyberturvallisuusympäristössä. Aktiivisen yhteistyön muotoja ovat muun muassa tutkimus- ja kehittä-

misyhteistyö, organisaatioiden työryhmätyöskentely, sopimusten valmistelutyö ja kansainväliseen harjoitustoimintaan osallistuminen. Suomelle tärkeitä foorumeita ovat esimerkiksi EU, YK, NATO, ETYJ ja OECD.

7. Kaikkien yhteiskunnan toimijoiden kyberosaamisen ja -ymmärryksen kehittäminen

Keskeisimpien yhteiskunnan toimijoiden kybertietoisuuden ja suorituskyvyn parantamisen lisäksi keskitytään yhteisten kyber- ja turvallisuusohjeistojen kehittämiseen. Myös yhteiskunnan elintärkeiden toimintojen kannalta keskeisimmät yritykset ja järjestöt otetaan mukaan harjoitustoimintaan kokonaisvaltaisemman valmiuden aikaansaamiseksi. Lisäksi perustetaan strateginen kyberturvallisuuden huippuosaamisen keskittymä. Sen tavoitteena on tarjota tutkimustyöhön ja tutkimustietoa hyödyntäville tahoille tapa tehdä tehokasta, tiivistä ja pitkäjänteistä yhteistyötä. Panostusta lisätään tutkimukseen, tuotekehittelyyn ja kolutukseen. Tämä luo vahvan edellytyksen kansallisen kyberosaamisen kehittymiselle. [13, s. 9]

8. Lainsäädännön keinoin varmistetaan edellytykset tehokkaaseen kyberturvallisuustoimintaan

Hallinnolliset ja elinkeinoelämän tahot selvittävät yhteistyönä lainsäädännön ja kehittämistarpeen kybertoimintaympäristöön liittyen. Selvityksen tuloksena laadittavat kehittämisehdotukset edistävät kyberturvallisuusstrategian tavoitteita. Lisäksi tarkoituksena on varmistaa lainsäädännön sallivan riittävät toimivaltuudet eri viranomaisille huolehtia yhteiskunnan elintärkeiden toimijoiden sekä valtion turvallisuuden suojaamisesta kyberuhkia vastaan. On myös huomioitava kansainvälisistä sopimuksista johtuvat esteet, rajoitteet ja velvoitteet, jotka voivat haitata tehokasta tiedonsaantia ja –välitystä viranomaisten ja muiden tahojen välillä. On myös arvioitava onko näille vastuuviranomaisille luotava lainsäädännön keinoin paremmat mahdollisuudet tiedonsaantiin ja kokoamiseen ennaltaehkäisevänä keinona. Kuitenkin siten, että samalla huomioidaan perusoikeudet kuten yksityisyyden suoja. Monet yritykset toteuttavat suurimman osan kyberkyvykkyyden, osaamisen ja palveluiden luomisen ja suojaamisen, sillä suuri osa yhteiskunnan kriittisestä infrastruktuurista on yksityisten tahojen omistamaa. Lainsäädännön keinoin tulee mahdollistaa myös liiketoiminnan

kehittämisen edellytykset. Se on edellytyksenä kansainväliselle kilpailukykyiselle ja vientimahdollisuudet omaavalle kyberosaamiselle. Täten Suomi kehittyy myös investointeja ja sijoituspäätöksiä houkuttavana kyberturvallisuuden toimintaympäristönä.

9. Viranomaisten ja elinkeinoelämän tahojen tehtävien määrittely sekä yhteiset perusteet vaatimusten hallinnalle

Selkeiden vastuiden ja tehtävien määrittely ja jakaminen on ehdoton edellytys kybertoiminnan kehittämiselle. Käytännössä jokaisen hallinnonalan on tehtävä arviointi ja analyysi riskien ja haavoittuvuuksien tunnistamisesta sekä niiden hallinnan tasosta. Tulosten perusteella on mahdollista laatia toimeenpano-ohjelmat kullekin hallinnonalalle. [13, s. 10]

10. Toimeenpanon valvomisen ja toteuman seuraaminen

Jokaisen toimialan strategian toimeenpanosta sekä kybertoimintaympäristön tehtävien toteuttamisesta vastaa jokin ministeriö tai virasto. Perustetaan Turvallisuuskomitea seuraamaan ja yhteen sovittamaan strategian toimeenpano. Päämäärinä ovat puutteiden tunnistaminen, vastuista varmistuminen ja päällekkäisen toiminnan välttäminen. Toimivaltainen viranomainen tekee asiasta säädetyt varsinaiset päätökset. [13, s. 11]

4 ESIMERKKEJÄ KYBERHYÖKKÄYKSISTÄ 2000-LUVULLA

4.1 Toinen Tšetšenian sota 1997-2001

Konfliktin aikana molemmat osapuolet, sekä venäläiset että tsetseenit, käyttivät hyväkseen kyberavaruutta operaatioon liittyvän tiedon kytkemiseen voidakseen hallita ja muokata julkisuuskuvaa.

