LAUREA AMMATTIKORKEAKOULU Uuden edellä

Kriittisten tietojärjestelmien suojaaminen kyberuhilta

Mika-Jan Pullinen

Leppävaara 2012

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Kriittisten tietojärjestelmien suojaaminen kyberuhilta

Mika-Jan Pullinen
Tietojenkäsittelyn koulutusohjelma, YAMK
Opinnäytetyö
Toukokuu 2012

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma, Ylempi AMK

Tiivistelmä

Mika Pullinen

Kriittisten tietojärjestelmien suojaaminen kyberuhilta

Vuosi 2012 Sivumäärä 86

Tutkimuskysymys ja Teema

Nykyaikana yhteiskunnan kriittisen infrastruktuurin toiminta on entistä enemmän riippuvainen tietojärjestelmistä. Opinnäytetyössä esitellään viime vuosina maailmalla tapahtuneita kyberhyökkäyksiä, joilla on ollut vaikutuksia kriittisten järjestelmien toimintaan. Kuvaamalla aiheeseen liittyvä keskeinen lainsäädäntö ja kansalliset toimijat, saadaan käsitys Suomen kyvykkyydestä puolustaa omia kriittisiä järjestelmiä. Lisäksi käydään läpi niiden maiden kyvykkyyksiä, jotka panostavat vahvasti kyberavaruuteen uutena sodankäynnin kenttänä.

Hyökkäykseen ja puolustukseen käytettävistä menetelmistä käsitellään suosituimmat, sekä ne tunnetut hyökkäysmenetelmät, jotka erityisesti voisivat aiheuttaa vahinkoa kriittiselle infrastruktuurille. Opinnäytetyön laatimisen yhteydessä kertyneiden havaintojen perusteella esitellään suosituksia kriittisten järjestelemien suojaamiseksi. Suosituksissa esitetään muun muassa, että järjestelmien omistajien vastuulla on tunnistaa kriittiset järjestelmät ja käynnistää niihin liittyvä tietoturva-auditointiprosessi. Kriittisille järjestelmille ehdotetaan lisäksi luotavan oma auditointikriteeristö, joka ei perustu pelkästään järjestelmässä olevan tiedon suojaustasoon, vaan myös järjestelmän toiminnan lamautumisen yhteiskunnallisiin vaikutuksiin.

Opinnäytetyössä on käytetty tutkimusotteena suunnittelututkimusta, jonka tavoitteena on luoda jotain uutta. Kriittisten järjestelmien suojaamisen apuvälineeksi on esitetty kolmiosaista mallia, joka on mahdollista jatkokehittää sovellukseksi. Suojausmallin luomisessa on hyödynnetty Hevnerin ryhmän seitsemää ohjetta. Ohjeet soveltuvat erityisesti tietojärjestelmätutkimukseen, jossa tavoitteena on kehittää jotain uutta. Mallissa esitetään suoritettavan uhka-analyysiä valtiollisten ja ei-valtiollisten toimijoiden muodostamien uhkien seuraamiseksi. Uhkien analysoinnin lisäksi kuvataan esimerkki kriittisten järjestelmien korkean tason tilannekuvan seuraamiseksi.

Suojausmallin avulla voidaan parhaimmillaan parantaa olennaisesti yhteiskunnan kannalta kriittisten tietojärjestelmien tietoturvaa. Opinnäytetyössä esiteltävät kyberhyökkäykset tuovat esille tietotekniikan jatkavasti kasvavan merkityksen sodankäynnissä. Yhteiskunnan kriittisiä järjestelmiä ei kuitenkaan suojata pelkästään valtiollisilta toimijoilta, vaan myös ei-valtiollisilta toimijoilta. Kyberterroristit, krakkerit ja haktivistit voivat hyökätä kriittisiä järjestelmiä vastaan. Opinnäytetyö tarjoaa tiivistetyn tietopaketin kyberturvallisuuteen liittyvistä asioista, tietoa voidaan hyödyntää esimerkiksi kyberturvallisuusstrategian rakentamisen yhteydessä.

Asiasanat: kriittiset järjestelmät, kyber, tietoturva, informaatiosodankäynti, hyökkäys, suojautuminen, uhka, suunnittelututkimus

Laurea-university of Applied Sciences
Laurea Leppävaara
Information Technology Programme
Information Systems and Data Communication

Abstract

Mika Pullinen

Protection of Critical Information Systems against Cyber Attacks

Year 2012 Pages 86

Critical infrastucture is nowadays more and more dependent on information systems. This thesis introduces cyber attacks which have had impact on critical information systems around the world. By describing Finnish legislation and key actors on the field of information security, one can make conclusions about Finnish national capabilities to defend our critical Information systems. Cyberwarfare capabilites of some nations which are strongly investing in the cyber domain, are also shortly described. Most common attack and defence methods are introduced along with those methods that can especially pose a threat to critical information systems. Recommendations to improve protection of critical systems are created based on the work done during composition of the thesis. The recommendations include the necessity to define which systems are critical. Furthermore, creating information security auditing criteria focusing on critical systems is suggested. The criteria should not only be based on the security classification of the data processed on the system. The effects that system malfunction or interruption of services would cause should be also considered.

Design Science is used as a research approach in the thesis. Design science is used for creating something new. The thesis introduces a model that can be used as an extra tool to protect critical systems. A new artefact is created based on Hevners seven guidelines. The model can be developed further to an application. Model includes a threat analysis of state and non-state actors. The model also includes an operational picture of the statuses of critical information systems.

Information Security of national Critical Information Systems can be significantly improved with this new defence model. The thesis hilights the growing meaning of information warfare alongside traditional warfare.

Keywords: critical information systems, cyber, information security, information warfare, attack methods, defence methods, threats, design science

Sisällys

1 Johdanto ja tutkimusmenetelmät

Organisoitu kyberhyökkäys voi vaarantaa kansallisen kriittisen infrastruktuurin turvallisuuden. Organisaatioiden kriittisten infrastruktuurien osiot ja niiden ulkoiset tukirakenteet, kuten Internet ja sen mekanismit, ovat merkittävä rajapinta potentiaaliselle kyberhyökkäykselle. Haavoittuvuudet johtuvat teknologisista heikkouksista sekä teknologian vääristä implementointi- ja valvontatavoista (Valkoinen talo 2011, 3). Nykyään valtaosa yhteiskunnan palveluista on tavalla tai toisella riippuvaista tietotekniikasta. Moderni tietoyhteiskunta on siten myös altis uudenlaisille uhkille, joista kaikkia on lähes mahdotonta ennakoida. Uusia tietoturvastandardeja, ohjeita ja kriteeristöjä, joiden avulla kyberuhilta suojaudutaan, on laadittu kansallisesti ja kansainvälisesti runsaasti viime vuosina (KATAKRI, VAHTI-ohjeet, PCI-DSS, ISO/IEC 27002, Common Criteria, ISF SOGP 2011). Opinnäytetyössä haetaan vastausta siihen, mitkä ovat ne kohteet, jotka ensisijaisesti tulisi turvata, ja mitä suojausmenetelmiä voidaan hyödyntää. Työssä selvitetään maailmalla sattuneita tietoturvatapauksia sekä sitä, miten kyberuhkiin on kansainvälisesti varauduttu. Näitä tietoja analysoimalla luodaan toimenpidesuosituksia Suomen kansallisen kyberturvallisuuden parantamiseksi yhteiskunnalle kriittisten tietojärjestelmien osalta.

