MAANPUOLUSTUSKORKEAKOULU

KYBERASEIDEN VAIKUTUS KRIITTISEN INFRASTRUKTUURIN TIETOJÄRJESTELMIIN

Kandidaatintutkielma

Kadetti
Jose Mäntylä

98. kadettikurssi
Kenttätykistölinja

Maaliskuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Kadettikurssi 98	Kenttätykistölinja
Tekijä Kadetti Jose Mäntylä	
Tutkielman nimi Kyberaseiden vaikutus kriittisen infrastruktuurin tietojärjestelmiin	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika 12.3.2014	Tekstisivuja 30

TIIVISTELMÄ

Työn tehtävänä on selvittää lähdemateriaalin avulla hyökkäys- ja puolustusmenetelmistä valtiolliseen kyberturvallisuuteen liittyvät keskeisimmät menetelmät ja niiden vaikutukset, tarkastelemalla niitä maailmalla tapahtuneiden kyberhyökkäyksien pohjalta. Tutkimuksella pyritään vastaamaan seuraaviin alakysymyksiin: minkä tyyppisiä kyberaseita käytetään kriittisen infrastruktuurin tietojärjestelmiä vastaan, mikä on niiden vaikutus ja millaisia kyberhyökkäyksiä valtioiden kriittisen infrastruktuurin tietojärjestelmiä vastaan maailmalla on toteutettu sekä miten ne kyetään suojaamaan näiltä kyberuhilta? Tavoitteena on, että tutkimuksella kasvatetaan lukijan tietämystä kyberavaruuden vaaroista ja kriittisen infrastruktuurin tietojärjestelmistä.

Keskeiset lähderyhmät ovat aiemmat tutkimukset, kirjallisuus, uutisartikkelit ja erityisesti sähköiset lähteet. Tärkeimpiä yksittäisiä lähteitä ovat muun muassa Suomen valtioneuvoston tuottama *Suomen kyberturvallisuustrategia-periaatepäätös* (2012) ja Mika-Jan Pullisen tekemä opinnäytetyö *Kriittisten tietojärjestelmien suojaaminen kyberuhilta* (2012). Tutkimusmenetelmänä käytetään kirjallisuuskatsausta.

Tietojärjestelmiin hyökätessä käytetään yhä ammattimaisempia välineitä. Hyökkäystarkoituksen pohjalta suunnitellut ja valmistetut hienostuneet ohjelmistot ovat usein kyberterroristien tai jopa valtiollisten toimijoiden suunnittelemia. Kyberhyökkäyksistä vain prosentti on ollut varsinaisia valtioiden tuottamia kyberaseita. Merkittävinä kyberhyökkäyksinä voidaan pitää muun muassa Stuxnet-tietokonematoa, Flame-vakoiluohjelmaa ja Shamoon-tietokonevirusta. Kyberhyökkäyksistä Stuxnet-tietokonemadolla kyettiin tuottamaan fyysistä vahinkoa tietojärjestelmiin kohdistuvan vaikutuksen lisäksi.

Kriittisen infrastruktuurin tietojärjestelmien suojaamisessa käytetään samoja menetelmiä kuin muissa yleisissä tietojärjestelmissä. Suojaus muodostuu kattavasta tietoturvasta, joka pitää sisällään hallinnollisen, henkilöstö-, fyysisen ja tietoliikenneturvallisuuden. Kriittisten tietojärjestelmien suojaus voidaan toteuttaa virustorjuntaohjelmistoilla, eristämällä kriittiset tietojärjestelmät yleisestä verkosta kokonaan, käyttämällä palomuuria, identiteetin- ja pääsynhallinnalla, vahvoilla salausmenetelmillä ja tekemällä omaa tietojärjestelmää vastaan koehyökkäyksiä, joilla löydetään tietojärjestelmän haavoittuvuudet.

AVAINSANAT

Kyberase, Kyberturvallisuus, Kybersodankäynti, Kriittinen infrastruktuuri, Tietojärjestelmät, Haittaohjelmat, Kriittisen informaatioinfrastruktuurin turvaaminen

KYBERASEIDEN VAIKUTUS KRIITTISEN INFRASTRUKTUURIN TIETOJÄRJESTELMIIN

SISÄLLYSLUETTELO

KUVALUETTELO

TAULUKKOLUETTELO

KYBERASEIDEN VAIKUTUS KRIITTISEN INFRASTRUKTUURIN TIETOJÄRJESTELMIIN

1 JOHDANTO

Elintarvikkeet pilaantuvat Espoon keskusvarastossa. Suomen suurimman logistiikkakeskuksen tietokoneet eivät ole toimineet päiviin ja tavara seisoo hyllyissä. Kuorma-autot odottavat tyhjinä lastauslaitureilla ja samalla laivat eivät pääse purkamaan tai lastaamaan tavaroita. Tietokoneiden ohjaama logistiikkaketju on romahtanut. Lehdet manaavat elintarvikepulaa ja vedenjakelu ei toimi. Ihmiset kärsivät samaan aikaan kun tietokonevikoja aiheuttavat haittaohjelmat ohjaavat tavaroita väärin paikkoihin ja sammuttavat osia kriittisen infrastruktuurin tärkeimmistä tietojärjestelmistä. Tämän kaltaisiin vaikutuksiin tuntematon vihollinen voisi pitkälle suunnitelluilla ja kaukaa toteutetulla kyberhyökkäyksellä päästä. [1]

Kyberaseiden vaikutusten tutkiminen on ajankohtaista, koska kyberhyökkäysten vaarallisuus, monimuotoisuus ja määrä ovat jatkuvassa kasvussa. Yhteiskunnan toimivuus on samanaikaisesti tullut yhä riippuvaisemmaksi tietojärjestelmistään. Tietoteknisten laitteiden ja järjestelmien toimimattomuus, informaatioinfrastruktuurin luhistuminen tai vakavat kyberhyökkäykset voivat aiheuttaa erittäin vakavia vaikutuksia julkisiin palveluihin, liike-elämään ja hallintoon, sekä niiden romahtaessa koko yhteiskunnan toimintaan. Valtiotasolla kyberturvallisuus on tällä hetkellä hyvin esillä, mistä kertoo muun muassa vuoden 2013 alussa julkaistu kyberturvallisuustrategia sekä viestintäviraston alaisuuteen vuonna 2014 perustettu kyberturvallisuuskeskus.

Tutkimuksella kasvatetaan lukijan tietämystä kyberavaruuden vaaroista ja kriittisen infrastruktuurin tietojärjestelmistä. Tietämys kyberuhista on pakollista, jotta ymmärretään tietojärjestelmien suojaamisen merkitys niitä vastaan.

1.1 Tutkimustehtävä ja -kysymykset

Tutkimustehtävänä on selvittää lähdemateriaalin avulla hyökkäys- ja puolustusmenetelmistä valtiolliseen kyberturvallisuuteen liittyvät keskeisimmät menetelmät ja niiden vaikutukset tarkastelemalla niitä maailmalla tapahtuneiden kyberhyökkäyksien pohjalta.

Tutkimuksen pääkysymys: Mitä kyberuhkia kriittisen infrastruktuurin tietojärjestelmät kohtaavat ja miten ne suojataan näiltä uhilta?

Alakysymykset:

- Minkä tyyppisiä kyberaseita käytetään kriittisen infrastruktuurin tietojärjestelmiä vastaan ja mikä on niiden vaikutus?
- Minkälaisia kyberhyökkäyksiä valtioiden kriittisen infrastruktuurin tietojärjestelmiä vastaan maailmalla on toteutettu?
- Miten kriittisen infrastruktuurin tietojärjestelmät kyetään suojaamaan näitä kyberaseilla toteutettavia hyökkäyksiä vastaan?

Tutkimus on osa kybertoimintaympäristöä tutkivaa ryhmätutkimusta. Tällä tutkimuksella vastataan kysymyksiin, joihin ryhmän toiset tutkimukset eivät pyri vastaamaan. Ryhmän työn tuloksena saadaan laaja käsitys kybertoimintaympäristöstä.

1.2 Tutkimusmetodin valinta

Tutkimuksessa käytetään tutkimusmenetelmänä kirjallisuuskatsausta. Sen avulla voidaan kriittisesti tarkastella aiemmissa tutkimuksessa esitettyjä väitteitä. Tutkimusmenetelmä valittiin myös siksi, että sen avulla pystytään tuomaan esille ja perustelemaan tutkijan omat näkökulmat, jolloin se myös toimii tutkimuksen tekemisen apuvälineenä. Tutkimusmenetelmän valinnalla varmistetaan myös tutkimustyön ainutlaatuisuus ja vältetään aiempien tutkimuksien toistamista.

1.3 Aiemmat tutkimukset ja rajaus

Kyberaseista on tehty lukuisia artikkeleja ja tutkimuksia. Niistä monet ovat vaikutusvaltaisten instituutioiden tai valtioiden tuottamia. Aikaisempaa kandidaatin tutkimustyötä Maanpuolustuskorkeakoulussa ei kyberaseiden vaikutuksesta ole tehty, mutta muissa yliopistoissa ja ammattikorkeakouluissa tuotettuja opinnäytetöitä sekä maisteri- ja väitöskirjatasoisia tutkimuksia aiheesta löytyy monia.

Kriittiseen infrastruktuurin tietojärjestelmiin kohdistuvista kyberhyökkäyksistä kertoo Mika-Jan Pullinen Laurea-ammattikorkeakoulussa tekemässään opinnäytetyössä: *Kriittisten tietojärjestelmien suojaaminen kyberuhilta* (2012). Opinnäytetyö käsittelee pitkälti samaa aihetta kuin tämä tutkimus, mutta siinä on keskitytty lähes pelkästään teknisen tietoturvan näkökulmaan, kun taas tässä tutkimuksessa aihetta tarkastellaan tämän lisäksi muista näkökulmista.

Jari Rantapelkosen ja Mirva Salmisen julkaisu *The Fog of Cyber Defence* (2013 Maanpuolustuskorkeakoulu) käsittelee kybersotaa monesta näkökulmasta muun muassa tarkastelemalla kyberuhkia maailmalta saatujen varoitusmerkkien pohjalta. Tutkimuksessa kyseistä lähdettä on käytetty muun muassa kyberaseiden ominaispiirteiden määrittämisessä.

Juhani Lillbackan Tampereen ammattikorkeakoulussa tekemässä opinnäytetyössä *Informaatiosodankäynti - Tietoverkkojen vaarat* (2012) määritellään menestyksekkäästi erityyppiset haittaohjelmat, joiden avulla tutkimukseen on ollut helpompi valita niistä kaikkein keskeisimmät.

Tärkeimmät lähderyhmät ovat aiemmat tutkimukset, kirjallisuus, uutisartikkelit ja erityisesti sähköiset lähteet. Sähköisistä lähteistä käytän tutkimuksessani esimerkiksi Puolustusvoimien tuottamaa kyberturvallisuuteen liittyviä artikkeleja ja julkaisuja, kuten ”Turvallinen Suomi – tietoja Suomen kokonaisturvallisuudesta” (2012) ja valtioneuvoston tuottama ”Suomen kyberturvallisuusstrategia – periaatepäätös” (24.1.2013).

Tutkimuksen aihetta rajataan käsittelemällä hyökkäys- ja puolustusmenetelmistä vain valtiolliseen kyberturvallisuuteen liittyvät keskeisimmät menetelmät ja niiden vaikutukset tarkastelemalla niitä maailmalla tapahtuneiden hyökkäystapausten pohjalta. Tutkimuksessa käsitellään tietoverkossa olevien järjestelmien lisäksi myös niitä kriittisen infrastruktuurin suojattavia kohteita, jotka ovat riippuvaisia omista sisäisistä tietojärjestelmistään.

1.4 Tärkeimmät käsitteet

Alla olevat tärkeimmät käsitteet ovat valtioneuvoston vuonna 2013 tuottaman kyberturvallisuusstrategian taustamuistiosta (pl. kyberase, kyberkonflikti, nollapäivähyökkäys, BIOS ja keskeisimmät menetelmät).

Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita, että sähköisiä toimintoja ja palveluja.

Kriittisellä informaatioinfrastruktuurilla tarkoitetaan yhteiskunnan elintärkeiden toimintojen tietojärjestelmien perustana olevia rakenteita ja toimintoja, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirtäminen, vastaanottaminen, varastoiminen tai muu käsitteleminen.

Kyber- sanaa käytetään lähes aina yhdyssanassa määriteosana. Sanan merkityssisältö liittyy sähköisessä muodossa olevan informaation (tietojen) käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tieto- ja tietokonejärjestelmiin.

Kyberase on sähkömagneettisessa ympäristössä vaikuttava haitta, jonka taustalla on valtio tai vastaava ryhmittymä kuten esimerkiksi terroristiorganisaatio [85, s. 16]

Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoiminta-ympäristöön voidaan luottaa ja jossa sen toiminta voidaan turvata.

Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkun kybertoimintaympäristöstä riippuvaisen toiminnon.

Tietojärjestelmällä tarkoitetaan ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuvaa järjestelmää, jonka tarkoituksena on informaatiota käsittelemällä tehostaa tai helpottaa tiettyä toimintaa tai mahdollistaa se.

Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus.