Myöhemmin konfliktin jo virallisesti päätyttyä, kun venäläiset Spetsnaz-erikoisjoukot hyökkäsivät vapauttamaan Tsetseeni-terroristien 26. lokakuuta 2002 Moskovan teatterissa panttivankeina pitämiä venäläisiä siviilejä, ilmoitettiin Venäjän federaation turvallisuuspalvelun FSB:n kaataneen kaksi tärkeää tsetseenien verkkosivustoa. [1, s. 3]

4.2 Digital Pearl Harbour 2002

U. S. Naval War College suoritti heinäkuussa 2002 kokeen, jossa kohdistetuilla kyberhyökkäyksillä iskettiin internetiä, sähkö- ja puhelinverkkoja sekä talousjärjestelmää vastaan. Koe osoitti internetin olevan haavoittuvaisin testatuista järjestelmistä. Yhdysvaltojen puhelinverkostoa ei onnistuttu haavoittamaan. [6, s. 36-37]

4.3 Viron pronssipatsaskiista 2007

Kyberhyökkäykset liittyivät Neuvostoliiton 1947 Tallinnaan pystyttämään pronssipatsaaseen. Sen virallinen nimi oli ”muistomerkki Tallinnan vapautumiselle”. Viron itsenäistyttyä 1991 heräsi kysymys neuvostoaikaisten muistomerkkien kohtalosta. Pronssipatsas jätettiin paikalleen, mutta siitä tuli toisessa maailmansodassa kaatuneiden muistomerkki. Tämä ei kuitenkaan estänyt patsasta muuttumasta kiistojen keskipisteeksi. Viron venäläiset järjestivät vuotuisia juhlia patsaan läheisyydessä 9.5. Venäjän niin kutsuttuna ”Voiton päivänä” sekä 22.9, Tallinnan vapautumisen vuosipäivänä. Tämä oli kuitenkin monien virolaisten mielestä vihamielinen ele, koska virolaisten puolelta katsottuna patsas on myös symboli Neuvostoliiton valloittamaksi

jäämisestä. Virolaisten näkökulmasta avoin venäläisten merkkien ja neuvostosymbolien esittäminen juhlien aikana oli miehittämisen ylistämistä.

Toukokuun yhdeksäntenä päivä 2006 patsaan luona tapahtui yhteenotto, kun venäläiset juhlijat hyökkäsivät Viron lippua kantaneiden mielenosoittajien kimppuun. Yhteenoton jälkeen alkoivat vaatimukset pronssipatsaan siirtämisestä pois Tallinnan keskustasta ja siirtämisestä muualle. Vuoden 2007 alussa Viron hallitus hyväksyi kaksi lakia, joiden nojalla Pronssipatsas ja muut samankaltaiset muistomerkit voitaisiin siirtää niille paremmin sopivalle paikalle. Valmistelut pronssipatsaan ja sen lähelle haudattujen neuvostosotilaiden siirtämisestä alkoivat 26.4.2007. Patsas ja sen lähiympäristö aidoitettiin ja asiaton pääsy sen luo estettiin. Samana iltana siirtoa vastustaneet venäläiset osallistuivat laajoihin mellakointeihin sekä levottomuuksiin, jotka kestivät läpi yön. Pronssipatsas siirrettiin suunnitellusti Tallinnan sotilashautausmaalle ja julkistettiin uudella paikalla 30.4. ja tilanne rauhoittui.

Mellakoiden aikaan 27.4. alkoivat kohdistetut kyberhyökkäykset Viroa vastaan. Kohteina olivat pääosin valtiollisten laitosten kotisivut. Hyökkäykset koostuivat laajasta roskapostittamisesta sekä niin kutsutuista DDOS-hyökkäyksistä. Huhtikuun viimeisenä päivänä hyökkäysten määrä lisääntyi merkittävästi. Hyökkäysten kohteena olevien internetsivujen määrä lisääntyi ja levisi kattamaan internetpalveluntarjoajat ja julkisen median. Hyökkäyksen jatkuivat päivittäisinä aina 16.5. asti, jonka jälkeen tilanne palautui lähes normaaliksi. Suurin osa hyökkäyksistä tuli Venäjän maaperältä ja niin tekniset seikat kuin hyökkäyksien vaatimat resurssit viittaavat Venäjän Duuman liittyneen hyökkäyksiin. Venäjän federaatio luonnollisesti kiisti kaikki kytkökset.