1.1 Toimeksiannon kuvaus ja rajaukset

Opinnäytteessä selvitetään, mitä kyberuhkia kansalliselle turvallisuudelle on olemassa esittelemällä viime vuosina esiintyneitä keskeisimpiä kyberhyökkäystapauksia ja arvioimalla lähitulevaisuuden uhkia. Työssä ei kuvata kansallisesti kriittisten järjestelmien teknisiä yksityiskohtia eikä käsitellä muuta kuin julkista tietoa. Opinnäytetyössä keskitytään ainoastaan teknisen tietoturvan näkökulmaan. Teknisellä tietoturvallisuudella tarkoitetaan organisaation tietotekniikkaan, kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttöön, liittyvää tietoturvallisuutta (Valtiovarainministeriö 2006, 29). Hallinnollinen turvallisuus, fyysinen turvallisuus ja henkilöstöturvallisuus rajataan työn ulkopuolelle. Rajaus pohjautuu opintokokonaisuuden sisältöön, joka on puhtaasti tietotekniikkapainotteinen.

Tietoturvastandardeissa ja kriteeristöissä on painotettu usein sitä, miten järjestelmiä tulisi kehittää turvallisemmiksi. Tässä opinnäytetyössä käsitellään ensin, miltä uhkilta järjestelmiä ollaan suojaamassa, ja analysoidaan uhkien pohjalta tarvittavat suojaustoimet. Selvittämällä, mitkä järjestelmät ovat kriittisiä, mitä tietoturvallisuusloukkauksia maailmalla on tapahtunut ja mitkä ovat tulevaisuuden trendit, voidaan suosittaa, mihin kohteisiin tietoturvastandardien ohjeistamat toimet tulisi ensisijaisesti kohdistaa. Samalla pyritään muodostamaan karkeaa tilannekuvaa maiden kyvykkyyksistä kyberhyökkäyksiin ja niiden torjuntaan.

Opinnäytetyöllä haetaan vastausta seuraaviin tutkimuskysymyksiin:

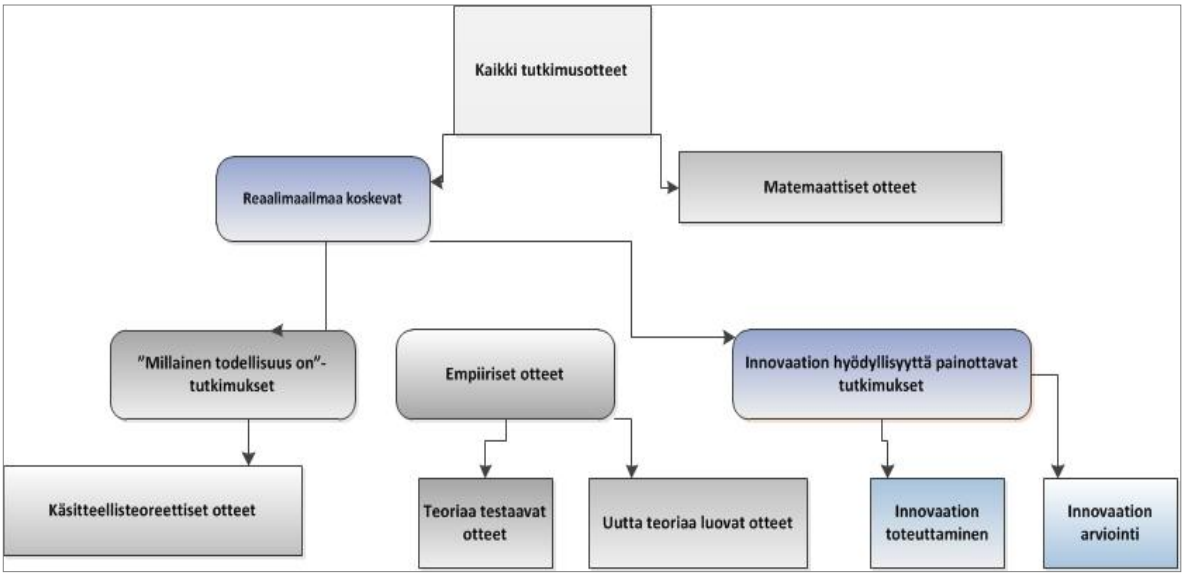
1. Miten kriittiset järjestelmät tulisi suojata?
2. Miten kansalliset ohjeistukset ja lainsäädäntö soveltuvat kriittisten tietojärjestelmien suojaamiseen?
3. Mitkä ovat kyberuhkia kansallisen turvallisuuden kannalta?
4. Mitkä ovat kriittisiä järjestelmiä?
5. Miten valittu tutkimusmenetelmä soveltuu tietoturvauhkilta suojaavaan kehikon luontiin?
6. Miten muissa maissa varaudutaan kybersodankäyntiin?

1.2 Aineisto ja sisältö

Suunnittelutieteellisen tutkimuksen metodiikan osalta lähteenä käytetään informaatioteknologiaan liittyvää kirjallisuutta ja tieteellisiä artikkeleja. Kybersodankäynnin uhkien kuvaamisessa ja kriittisten järjestelmien tunnistamisessa hyödynnetään aiheeseen liittyvää kirjallisuutta ja julkisia tietolähteitä. Kriittisten järjestelmiin liittyviä hyökkäys- sekä suojausmenetelmiä käydään läpi teknisen kirjallisuuden ja julkisten lähteiden avulla.

1.3 Tutkimusmetodin valinta

Tutkimusmetodin valinnassa on hyödynnetty Järvisen ja Järvisen tutkimusmetodien taksonomiaa (kuva 1). Tutkimusotteet on jaettavissa kahteen luokkaan sen mukaan, tutkitaanko reaalimaailmaa vai sellaisia symbolijärjestelmiä, joille ei ole vastinetta reaalimaailmassa (Järvinen & Järvinen 2004, 9). Jälkimmäinen näistä käsittää matemaattiset tutkimukset, joten ei-reaalimaailmaan soveltuvat tutkimusmetodit voidaan rajata suoraan pois tämän aihealueen yhteydestä. Reaalimaailmaa koskevat tutkimusotteet on jaettavissa kahteen luokkaan sen mukaan, painotetaanko reaalitodellisuutta vai innovaation hyödyllisyyttä. Reaalimaailmaan liittyvät tutkimusotteet voidaan jakaa edelleen kahteen ryhmään, joista toisessa käsitellään empiirisiä tutkimusotteita ja toisessa käsitteellis-teoreettisia otteita. Käsitteellis-teoreettiset tutkimukset liittyvät tietyn ilmiön analysointiin tai määrittelyyn siitä, mitä tietystä ilmiöstä oletetaan. Empiiriset tutkimusotteet ovat jaettavissa teoriaa testaaviin sekä uutta teoriaa luoviin (Järvinen 2004, 8-10).



Kuva 1: Tutkimusmetodien valinta Järvisen ja Järvisen tutkimusmetodien taksonomian pohjalta.

Tämän työn tavoitteena ei ole luoda uutta teoriaa eikä testata teoriaa, eikä se liity tietyn ilmiön analysointiin tai määrittelyyn. Täten tutkimusmetodeista voidaan rajata pois kaikki reaalimaailmaa koskevat tutkimusotteet, joissa käsittelyn painopisteenä on se, millainen todellisuus on. Tällä poissulkevalla tutkimusotteiden valintatavalla päädytään siihen, että Järvisen ja Järvisen esittämästä tutkimusmetodien taksonomiasta jäljelle jäävät ainoastaan innovaation hyödyllisyyttä painottavat tutkimusmetodit. Edellä mainitut metodit ovat jaettavissa kahteen joukkoon, joista toinen sisältää innovaation toteuttamisen ja toinen innovaation arvioinnin (Järvinen 2004, 10). Opinnäytetyön tehtävänantona on selvittää, mitkä ovat kriittisten järjestelmien kannalta kyberuhkia ja miten niiltä voidaan suojautua. Suojautumismenetelmät tunnistettuja uhkia vastaan ovat työn varsinainen innovaatio. Jatkossa innovaatiosta käytetään sanaa artefakti, joka viittaa tekniseen innovaatioon. Artefaktin toteuttamisen lisäksi työssä arvioidaan, miten artefakti vastaa tavoitteenasettelua ja miten sitä voidaan hyödyntää jatkossa, eli arvioidaan artefakti. Hevner ja muut ovat esittäneet seitsemän ohjetta suunnittelutieteellisen tutkimuksen tekemiseksi. Artefakti suunnitellaan, toteutetaan ja arvioidaan heidän ohjeittensa pohjalta.