Nollapäivähyökkäys tarkoittaa tietoturva-aukkoon tehtyä hyökkäystä, jota ei olemassa olevilla korjauksilla voida estää. Haavoittuvuus hyökkäykselle syntyy, kun joku löytää aukon ja ilmoittaa tai jättää ilmoittamatta siitä ohjelman kehittäjille, tai kun tietoturva-aukkoa ei ilmoituksesta huolimatta paikata. [81]

BIOS (Basic Input-Output System) on järjestelmän alustusohjelma, joka on upotettu kiinteästi emolevyn BIOS-piiriin. Ohjelma aktivoituu automaattisesti ensimmäisenä, kun tietokonetta käynnistetään. BIOS lataa käyttöjärjestelmän keskusmuistiin ja hoitaa myös alkeellisen laitehallinnan, eli tukee näppäimistöä, näyttöä ja BIOS-taltiota. [17]

2 KYBERASEIDEN VAIKUTUS KRIITTISEN INFRASTRUKTUURIN TIETOJÄRJESTELMIIN

2.1 Kriittisen infrastruktuurin tietojärjestelmät

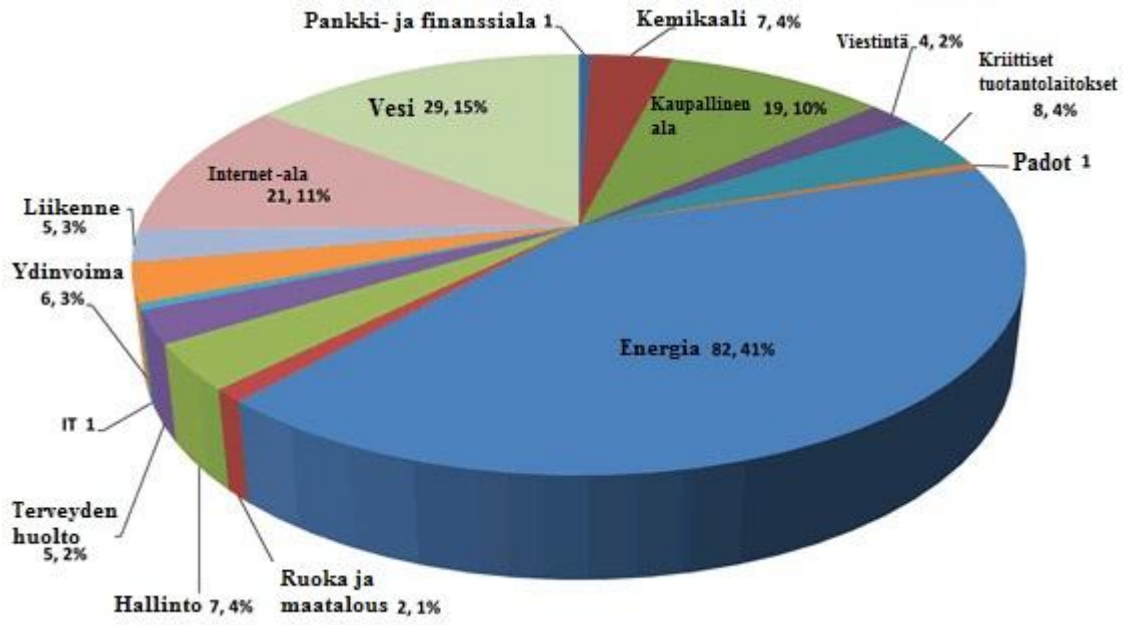
Kriittinen infrastruktuuri käsittää rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Nämä rakenteet pitävät sisällään tietojärjestelmiä, joiden tehtävänä on sähköisessä muodossa olevan informaation lähettäminen, siirtäminen, vastaanottaminen, varastoiminen ja käsitteleminen. [2] Kriittisen infrastruktuurin toimintojen ja palveluiden toimintakyvyn tuhoutumisella olisi vakavia vaikutuksia yhteiskunnan turvallisuuteen sekä sosiaaliseen ja taloudelliseen hyvinvointiin [3].

Kyberhyökkäyksillä kyetään vaikuttamaan kriittiseen infrastruktuuriin ja yhteiskunnan elintärkeisiin palveluihin tuotammalla niissä suuria häiriöitä tai lamaannuksia [2]. On tärkeää erottaa kriittiseen infrastruktuuriin tai niiden tietojärjestelmiin kohdistuvat uhat. Hyökätäkseen vesivoimalan valvontajärjestelmää vastaan, krakkeri voi aloittaa hyökkäyksen mistä päin maailmaa tahansa, kunhan hän löytää vain sopivan yhteyden kohdejärjestelmään. Tämä vaati erilaisen ajatustavan ja suojaustoimenpiteet kuin esimerkiksi pommihyökkäys ydinvoimalaan, jossa tekijä on fyysisesti läsnä. [4, s. 19]

Puolustusvoimien tietoverkot rakentuvat pääsääntöisesti yhteiskunnan tietoliikenneinfrastruktuurille ja ovat näin aina haavoittuvaisia vastustajan tietoverkko-operaatioille sekä fyysiselle tuhoamiselle. Näiden tietoverkkojen haavoittuvuus kasvaa, kun eri tietojärjestelmiä liitetään keskenään käyttäen siviiliyhteiskunnan tietoliikenneinfrastruktuuria. Ilman suojaustoimenpiteitä tietoverkkojen liitynnät tarjoavat vastustajalle takaportin, jonka avulla voidaan päästä luvattomasti tietojärjestelmän sisälle mistä tahansa maailmasta. [82, s. 22]

Ensimmäisenä kyberhyökkäyksenä voidaan pitää vuoden 1982 tapausta, jolloin Neuvostoliitto varasti kanadalaiselta yritykseltä tahallaan väärin koodatun hallintaohjelman, jonka seurauksena haittaohjelma aktivoitui putkiston painetestin aikana ja aiheutti öljyputken räjähdyksen [80].

Kyberhyökkäyksiä tehdään maailmalla kaiken aikaa. Yhdysvaltain ICS-CERT:n [5] mukaan vuoden 2012 syyskuuhun mennessä maan huoltovarmuuteen vaikuttavien laitoksien järjestelmiin onnistuttiin hyökkäämään 198 kertaa kuluvan vuoden aikana.



Kuva 1: Yhdysvalloissa onnistuneet kyberasehyökkäykset kriittisen infrastruktuurin eri sektoreita vastaan kuluvan vuoden 2012 syyskuuhun mennessä [5]

80 prosenttia Suomen kriittisestä infrastruktuurista on yksityisessä omistuksessa [6]. Yksityisiin yrityksiin kohdistuvilla kyberaseiskuilla kuten palvelunestohyökkäyksillä kyetään pahimmissa uhkakuvissa jopa lamauttamaan junaliikenne käyttämällä hyväksi GSM-liikenteen salauksen murtoa ja vääriin käsiin helposti päätyviä R-GSM-tekniikan salausavaimia [7]. Kyberuhka voi olla myös hakkereiden yritys verkkopankkijärjestelmien kaatamiseksi tai vieraan valtion hyökkäys sähköverkon vauriottamiseksi [6].

Suojattava kohde	Selite
Energiansiirto ja -jakeluverkot	Ohjaus-, hallinta-, jakelu- ja valvontajärjestelmät
Tietoliikenne	Puhelinverkot, taktiset kenttäradiover-kot, IP-pohjaiset avoimet tai suljetut verkot, matkapuhelinverkot, satelliitti-verkot
Vedenjakelu	Ohjaus-, hallinta-, jakelu- ja valvontajärjestelmät
Elintarvikepalvelut	Elintarvikkeiden tuotanto- ja jakelujärjestelmät
Kuljetuslogistiikka	Polttoainejakelu-, rautatietieverkko-, lennonjohto- ym. järjestel-mät
Terveyspalvelut	Potilas- ja lääketietojärjestelmät sekä lääke- ja rokotetuotanto
Turvallisuuspalvelut	Poliisin, tullin, puolustusvoimien ym. järjestelmät. Rajavalvonta, sotilaallinen voimankäyttö, rikollisuudentorjunta
Ympäristöturvallisuus	Suuronnettomuuksilta, luonnonkatastrofeilta sekä ympäristöuhilta varautumis- ja toipumisjärjestelmät
Finanssiala	Rahoitus- ja maksujärjestelmät

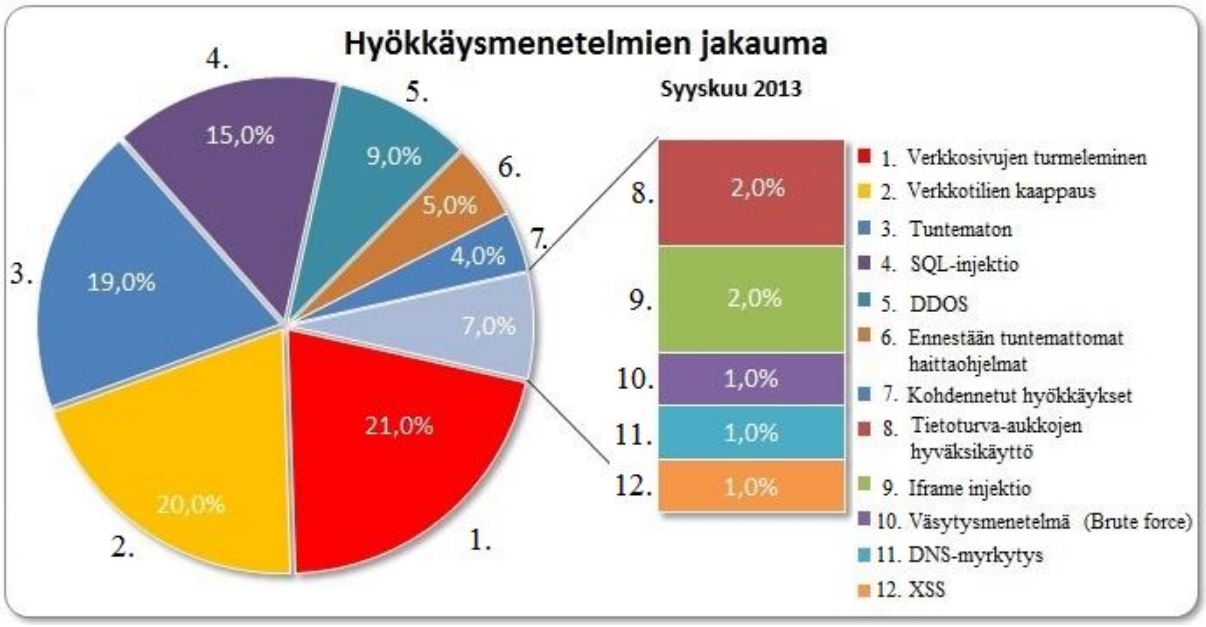
Taulukko 1: Kriittiset tietojärjestelmät, joihin kyberaseilla kyetään vaikuttamaan [46, s. 15]

2.2 Hyökkäysmenetelmät ja kohteen valinta

Kyberympäristöön kohdistuneet hyökkäykset ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi yksilöiden, yritysten ja koko yhteiskunnan kannalta. Muutokset tässä toimintaympäristössä ovat nopeita ja vaikutuksia vastaan on lähes mahdotonta varautua. Varautuminen ja uhkien torjuminen edellyttää kaikkien yhteiskunnan osapuolien entistä nopeampaa, paremmin koordinoitua sekä läpinäkyvämpää toimintaa. [2]

Hyökkäysmenetelmien kehittäjät ovat ammattimaisempia kuin ennen ja nykypäivänä kehittäjiin voidaan laskea kuuluvuksi myös valtiolliset toimijat. Lähes kuka vain kykenee tekemään hyökkäyksen verkoista löytyvien valmisohjelmistojen avulla. Valmisohjelmistoja käyttävät pääsääntöisesti kokeilunhaluiset nuoret, mutta tämän lisäksi rikolliset saattavat käyttää niitä taloudellisen hyödyn saavuttamiseksi. [8, s. 262–263; 2, s. 1]

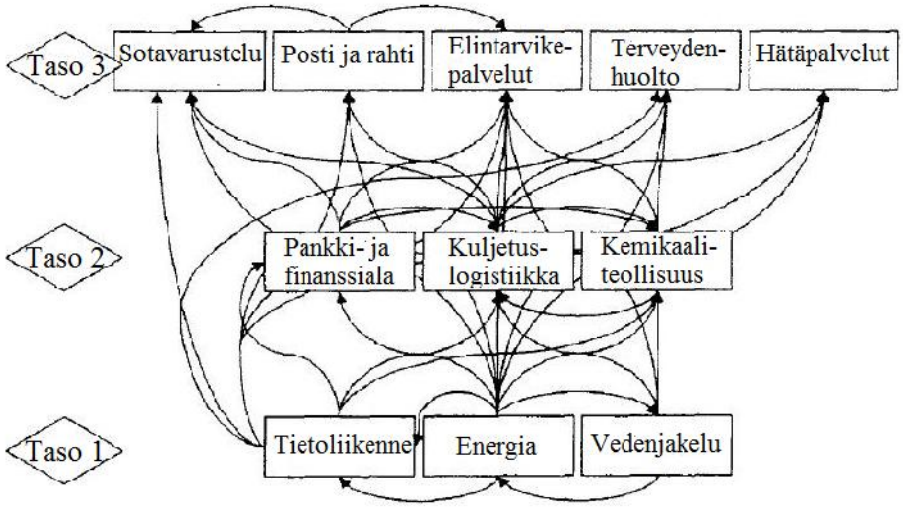
Hyökkäystarkoituksen pohjalta suunnitellut ja valmistetut hienostuneet ohjelmistot ovat usein kyberterroristien tai jopa valtiollisten toimijoiden suunnittelemia. Suurvaltojen ja sellaiseksi havittelevien maiden valmistamat kyberaseet ovat valtavia koodiryppäitä, joilla voitaisiin kaataa esimerkiksi vieraiden valtioiden sähköverkkoja, verkkopankkeja tai öljykuljetusten logistiikkaa säätteleviä tietoverkkoja. Näillä aseilla kyettäisiin iskemään valtioiden elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin niin, että valtiot lamautuisivat ilman laukaustakaan. [8, s. 262–263; 2, s. 1; 80] Hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja kriisiaikana yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen rinnalla [8, s. 262–263; 2, s. 1].



Kuva 2: Yleisten hyökkäysmenetelmien jakauma [78]

Kyberhyökkäyksissä kohde on tarkkaan valittu hyökkääjään motiivien perusteella ja niissä tavoitellaan merkittävää taloudellista hyötyä tai halutaan tuottaa mahdollisimman paljon vahinkoa kohteelle. Valikoivan maalinnuksen johdosta se poikkeaa yleisistä haittaohjelmista, jotka iskevät satunnaisiin kohteisiin skannaamalla laajaa osoiteavaruutta ja tunkeutumalla tarvittavia ominaisuuksia omaaviin kohteisiin, jotka ovat helposti haltuunotettavia automaattisilla työkaluilla. [10; 11, s. 8; 85, s. 16] Taloudellisesta hyödystä puhuttaessa todettakoon, että verkkorikollisuudessa liikkuu Symantecin mukaan nykypäivänä enemmän rahaa kuin huumerikollisuudessa [9].