Venäjä on myös kieltänyt olevansa vastuussa muista toimista Viroa vastaan. Kuitenkin jo vuoden 2007 alussa Venäjän federaation johto varoitti Viroa siirtämästä pronssipatsasta ja 23.4. se jätti kirjallisen diplomaattisen viestin asiasta. Jo ennen patsaan siirtoa Venäjän valtion hallitsemissa viestintävälineissä hyökättiin sanallisesti Viroa vastaan. Lisäksi mellakoiden aikana Venäjän Tallinnan suurlähetystö oli läheisissä väleissä mellakoiden johtajien kanssa. Moskovassa puolestaan Viroa vastustaneet mielenosoittajat piirittivät Viron suurlähetystöä viikon estäen sen normaalin toiminnan. Käytännössä Venäjä myös asetti Virolle taloudellisia pakotteita aloittamalla virolaisten tuotteiden boikotoinnin Venäjällä. [16, s. 86-87]

Tavoitteena ei ollut tunkeutua järjestelmiin, vaan estää muiden käyttäjien pääsy. Vaikka selvää yhteyttä Venäjän hallitukseen ei löytynyt, myönsi Duuman Sergei Markoviin liitetty Konstantin Goloskokov joidenkin tahojen olleen mukana iskuissa.

Vastaavanlaisia hyökkäyksiä on toteutettu luottokorttiyhtiöitä, Israelilaisia pankkeja ja pörssejä sekä esimerkiksi Hizbollahia, Hamasia ja palestiinalaisia tietoverkkoja vastaan. Kosovon kriisissä 1999 Pohjois-Atlantin sotilasliitto pysäytti vastaavanlaisilla kyberhyökkäyksillä serbialaisia tietoverkkoja ja Jugoslavialaiset aktivistit yrittivät muuttaa kyberavaruudessa ollutta tietoa tukemaan omia tavoitteitaan. [1, s.3; 6, s.39-40]

4.4 Georgiansota 2008

Georgiansodassa ensimmäisen kerran kyberhyökkäyksiä seurasi kahden valtion välinen suora sotilaallinen konflikti, joka toteutui maalla, meressä ja ilmassa. Tarkkaan suunniteltujen kyberhyökkäysten sarjan kohteena olivat Georgian hallituksen internetsivujen lisäksi Yhdysvaltojen ja Iso-Britannian suurlähetystöjen sivustot. Hyökkäysten seurauksena Georgian valtiovalta joutui tukeutumaan ulkopuolisten valtioiden tietojärjestelmien tukeen. [1, s. 3; 6, s. 40-41]

Konfliktilla on peruja vuosiin 1991-1992, jolloin Etelä-Ossetia pyrki eroamaan emämaastaan Georgiasta. Vuosina 1992-1993 itsenäisyyskiista johti aseellisiin taisteluihin ja osa georgialaisista joutui pakenemaan. Taisteluiden seurauksena Georgiaan kuulunut Abhasian alue siirtyi hallinnoltaan venäläismielisille paikallishallinnoille. Georgian johto katsoi Venäjän antaneen tukea edellä mainituille separatisteille, mikä johti Venäjä-suhteiden kiristymiseen. Venäjän päämääränä oli tuolloin jo Georgian itsenäisyyden kyseenalaistaminen ja asemansa säilyttäminen etupiirissään. [17, s. 43]

Venäjän ja Georgian välit tulehtuivat uudelleen 2004 vallankumousta seuranneen uuden presidentin Mikhail Saakasvilin länsimyönteisestä politiikasta johtuen. Kesäkuussa 2004 georgialaiset puuttuivat venäläisten asekuljetuksiin, minkä seurauksena Venäjä katkaisi sähkön syötön Georgian alueelle. Venäjä katkaisi myös liikenneyhteyden Venäjälle Georgian sotilastietä pitkin saman vuoden syyskuussa. 2005 allekirjoitettiin sopimus, jonka mukaan Venäjä vetäisi joukkonsa pois Georgian alueelta vuoden 2008 loppuun mennessä. Vuonna 2007 kuitenkin sotilaallinen voima tuli sel-

västi mukaan Venäjän painostuskeinoihin, kun ilmavoimien hyökkäykset alkoivat Georgian hallintorakennuksia vastaan Kodorin solan alueella maaliskuussa. [17, s. 45-46]

4.5 Kirgisia 2009

Kirgisian riippuvuus Venäjän kautta kulkevista verkkoyhteyksistä muuhun maailman johti internetin käyttömahdollisuuden katkeamiseen jopa kymmenen päivän ajaksi 18.-28. tammikuuta 2009. Kirgisiassa käydyn poliittisen valtataistelun yhteydessä Venäjä painosti Kirgisiaa sulkemaan yhdysvaltalaisen lentotukikohdan maassa, minkä seurauksena verkko-operaattoreiden toimintamahdollisuudet estyivät.