1.4 Suunnittelutieteellinen tutkimus ja tietojärjestelmät

Suunnittelutiede (engl. design science) on tietoyhteiskunnan kehittymisen myötä laajentunut koskettamaan tietoteknisiä järjestelmiä. Suunnittelu on integroiva prosessi – osien syntetisointia kokonaisuudeksi. Tiede on looginen ja järjestelmällinen menetelmä tutkia sekä järkeistää tietoa ja kokemuksia (Brown & Cook & Gabel 2011, 5).

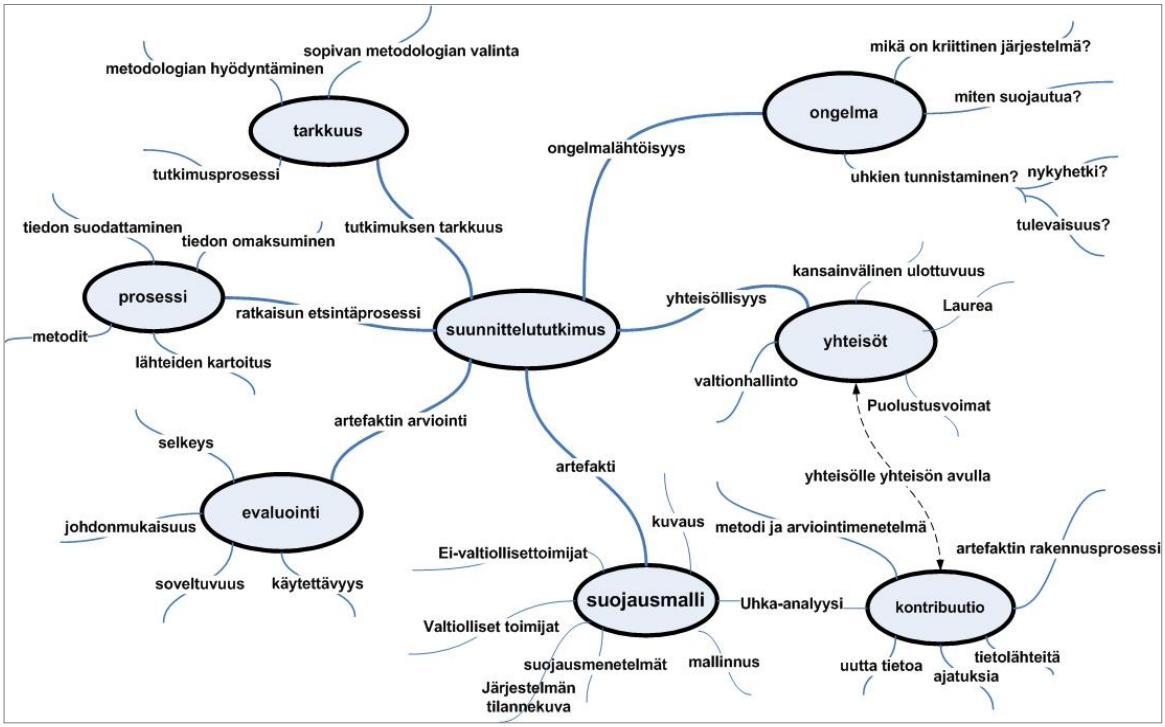
Buckminster Fuller, jota pidetään yleisesti termin suunnittelutiede keksijänä, määritti sanan järjestelmä (system) seuraavalla tavalla. Järjestelmä koostuu kahdesta tai useammasta toisiinsa liittyvästä elementistä, jotka voivat olla jakautuneet useampaan osaan. Ihmisen keho on järjestelmä, joka koostuu elimistä, soluista, molekyyleistä, atomeista ja niin edelleen. Tutkija Robert Blissmer on kirjoittanut järjestelmistä seuraavasti: ”Sen vuoksi, että maailmankaikkeus on suurin tiedossa oleva järjestelmä, kaikki muu määriteltävissä oleva jakautuu kahteen lähtökohtaiseen osaan: järjestelmään itseensä ja sen ympäristöön” (Brown ym. 2011, 7). Informaatioteknologiaan liittyvissä tutkimuksissa ei keskitytä luonnonilmiöihin, vaan keinotekoisiin ilmiöihin. Niissä käsitellään ihmisten luomia keksintöjä, kuten tietoliikennetekniikoita, salausjärjestelmiä ja tietojärjestelmiä. Tähän tietotekniikan mukanaan tuomaan ulottuvuuteen Hevner ja muut ovat kehittäneet uusia suunnittelututkimusta hyödyntäviä malleja ja laajennuksia (Hevner & March & Park & Ram 2004, 77).

Opinnäytetyössä käsitellään kriittisten tietojärjestelmien suojaamista, joten on oleellista selvittää tietojärjestelmän käsite suunnittelutieteen näkökulmasta ja kriittisen tietojärjestelmän toiminta yhteiskunnan näkökulmasta. Fuller määritti järjestelmän useasta osasta koostuvana kokonaisuutena. Steven Alterin mukaan järjestelmän, kuten vaikka ihmisen tai laitteen, toimintaa voidaan kehittää tietojärjestelmän avulla. Olemassa oleva laite tai ihminen voidaan jossain tapauksessa myös korvata osittain tietojärjestelmän avulla. Tietojärjestelmä palvelee tiettyä käyttötarkoitusta ja keskittyy tiedon prosessointiin, joka käsittää tiedon siirtämistä, tallentamista, hakemista, arkistointia, muokkaamista ja esittämistä (Alter 2008, 451). Opinnäytteessä käytetään tätä Alterin esittämää määritelmää yleiskäsitteenä sanasta tietojärjestelmä.

1.5 Hevnerin ryhmän seitsemän ohjetta

Hevner ja hänen ryhmänsä kehittivät seitsemän ohjetta, jotka auttavat tietojärjestelmätutkijoita suorittamaan, arvioimaan ja esittämään suunnittelutieteellistä tutkimusta. Nämä seitsemän ohjetta koostuvat artefaktista, ongelmakeskeisyydestä, evaluoinnista, tutkimuksen kontribuutiosta, tieteellisestä eksaktiudesta, tutkimusprosessista ja yhteisöllisyydestä. Ensimmäisessä ohjeessa käsitellään artefaktia, mikä tarkoittaa, että suunnittelututkimuksen täytyy tuottaa toteuttamiskelpoinen artefakti, joka muodostuu konstruktiosta, mallista, metodista tai instanssista, joka on implementoitu ja testattu (Hevner ym. 2004, 82-83). Tässä työssä artefakti koostuu suojausmallista, joka sisältää suojattavan järjestelmän tilannekuvan sekä valtiollisten ja ei-valtiollisten toimijoiden uhka-analyysin.

Hevnerin ryhmän seitsemän ohjeen hyödyntäminen opinnäytetyössä on mallinnettu kuvassa 2. Hevnerin toinen ohje kuvaa ongelmakeskeisyyden, jossa teknologiaperustaisen ratkaisun on vastattava merkittävään ja oleelliseen liiketoimintakeskeiseen ongelmaan. Kolmas ohje korostaa eksaktin tieteellisen tutkimusotteen käyttämistä; tutkimusotteessa artefaktin käytettävyys, laatu ja tehokkuus on osoitettava evaluointimenetelmien avulla. Neljännessä ohjeessa käsitellään yhteisöllisyyttä, jonka avulla suunnittelututkimuksen tulee tuottaa selkeää ja todennettavaa kontribuutiota tiedeyhteisölle (Hevner ym. 2004, 81-90). Kontribuutio muodostuu artefaktin innovaatiosta ja uskottavista väitteistä, joilla osoitetaan sen hyödyllisyys (March & Smith 1995, 260). Viidennessä ohjeessa keskitytään tieteelliseen tarkkuuteen: eksaktien tieteellisten menetelmien käyttäminen on osoitettava artefaktin rakentamisen ja evaluoinnin yhteydessä. Kuudes ohje sisältää ratkaisunetsintäprosessin, jossa valitaan tutkimusmenetelmä, kartoitetaan lähteitä, suodatetaan ja omaksutaan tietoa. Viimeisessä ohjeessa kehotetaan julkaisemaan työ sekä tieteellisessä yhteisössä että tutkimuksen viitekehyksen piiriin kuuluvassa toimialakentässä.