Kohteen valinnassa pitää ottaa huomioon, että kaikki kriittiset infrastruktuurit ovat riippuvaisia toisista infrastruktuureista, joten hyökkäämällä yhteen kohteeseen saatetaan lamauttaa monta muuta. Kuvasta 2 voidaan todeta, että esimerkiksi terveyspalvelut ovat riippuvaisia kuljetuslogistiikasta ja tietoliikenteestä. Hyökkäämällä onnistuneesti hierarkiassa tärkeimpiin infrastruktuureihin, kuten tietoliikenteeseen, energiansiirto- ja jakeluverkkoihin tai vedenjakeluun kyettäisiin lamauttamaan koko yhteiskunta tai hyvin suuri osa sen tuottamista palveluista. [12]



Kuva 3: Tasot ja riippuvuussuhteet kriittisen infrastruktuurin sektoreissa [12]

Taulukossa 2 on kuvattu kyberuhkia muodostavien toimijoiden eroavaisuuksia. Luokittelu ei ole aina yksiselitteistä ja lähes kaikki toimijat käyttävät ajoittain samankaltaisia hyökkäysmenetelmiä. [13]

	Motivaatio	Kohde	Menetelmiä
Haktivismi	Poliittinen tai sosiaalinen muutos	Päätöksentekijät tai viattomat uhrit	Protesti verkkosivustoilla, palvelunestohyökkäykset, tietomurrot
Krakkerointi, black hat - hakkerointi	Oman egon pönkitys, henkilökohtainen vihamielisyys	Yksilöt, yritykset, valtiot	Haittaohjelmat, madot, virukset, skriptit
Kyberrikollisuus	Taloudellinen hyöty	Yksilöt, yritykset	Identiteettivarkaudet, palvelunestohyökkäykset kiristyskeinona, petokseen suunnitellut haittaohjelmat, rahanpesu
Kybertiedustelu	Sotilaallinen tai poliittinen hyöty	Yksilöt, yritykset, valtiot	Lukuisia tekniikoita tiedonhankintaan
Kyberterrorismi	Sotilaallinen tai poliittinen hyöty, terroristien rekrytointi ja koulutus	Yksilöt, yritykset, uskonnolliset instituutiot, kriittinen infrastruktuuri, valtiot	Identiteettivarkaudet, palvelunestohyökkäykset kiristyskeinona, petokseen suunnitellut haittaohjelmat, rahanpesu
Kybersodankäynti	Poliittinen tai sotilaallinen hyöty	Kriittinen infrastruktuuri, yksityiset tai julkishallinnon tietojärjestelmät	Lukuisia tekniikoita hyökkäykseen ja puolustukseen, yhdistäminen kineettiseen sodankäyntiin

Taulukko 2: Kyberuhkia muodostavat toimijat [13]

Motivaatiot jakautuvat niin, että noin 45 prosenttia kyberhyökkäyksistä on haktivismia, 44 prosenttia kyberrikollisuutta, 10 prosenttia kybersalakuuntelua ja vain yksi prosentti varsinaista valtiollista kybersodankäyntiä. Kyberterroristien toteuttamia kyberhyökkäyksiä on esiintynyt maailmalla vain yksittäisinä tapauksina. [78; 61]

Jos hyökkääjä päättää, ettei ole kannattavaa tuottaa itse kyberasetta, markkinoilla on myynnissä valmiita menetelmiä. Ostovalinnassa päätökseen vaikuttaa muun muassa hyökkäysmenetelmän hinta ja tehokkuus. [47]

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Taulukko 3: Nollapäivähyökkäyksien hinnasto [47, s. 6]

Kyberaseiden kehittely eli koodin kirjoittaminen on halpaa, kun vertaa sitä esimerkiksi modernin häivehävittäjän hintaan. Hävittäjän hinta nousee helposti miljardiin, kun taas haittaohjelmien koodaaminen tulee maksamaan korkeimmillaan vain miljoonia. [80]

2.3 Kyberaseiden ominaispiirteet ja toimintavaiheet

Kyberaseet voidaan jakaa tiedusteleviin, tuhoaviin, disinformaatiota levittäviin ja valvoviin tyyppeihin, kohteessa tapahtuvan vaikutuksen mukaan. [84, s. 47; 61; 85, s. 16] Kyberase perustuu kohdeympäristön haavoittuvuuden hyväksikäyttöön ja tämän kautta saadun käyttövaltuuden avulla toteutettavaan vaikutukseen. Kyberaseille on tyypillistä toimitusriippumattomuus, salassa pysyminen, vastatoimet paljastuessa, allekirjoitukset ja itsetuho. Salassa pysymistä pyritään edistämään hitaalla leviämisellä kohdejärjestelmässä, pienellä koolla ja piiloutumiskyvyllä, kun paljastuminen on todennäköistä. [61, 225; 85, s. 16–17]

Kaikki kyberasetyypit sisältävät toistensa kanssa samankaltaisia toimintavaiheita. Tietojärjestelmään tunkeutumiseen tarkoitettu kohdennettu hyökkäys aloitetaan kohteen tiedustelulla. Kohdeorganisaatioista hankitaan tietoa avoimista lähteistä ja tekemällä tiedustelua ohjelmistoista, joita kohdeorganisaatio käyttää. Kohdeorganisaation verkkolaitteet, kuten reititin ja kytkin, antavat epäsuorasti kysyjälle tietoa sisäverkon rakenteesta. [10; 14, s. 18]

Kohdejärjestelmästä pyritään ensimmäisessä vaiheessa löytämään haavoittuvuus. Niitä voivat olla tunnetut, paikkaamattomat haavoittuvuudet (ml. nollapäivä) ohjelmistoissa ja laitteistoissa, kohdeympäristön arkkitehtuurin, fyysisen- tai henkilöturvallisuuden heikkous ja turvamekanismin kiertäminen tai läpäiseminen. [85, s. 17]

Haavoittuvuuden löydyttyä alkaa toinen vaihe. Tässä vaiheessa kohdejärjestelmään toimitetaan ylimääräinen koodi eli haittaohjelma, joka jaetaan kahteen osaan: lataajaan ja tiedonkeruuseen tai tuhoon erikoistuvaan haittakoodiin. Lataaja voidaan toimittaa kohteeseen sähköpostin dokumenttien liitteiden avulla tai jopa ujuttamalla se kohdeverkkoon Flash-muistiin perustuvalla tiedontallennusvälineellä. Kolmannessa vaiheessa hyökkääjä aktivoi haittaohjelman ja lataaja hakee varsinaisen tiedonkeruu- tai haittakoodin hyökkääjän määrittelemästä paikasta. [10; 85]

Neljännessä vaiheessa aloitetaan kohdejärjestelmän tiedonkeruu tai tuhoaminen. Haittaohjelma saa esimerkiksi Keylogger-tyyppisellä menetelmällä talteen kohdejärjestelmän

näppäinpainallukset ja näkee ruutunäkymän etänä. Tarvittaessa haittaohjelma kykenee käsittelemään työaseman muistia ja tallennuslaitteita tekemällä kohteessaan järjestelmää haittaavia muutoksia. [10; 85]

Tiedonkeruuseen perustuvat kyberaseet sisältävät usein viidennen vaiheen. Tässä vaiheessa tiedot lähetetään ulos kohdejärjestelmästä. Kuljetus voidaan toteuttaa lähes millä tahansa tiedonsiirtoprotokollalla. Tiedon kuljetus voidaan toteuttaa myös fyysisesti, mutta tämä kasvattaa toteutuksen paljastumisriskiä ja kustannuksia. Viides vaihe voi jäädä pois, jos kyberaseen tarkoitus on vain ollut tehdä tuhoa kohdejärjestelmässä. Tietojärjestelmiin tunkeutumisessa voi olla enemmän vaiheita, mutta voidaan sanoa, että mitä heikommin järjestelmä on suojattu, sitä useampi vaiheista voidaan jättää pois. [10; 85]

2.4 Virukset ja haittaohjelmat

Tietokoneohjelmat ovat kaikkien tietojärjestelmien perusta. Tämä riippuvuussuhde tekee tietojärjestelmistä haavoittuvaisia haittaohjelmille, joita on erikseen ohjelmoitu kopioitumaan itsenäisesti ja toimimaan vakoiluun, häirintään tai vastaavaan tarkoitukseen, kuten kyberaseena. [82, s. 22]

Haittaohjelmat ovat haitallista ohjelmakoodia. Haitallista ohjelmakoodia voi syntyä tahattomasti ohjelmointivirheistä ja yhteensopivuusongelmista johtuen, mutta se voidaan toteuttaa myös tahallisesti, jolloin kyse on haittaohjelmista. Kyberaseina käytettävät haittaohjelmat ovat aina tahallisesti tuotettuja ja niitä on vaikeaa tai mahdotonta havaita ennen kuin vahinko on jo aiheutettu. [15; 80]

Haittaohjelmat voidaan jakaa useampaan eri ryhmään. Haittaohjelmien lajittelun perusteina käytetään usein niiden käyttötapaa. [15, s. 34] Mainosohjelmat pyrkivät välittämään käyttäjälle mainoksia, huijausohjelmistot pyrkivät huijaamaan käyttäjältä rahaa tai luottokorttitietoja, madot pyrkivät leviämään järjestelmien välillä automaattisesti, troijalaiset sekä takaporttiohjelmat yrittävät saada kohdelaitteen haltuun, vakoiluohjelmat pyrkivät keräämään tietoa järjestelmistä sekä lähettämään sitä eteenpäin ja virukset kykenevät monistamaan itseään tietojärjestelmän muihin tiedostoihin. [16, s. 11; 17, s. 13]

2.4.1 Tietokonevirus

Tietokonevirus on haittaohjelmatyyppi, joka leviää liittämällä itsensä ohjelman tai dokumentin käynnistystiedoston osaksi. Ne eivät tietokonemadoista poiketen leviä itsestään,

vaan ovat riippuvaisia järjestelmän käyttäjän toimista. Viruksia on olemassa kahta eri tyyppiä: suoraan toimivia ja muistinvaraisia. [18; 19, s. 19]

Suoraan toimivat tietokonevirukset etsivät aktivoiduttuaan saastutettavia kohteita ja saastuttavat ne. Saastumisen jälkeen tietokonevirus käynnistää isäntäohjelmansa ja lopettaa toimintansa jääden odottamaan seuraavaa aktivointikertaa. [19, s. 19]

Muistinvaraiset tietokonevirukset taas eivät etsi saastutettavia kohteita, kun ne aktivoituvat. Ne sen sijaan lataavat itsensä työmuistiin aktivoitumisen yhteydessä ja siirtävät hallinnan isäntäohjelmalle. Tietokonevirus pysyy aktiivisena taustalla ja saastuttaa uusia tiedostoja, kun käyttöjärjestelmä tai muut ohjelmat niitä käyttävät. [19, s. 19]

Tietokonevirukset voivat tehdä itsestään toimivan kopion ja kasvattaa lukumääräänsä järjestelmässä suuriin lukemiin. Viruksen aiheuttama liikenne tukkii tietokoneen käytössä olevaa verkkoa ja lukitsee järjestelmiä lukuisien avausyrityksien epäonnistumisien takia. Pahimmillaan virus voi jopa tuhota tietokoneen BIOS-muistin, jonka jälkeen tietokone ei enää käynnisty. Viruksien vaikutukset kohdejärjestelmässä saattaavat olla hyvin vakavia ja pysyviä. [20, s. 17; 21]

Tarkoitukseen suunniteltua tietokonevirusta kyetään käyttämään kyberaseena. Shamoon – viruksella tuotettiin elokuussa 2012 saudiarabialaisen Saudi Aramco -öljy-yhtiön sisäisessä verkossa huomattavaa vahinkoa. Virus oli kohdennettu juuri energiayhtiötä vastaan. Virus saastutti yhteensä 30 000 yhtiön työasemaa. Yhtiö joutui sulkemaan verkkonsa, jonka jälkeen tietojärjestelmien korjaus ja viruksen poisto vei viikon. Öljyntuotanto oli tämän ajan keskeytetty. [22]

Lokakuussa 2012 Mariposa-tyyppinen tietokonevirus sammutti Yhdysvalloissa sijaitsevan sähkötehtaan turbiinit kolmeksi viikoksi. Tietokonevirus tuhosi kymmenen tehtaan valvomo-tietokoneista. Alun perin se pääsi sisäisen verkon järjestelmään USB-tikun väärinkäytön johdosta. [5, s. 2]

2.4.2 Tietokonemato

Tietokonemadot ovat ohjelmia, jotka toimivat ja lisääntyvät itsenäisesti sekä liikkuvat verkkoyhteyksiä pitkin. Tietokonematojen ja tietokonevirusten erona on niiden lisääntyminen ja leviäminen [19, s. 22]. Madot tarttuvat tietokoneelle tietoturva-aukkojen ja sähköpostin kautta. Ne hidastavat tietokoneen toimintoja, tuhoavat tiedostoja, aiheuttavat internetin

häiriöitä ja käytön estymistä sekä täyttävät kiintolevyä omalla kopionnillaan ilman, että käyttäjä sitä aina huomaa [23].

Tietokonemadot saattavat asentaa tietokoneeseen backdoor-haittaohjelman, jonka avulla kone saatetaan liittää osaksi bottiverkkoa [24]. Tietokonemadoilla kyetään hankkimaan taloudellista hyötyä tai uhkaamaan tietojärjestelmiä bottiverkkoja hyväksi käyttämällä. Bitcoin-mato osoitti vuoden 2013 huhtikuussa, että kaapattujen koneiden suorituskyvyn hyväksikäytöllä virtuaalisen rahan louhintaan ohjelman tekijät voivat ansaita jopa fyysistä rahaa. [25] Bottiverkoilla kyettäisiin tämän lisäksi tuottamaan muun muassa palvelunestohyökkäyksiä julkisen sektorin laitoksien tai pankkien kotisivuja vastaan, jolloin ne pahimmassa tapauksessa saataisiin kaadettua kokonaan [26].