5 JOHTOPÄÄTÖKSET

Suomen kyberturvallisuuden strategiassa linjataan, että Suomi vahvistaa kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan. Kansainvälisen yhteistoiminnan tavoitteena on vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä, jotta kansallisen kyberturvallisuuden tasoa voidaan kohottaa. Yhteistyön lähtökohtana niin Naton kuin Euroopan Unionin kanssa on molempia osapuolia hyödyttävä ja resursseja säästävä toiminta. Naton yhteistyömahdollisuuksien lähtökohtana on toiminta rauhankumppanuusmaana ja EU:n jäsenmaana. Kyberpuolustus koetaan usein herkäksi aiheeksi, mutta perustason toiminnoissa yhteistyömahdollisuudet ovat hyvät vaarantamatta kansallista kriittistä tietoa. Tästä on hyvänä esimerkkinä tutkimus- ja kehittämistyö sekä koulutus- ja harjoitustoiminta. [8, s. 13]

Informaatioteknisellä järjestelmällä tulee olla oppiva organisaatio joka kehittää tietotaitoaan ja kykyään samaa tahtia kuin uudet järjestelmät kehittyvät ja niitä syntyy. Toimiakseen organisaatio tarvitsee selvät linjat siihen, mitä vastaan tulee toimia ja mitä vastaan kyetään toimimaan yhdessä esimerkiksi puolustusvoimien ja yhteiskun-

nan tasolla. Kyberhyökkäys on täten ikään kuin strateginen ase taktisessa toiminnassa. [6, s. 76]

Puolustusvoimien on kyettävä hallitsemaan sekä psykologiset että tekniset näkökulman kybersodankäynnissä. Tästä syystä rajalliset resurssit tulee jakaa tavoitellun tehokkuuden saavuttamiseksi. Tämä onnistuu esimerkiksi oikeanlaisten yhteistyökumppaneiden avulla. Pienvaltiossa korkeatasoista teknologiaa löytyy yritysmaailmasta ja yliopistoista. Yritys- ja yliopistomaailma voi pääosin suuntautua teknisiin näkökulmiin kun taas puolustusvoimat voi keskittää voimavaransa psykologisiin osiin. Tämä jako on looginen jo siksi, että yritysten ja yliopistojen toiminta on muutenkin riippuvaista uusista tutkimuksista ja tiedosta. Näiden tutkimusten rahoittaminen on mahdollista muutenkin kuin valtion avustuksella, koska niillä on myös kaupallista arvoa. Sen sijaan puolustusvoimilla on tapana keskittyä johtamiseen ja päätöksentekoon sekä niihin vaikuttamiseen. Tätä taitoa löytyy puolustusvoimien tietoverkkooperaatioiden asiantuntijoilta psykologisen sodankäynnin hallinnan lisäksi.[6, s. 77]

Puolustusvoimien pitää tukea ja vahvistaa muiden puolustushaarojen kybertoimintakykyä mahdollisessa kriisitilanteessa. Tämä edellyttää valmistautumista rauhan aikana. Osa tästä valmistautumisesta voi sisältää laitonta toimintaa elintärkeiden järjestelmien ja välttämättömän tiedon turvaamiseksi. Toiminta on suunnattava kykyyn havaita hyökkäyksen mahdollistavat haavoittuvuudet. [6, s.77-78]

Jokaisessa nykypäivänpoliittisessa ja sotilaallisessa konfliktissa on jonkin verran, joskus enemmän joskus vähemmän, kyberulottuvuutta. Hyökkääjillä on käytettävissään laaja ja tehokas arsenaali kyberstrategioita ja -taktiikoita. Internet on todella haavoittuvainen hyökkäyksille ja sen käytön lisääntyminen tarkoittanee, että tulevaisuudessa voitot kyberavaruudessa tulevat linkittymään vahvasti voittoihin perinteisissä maataisteluissa. Kybertaktiikassa esimerkiksi valtiollisella hyökkääjällä on todella hyvä hyötysuhde verrattaessa riskejä ja tappioita mahdolliseen onnistumiseen, mikä tekee siitä erityisen houkuttelevaa. Käytännössä kysymys ei enää ole onnistutaanko valtiotason turvallisuussuunnittelijat yllättämään kyberhyökkäyksillä, vaan milloin se tapahtuu ja missä olosuhteissa tai mittakaavassa.