Kuva 2: Artefaktin muodostaminen Hevnerin ohjeiden mukaan.

1.6 Opinnäytetyön rakenne suhteessa tutkimusmenetelmään

Opinnäyteyön ensimmäinen ja viimeinen luku käsittelevät Hevnerin ohjeiden kohtia tieteellinen tarkkuus ja evaluointi. Ensimmäisessä luvussa valitaan tutkimusmenetelmä ja perustellaan valinta. Tutkimusmenetelmän valinta ja hyödyntäminen kuvataan ensimmäisessä luvussa, kun taas viimeisessä luvussa saatuja tuloksia verrataan evaluoinnin jälkeen ensimmäisessä luvussa esitettyihin tutkimuskysymyksiin. Hevnerin kuudennen ohjeen mukainen tutkimusprosessi luonnehtii koko työtä: siihen sisältyy muun muassa lähteiden kartoittaminen, tiedon suodattaminen ja omaksuminen sekä ratkaisun etsintä (kuva 2). Viimeinen luku käsittelee myös työstä saatavaa kontribuutiota ja työyhteisöllisyyttä, jotka Hevnerin ryhmä on esittänyt ohjeissaan neljä ja seitsemän.

Luvussa kaksi esitellään kybersodankäynti käsitteenä sekä kuvataan yhteiskunnan kannalta kriittiset järjestelmät ja aiheeseen liittyvä lainsäädäntö. Kolmas luku selvittää kybersodankäyntiin liittyviä tapauksia maailmalta. Neljännessä ja viidennessä luvussa käsitellään hyökkäys- sekä puolustusmenetelmiä teknisestä näkökulmasta. Toinen ja kolmas luku sivuavat Hevnerin ohjeista tutkimusprosessin lisäksi ongelmalähtöisyyttä. Niissä määritellään, mikä on kriittinen järjestelmä ja mitä uhkia kriittisille järjestelmille on olemassa. Kuudennessa luvussa esitellään varsinainen artefakti, joka tarjoaa uhkiin liittyviä seurantatyökaluja kriittisten järjestelmien suojaamisen avuksi.

2 Kybersodankäynti ja kriittiset tietojärjestelmät

Kyber-alkuisten sanojen käyttö on laajentunut erityisesti 2000-luvulla, mutta niiden juuret juontavat viime vuosisadan puoliväliin. Norbert Wiener julkaisi vuonna 1948 kirjan nimeltä Cybernetics, joka käsittelee järjestelmien hallinta- ja viestintätapahtumien teoriaa. Kybernetiikka tutkii itseohjautuvia järjestelmiä, ja sitä hyödynnetään biologisten sekä teknisten järjestelmien mallinnukseen (McGarry 2008).

Sana kyber yleistyi William Gibsonin vuonna 1984 julkaiseman Neuromancer-tieteisnovellin ansiosta (Kramer & Starr & Wentz 2010, 24). Yksi usein käytetty kyber-alkuinen termi on kyberavaruus. Clarken mukaan kyberavaruus koostuu kaikista maailman verkoista sekä jokaisesta laitteesta, joihin niiden avulla otetaan yhteyttä (Clarke & Knake 2010, 10).

Kybersodankäynnin käsite on jalostunut aiemmin laajasti käytetystä informaatiosodankäynnin käsitteestä. Tom Rona julkaisi vuonna 1976 informaatiosodankäynnin konseptin. Informaatiosodankäynnistä ja kybersodankäynnistä on useita hiukan toisistaan poikkeavia käsityksiä, joiden semanttisiin yksityiskohtiin ei ole tarkoituksenmukaista tarttua tässä työssä. Kybersodankäynnin taistelukenttä voi siten rajoittua yksittäiseen laitteeseen tai sen komponenttiin tai koskettaa jopa maailmanlaajuisia verkkoja (Kramer ym. 2010, 30-34).Yhdysvaltain puolustusministeriö ja Pohjois-Atlantin sotilasliitto NATO luokittelevat kyberavaruuden viidenneksi sodankäynnin toimintaympäristöksi (engl. domain) perinteisten maa-, meri-, ilma- ja avaruustoimintaympäristöjen lisäksi (Yhdysvaltojen puolustusministeriö 2011, 5). Sotilas- ja tiedustelujohtajat ovat yhtä mieltä siitä, että seuraava suuri sota käydään perinteisen taistelukentän sijasta todennäköisemmin kyberavaruudessa (Stiennon 2010, 173).

Termi kyberterrorismi muodostui ensimmäisen kerran vuonna 1996 kyberavaruus- ja terrorismi-sanojen yhdistelmästä. Ensimmäisenä termiä alkoi käyttää Yhdysvaltojen armeija. Vuonna 1998 Yhdysvaltojen kansainvälisten ja strategisten tutkimusten laitos julkaisi raportin nimeltä Cybercrime, Cyberterrorism, Cyberwarfare, Averting an electronic Waterloo. Siinä pohdittiin kyber-alkuisten käsitteiden suhteita sekä sitä, mitä uhkia kyberavaruudessa on muodostumassa ja mitkä ovat niiden vaikutukset (Clarke ym. 2010, 8). Kyberterrorismi on tietotekninen hyökkäys tai uhka, jolla pelotellaan tai pakotetaan hallituksia tai yhteisöjä terroristien tavoitteiden saavuttamiseksi. Useimmiten kyberterroristin tavoitteet ovat poliittisia, uskonnollisia tai ideologisia. Hyökkäyksen on aiheutettava riittävää tuhoa tai sekasortoa, mikä luo perinteisiin terrori-iskuihin verrattavaa pelkoa. Tällainen isku voi olla lentokoneen pudottaminen, sähköverkon lamauttaminen tai juomaveden saastuttaminen, tai se voi kohdistua taloudellisiin järjestelmiin (Kramer ym. 2010, 438).

Kybersodankäynti on yksittäisen maan tai usean maan liittouman käynnistämä hyökkäys tietojärjestelmiä ja tietoverkkoja vastaan, tavoitteena aiheuttaa viholliselle tappioita. Päältäpäin katsottuna kyberrikollisuus, kyberterrorismi ja kybersodankäynti voivat vaikuttaa varsin samankaltaisilta.

Käsitteiden eroavaisuuksia voidaan hahmottaa kuvitteellisen esimerkin avulla: Sairaalan tietokantaan murtaudutaan ja suuryritystä johtavan henkilön potilastietoja väärennetään. Kyseinen yritys on ollut pitkään kansalaisaktivistien kritiikin kohteena ympäristöä saastuttavan toimintansa johdosta. Murtautuja poistaa johtajan potilastiedoista tiedon hänelle vaaralliseste allergiasta, mikä aiheuttaa johtajan kuoleman, kun hänelle annetaan väärä lääkitys. Tässä tapauksessa merkitys ei ole tekijän käyttämissä menetelmissä, vaan teon tarkoituksessa. Mikäli teko johtui kahden henkilön huonoista väleistä, kyse on kyberrikollisuuden lisäksi murhasta. Mikäli tekijä myöhemmin ilmoittaisi, että hän on valmis samanlaisiin tekoihin, jollei hänen esittämiinsä vaatimuksiinsa vastata, on kyse kyberterrorismista. Kybersodankäynnin tunnusmerkit täyttyisivät vasta, jos vieraan valtiovallan kybersotilaat suorittaisivat iskun suuryrityksen johtajan potilastietoihin tavoitellen johtajan kuolemalla strategista etua valtiolleen (Janczewski & Collard 2009, 16).