Tietokonemadoilla voidaan nykypäivänä tuottaa myös fyysistä vahinkoa. Stuxnet-mato oli Iranin uraanin rikastamiseen tarkoitettujen laitoksien sisäiseen verkkoon tarttunut haittaohjelma, joka kykeni vakoilemaan ja uudelleen ohjelmoimaan laitosten Windows-pohjaisia tuotantojärjestelmiä. Mato kulkeutui uraanin rikastamiseen tarkoitettujen laitoksien tietojärjestelmiin ulkoisen tiedonsiirtovälineen välityksellä [27]. Kyseessä oli myös ensimmäinen ’rootkitin’ omaava tietokonemato. Iranin ydinohjelmaa hidastaneen madon on myös epäilty olevan ohjelmoitu Israelin ja Yhdysvaltojen yhteistyön tuloksena [19, s. 39]

Mato käytti hyväksi laitoksen Windows-järjestelmien neljää nollapäivähaavoittuvuutta. Windows-järjestelmien lisäksi se saastutti Siemensin ohjausjärjestelmiä [28]. Saastuneet ohjaustietokoneet lähettivät virheellisiä ohjearvoja taajuusmuuttujille, jotka syöttivät väärää tehoa uraanin rikastamiseen tarvittaviin sentrifugeihin, jolloin niiden pyörimisnopeus oli väärä ja ne hajosivat [29]. Stuxnet oli niin monimutkainen, että tietoturva-asiantuntijoiden mielestä valtiollisten toimijoiden on ollut oltava sen takana [30]. Stuxnet-mato oli myös ehkä vastuussa intialaisen Siemens-laitteistoon pohjautuvan tietoliikennesatelliitin tuhoutumisesta [31].

Ennen 2010-lukua haittaohjelmiin perustuvat kyberuhat olivat enemmän tai vähemmän hakkereiden, aktivistien tai rikollisten aiheuttamia. Valtiolliset kyberhyökkäykset lähinnä palvelunestohyökkäyksiä tai hakkerointeja. Stuxnet osoitti, että pitkälle kehitetyillä ja monimutkaisilla haittaohjelmiin perustuvilla kyberaseilla valtiolliset toimijat kykenevät tuottamaan jopa fyysistä vahinkoa, ilman varsinaista kineettistä vaikutusta. Yksittäiset toimijat eivät tähän kykene, sillä Stuxnetin kaltaisen madon koodaustyö vie kymmeniä miestyövuosia. [32; 33]

2.4.3 Vakoiluohjelmat

Vakoiluohjelma eli Spyware on haittaohjelma, joka pyrkii keräämään tietoa haittaohjelman suorittavasta tietojärjestelmästä ja sen käyttäjästä sekä välittää nämä tiedot haluttuun osoitteeseen. Tietoa voivat olla IP- ja DNS-tiedot, luottokorttitiedot, pankkitunnukset, salasanat ja käyttäjätunnukset, selaimen selaushistoria sekä dokumenttien sisältö. Tätä tietoa käytetään mainonnan, taloudellisen tai jopa poliittisen hyödyn saantiin. Vakoiluohjelma asentaa itsensä tietokoneeseen ilmaisohjelmien ohessa siten, että käyttäjä ei tätä yleensä huomaa. [34; 35]

Vakoiluohjelma on vain harvoin tietokoneen ainoa haittaohjelma. Tietokoneet, joissa on jo vakoiluohjelma, ovat alttiita myös muille haittaohjelmille. Käyttäjät saattavat kokea tietokoneissaan haitallista toimintaa ja järjestelmän merkittävää hidastumista. Haittavaikutukset korostuvat erityisesti silloin, kun tietokoneessa on monen vakoiluohjelman samanaikainen tartunta. Vakoiluohjelmat aiheuttavat käyttäjän tahdosta riippumatonta suorittimen toimintaa, ylimääräistä verkkoliikenteen ja kiintolevyn käyttöä sekä joskus jopa ohjelmien ja järjestelmien kaatumisia. [34; 35]

Flame-nimen saanut vakoiluohjelma osoitti, että niitä käytetään myös kyberaseina. Leviämistapansa johdosta Flamea pidetään myös tietokonematona. Flame oli maailman monimutkaisin vakoiluohjelma, kun se havaittiin vuonna 2012. Haittaohjelma oli poikkeuksellisen laaja 20 megatavun tiedostokoollaan. [36; 85, s. 20] Se oli kehitetty laajamittaisen verkkovakoilun työkaluksi Yhdysvaltojen ja Israelin toimesta Iraniin kohdistuvan Olympic Games-nimiseen kyberhyökkäykseen liittyen [33]. Flame keräsi erittäin monipuolisesti tietoa pitkän aikaa muun muassa saastuneiden tietokoneiden näppäimistöstä, kiintolevyltä, näytöltä, Skype-puheluista, verkkoyhteyksistä ja järjestelmäprosesseista. Haittaohjelma valitsi lähinnä kohteekseen Microsoft Windows-käyttöjärjestelmän käyttäjiä Keski-idän valtioiden alueelta. [33; 36; 85, s. 20]

Iranin kansallisen CERT:n [37] mukaan yksikään 43 virustorjuntaohjelmasta ei havainnut haittaohjelmaa tuona aikana. Lopulta Stuxnettiä 20 kertaa monimutkaisempi vakoiluohjelma poisti itsensä ja hävitti jälkensä. Tapaus osoitti, että Flamen kaltaista monipuolista vakoiluohjelmaa kyetään käyttämään kyberaseena muun muassa SCADA-valvomo-ohjelmistoja sekä muita kriittisen infrastruktuurin tietojärjestelmiä vastaan jopa kuukausia ilman niiden havaitsemista. [38; 39]

Toinen tunnettu kyberaseena käytetty vakoiluohjelma on Mahdi. Mahdi-vakoiluohjelma ei kuitenkaan ollut kovin edistynyt ja se oli koodattu vanhanaikaisella Delphi-koodauskielellä. Vakoiluohjelman uhriksi joutui Lähi-Idän maista erityisesti Iranin kriittisen infrastruktuurin insinöörifirmat, finanssialan yritykset, hallituksen virastot ja lähetystöt. Virastoista saatiin lähes vuoden kestävän tiedonkeruuvaiheen aikana kerättyä gigatavujen verran luottamuksellista dataa. [40]

2.4.4 Troijalainen

Troijalainen on haittaohjelma, joka tekee jotain muuta, kuin mitä se näyttäisi tekevän. Ne voivat muun muassa käynnistää saastuneessa tietokoneessa madon tai viruksen, aiheuttaa tuhoja kuten järjestelmien kaatumisia, avata takaoven järjestelmän etäkäyttöön tai aiheuttaa muun haavoittuvuuden. Ne kykenevät pahimmillaan tietojen tuhoamiseen ja tiedonhakuun jättämättä itsestään jälkiä. Niillä ei ole varsinaista mekanismia, jolla ne pääsevät järjestelmään, vaan järjestelmän käyttäjä asentaa ne itse, luullen esimerkiksi sähköpostin liitteenä olevaa ohjelmaa joksikin hyödylliseksi [41, s. 2].

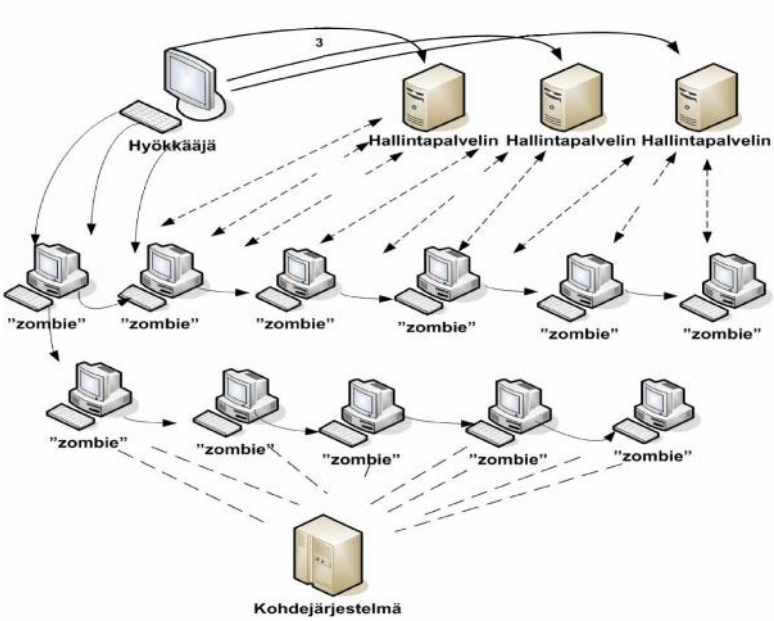
Troijalaiset olivat vuonna 2008 yleisimpiä haittaohjelmia maailmalla, sillä ne kattoivat 83 prosenttia kaikista haittaohjelmahavainnoista. Esiintyvyys on siitä lähtien ollut pienessä laskussa ja on nykyään arviolta noin 75 prosenttia. Tarkasteltaessa kriittistä infrastruktuuria, energia- ja öljysektorin laitoksiin hyökätään neljä kertaa useammin troijalaisilla kuin muiden kriittisen infrastruktuurin sektoreiden laitoksiin. [42, 43, 78]

Kyberaseeksi soveltuvia työkaluja on monenlaisia. Näistä yksi tunnetuimpia on FinFisher, joka on englantilaisen Gamma Group:n tuottama, tiedusteluratkaisuna markkinoitava tuoteperhe. Fin-ohjelmistoja käytetään etäkäyttöön ja tietojenkeruuseen, kuten salakuunteluun, näppäinpainalluksien vakoiluun ja ruutukaappauksiin, jossa kohde on ostajan vapaasti valittavana joko kohdennettuna tai massana. Tyypiltään Fin-ohjelmistoja pidetään troijalaisina, koska ne naamioituvat tai toimivat osana tunnettua ohjelmistoa, kuten esimerkiksi Firefox-selainta. Leviäminen tapahtuu tyypillisesti tunnettujen ohjelmistojen päivityskanavien osana. [85; s. 23]

Trojalaisten vakavuudesta kertoo Etelä-Koreassa heinäkuussa 2011 sattunut tapaus, jossa internetpalveluja tarjoavaa yritystä, SK Communications, vastaan troijalaisella toteutettu kyberhyökkäys paljasti 35 miljoonan ihmisen nimet, puhelinnumerot, sähköpostiosoitteet ja sosiaaliturvatunnukset [45].

2.5 Tulvahyökkäykset ja bottiverkko

Haittaohjelmien avulla hyökkääjä saa kontrollin käyttäjien työasemista ja pystyy hallitsemaan niitä etänä. Kontrolloiduista zombie-tietokoneista muodostetaan bottiverkko, jota voidaan käyttää hajautettuihin palvelunestohyökkäyksiin. Haittaohjelmaan on kovakoodattu hyökkäyksen ajankohta ja kohde, mutta niitä voidaan vielä jälkeenpäin muuttaa dynaamisesti. [46, s. 36] Hyökkääjä aloittaa hajautetun palvelunestohyökkäyksen antamalla hyökkäyskäskyn hallintapalvelimen välityksellä kaapatuille tietokoneille. Kohdejärjestelmä ylikuormittuu palvelupyynnöistä, mikä lopulta jumiuttaa tai kaataa kohdepalvelimen. Hyökkäystavan etuna on se, että niitä on mahdotonta estää ennakkoon. [48, s. 1-2]



Kuva 4: Hajautettu palvelunestohyökkäys [46, s. 37]

Hajautettuja palvelunestohyökkäyksiä on käytetty kyberaseena jo yli vuosikymmenen ajan. Kolmannes yhdysvaltalaisista kriittisen infrastruktuurin yrityksien palvelimista kohtaa massiivisia tulvahyökkäyksiä joka kuukausi. Tulvahyökkäyksistä suurin osa kohdistui öljy- ja kaasuyhtiöihin. Öljy- ja kaasuyhtiöistä kaksi kolmasosaa kertoi joutuneensa massiivisen tulvahyökkäyksen kohteeksi. Hyökkäyksien uhreista kaksi kolmasosaa koki hyökkäyksien vaikuttaneen heidän toimintaansa estämällä kotisivujen käytön, haittaamalla merkittävästi yhtiön sähköpostiliikennettä ja internet-puheluita sekä muita operationaalisia toimia. [51]

Tulvahyökkäyksiä vastaan on huomattavasti helpompi suojautua kuin esimerkiksi Stuxnetin kaltaista monimutkaista tietokonematoa vastaan. Usein yritykset sivuuttavat uhkakuvat, koska organisaatiossa ei ymmärretä täysin vahinkoa, joka hyökkäyksellä saataisiin aikaiseksi. [50; 52]

Vuonna 2010 Anonymous-hakkeriryhmä toteutti tulvahyökkäyksen Mastercard.com-verkkosivua vastaan. Ryhmä hyökkäsi onnistuneesti sivustoa vastaan massiivisella tulvahyökkäyksellä, ruuhkauttaen sivuston palvelimet niin, että sivustolle ei kenelläkään ollut pääsyä tunteihin. Motiivina tekoon oli luottokorttiyhtiön päätös estää kyky maksaa tukea Wikileaks-nimiselle järjestölle. Ryhmä hyökkäsi myös PayPal-maksuvälitysyhtiötä vastaan, mutta sen maksunvälityspalvelimet kestivät nämä tulvahyökkäykset ilman häiriöitä. [49]