Kyberhyökkäys sotilaallista verkkoa tai järjestelmää vastaan voi olla työlästä. Toisaalta hakkereilla on käytettävissään hämmästyttävän paljon ilmaisia sovelluksia ja ohjelmia, joilla taitava ja osaava hyökkääjä kykenee saamaan aikaan merkittävää tu-

hoa. Hyökkääjät ovat usein tietoisia järjestelmien heikkouksista ja haavoittuvuuksista ja itse hyökkäystä edeltää monesti avoimien lähteiden tiedustelua.

LÄHTEET

- **Kirja**

[1] Carr, J. *Inside cyber warfare.* 1st ed. USA: O'Reilly, 2009. 212 s. ISBN 978-0-596-80215-8.

[2] Forno, R. & Baklarz, R. *The Art of information warfare*. 2nd ed. Universal Publishers, 1999. 180 s. ISBN 1-58112-857-6.

[3] Candolin, C. *Securing military decision making in a network-centric environment*. Helsinki: Picaset Oy, 2005. 141 s. ISBN 951-22-7980-0.

[4] Tekniikan laitos. *Julkaisusarja 4: Teknisen kehityksen suuntalinjat.* Helsinki: Edita Oyj, 2002. 216 s. ISBN 951-25-1338-2.

[5] Liimatainen, H., Rantapelkonen, J. *Informaatioajan viestitaktisia ajatuksia.* Loimaa: Loimaan Kirjapaino Oy, 2000. 224 s. ISBN 952-91-2444-9.

[6] Kantola, H. *Datanätverksattacker, trend eller nödvändighet? – Ur ett småstatsperspektiv.* Helsinki: Försvarshögskolan, 2011. 96 s.

[9] Palojärvi, P. *A battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict.* Helsinki: University of Helsinki, 2009. 186 s. ISBN 978-952-10-6009-0.

[10] Andress, J., Winterfeld S. *Cyber warfare Tehchniques, Tactics and Tools for Security Practioners.* USA: Elsevier, 2011. 289 s. ISBN 978-1-59749-637-7.

[11] Gompert, D., Lachow I., Perkins J. *Battle-wise Seeking Time-information Superiority in Networked Warfare.* Washington, D.C.: Center for Technology and National Security Policy by National Defence University Press, 2006. 174 s. ISBN 1-57906-072-2.

[14] Rantamäki, V. *Verkko-operaatiot tietoverkkosodankäynnissä.* Helsinki: Maanpuolustuskorkeakoulu, 2012. 25 s.

[15] Vankka, J. *Cyber warfare.* Helsinki: Maanpuolustuskorkeakoulu. 2013. 127 s. ISBN 978-951-25-2455-6.

[16] Rantapelkonen, J. & Salminen, M. *The fog of cyber defence.* Helsinki: Maanpuolustuskorkeakoulu, 2013. 248 s. ISBN 978-951-25-2430-3.

- **Internetsivu**

[7] Björkman, J. *Palvelunestohyökkäykset ja niiltä suojautuminen.* Haaga-Helia ammattikorkeakoulu. [viitattu 6.8.2013]. Saatavissa: http://files.kotisivukone.com/plaa.julkaisee.fi/tiedostot/palvelunestohyokkaykset.pdf

[13] *Suomen kyberturvallisuusstrategia ja taustamuistio.* 2/2013 http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit/doc_download/49-suomen-kyberturvallisuusstrategia-ja-taustamuistio

[17] Tähtinen, J. *Georgian sodan tarkastelu strategisen iskun toteutusperiaatteiden ja torjunnan näkökulmasta.* Helsinki: 2013. 143 s. https://www.doria.fi/bitstream/handle/10024/92637/Y2681_T%C3%A4htinenJP_YEK56.pdf?sequence=2

- **Lehti**

[8] Roivainen, H. *Kyberpuolustus Natossa ja EU:ssa*. Sotilasaikakauslehti Elokuu 8|2013.

[12] Kontiainen, T. *Yhteiskunnan osaamista hyödynnetään.* Ruotuväki 18/2013