Sota- ja taisteluteorioissa toiminta jaetaan yleensä kolmeen tasoon, jotka ovat strateginen, operatiivinen ja taktinen (Huopana 2011, 5). Kyberavaruus voidaan jaotella toimintaympäristönä taktiselle, operatiiviselle ja strategiselle tasolle, aivan kuten perinteisessä sodankäynnissä on totuttu. Tietojärjestelmiä on myös jo vuosikausia suunniteltu eri tarpeisiin sen mukaan, millä toimintatasolla niitä sodankäynnissä käytetään. Vielä 1990-luvun alkupuolella kyberavaruutta pidettiin normaalista fyysisestä todellisuudesta poikkeavana ympäristönä. Todellisuudessa se on fyysinen ympäristö, joka muodostuu fyysisistä verkoista ja järjestelmistä, joita hallinnoidaan ohjelmistojen ja tietoliikenneprotokollien avulla. (Kramer ym. 2010, 254). Taulukossa 1 on kuvattu kyberavaruuden kerrokset eräänlaisena mukaelmana OSI-mallista, joka on tunnettu tiedonsiirtoprotokollien viitemalli. Taulukko pohjautuu Kramerin kirjassa Cyber War: The Next threat to National Security and what to do about it esitettyyn ajatukseen (Kramer ym. 2010, 283-287).

Kerros	Selite	Esimerkkejä
Kyber	Tietopääoma, älykkyys	Tietoaineisto, käskyt, tietämys, ajatukset, suunnitelmat10
Verkkopalvelut	Palvelut, joiden käyttäjiä voivat olla ihmiset, tekniset laitteet tai tietojärjestelmät.	Sähköposti, aikapalvelu, tietoliikenteen salauspalvelut, kollaboraatiopalvelut
Fyysinen verkko	Infrastruktuuri, jonka päällä verkkopalveluita ajetaan. Muodostuu peruskomponenteista, joilla lähetetään elektronisia ja elektromagneettisia signaaleja	Puhelinverkot, taktiset kenttäradioverkot, IP-pohjaiset avoimet tai suljetut verkot, matkapuhelinverkot, satelliittiverkot
Peruskomponentit	Fyysiset elementit	Lähettimet, vastaanottimet, verkkokaapelit, reitittimet, modeemit

Taulukko 1: Kyberavaruuden kerrokset, muunnelma Kramerin esittämästä ajatuksesta

Kansallinen suorituskyky digitaalisella taistelukentällä muodostuu kolmesta tekijästä: kyvykkyydestä suorittaa kyberhyökkäyksiä, kyseisen maan riippuvuudesta tietoverkoista sekä keinoista puolustaa omia verkkoja ja tietojärjestelmiä. Yksittäisen maan on kyettävä esimerkiksi katkaisemaan kotimaahan ulkopuolelta kohdistuva verkkoliikenne. Yhdysvalloissa on tutkittu sitä, miten taktisen tason tietojärjestelmät käytännössä vaikuttavat sodankäyntiin. Tuloksista ilmenee, että vihollisen tappiot ovat yli kaksinkertaiset, kun hyödynnetään tietojärjestelmiä pelkän puheliikennepohjaisen käskynjaon lisäksi. Tämä on kuitenkin vasta alkua verrattuna siihen, millaisia vaikutuksia sodan tulokseen tietotekniikalla voidaan saada aikaiseksi iskemällä vihollisen kriittiseen infrastruktuuriin (Kramer ym. 2010, 287).

2.1 Kriittiset tietojärjestelmät

Kriittiseen infrastruktuuriin (Critical Infrastructure, CI) kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluita, joiden toimintakyvyn menettämisellä tai tuhoutumisella on halvaannuttava vaikutus yhteiskunnan turvallisuudelle sekä sosiaaliselle tai taloudelliselle hyvinvoinnille. Kriittisen infrastruktuurin suojeleminen (Critical Infrastrucure Protection, CIP) sisältää ne keinot, joilla kriittiseen infrastruktuuriin kohdistuvilta uhkilta voidaan suojautua. Kriittisen infrastruktuurin suojaamisen alakäsite on kriittisen tietoteknisen infrastruktuurin suojaaminen (Critical Information Infrastructure Protection, CIIP), jossa on haluttu korostaa tietotekniikan merkitystä suojaustoimissa. (Dunn & Mauer 2006, 178). Kriittisen infrastruktuurin ja kriittisen tietoteknisen infrastruktuurin käsitteiden eroa ei kuitenkaan ole selkeästi määritelty. Usein näillä käsitteillä ymmärretään eri asioita toimijan mukaan. Pelkät infrastruktuurit eivät ole itsessään kriittisiä, vaan kriittisiä ovat ne yhteiskunnalliset

toiminnot, joita infrastruktuurit mahdollistavat. Myöskään infrastruktuurijärjestelmä kokonaisuutena ei ole kriittinen, vaan sen sisällä olevilla komponenteilla on eriasteisia vaikutuksia järjestelmän toimivuudelle (Hagestam 2005, 16).

Professori Stefan Katzenbeisser esitelmöi joulukuussa 2011 Berliinissä yhteiskunnan haavoittuvuudesta kyberhyökkäyksille. Hän kuvasi muun muassa, miten palvelunestohyökkäyksillä saadaan lamautettua junaliikenne. Junaliikennettä ohjaavat vaihdejärjestelmät ovat perinteisesti olleet irti tietoliikenneverkoista, mutta nykyään junien ja vaihdejärjestelmien välinen liikenne hoidetaan yhä enemmän langattomia teknologioita hyödyntäen. Junaliikenteessä käytetään perinteistä GSM-liikennettä turvallisempaa R-GSM-tekniikkaa. Professori Katzenbeisserin mukaan suurin riski liittyy salausavaimien turvallisuuteen. Avaimia ladataan usein USB-tikuille, joita kierrätetään organisaation sisällä ennen kuin toimitetaan paikan päälle asennettavaksi. Tämä kasvattaa riskiä avainten joutumisesta vääriin käsiin. Vastaavia uhkia on tunnistettavissa raideliikenteen lisäksi muissa yhteiskunnalle tärkeissä kuljetuslogistiikkajärjestelmissä (Holmes 2011).

Vuonna 2010 päivitetyn yhteiskunnan turvallisuusstrategian (YTS) uhka-arvioissa on huomioitu muiden uhkien lisäksi kyberuhat. Strategian tavoitteena on turvata valtion itsenäisyys, yhteiskuntamme turvallisuus ja väestön elinmahdollisuudet kaikissa tilanteissa. Elintärkeiden toimintojen turvaaminen perustuu pitkäjänteiseen ja riittävään suorituskykyjen kehittämiseen, niiden oikea-aikaiseen ja joustavaan käyttöönottoon sekä kykyyn hyödyntää jo käyttöönotettuja suorituskykyjä. (Cederberg 2011, 30-31). Strategiassa esitetyissä uhkamalleissa on mainittu erikseen kyberuhkat, mutta muitakin uhkia tarkasteltaessa voidaan havaita, että niihin kaikkiin liittyy merkittävällä tavalla tietojärjestelmiä. Useimmilla Euroopan mailla on sisäisesti määritelty maakohtainen kriittinen infrastruktuuri, joka on Euroopan unionin tasolla yhdistetty yhteismitalliseksi kaikkia maita koskevaksi luetteloksi, osana eurooppalaista kriittisen infrastruktuurin suojeluohjelmaa . Taulukossa 2 on kuvattu yhteiskunnan kriittiseen infrastruktuuriin kohdistuvat uhkat. Taulukko on muodostettu yhdistelemällä yhteiskunnan turvallisuusstrategiassa ja Euroopan unionissa lueteltuja kriittisen infrastruktuurin kohteita siten, että mukaan on poimittu sellaisia kohteita, joissa on selkeästi tunnistettavissa tietotekninen ulottuvuus.