Viron pankkeja, valtion virastoja ja tietoliikenneinfrastruktuuria vastaan hyökättiin vuonna 2007 massiivisella tulvahyökkäyksellä. Viron hallinnon matkapuhelimet ja faksit tukkeutuivat puheluista ja pankkien sekä hallinnon keskeisimmät palvelimet jumittuivat. Hyökkäykset jatkuivat viikkoja ja ne loppuivat vasta, kun lähes koko verkkoliikenne Viron ulkopuolelle katkaistiin. [53, s. 87-90]

Viroon kohdistuneet hyökkäykset olivat hyvin todennäköisesti yksittäisen järjestön toteuttama kyberterrorismiin liittyvä teko. Vaikka kyseiset palvelunestohyökkäykset eivät olisi olleet valtiollisen tahon toteuttamia, ne demonstroivat kyberhyökkäysmallin, jonka johdosta tietojärjestelmistä riippuvaisen maan elintärkeitä toimintoja kyetään häiritsemään. [54]

Georgian (2008) konfliktissa kybersodankäynnissä ensimmäistä kertaa tarkoituksena oli selkeästi ja näkyvästi vaikuttaa palvelunestohyökkäyksillä valtiolliseen vastustajaan. Iskut toteutettiin pääosin palvelunestohyökkäyksillä. Ensimmäistä kertaa historiassa toteutettiin samanaikaisesti sekä tavanomaista että kybersodankäyntiä. [54]

2.6 SQL-injektio

SQL-kielellä tietokantaan kyetään tekemään tiedonhakuja, lisäyksiä, muokkauksia ja poistoja. World Wide Web-pohjaiset sovellukset ovat hyvin alttiita SQL-injektioon pohjautuviin kyberhyökkäyksiin. SQL-injektioiden avulla kyberaseen kohteena olevaan sovellukseen voidaan syöttää haitallisia SQL-lauseita. [8, s. 162]

Aalto-yliopistossa tuotetun Suomen automaatioverkkojen haavoittuvuus-raportin mukaan [55] Shodan-haun perusteella löydetyistä suomalaisista tehdasautomaatiolaitteista noin 60 prosentista löytyi yleisessä tiedossa oleva haavoittuvuus. Näihin kaikkiin laitteisiin kuka tahansa voi ottaa yhteyden internetin välityksellä. Tehdasautomaatiolaitteiden internet-pohjaisista käyttöliittymistä löytyi Kasperskyn vuonna 2012 tuottaman analyysin mukaan yli tuhat haavoittuvuutta, joista yli 90 prosentissa oltaisiin kyetty käyttämään SQL-injektiota tai puskurin ylivuotovirhettä. [56]

Vuonna 2009 Albert Gonzales ja kaksi tuntemattomaksi jäänyttä venäläistä sai SQL-injektiolla Yhdysvalloissa käsiinsä 130 miljoonan ihmisen luottokorttitiedot. Gonzales pääsi käsiksi vähittäiskauppojen tietojärjestelmiin SQL-injektion avulla. Tarkoituksena hänellä oli myydä luottokorttien tiedot eteenpäin. [57]

2.7 Rootkit

Yksinkertaiset hyökkäykseen tarkoitetut rootkitit ovat piilotettuja takaoviohjelmia, mitkä piilottavat toimintansa ja jättävät kohdejärjestelmässä tietoliikenneportteja auki tuleville hyökkäyksille. Rootkittejä on useaa eri tyyppiä, mutta pääsääntöisesti ne sisältävät menetelmiä tai työkaluja hyökkäyksen peittämiseksi, kuten Stuxnet-tietokonemadossa ollut rootkit. [31] Työkalu pyrkii piilottamaan järjestelmän normaalista poikkeavat prosessit. Edistyneimmät rootkitit eivät pelkästään korvaa kohdejärjestelmän tiedostoja, vaan pyrkivät päivittämään käyttöjärjestelmän ydintä eli kerneliä. Näin edistynyttä rootkittiä tunkeutumisenestojärjestelmien on hyvin vaikeaa huomata. [58, s. 643-644]

Rootkitin tekemä takaovi avaa krakkerille pääsyn kriittisen infrastruktuurin tietojärjestelmään. Eräissä sähkövoimaloissa, sotilaslaitoksissa ja taistelualuksissa käytetään CodeSys-ohjelmistoa. Ohjelmistossa on toiminto, jonka avulla kuka vain kykenee kontrolloimaan koko laitosta oikeantyyppisillä komennoilla etäinternet-yhteyden avulla ja ilman minkäänlaista tunnistusta. Shodan-haun perusteella yleisestä verkosta löytyi maailmalta 117 laitosta, joiden toiminta kyettäisiin tietoturva-aukkoa hyväksikäyttävällä kyberhyökkäyksellä sammuttamaan. [59]

Kriittisen infrastruktuurin tietojärjestelmiin voidaan asentaa rootkittejä ennen toimitusta laitteistojen valmistus- ja toimitusvaiheessa. Eri sektoreiden laitoksien laitteistoihin valmiiksi asennetut rootkitit avaavat takaoven hyökkääjälle mahdollistaen tiedustelun tai jopa kyberhyökkäyksen toteutuksen. Kreikassa salakuunneltiin vuosina 2004 ja 2005 parlamentin jäseniä ja puolustusvoimien työntekijöitä puhelinkeskukseen asennetun rootkitin avulla. Rootkitin olemassaolo huomattiin vasta vuotta myöhemmin päivityksen yhteydessä. [60]

2.8 Verkkohyökkäystekniikat

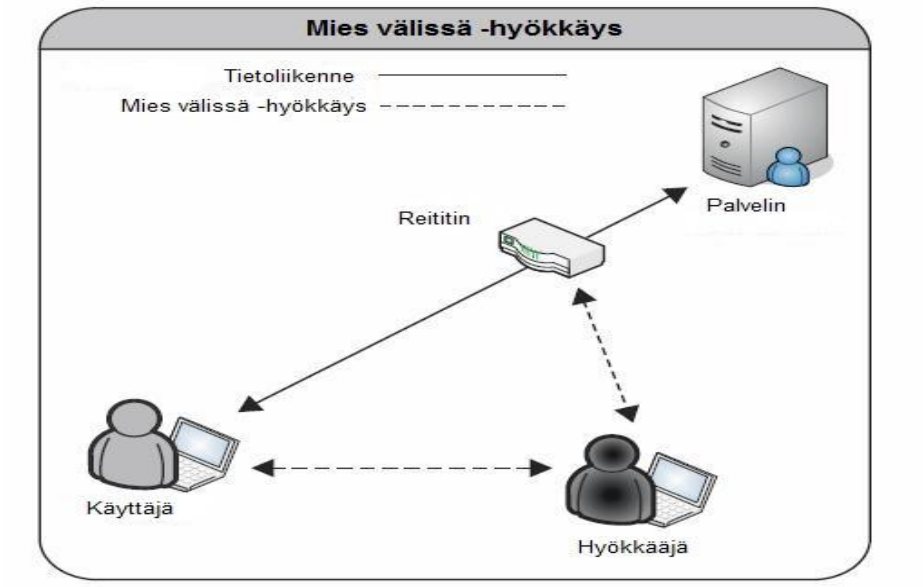
Verkkohyökkäyksessä tietoverkon ja siihen kytkettyjen laitteiden välistä verkkoliikennettä häiritään, heikennetään, estetään, kaapataan, muutetaan tai jopa tuhotaan. Hyökkäys voi kohdistua tämän lisäksi tietoverkossa oleviin laitteistojen sisältämiin tietoihin. Erilaisia verkkohyökkäystekniikoita on muun muassa perinteinen verkkohyökkäys,

verkkoanalysaattorihyökkäys, salakuuntelu, tiedon muuttaminen, väärennöshyökkäys ja mies välissä -hyökkäys. [19]

2.8.1 Mies välissä -hyökkäys

Mies välissä -hyökkäys on yksi tehokkaimmista verkkohyökkäysmenetelmistä kriittisen infrastruktuurin tietojärjestelmiä vastaan [19]. Hyökkäyksen onnistuessa tunkeutuja kykenee lukemaan ja muokkaamaan viestiä kahden osapuolen välillä niin, ettei kumpikaan heistä kykene huomaamaan linjan vaarantumista. Hyökkäysmenetelmää on perinteisesti käytetty myös salakuunteluun. [61, s. 215; 62]

Avoimien WLAN-tukiasemien kautta tehty hyökkäys on helppo tapa päästä käsiksi yhteyttä käyttävien osapuolien välisiin tietoihin. Tätä vain harva käyttäjä ottaa huomioon käyttäessään esimerkiksi junassa toimivaa avointa tukiasemaa. Käyttäjiä huijataan myös usein erilaisille huijaussivustoille. Hyökkääjä ohjaa yleisten verkkopankkien käyttäjät huijaussivustoille, joissa he huolimattomasti antavat tilitietonsa. Tämän tyyppisiä hyökkäystapauksia esiintyy päivittäin myös Suomessa. [46, s. 50]



Kuva 5: Yksinkertainen mies välissä -hyökkäys [62, s. 103]

Vuonna 2001 Australiassa vesiyhtiön entinen työntekijä kykeni käyttämään hyväksi yrityksen langattoman verkon haavoittuvuutta ja pääsi käsiksi veden ja jäteveden ohjausjärjestelmiin. Kyberhyökkäystä luultiin aluksi vain ohjelmointivirheeksi. Krakkeri kykeni pysäyttämään vesilaitoksen pumput, estämään järjestelmien hälytykset ja kommunikoinnin keskuksen sekä pumppuasemien välillä. Hyökkäykset kyettiin lopettamaan vasta kuukautta myöhemmin. [70]

2.8.2 Salasanan murtaminen

Salasanan murtamisessa yritetään murtaa väsytysmenetelmällä (brute force) järjestelmän suojauksessa käytetty salasana, käymällä läpi kaikki mahdolliset vaihtoehdot. Salasanan arvaamiseen käytetään tietokoneiden tai pilvipalveluiden tuottamaa laskentatehoa. Uusimmat suojausalgoritmit tekevät menetelmästä ajallisesti hyökkääjän kannalta turhan. Tämän takia hyökkäyksen apuna onnistuneessa hyökkäyksessä käytetään ajallisesti monin verroin kannattavampaa sanakirjahyökkäystä, jossa valmiiksi lasketut sanataulukot ovat apuna salauksen murtamiseksi. [63, s. 1-2] Suurimmat tietoturvaheikkoudet salasanassa esiintyy silloin, kun salasana ja käyttäjätunnus on yhdistetty tai salasanassa on liian vähän merkkejä. Järjestelmään pääsyyn ei kuitenkaan aina tarvita salasanan murtamista. Vanhoissa palvelimissa käyttäjätiedot lähetetään ilman salausta, jolloin niiden hyväksikäyttö on suhteellisen helppoa. [64]

Venäläiset krakkerit hajottivat vuoden 2011 marraskuussa Yhdysvaltain Illinoisissa sijaitsevan vesilaitoksen vesipumpun, jonka johdosta tuhansia koteja oli hetken ilman vettä. Krakkerit pääsivät helposti järjestelmään, koska se oli salattu kolmen merkin pituisella salasanalla. Päästyään järjestelmään he sulkivat ja käynnistivät pumpun toistuvasti uudelleen, jolloin pumppu hajosi. [65] Jos salausmenetelmät olisivat olleet vahvempia, hyökkääjät olisivat päässeet samaan vaikutukseen tietokonevirusta käyttämällä [66]. Viikkoa myöhemmin viranomaiset kiistivät hyökkäyksen ja sanoivat pumpun hajoamisen johtuneen luonnollisesta loppuun kulumisesta ja että epäillyt kyberhyökkäykset johtuivat väärinymmärryksestä [79]. Vaikka tapaus osoittautui vääräksi hälytykseksi, hyökkäys olisi ollut helppo toteuttaa niin heikosti suojattuun tietojärjestelmään. Salaamattomat tai heikosti salatut yhteydet ja järjestelmät ovat aina vakava tietoturvauhka kriittiselle infrastruktuurille.

Yhdysvalloissa toimivan Niagara-nimisen valmistajan rakennusautomaatiojärjestelmästä löytyi vuonna 2012 vakava tietoturvauhka. Kyseistä järjestelmää käytetään edelleen monissa Yhdysvaltojen sairaaloissa, armeijan ja hallituksen kiinteistöissä. Niagaran etähallintaohjelmistosta löytyi takaovi, jonka avulla tunkeutuja kykenee kirjautumaan järjestelmään ilman minkäänlaista tunnistautumista. Suomessa samanlaisia haavoittuvuuden omaavia Niagara-versioita käytetään 184 eri laitoksessa. [55, s. 7]

3 SUOJAUTUMISMENETELMÄT KYBERASEIDEN VAIKUTUKSILTA

3.1 Suomen Kyberturvallisuusstrategia

Nykypäivänä kyberulottuvuuden uhat ymmärretään Suomessa valtionjohtotasolla. Valtioneuvosto julkaisi vuoden 2013 tammikuussa Suomen kyberturvallisuusstrategia-periaatepäätöksen. Strategiassa kuvataan Suomen kyberturvallisuuden toimintamalli, johon kuuluu kyberturvallisuuden johtaminen ja kansallinen koordinaatio, visio ja strategiset linjaukset. [2]

Suomen kyberturvallisuuden visiona [2] on, että

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

Toimintamallissa määritellään, että kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta ja sen johtamisen ylimmän tason muodostaa valtioneuvosto. Kyberhäiriötilanteessa valtioneuvostolla ja eri toimijoilla on oltava käytössä luotettava ja ajantasainen kyberturvallisuuden tilannekuva. Kansallinen kyberuhkien sietokyky eli kyberresilienssi määritetään varautumis- ja ennakointikyvyn, kyberhäiriötilanteen aikaisen toimintakyvyn ja kyberhäiriön jälkeisen toipumis- ja palautumiskyvyn perusteella. Kyberturvallisuutta pitää kehittää jatkuvasti. Tämä varmistetaan niin, että Suomessa on voimassa sellaiset lait ja kannustimet, jotka tukevat kyberturvallisuuden alueen yritystoimintaa ja sen kehittymistä. [2, s. 5]

Kansallista kyberturvallisuutta kehitetään strategisten linjausten mukaisesti. Linjauksilla luodaan edellytykset kyberturvallisuuden vision toteutumiselle. Strategisten linjauksien mukaan Suomessa luodaan kybertoimintaan liittyvä yhteistoimintamalli, parannetaan eri toimijoiden tilannetietoisuutta ja -ymmärrystä, kehitetään kriittisen infrastruktuurin kybersietokykyä ja huolehditaan, että eri viranomaisilla on tarvittava kyberpuolustuskyky. [2,

s. 6-11] Kyberturvallisuustrategia velvoittaa myös Puolustusvoimia osana yhteiskuntaa suunnitelmalliseen kybersuorituskyvyn kehittämiseen [82, s. 20].