Suojattava kohde	Selite
Energiansiirto ja -jakeluverkot	Ohjaus-, hallinta-, jakelu- ja valvontajärjestelmät
Tietoliikenne	Katso taulukon 1 kohta fyysiset verkot
Vedenjakelu	Ohjaus-, hallinta-, jakelu- ja valvontajärjestelmät
Elintarvikepalvelut	Elintarvikkeiden tuotanto- ja jakelujärjestelmät
Kuljetuslogistiikka	Polttoainejakelu-, rautatietieverkko-, lennonjohto- ym. järjestelmät
Terveyspalvelut	Potilas- ja lääketietojärjestelmät sekä lääke- ja rokotetuotanto
Turvallisuuspalvelut	Poliisin, tullin, puolustusvoimien ym. järjestelmät. Rajavalvonta, sotilaallinen voimankäyttö, rikollisuudentorjunta
Ympäristöturvallisuus	Suuronnettomuuksilta, luonnonkatastrofeilta sekä ympäristöuhkilta varautumis- ja toipumisjärjestelmät
Finanssiala	Rahoitus- ja maksujärjestelmät

Taulukko 2: Kriittisen infrastruktuurin tietojärjestelmät

Kriittisen infrastruktuurin suojelussa suunnitellaan ja otetaan käyttöön ennaltaehkäiseviä menetelmiä, joiden tavoitteena on vähentää sodan, luonnonkatastrofin, suuronnettomuuden, siviililevottomuuden, vandalismin tai terrorismin aiheuttamaa riskiä. Monet kriittiset infrastruktuurit ovat hiljalleen muuttuneet toisistaan riippuvaisiksi, ja ne kuuluvat useille eri omistajille. Esimerkiksi sähkönjakelun katkeaminen vaikuttaa useaan muuhun kriittisen infrastruktuuriin ja erityisesti niihin liittyviin tietojärjestelmiin. Kriittinen infrastruktuuri linkittyy usein myös yli maan rajojen: öljyputket, rautatieverkot, maksuliikennejärjestelmät ja lentoliikenteen hallintajärjestelmät ovat usein kietoutuneet yhteen (Yhteiskunnan turvallisuusstrategia 2010, 66-74). Yleisradio uutisoi 24.3.2012, että pahin uhkakuva Suomelle on viiden minuutin kybersota, johon sisältyisi pankkien välisen maksuliikenteen pysäyttäminen, elintarviketoimitusten logistiikkajärjestelmien sekoittaminen, sähkönsiirtoverkon häiritseminen, tietoliikenneyhteyksien katkaiseminen sekä liikenteen häiritseminen (Yleisradio 2012) .

Suomessa Huoltovarmuuskeskus on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on huoltovarmuuden parantamiseen liittyvä suunnittelu ja operatiivinen toiminta. Huoltovarmuuskeskus määrittelee kriittisen infrastruktuurin käsitteen seuraavasti: ”Kriittinen Infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan jatkuvalle toiminnalle” (Huoltovarmuuskeskus 2011). Kriittisimpiä kohdeorganisaatioita tietojärjestelmien turvallisuuden osalta Suomessa ovat turvallisuusviranomaiset, julkishallinto, korkean teknologian yritykset, tietoliikenne- ja viestintäyritykset, pankit ja rahoituslaitokset sekä oppilaitokset (Puolustustaloudellinen suunnittelukunta 2000, 4).

Kriittisen infrastruktuurin turvaamisessa on huoltovarmuuskeskuksen määritelmän mukaan kolme ulottuvuutta: poliittinen, taloudellinen ja tekninen. Poliittiseen ulottuvuuteen sisältyy lainsäädäntö, kansalliset turvallisuustarpeet sekä niihin liittyvä kansainvälinen yhteistyö. Ta-

voitteena on saavuttaa samankaltaisia ratkaisuja maissa, joiden infrastruktuurin rakenteet ovat perusperiaatteiltaan yhteneväisiä. Poliittiseen ulottuvuuteen kuuluu eri maiden tarve tehdä yhteistyötä teknisen yhteistyön lisäksi yhtenäisen lainsäädännön ja turvallisuuspolitiikan saavuttamiseksi. Taloudellinen ulottuvuus sisältää kaikki taloudelliset toimijat, jotka rakentavat, omistavat ja hallinnoivat infrastruktuurijärjestelmiä. Tässä opinnäytetyössä painopisteenä oleva tekninen ulottuvuus puolestaan käsittää ne käytännön ratkaisut ja toimet, joita valtiot ja niiden sisäiset toimijat tekevät kriittisen infrastruktuurin toimintavarmuuden takaamiseksi muuttuvassa teknisessä ympäristössä. Näiden kolmen ulottuvuuden tulee toimia keskenään. Erityisen tärkeää turvallisuuden kehittämisessä on julkisen ja yksityisen sektorin sekä kansalaisjärjestöjen yhteistoiminta (Hagestam 2005, 16).

2.2 Keskeiset ohjeistukset ja lainsäädäntö Suomessa

Suomessa Valtiohallinnon tietoturvallisuuden johtoryhmä (VAHTI) julkaisee tietoturvaohjeita ja määräyksiä. Lokakuussa 2011 voimassa olevia ohjeita oli yhteensä 42 kappaletta, joista uusimmat ohjeet olivat vuodelta 2010 ja vanhimmat vuodelta 2000 (Valtiovarainministeriö 2011).

Puolustusministeriön johtovastuulle asetettiin vuonna 2008 luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö. Kansallisen turvallisuusauditointikriteeristön (KATAKRI) valmisteluun osallistui yli sata henkilöä viranomais-, järjestö- ja yrityskentästä. KATAKRIn ensimmäinen versio valmistui vuonna 2009 ja toinen versio julkaistiin vuonna 2011, kolmas versio on valmisteilla. KATAKRIn tarkoituksena on olla kansainvälisten tietoturvavelvollisuuksien täyttämisen työkalu sekä varmistaa valtionhallinnolle ulkoisia palveluita tarjoavan tahon toimintakyky turvallisuusluokitelluissa hankkeissa. Kriteeristö on pyritty rakentamaan ristiriidattomaksi VAHTI-ohjeiden ja muiden tietoturvaan liittyvien ohjeiden ja suositusten kanssa. Se tarjoaa myös yhtenäiset käytännöt kansallisen tason tietoturva-auditoinnille yksityiselle sektorille (Puolustusministeriö 2011a).

Valtiohallinnon eri toimintayksiköillä on käytössä KATAKRIn ja VAHTI-ohjeiden lisäksi omia tietoturvaan liittyviä ohjeistuksia ja määräyksiä. Suomessa voimassa olevia teknistä tietoturvaa koskevia lakeja ja asetuksia on kuvattu taulukossa 3. Niistä on havaittavissa, että lakien painopiste on viranomaisille asetetuissa vaatimuksissa ja tiedon suojaamisessa. Vuonna 2014 on tulossa voimaan uusi esitutkinta- ja pakkokeinolaki, joka on saanut paljon kritiikkiä, koska asiantuntijoiden mukaan se vaikeuttaa tietomurtojen tutkimista . Toisaalta se antaisi poliisille mahdollisuuden asentaa rikoksesta epäillyn tietokoneelle vakoilu- ja seurantaohjelmia. Jos laki toteutuu, se astuu voimaan vuonna 2014 (Vänskä 2012).

1.7.2010/681 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa Sisältö/tarkoitus: valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevat yleiset tietoturvallisuusvaatimukset sekä asiakirjojen luokittelun perusteet ja luokittelua vastaavat asiakirjojen käsittelyssä noudatettavat tietoturvallisuusvaatimukset
24.6.2004/588 Laki kansainvälisistä tietoturvallisuusvelvoitteista Sisältö/tarkoitus: viranomaisilta edelletyt toimenpiteet kansainvälisten tietoturvallisuusvelvollisuuksien täyttämiseksi
16.6/2004/516 Sähköisen viestinnän tietosuojalaki Sisältö/tarkoitus: turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä
30.11.2001/1117 Laki eräiden suojauksen purkujärjestelmien kieltämisestä Sisältö/tarkoitus: televerkon avulla tarjottavien tietoyhteiskunnan palvelujen suojaamiseen niiden suojauksen purkujärjestelmien oikeudetonta käyttöä vastaan
12.11.1999/1030 Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta Sisältö/tarkoitus: Viranomaisten on selvitettävä ja arvioitava asiakirjansa ja tietojärjestelmänsä sekä niihin talletettujen tietojen merkitys samoin kuin asiakirja- ja tietohallintonsa. Toimenpiteiden tarvetta arvioitaessa on kiinnitettävä huomiota siihen, kuinka toteutetaan 1) oikeus saada tietoja viranomaisten julkisista asiakirjoista 2) velvollisuus tuottaa ja jakaa tietoja sekä antaa tietoja keskeneräisistä asioista 3) henkilötietojen, erityisesti arkaluonteisten tietojen, suojaaminen 4) salassa pidettäviksi säädettyjen tietojen suojaaminen 5) tietojen käyttötarkoituksia koskevat rajoitukset 6) tietojen käytettävyys, eheys ja laatu viranomaisen tehtävän hoidossa ja viranomaisten yhteistyössä 7) tietojen laatu erityisesti käytettäessä niitä yksilöitä ja yhteisöjä koskevan päätöksenteon pohjana tai oikeuksien ja velvollisuuksien osoittajina. Hyvän tiedonhallintatavan toteuttamiseksi on lisäksi selvitettävä ja arvioitava tietojen saatavuuteen, käytettävyyteen, laatuun ja suojaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat sekä niiden vähentämiseksi ja poistamiseksi käytettävissä olevat keinot ja niiden kustannukset sekä muut vaikutukset.
18.12.1992 (1390/1992) Laki huoltovarmuuden turvaamisesta Lain tarkoituksena on poikkeusolojen ja niihin verrattavissa olevien vakavien häiriöiden varalta turvata väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömät taloudelliset toiminnot ja niihin liittyvät tekniset järjestelmät.
24.1.2003/13 Laki sähköisestä asioinnista viranomaistoiminnassa Sisältö/tarkoitus: lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa edistämällä sähköisten tiedonsiirtomenetelmien käyttöä.
22.4.1999/523 Henkilötietolaki Sisältö/tarkoitus: lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Taulukko 3: Tietoturvalait ja asetukset.

Näiden lakien ja asetusten lisäksi EU on antanut direktiivin 2008/114/EU kriittisen infrastruktuurin suojaamisesta. Sen tarkoituksena on turvata ne infrastruktuurit, jotka palvelevat kahta tai useampaa unionin jäsenvaltiota. Aluksi direktiivi koskee energia- ja logistiikkasektoreita (Lucas & Necesal 2011. 1249-1250).

Vuoden 2012 loppuun mennessä Suomessa julkaistaan kyberstrategia, jonka suunnitteluun osallistuu 17 julkishallinnon ja elinkeinoelämän asiantuntijaa. Tarkoituksena on selvittää, miten yhteiskunnan elintärkeät toiminnot suojataan. Arviolta noin 80 prosenttia yhteiskunnan kriittisistä toiminnoista on yksityisessä omistuksessa, joten elinkeinoelämän osallistuminen strategian suunnitteluun on tärkeää. Strategia määrittää kansallisten toimijoiden väliset suhteet ja vastuualueet sekä sen, mitä tietoturvauhkia Suomi tulevaisuudessa kohtaa ja miten niihin voidaan valmistautua. Uudessa hallitusohjelmassa on otettu esille kyberuhat. Hallitusohjelman yhtenä tavoitteena on rakentaa suomesta kyberturvallisuuden johtomaa vuoteen 2016 mennessä (Mäkelä 2011).

2.3 Kansalliset tietoturvatoimijat

Ulkoasiainministeriöllä on kansainvälisten tietoturvavelvoitteiden kokonaisvastuu Suomessa. Tehtäviin sisältyvät kansallisen turvallisuusviranomaisen (National Security Authority, NSA) vastuut. Suojelupoliisille ja Pääesikunnalle on ositettu omia vastuualueita kansallisen turvallisuusviranomaisen toimintakentästä. Ne toimivat määrättynä turvallisuusviranomaisena (Designated Security Authority, DSA). Tietoturvaloukkauksiin liittyvä CERT-toiminta (Computer Emergency Response Team) kuuluu Viestintäviraston vastuulle. Virallisia CERT-yksiköitä on maailmanlaajuisesti useita kymmeniä. Viestintäviraston CERT-yksikkö käyttää lyhennettä CERT-FI sekä englanninkielistä nimeä The National Computer Security Incident Response Team of Finland. Yksikön vastuualueita ovat tietoturvaloukkausten ennaltaehkäisy, havainnointi ja ratkaisu sekä tietoturvauhkista tiedottaminen (CERT-FI 2011, 11).

Viestintävirastolle kuuluu myös NCSA-FI-kokonaisuus (National Communication Security Authority of Finland), johon sisältyy kansalliseen turvallisuustoimintaan liittyvä ohjeistus, kansainvälisen tietoturvaluokitellun aineiston käsittelyn ohjeistus sekä turvallisuussopimusten valmisteluun liittyviä tehtäviä. Näiden lisäksi NCSA-yksikköön kuuluvat SAA- (Security Accreditation Authority), CAA- (Crypto Aproval Authority), ja CDA-toiminnot (Crypto Distribution Authority). Viestintäviraston SAA vastaa tietojärjestelmien hyväksynnästä silloin, kun niiden on täytettävä kansainväliset tietoturvavelvoitteet. Salaustuotteiden ja -menetelmien hyväksynnästä vastaava Viestintäviraston CAA toimii yhteistoiminnassa muiden valtionhallinnon kryptologia-

asiantuntijoiden kanssa. Salatun aineiston jakelusta vastaa Viestintävirastossa CDA (CERT-FI 2011, 11).

Tietojärjestelmät, joissa käsitellään kansainvälistä luottamuksellista tai sitä arkaluontoisempaa tietoa, tulee suojata TEMPEST-toimien avulla. Termillä TEMPEST tarkoitetaan sähkömagneettisen hajasäteilyn vaarojen tunnistamista ja minimointia. Tietojärjestelmiltä edellytettävien kansainvälisten vaatimusten täyttämiseksi Viestintävirastoon on sijoitettu kansallisen TEMPEST-viranomaisen tehtävät (CERT-FI 2011, 11).

Huoltovarmuuskeskuksen tavoite on turvata poikkeusolojen ja normaaliaikojen vakavien häiriöiden varalta yhteiskunnan kriittiset toiminnot. Nykyisin sen toiminnan painopiste on nimenomaan kriittisten tietotojärjestelmien toimintakyvyn varmistaminen. Näihin liittyviä asioita ovat uhkien tunnistaminen ja analysointi sekä teknisten varajärjestelmien luominen ja ylläpito. Huoltovarmuuskeskuksen hankkeissa kehitetään jatkuvuudenhallintaa parantavia menetelmiä ja työkaluja. Viestintävirasto ja Huoltovarmuuskeskus järjestävät yhteistyössä kriittisen infrastruktuurin suojaamista käsitteleviä CIP-seminaareja (Huoltovarmuuskeskus 2011).

Valtionhallinnon tietoturvallisuuden johtoryhmä on valtionvarainministeriön asettama hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elin. Se käsittelee kaikki merkittävät valtionhallinnon tietoturvallisuuslinjaukset. VAHTIn tavoitteisiin kuuluu tietoturvan yhdistäminen kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta; lisäksi VAHTI edistää verkostomaisen tietoturvayhteistyön kehittämistä julkishallinnossa. VAHTI on julkaissut tietoturvaohjeistuksista kokoelman, joka on kansainvälisestikin mitattuna yksi laajimmista (Valtiovarainministeriö 2010).