Strategiassa kyberturvallisuuden edistäminen nähdään samanlaisena kuin monien muiden maiden vastaavissa strategioissa. Maailmalla kyberturvallisuuden edistämisessä keskeisenä nähdään muun muassa koulutuksen lisääminen, tilannekuvan kokoaminen, lainsäädännön kehittäminen ja tietojenvaihdon lisääminen sekä tietoturvan parantaminen. [82, s. 21]

Vuoden 2014 alussa perustettiin Viestintäviraston alaisuuteen Kyberturvallisuuskeskus. Kyberturvallisuuskeskuksen tehtävänä on kyberturvallisuusuhkien seuraaminen, kyberturvallisuutta koskevan tiedon kokoaminen eri lähteistä sekä sen jalostaminen ja jakaminen eri toimijoille. Kyberturvallisuuskeskus myös varoittaa yhteiskunnan elintärkeiden toimintojen kannalta tärkeitä yrityksiä ja viranomaisia Suomea uhkaavista tietoturvapoikkeamista sekä pyydettäessä avustaa näihin uhkiin varautumisessa. [83]

3.2 Kriittisen tietojärjestelmän suojaaminen

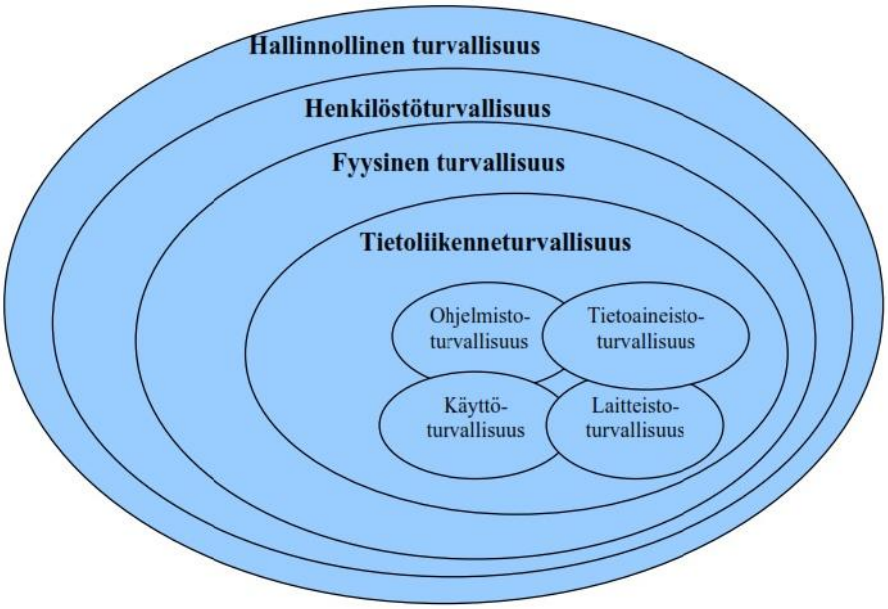
Tietokoneohjelmien käsittelemä tieto on eheää ja käyttökelpoista, mikäli se säilyy muuttumattomana. Tämän tiedon muuttumattomuuden varmistaminen taataan tietoturvallisuussovellusten avulla (palomuuri, päivitykset, virustorjuntaohjelmat…). Automatisoituina ne mahdollistavat eheyden, luottamuksellisuuden ja käytettävyyden, mutta johtuen usein säännönmukaisesta toimintatavasta ne mahdollistavat myös potentiaalisten haavoittuvuuksien hyödyntämisen. [82, s. 22]

Kriittisen infrastruktuurin tietojärjestelmien suojaamisessa käytetään samoja menetelmiä kuin yleisissä tietojärjestelmissä. Kriittisten tietojärjestelmien suojaaminen on tärkeää, koska ulkopuolisen pääsy kriittisiin tietojärjestelmiin vaikuttaa niiden toimivuuteen hyvin pitkiä aikoja, samalla vaikuttaen muihin kriittisiin tietojärjestelmiin ja pahimmillaan koko yhteiskuntaan. [67]

Kriittisten tietojärjestelmien suojauksen pitäisi muodostua kattavasta tietoturvasta [67]. Tietoturvan pyrkimyksenä on tiedon saatavuuden, oikeellisuuden ja luottamuksellisuuden säilyttäminen tiedon käsittelyn, säilytyksen sekä tiedonsiirron aikana. Tämän epäonnistuminen saattaa johtaa vakaviin seurauksiin. [68, s. 9]

Suomen valtionhallinnon virallinen tietoturvan määritelmä on niin kutsuttu Sipulimalli (ks. kuva 5). Tietoturva jaetaan kahdeksaan eri osa-alueeseen. Hallinnollinen tietoturva pitää

sisällään organisaation tietoturvallisuuteen tekemät linjaukset ja yleisen tietoturvan toimintapolitiikan. Henkilöstöturvallisuus koskee työntekijöitä, heidän ohjeistamista ja kouluttamista. Fyysinen turvallisuus käsittää organisaation toimitilojen fyysisen suojauksen. Tietoliikenteen turvallisuudella taataan tietoliikenteen jatkuvuus, siirrettävän tiedon salaus ja eheys. Laitteistoturvallisuus pitää sisällään tietokoneiden ja verkon toimivuuden. Ohjelmistoturvallisuus käsittää käytettävien ohjelmistojen suojaamisen. Tietoaineistoturvallisuus käsittää levyjen, nauhojen ja tulosteiden turvallisen käsittelyn niin, etteivät luottamukselliset tiedot joudu vääriin käsiin. Käyttöturvallisuus on tietokoneiden ja verkkojen aktiivilaitteiden päivittäiseen käyttöön liittyvien asioiden turvaamista. [69, s. 112]



Kuva 6: Suomen valtionhallinnon virallinen määritelmä tietoturvalle nk. Sipulimalli [68, s. 9]

3.2.1 Virustorjuntaohjelmistot

Virustorjuntaohjelmilla etsitään ja tuhotaan tietojärjestelmästä haittaohjelmia. Tunnistamisessa käytetään avuksi aiemmista haittaohjelmatartunnoista saatuja tunnisteita. [16] Pelkästään tunnisteiden pohjalta toimiva torjuntaohjelmisto ei kuitenkaan kykene torjumaan ennalta tuntemattomia kyberaseina käytettäviä nollapäivähyökkäyksiä, joissa hyökkääjät toimivat reaaliajassa [51, s. 8].

Uuden sukupolven torjuntaohjelmistot tutkivat lähteitä, joista tartunta on saatu ja vaikuttavat näin käyttäjään esittämällä sivuston maineen etukäteen. Uudet torjuntaohjelmat kykenevät torjumaan ennalta tuntemattomia uhkia heuristiikan avulla, jossa torjuntaohjelma etsii haittaohjelmia haittaohjelmille tyypillisen koodin tai sen pienten muutosten avulla. Epäiltyjä

haittaohjelmia voidaan myös avata torjuntaohjelman tekemässä hiekkalaatikossa, jolloin torjuntaohjelma tutkii ohjelman käytöstä. [51, s. 8; 73]

3.2.2 Kriittisten tietojärjestelmien eristäminen yleisestä verkosta

Nykypäivänä useat tietoverkot ovat kytketty toisiinsa. Turvallisin vaihtoehto olisi eristää kriittisen infrastruktuurin tietojärjestelmät muista tietoverkoista. Usein näiden järjestelmien hallinta vaatii sitä, että niitä kyetään hallinnoimaan etänä. Tällöin verkkojen välistä tietoliikennettä on kontrolloitava ja salattava, jotta minimoitaisiin onnistuneen kyberhyökkäyksen riski. Eristämiseen voidaan käyttää esimerkiksi palomuuria tai tunkeutumisenesto- ja havaitsemisjärjestelmiä. [67, s. 8; 71, s. 3]

Palomuuri on tekninen järjestely, jonka tarkoitus on estää asiaton pääsy verkosta toiseen. Se pitäisi sijoittaa kaikissa tietojärjestelmissä kohtaan, jossa verkkoliikenteen sisällön luettavuus on kyseenalainen ja jossa sillä kyetään rajaamaan sisäverkon liikenteessä vain tietyt palvelut tietylle käyttäjälle. [71, s. 3; 72, s. 118]

Palomuurin tärkein elementti on pakettisuodatus, jonka avulla verkkoliikenteestä suodatetaan yksittäiset paketit protokollien, porttien ja IP-osoitteiden perusteella sallimalla tai estämällä niiden kulku. Kriittisissä tietojärjestelmissä korostuu turvallisuus, jolloin turvallinen tapa on lähtökohtaisesti estää kaikki portit ja arvot ja tarpeen mukaan sallia niitä. [71, s. 3; 72, s. 118] Järjestelmän suojaksi asennettu virustorjuntaohjelmisto ja palomuuri eivät yhdessäkään suojaa järjestelmää kaikilta hyökkäyksiltä, mutta ne ovat osa kattavaa tietoturvaratkaisua. Palomuurit kyetään aina kiertämään siihen suunnitellulla hyökkäyksellä. [71, s. 42-49]

Vaikka järjestelmän palomuuri ja muut suojajärjestelmät olisivat kunnossa, siihen saatetaan tunkeutua järjestelmän sisä- tai ulkopuolelta. Mikäli järjestelmään on kyetty tunkeutumaan, on tärkeää havaita tunkeutuminen nopeasti ja estää syntyneen haavoittuvuuden jatkuva hyväksikäyttö. Tätä tehtävää varten tietojärjestelmiin on kehitetty automaattisia tunkeutumisenesto- ja havaitsemisjärjestelmiä. [15, s. 52]

Tunkeutumisenestojärjestelmä (IPS, Intrusion Prevention System) estää hyökkääjän pääsyn tietojärjestelmään. IDPS-järjestelmät sisältävät sekä havaitsemis- että estojärjestelmän. Järjestelmä estää haavoittuviin palveluihin kohdistuvat kyberhyökkäykset, joita ovat luvattomat kirjautumisyritykset, arkaluontoisen tiedon vuodot ja haittaohjelmat. Järjestelmä kykenee pääsynhallintaan ohjelmakohtaisesti, eikä palomuurin tyyppisesti porttien tai IP-osoitteiden perusteella. [74, s. 14-16]

3.2.3 Identiteetin- ja pääsynhallinta

Luotettavalla identiteetin- ja pääsynhallinnalla pyritään siihen, että saatetaan oikea informaatio oikeille ihmisille oikeaan aikaan [75, s. 33]. Käyttäjän tunnistus voidaan suorittaa laitteen, henkilön tai ohjelmiston avulla. Pääsynhallinnalla pyritään varmistamaan se, että vain tietyt henkilöt pääsevät käsiksi heidän tarvitsemiinsa resursseihin. Yleisesti henkilöiden tunnistamiseen käytetään menetelmiä kuten PIN-koodia tai salasanaa, mutta ne ovat paljastuessaan hyödyttömiä. [76, s. 12-13; 72, s. 70] Kriittisten tietojärjestelmien tunnistuksessa pitäisi yleisten tapojen lisäksi käyttää myös fyysisiä elementtejä, kuten toimikortteja. Tällöin hyökkääjän on saatava haltuunsa salasanan tai PIN-koodin lisäksi myös fyysinen toimikortti. [58, s. 161; 76, s. 12-13]

Pääsynhallinnan avulla kontrolloidaan sitä pääseekö käyttäjä halutun järjestelmän tarjoamaan resurssiin. Tyypillisiä käyttäjän toimintoja ovat luku-, poisto-, kirjoitus-, suoritus- ja hakutoiminnot. Pääsynhallinta on keskeisin tietoturvamenetelmä tiedon luottamuksellisuuden eheyden ja saatavuuden takaamiseksi. [72, s. 71]

Roolipohjainen pääsynhallinta on isoissa organisaatiossa kaikkein helpoin ja vähiten työllistävä pääsynhallintamalli. Oikeudet sidotaan tehtävänimikkeeseen tai tiettyyn tehtävään organisaatioissa. Tietyssä roolissa toimivalla henkilöllä on vain näkymä ja muutosoikeudet niihin tietoihin, jota hänen työskentelyssä edellytetään. [76, s. 33; 58, s. 214-216]

Pääsynhallinnassa on myös tärkeää, että kahden tekijän välinen kommunikointi salataan käyttäjätunnistukseen kykenevillä laitteistoilla tai vahvalla salauksella, jotta tarpeettomille ihmisille ei esitetä heille kuulumatonta tietoa. Yksityisyyden takaamiseksi kommunikoinnissa pitäisi käyttää virtuaalista erillisverkkoa eli VPN-yhteyttä. [67, s. 10]

3.2.4 Salausmenetelmät

Kriittisten tietojärjestelmien tiedonsiirto ja tiedon säilyttäminen pitäisi toteuttaa salattuna. Salausmenetelmät pohjautuvat usein ohjelmisto- tai laitteistopohjaiseen salaukseen. Salausmenetelmän vahvuus rakentuu algoritmista, salausavaimesta ja sen pituudesta, käynnistysvektoreista ja siitä, miten ne toimivat yhdessä. [58, s. 670-668]

Salausavaimet ovat tietyn pituisia merkkijonoja. Käytettävä avain valitaan satunnaisesti avainavaruudesta avaingeneraattorilla. Valinnan pitää olla satunnainen, jotta hyökkääjä ei kykene murtamaan salausta vain arvaamalla avaimen. Kriittisten tietojärjestelmien

avaingeneraattorien tulisi käyttää hyväksi koko avainavaruutta ja pyrkiä valitsemaan avaimien arvot mahdollisimman satunnaisesti. [58, s. 669]

Salauksessa voidaan käyttää symmetrisiä tai epäsymmetrisiä algoritmeja, tiivistefunktioita ja varmenteita. [46] Symmetrisessä algoritmissa käytetään yhtä salausavainta, joka on sekä lähettäjällä että vastaanottajalla sama. Tunnetuin ja vielä murtamattomin symmetrinen algoritmi on AES-lohkosalausalgoritmi. Epäsymmetrisessä salauksessa käytetään kahta avainta, joista toinen on julkinen ja toinen salainen. Sähköpostin salaus on yleisin epäsymmetrisen salauksen käyttökohde. Viesti salataan julkisella avaimella ja vastaanottaja purkaa salauksen salaisella avaimellaan. [58, s. 681-684; 72, s. 70-72]

Tiivistefunktiot ovat lyhyitä vakiomittaisia merkkijonoja, joiden perusteella ei voida päätellä viestin sisältöä vaan se, ettei viesti ole matkalla muuttunut. Käyttäjien salasanoja ei usein tallenneta palvelimille vaan niiden sijaan tallenetaan salasanojen tiivisteet. Salasanatiivisteiden kohdalla tiivisteiden murtaminen on vakavampi turvallisuusongelma, kuin viestien tiivisteiden kohdalla. Murron jälkeen krakkeri voi luettuaan salasanatiivisteen palvelimen tiedostosta generoida itselleen toisen, täysin toimivan salasanan. [44, s. 1-2;72, s. 73-74]

Varmenteita eli sertifikaatteja käytetään palveluiden, laitteiden ja henkilöiden tunnistamisessa. [72, s. 73-74] Varmentajaan kohdistuneen tietomurron jälkeen varmenteet menettävät luotettavuutensa, joten kriittisten tietojärjestelmien varmenteita tehtäessä pitäisi harkita, käytetäänkö julkisesti tunnettujen varmenteiden sijasta organisaation itse allekirjoittamia varmenteita. [46, s. 62]

3.2.5 Koehyökkäys

Kriittisistä tietojärjestelmistä ja näiden järjestelmien verkkolaitteista etsitään teknisiä heikkouksia erilaisien menetelmien, kuten koehyökkäyksen avulla [46, s. 55]. Koehyökkäys eli penetraatiotestaus on tietojärjestelmän tietoturvan arviointia mallintamalla rikollista hyökkääjää. Testauksen avulla etsitään helpoin tapa järjestelmään tunkeutumiseen ja väärinkäyttöön hyödyntämällä automaattisia ja manuaalisia työkaluja. Kun reitti tunnetaan, se on mahdollista tukkia ennen vahingon aiheutumista. [77]

3.2.6 Järjestelmien käytettävyys

Kriittisiä tietojärjestelmiä suunniteltaessa tavoitteena ei saa olla pelkästään turvallisuus. Turvallisuuden pitää kulkea käsi kädessä järjestelmien saatavuuden, yhdistettävyyden ja luotettavuuden kanssa. Tästä syystä esimerkiksi järjestelmien päivitykset ja huoltotoimenpiteet pitää toteuttaa niin, ettei kriittisiä järjestelmiä tarvitse toimenpiteen aikana kokonaan sulkea. [71, s. 67, s. 12]

Suunnittelussa tasapainottelu turvallisuuden ja käytettävyyden välillä pitää olla erittäin hienovaraista ja siinä kohdataan useita verkkojen suunnitteluun liittyviä haasteita. Turvallisinta oli eristää järjestelmä kokonaan yleisestä verkosta, mutta jos laitosta pitää pystyä valvomaan etänä, kilpailussa usein käytettävyys eli viimeinen vaihtoehto voittaa. [71, s. 67, s. 12]

Keinot käytettävään tietojärjestelmään [67, s. 12]:

- tee tietojärjestelmien huollot ja päivitykset niin, etteivät ne vaadi järjestelmien sulkemista
- suunnittele tietojärjestelmät mahdollisimman pitkäikäisiksi
- minimoi testaukset ja alhaalla oloajat tietojärjestelmien päivityksien aikana
- suojaa tietojärjestelmät vielä ennestään tuntemattomilta uhilta
- estä kriittisimpiin tietojärjestelmiin pääsy yksittäiseltä henkilöltä
- noudata kriittisten tietojärjestelmien onnistuneessa suojaamisessa käytettyjä malleja ja tapoja
- suorita turvallisuuteen liittyvät toimenpiteet niin nopeasti, etteivät ne vaikuta tietojärjestelmien suorituskykyyn

4 JOHTOPÄÄTÖKSET

4.1 Kyberuhat ja niiden kohtaaminen

Kyberavaruus on nykyajan taistelukenttä. Uusin Suomen ulkoasiainministeriöön kohdistunut tapaus toi mediassa esille puutteet kansainvälisessä lainsäädännössä ja menetelmissä puuttua niihin. Tällä hetkellä kansainvälinen oikeus ei esimerkiksi pidä globaalia salakuuntelua rikollistoimintana. Pahimmillaan valtioiden päämiesten puhelimia on kyetty salakuuntelemaan ilman seuraamuksia.

Tietojärjestelmiin hyökätessä käytetään yhä ammattimaisempia välineitä. Hyökkäystarkoituksen pohjalta suunnitellut ja valmistetut hienostuneet ohjelmistot ovat usein kyberterroristien tai jopa valtiollisten toimijoiden suunnittelemia. Kyberhyökkääjä käyttää hyväksi hyökkäyksessään muun muassa tietokoneviruksia, haittaohjelmia, palvelunestohyökkäyksiä, SQL-injektiota, rootkit-ohjelmistoja, mies välissä-hyökkäystä ja salasanan murtamista. Näillä eri välineillä toteutetaan maailmalla vuosittain miljardeja kyberhyökkäyksiä, mutta niistä vain yksi sadasosa on ollut varsinaisia valtioiden tuottamia kyberaseita.

Valtiollisten toimijoiden hyökkäysmenetelmät ovat usein pitkälle kehiteltyjä ja monimutkaisia kyberaseita. Määrällisesti ne ovat vielä hyvin vähäisiä, mutta nykypäivän trendi on se, että valtiot tulevat yhä enemmän aktiivisemmiksi kyberympäristössä. Ennen 2010-lukua ei valtiollisella tasolla monimutkaisia kyberaseita juurikaan kehitelty, pois lukien muutamia pitkään salassa pysyneitä tapauksia, kuten vuoden 1982 Neuvostoliiton öljyputken räjähdys. Kaikki aikaisemmat kyberasehyökkäykset olivat pitkälti palvelunestohyökkäyksiä ja hakkerointeja.

Mielestäni merkittävimpiä kyberaseita ovat olleet Stuxnet-tietokonemato ja Shamoon-virus, koska niillä kyettiin tuottamaan ensimmäistä kertaa jopa fyysistä vahinkoa kriittisen infrastruktuurin tietojärjestelmiin sekä huomattavaa taloudellista tappiota kohdeorganisaatioille.

Kriittinen infrastruktuuri on kaikkiaan 80-prosenttisesti yksityisessä omistuksessa, ja osa siitä on hyvin vanhanaikaisilla menetelmillä suojattua tai pahimmassa tapauksessa suojausta ei ole huomioitu lainkaan, koska laitos ei ole kiinni yleisessä verkossa. Tällä hetkellä toteutetulla laajalla kyberoperaatiolla kyettäisiin hyvin todennäköisesti lamauttamaan suurin osa yhteiskuntamme informaatioinfrastruktuurista.

Kriittisen infrastruktuurin tietojärjestelmien suojaamisessa käytetään samoja menetelmiä kuin muissa yleisissä tietojärjestelmissä. Suojaus muodostuu kattavasta tietoturvasta, joka pitää sisällään hallinnollisen, fyysisen, henkilöstö- ja tietoliikenneturvallisuuden.

Kriittisten tietojärjestelmien suojaus voidaan toteuttaa:

- virustorjuntaohjelmistoilla, jotka etsivät ja tuhoavat tietojärjestelmästä haittaohjelmia
- eristämällä kriittiset tietojärjestelmät yleisestä verkosta kokonaan
- käyttämällä palomuuria
- identiteetin- ja pääsynhallinnalla, jonka avulla oikea informaatio saadaan oikeille ihmisille oikeaan aikaan
- vahvoilla salausmenetelmillä
- tekemällä omaa tietojärjestelmää vastaan koehyökkäyksiä, joilla löydetään tietojärjestelmän haavoittuvuudet

Tietoturvaa suunniteltaessa tavoitteena ei kuitenkaan saisi pelkästään olla turvallisuus, vaan turvallisuuden pitäisi kulkea käsi kädessä järjestelmän, yhdistettävyyden ja luotettavuuden kanssa.

Tiedottamista pitäisi parantaa eli olisi hyvä, että tietoa uhista ja suojautumismenetelmistä jaettaisiin enemmän valtiollisessa mediassa myös kansalaisille. Tällä hetkellä vain harvat tiedostavat, että yksittäinen krakkeri kykenee tuottamaan muutamassa minuutissa kyberaseilla enemmän vahinkoa yhteiskunnan elintärkeisiin toimintoihin kuin kokonainen armeija kykenee tuottamaan päivässä tai jopa viikoissa.

4.2 Tutkimusprosessi

Tutkimusta voitaisiin soveltaa tulevissa kandidaatintutkimuksissa ja jopa tarkennettuna jonkin tasoisessa tiedottamisessa. Lisätutkimuksena voitaisiin laatia viranomaiskäyttöön tarkempia kuvauksia tiettyjen kyberaseiden vaikutuksista sekä eri suojautumismenetelmistä niitä vastaan.

Tutkimustyössä käytettiin paljon lähteitä, mutta usein jouduttiin tarkastelemaan kyberasekonflikteja muun muassa luotettavien uutistahojen näkökulmasta, jolloin tapahtumien kulusta ei aina ole täysin varmaa tietoa. On myös huomioitava, että tietoturvayhtiöltä saatu materiaali ei aina ole objektiivista. Lähdemateriaalista löytyy monia

eritasoisia oppilaitoksien teettämiä tutkimuksia, jotka usein vahvistivat nämä uutistahojen ja tietoturvayhtiöiden esittämät tiedot oikeiksi.

Suhteutettuna aiempaan kandidaattitutkimusten vähäisyyteen Maanpuolustuskorkeakoululla, tietoa muista lähteistä löytyi tutkimuksen tekoon paljon. Muualla tuotettuja aiempia tutkimuksia saatiin tuotua esille laajemmasta näkökulmasta tarkasteltuna, eikä tutkimuksen aikana pureuduttu niin tarkkoihin yksityiskohtiin, kuin joissain aiemmissa tutkimuksissa. Tutkimuskysymyksiin ja -tehtävään kyetään näillä tutkimustuloksilla vastaamaan.

LÄHDELUETTELO

[1] Koskinen, M. *Isku Suomeen: Miten meidän kävisi, jos kyberviholinen hyökkäisi?* Nyt, 16.11.2012.

[2] Valtioneuvosto. *Suomen Kyberturvallisuusstrategia – periaatepäätös.* Helsinki, 2013.

[3] Dunn, M. & Mauer. V. *International CIIP Handbook.* Toinen painos toim. Zürich: ETH Zürich, 2006.

[4] Bleier, T. *An Analysis of ICT Influence Factors*. Pro gradu-tutkielma. Krems, 2011. Donau universität.

[5] ICS-CERT. *Monthly Monitor (ICS-MM201210)* [verkkojulkaisu]. 2012 [viitattu 25.4 2013]. Saatavissa: http://ics-cert.us-cert.gov/monitors/ICS-MM201210.

[6] Hiltunen, A.-K. *Suomi turvaa kriittistä infrastruktuuria*. Ulkopolitiikka, 5.12.2012.

[7] BBC News. *Train-switching technology 'poses hacking threat'* [verkkojulkaisu]. 2011. [viitattu 18.4.2013]. Saatavissa: http://www.bbc.co.uk/news/technology-16347248.

[8] Janczweski, L. & Collard, A. *Cyberwarfare and Cyber Terrorism.* Toinen painos toim. Herheys Yhdysvallat: IGI Global, 2009.

[9] Skantz, E. & Kestilä, M. *Tietoturvatutkimus: yli miljoona ihmistä maailmassa joutuu verkkorikollisuuden uhriksi päivittäin* [verkkojulkaisu]. 2011. [viitattu 22.4.2013]. Saatavissa: http://www.symantec.com/fi/fi/about/news/rele-ase/article.jsp?prid=2011-0907_01.

[10] Heinonen, A. *Verkkohyökkäysinformaation keskitetty analysointi.* Diplomityö. Espoo, 2003. Tekninen Korkeakoulu.

[11] VAHTI. *Toimet tietoturvaloukkaustilanteessa.* Helsinki: Valtionvarainministeriö, 2001.

[12] Lewis, J. *Cyber Security and Critical Infrastructure Protection*. Homeland Security. Praeger, Yhdysvallat, 2006.

[13] Kramer, F., Starr, S. & Wentz, L. *Cyberpower and National Security. National Defense University.* Virginia, Yhdysvallat: Potomac Books, 2009.

[14] Valtioneuvosto. *Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä*. Helsinki, 2009.

[15] Savolainen, N. *Esikuntapanssariajoneuvojen tietoliikennelaitteiden tietoturvan ratkaisuvaihtoehtoja*. Pro gradu. Helsinki, 2005. Maanpuolustuskorkeakoulu.

[16] Moisander, J. *Tietoturva Microsoft Windows - verkoissa.* Opinnäytetyö. Forssa, 2012. Hämeen ammattikorkeakoulu.

[17] Tietokoneopas.com. *BIOS-asetusten tekeminen* [verkkojulkaisu]. [viitattu 30.1.2013]. Saatavissa: http://www.tietokoneopas.com/kokoaminen/bios/

[18] Chen, T. & Robert, J.-M. *The evolution of Viruses and Worms* [verkkojulkaisu]. 2003. [viitattu 22.4.2013]. Saatavissa: http://lyle.smu.edu/~tchen/pa-pers/statmethods20-04.pdf.

[19] Lillbacka, J. *Infromaatiosodankäynti - tietoverkkojen vaarat*. Opinnäytetyö. Tampere, 2012. Tampereen Ammattikorkeakoulu.

[20] Vesterinen, T. *PC:n ja Internetin tietoturva. Opinnäytetyö.* Seinäjoki, 2010. Seinäjoen ammattikorkeakoulu.

[21] Filiol, E. *Computer viruses: from theory to applications.* Ensimmäinen painos toim. Sveitsi: Birkhäuser, 2005.

[22] Sandle, T. *Shamoon virus attacks Saudi oil company*. Digital Journal 18.8.2012.

[23] AntivirusWorld. *How does anti-virus software work?* [verkkojulkaisu]. 2009. [viitattu 18.4.2010]. Saatavissa: http://www.antivirusworld.com/articles/antivirus.php.

[24] Panda Security. *Worms* [verkkojulkaisu]. 2007. [viitattu 23.4.2013]. Saatavissa: http://www.pandasecurity.com/homeusers/security-info/classic-mal-ware/worm.

[25] Gallagher, S. *Arstechnica: Hide your kids, hide your BTC: Bitcoin-stealing malware emerges* [verkkojulkaisu]. 2013. [viitattu 23.4.2013]. Saatavissa: http://arstechnica.com/secu-rity/2013/04/hide-your-kids-hide-your-btc-bitcoin-stealing-malware-emerges.

[26] Juppi, E. *Palvelunestohyökkäykset ja muut yrityksen tietoturvauhat*. Opinnäytetyö. Kajaani, 2008. Kajaanin ammattikorkeakoulu.

[27] McMillan, R. *Siemens: Stuxnet worm hit industrial systems* [verkkojulkaisu]. 2009. [viitattu 23.4.2013]. Saatavissa: http://goo.gl/YcL1g.

[28] Yle, *Israel testasi Stuxnet-matoa ennen verkkohyökkäystä Iraniin* [verkkojulkaisu]. 2012. [viitattu 23.4.2013]. Saatavissa: http://yle.fi/uutiset/nyt_is-rael_tes-tasi_stuxnetmatoa_ennen_verkkohyokkaysta_iraniin/2291502.

[29] Chien, E. *Stuxnet: A Breakthrough* [verkkojulkaisu]. 2010. [viitattu 23.4.2013]. Saatavissa: http://www.symantec.com/connect/blogs/stuxnet-breakthrough.

[30] Broad, W. Markoff, J. & Sanger, D. *Israeli Test on Worm Called Crucial in Iran Nuclear Delay* [verkkojulkaisu]. 2011. [viitattu 23.4.2013]. Saatavissa: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

[31] Woodward, P. *Israel: smart enough to create Stuxnet and stupid enough to use it* [verkkojulkaisu]. 2010. [viitattu 2.5.2013]. Saatavissa: http://warincontext.org/20-10/10/01/israel-smart-enough-to-create-stuxnet-and-stupid-enough-to-use-it.

[32] F-secure, *Stuxnet Questions and Answers* [verkkojulkaisu]. 2010. [viitattu 23.4.2013]. Saatavissa: http://www.f-secure.com/weblog/archives/0000-2040.html.

[33] Sanger, D. *Obama Order Sped Up Wave of Cyberattacks Against Iran.* The New York Times, 1.6.2012. [viitattu 24.4.2013]. Saatavissa: http://goo.gl/oo38Cs.

[34] Read, J. *Spyware Explained* [verkkojulkaisu]. 2004. [viitattu 24.4.2013]. Saatavissa: http://www.informit.com/articles/article.as-px?p=174140.

[35] Panda Security. *Spyware* [verkkojulkaisu]. 2013. [viitattu 24.4.2013]. Saatavissa: http://www.pandasecurity.com/homeusers/security-info/cybercrime/spyware.

[36] SecMeter. *Verkkosodankäynti* [verkkojulkaisu]. 2013. [viitattu 24.4.2013]. Saatavissa: http://www.sec-meter.com/verkkosodankaynti.html.

[37] Iran National CERT. *Identification of a New Targeted Cyber-Attack* [verkkojulkaisu]. 2012. [viitattu 24.4.2013]. Saatavissa: http://www.certcc.ir/index.php?name=news&file=ar-ticle&sid=1894.

[38] CrySys Lab. *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks,* Budapest, 2012. Budapest University of Technology and Economics.

[39] Aleks. *The Flame: Questions and Answers,* Moskova: Kaspersky Lab, 2012.

[40] Zetter, K. *Wired: Mahdi, the Messiah, Found Infecting Systems in Iran* [verkkojulkaisu]. Israel, 2012 [viitattu 25.4.2013]. Saatavissa: http://www.wired.com/thr-eat-level/20-12/07/mahdi.

[41] Crapanzano, J. *SANS Institute: Deconstructing SubSeven, the Trojan Horse of Choice,* Bethesda, 2003.

[42] BitDefender. *BitDefender Malware and Spam Survey finds E-Threats Adapting to Behavioral Trends* [verkkojulkaisu]. 2009. [viitattu 25.4.2013]. Saatavissa: http://goo.gl/jflPs.

[43] ScanSafe. *Annual global threat report* [verkkojulkaisu]. Lontoo, 2009. Saatavissa: http://www.slideshare.net/kimrenejensen/scansafe-annual-global-threat-report-2009.

[44] Teeriaho, Jouko. *Salausmenetelmät* [verkkojulkaisu]. 2006. Rovaniemen ammattikorkeakoulu. Saatavissa: http://ta.ramk.fi/~jouko.teeriaho/krypto2006/salausmenetelmat2_7tiivisteetMACitallekirjoitus.pdf

[45] Command Five Pty Ltd. *SK Hack by an Advanced Persisten Threat* [verkkojulkaisu]. 2011. [viitattu 25.4.2013]. Saatavissa: http://www.command-five.com/papers/C5_APT_SK-Hack.pdf.

[46] Pullinen, M.-J. *Kriittisten tietojärjestelmien suojaaminen kyberuhilta.* Opinnäytetyö. Espoo, 2012. Laurea-ammattikorkeakoulu.

[47] Forbes. *Shopping For Zero-Days: A Price List For Hackers Secret Software Exploits* [viitattu 6.11.2013]. 2012. Saatavissa: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits.

[48] Specht, S. & Lee, R. 2004. *Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures,* Princeton, 2004. Princeton University.

[49] Addley, E. & Halliday, J. *The Guardian: Operation Payback cripples MasterCard site in revenge for WikiLeaks ban* [verkkojulkaisu]. 2010. [viitattu 27.4.2013]. Saatavissa: http://www.guardian.co.uk/me-dia/2010/dec/08/operation-payback-mastercard-website-wikileaks.

[50] Mele, S. *Cyber-weapons: legal and strategic aspects.* Italian Institute of Strategic Studies [verkkojulkaisu]. Versio 2. Italia. 2013. [viitattu 6.11.2013]. Saatavissa: http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf.

[51] McAfee. *In the Crossfire - Critical Infrastructure in the Age of Cyber War* [verkkojulkaisu]. 2010. [viitattu 27.4.2013]. Saatavissa: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.

[52] McAfee. *In the Dark: Crucial industries Confront Cyberattacks* [verkkojulkaisu]. , 2011. [viitattu 27.4.2013]. Saatavissa: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf.

[53] Stiennon, R. *Surviving Cyberwar.* Plymouth: Government Institutes, 2010.

[54] Geers, K. *Strategi Cyber Security.* CCD COE Publications, 2011.

[55] Tillikainen, S. & Manner, J. *Suomen automaatioverkkojen haavoittuvuus,* Helsinki, 2013. Aalto-yliopisto.

[56] Mimoso, M. *Threatpost* [verkkojulkaisu]. 2013. [viitattu 29.4.2013]. Saatavissa: http://threatpost.com/shodan-search-engine-project-enumerates-internet-facing-critical-infrastructure-devices-010913.

[57] BBC News, 2009. *US man 'stole 130m card numbers'* [verkkojulkaisu]. [viitattu 29.4.2013]. Saatavissa: http://news.bbc.co.uk/1/hi/world/americas/8206305.stm.

[58] Harris, S. *CISSP All-In-One Exam guide.* 4. painos toim. McGraw-Hill, 2008.

[59] Goodin, D. *Arstechnica: Backdoor in computer controls opens critical infrastructure to hackers* [verkkojulkaisu]. 2012. [viitattu 2.5.2013]. Saatavissa: http://arstechnica.com/secu-rity/2012/10/backdoor-in-computer-controls-opens-critical-infrastructure-to-hackers.

[60] Academic. *Greek telephone tapping case 2004-2005* [verkkojulkaisu]. 2010. [viitattu 3.5.2013]. Saatavissa: http://en.academic.ru/dic.nsf/enwiki/1894956.

[61] Rantapelkonen, J. & Salminen, M. *The Fog of Cyber Defence.* Helsinki: Juvenes Print Oy, 2013. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos. ISBN 978-951-25-2430-3.

[62] Borkin, M., Prowell, S. & Kraus, R. *Seven Deadliest Network Attacks.* Waltham: Syngress, 2010.

[63] Nurminen, J. *Password Crackers.* Lappeenranta, 2002.

[64] Spencer, W. *Tech-Faq: Understanding Network Attacks* [verkkojulkaisu]. [viitattu 3.5.2013]. Saatavissa: http://www.tech-faq.com/network-attacks.html.

[65] BBC News: Techology. *Hackers 'hit' US water treatment systems* [verkkojulkaisu]. 2011. [viitattu 25.4.2012]. Saatavissa: http://www.bbc.co.uk/news/technology-15817335.

[66] Cohen, J. *Most Dangerous Computer Virus Threatens Critical Infrastructure* [verkkojulkaisu]. 2012.

[67] McAfee. *Five Ways to Protect Critical Infrastructure* [verkkojulkaisu]. 2010. Saatavissa: http://goo.gl/pL9Yqy.

[68] Sampakoski, I. & Sihvo, J. *Tietoturvaohjeistus.* Opinnäytetyö. Tampere, 2006. Tampereen Ammattikorkeakoulu. Saatavissa: http://publications.theseus.fi/bit-stream/handle/10024/10117/TMP.objres.848.pdf?sequence=2.

[69] Järvinen, P. *Tietoturva & yksityisyys.* Jyväskylä: Docendo, 2002. ISBN 978-951-8-46152-7.

[70] Smith, T. *Hacker jailed for revenge sewage attacks: The Register* [verkkojulkaisu]. 2001. [viitattu 3.6.2013]. Saatavissa: http://www.theregister.co.uk/2001/10/31/hac-ker_jailed_for_reven-ge_sewage.

[71] Office of Energy Assurance U.S. Department of Energy. *21 Steps to Improve Cyber Security of SCADA Networks.* 2011.

[72] Andress, J. & Winterfeld, S. *Cyber Warfare Techniques, Tactics and Tools for Security Pratctitioners.* Walthan, Yhdysvallat: Syngress Publishing, 2011.

[73] F-Secure. *F-Secure Anti-Virus datasheet.* San Jose. 2012

[74] Sillberg, R. *Tietoverkkoon tunkeutumisen havaitseminen SNORT:in avulla.* Opinnäytetyö. Pori, 2008. Satakunnan ammatikorkeakoulu.

[75] Raatikainen, K. *Johdatus tietojenkäsittelytieteeseen: Tarinoita tietojenkäsittelytieteen osa-alueilta -luentomoniste*. Helsinki, 2007. Helsingin yliopisto.

[76] Linden, M. *Identiteetin- ja pääsynhallinta –luentomoniste.* Tampere, 2012. Tampereen Yliopisto.

[77] Silverskin Information Security Oy. *Tietoturvatarkastukset* [verkkojulkaisu]. [viitattu 29.7.2013]. Saatavissa: http://www.silverskin.com/palvelut/tietoturva-tarkastukset.

[78] Passeri, Paolo. *September 2013 Cyber Attacks Statistics* [verkkojulkaisu]. [viitattu 14.11.2013]. Saatavissa: http://hackmageddon.com/category/security/cyber-attacks-statistics.

[79] Zetter, Kim. Wired: *Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report* [verkkojulkaisu]. [viitattu 14.11.2013]. Saatavissa: http://www.wired.com/threat-level/2011/11/water-pump-hack-mystery-solved.

[80] Hiltunen, A-K. Ulkopolitiikka: *Kyberasekilpa kiihtyy* [verkkojulkaisu]. [viitattu 14.11.2013]. Saatavissa: http://www.ulkopolitiikka.fi/artikkeli/1063/kyber-asekilpa_kiihtyy.

[81] SearchSecurity. *Zero-day exploit* [verkkojulkaisu]. [viitattu 14.11.2013]. Saatavissa: http://searchsecurity.techtarget.com/definition/zero-day-exploit.

[82] Sotilasaikakausilehti. *Sotilaalliset kybersuorituskyvyt – Toimintaympäristön tarkastelua, osa 1.* 12/2013.

[83] Viestintävirasto. *Kyberturvallisuuskeskus vahvistaa Viestintäviraston nykyisiä tietoturvatehtäviä* [verkkojulkaisu]. [viitattu 28.1.2013]. Saatavissa: https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2013/kyberturvallisuuskeskusvahvistaaviestintavirastonnykyisiatietoturvatehtavia.html

[84] Kiravuo, T. & Särelä, M. & Manner, J. *Kybersodan taistelukentät*. Sotilasaikakauslehti, 2013. ISSN 0038-1675

[85] CGI. *Offensiivioperaatiot, Kyberaseet* [näyttöesitys]. [viitattu 29.1.2014].