Puolustusvoimat kehittää nopeasti kykyä vastata kyberhyökkäyksiin. Puolustusministeri Stefan Wallinin mukaan edes armeijan säästöt eivät saa estää uuden suorituskyvyn rakentamista. Puolustusvoimat aloitti ensimmäisten ammattilaisten palkkaamisen lokakuussa 2011. Puolustusministerin mukaan tietoverkkopuolustukselta vaaditaan jatkuvaa valmiutta, sillä hyökkäyksiä tulee myös rauhan aikana. Vuonna 2012 valmistuva kyberstrategia linjaa puolustusvoimien vastuualueita kybersodankäynnissä (Kerkkänen 2011).

Suomessa toimii useita kansainvälisesti arvostettuja tietoturva-alan yrityksiä, kuten F-Secure ja Stonesoft. Nämä ovat myös omalta osaltaan merkittäviä tekijöitä kansallisesti kriittisen infrastruktuurin suojaamisessa. Mahdollisen kybersodan syttymisen kannalta merkittävää on luonnollisesti kotimaisten osaajien määrä sekä yritysten toimipisteiden ja toimintojen sijoittuminen Suomeen. Kansainvälisten tietoturvayritysten lisäksi Suomessa on lukuisia kotimaisia yrityksiä, jotka tarjoavat tietoturvalaitteiden ja -ohjelmistojen lisäksi konsultaatiota. Konsultaatiopalveluita voidaan hyödyntää tietojärjestelmän mukaan teknisen tietoturva-auditoinnin

suunnitteluun ja toteutukseen. Yritysten ohella Suomessa toimii aktiivisia tietoturvayhteisöjä ja -yhdistyksiä, kuten Tietoturva Ry (Huhtakangas 2011).

3 Kyberhyökkäystapauksia maailmalta ja maiden suorituskyvystä

Kyberavaruudessa uhkan muodostavat toimijat voidaan luokitella eri ryhmiin niiden käyttämien metodien sekä kohteiden ja motiivien perusteella. Siinä, missä kyberrikollinen tavoittelee taloudellista hyötyä, kyberterroristin motiivina voi olla poliittinen muutos. Vastaavasti haktivistien tavoite on usein saada esitettyä protestiviestinsä murtautumalla verkkosivustolle, aiheuttamalla palvelunestohyökkäys tai suorittamalla tietomurto. Krakkereiden ja black hat -hakkereiden tavoitteena on kasvattaa omaa mainettaan alan piireissä ja osoittaa kyvykkyyttään aiheuttamalla vahinkoa tietojärjestelmille.

Pääesikunnan tietoverkkopuolustussektorin johtajan Catharina Candolinin mukaan uhkatekijät voidaan jakaa karkeasti kahteen luokkaan: valtiollisiin ja ei-valtiollisiin. Valtiolliset uhkatekijät muodostuvat asevoimista sekä tiedusteluorganisaatioista, ja ei-valtiollisiin kuuluvat haktivistit, verkkorikolliset ja terroristit (Kotilainen & Lehto 2011, 39). Taulukossa 4 on kuvattu uhkia muodostavien tekijöiden eroavaisuuksia. Siitä on havaittavissa, että uhkatekijöiden luokittelu ei ole aina yksiselitteistä; kybertiedustelu voi kuulua osaksi kybersodankäyntiä, kun sillä tavoitellaan sotilaallista etua. Lähes kaikilla toimijoilla on käytettävissään samankaltaisia menetelmiä toisistaan poikkeavien tavoitteiden saavuttamiseksi.

	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 4: Kyberuhkia muodostavat toimijat (Kramer ym. 2010).

Seuraavissa alaluvuissa käsitellään eri toimijoiden kyberhyökkäyksiä maailmalla sekä eri maiden valmiutta kybersodankäyntiin ja kyberuhkien torjuntaan.

3.1 Pohjoismaat

Pohjoismaissa on tehty keskimäärin vähemmän kyberhyökkäyksiä muihin maihin verrattuna. Suomessa haittaohjelmia julkaisevia sivustoja vuonna 2010 oli noin 0,03 % sivustoista ja haittaohjelmia löytyi 2,3 %:ssa työasemista. Muiden pohjoismaiden lukemat ovat hyvin lähellä samaa luokkaa. Luvut ovat noin neljäsosan maailman keskiarvosta. Yleisimmät virus- ja haittaohjelmat pohjoismaissa ovat mainosohjelmat ja erilaiset troijalaiset sekä backdoor-ohjelmat (Microsoft 2011, 55-60, 94).

Norjan puolustusministeriöön tehtiin laaja tietomurtoyritys vuoden 2011 keväällä, kun useat sadat työntekijät vastaanottivat viestin, joka sisälsi viruksen. Viruksen lähettäjä oli naamioitu siten, että viesti näytti tulevan toisesta Norjan valtion virastosta. Viestin liitetiedosto sisälsi viruksen, joka avattuna mahdollisti murtautumisen työasemaan. Virus kuitenkin tunnistettiin nopeasti, ja Norjan armeijan mukaan turvaluokiteltua tietoa ei ehditty varastaa. Tapaus sattui pian sen jälkeen, kun Norja oli tehnyt päätöksen osallistua Libyan sotilasoperaatioon (Berglund 2011).

Suomessa tuli ilmi 5.11.2011 tähän mennessä maan laajin tiedossa oleva tietomurto, kun Internetissä julkaistiin noin 16 000 ihmisen henkilötiedot, joihin sisältyi nimiä, henkilötunnuksia, kotiosoitteita sekä puhelinnumeroita. Kaksi päivää myöhemmin pastebin.com-sivustolla julkaistiin Anonymous Finlandin nimissä tiedote, jossa otettiin vastuu tietomurroista ja esitettiin poliittisia vaatimuksia. Myöhemmin samana päivänä samalle sivustolle julkaistiin tiedote, jossa kiistettiin, että Anonymous Finlandin olisi lähettänyt edellisen viestin sekä vastuu tietomurrosta. Lauantaina 12.11.2011 julkaistiin lähes 500 000 sähköpostiosoitetta sisältävä lista. Lisäksi salasanoja, joiden väitettiin kuuluvan näihin sähköposteihin, julkaistiin erillisessä listassa yhteensä 14 600 kappaletta. Samalla listan julkaisija ilmoitti lähettävänsä myöhemmin täydellisen luettelon salasanoista ja sähköpostiosoitteista. Vastuu teosta otettiin jälleen Anonymous Finland -ryhmän nimissä pastebin.com-sivustolla (Pohjonen 2011).

Tanskalainen sanomalehti Jyllands-Posten julkaisi vuonna 2005 humoristisen sarjakuvan, jossa esiintyi profeetta Mohammed. Uutislehti perusteli julkaisua kontribuutiona jatkuvaan keskusteluun itsesensuurista ja siitä, saako Islamia kritisoida. Tanskalaiset muslimiyhteisöt alkoivat protestoida, ja protestit levisivät nopeasti maailmalle. Tämän jälkeen alkoi tapahtua maailmanlaajuisia hyökkäyksiä tanskalaisia verkkosivustoja kohtaan. Jihadistien verkkosivustot koordinoivat hyökkäyksiä ja kehottivat suorittamaan lisää hyökkäyksiä kohti kaikkia tanskalaisia www-sivustoja. Sivustoilla kehotettiin myös boikotoimaan kaikkia tanskalaisia tuotteita (Carr 2009).

Joulukuussa 2010 Ruotsin syyttäjänviraston sivuille kohdistettiin palvelunestohyökkäys, joka sulki sivut vuorokaudeksi. Lisäksi toinen hyökkäys kohdistettiin tukholmalaiseen asianajotoimistoon. Hyökkäys katkaisi asianajotoimiston tietoliikenteen. Asianajotoimisto edusti kahta naista, jotka syyttivät Wikileaks-sivuston keulahahmoa Julian Assangea raiskauksesta. Wikileaksiin on yhdistetty monta muutakin hyökkäystä sen julkistettua 250 000 luottamuksellista muistiota. Esimerkiksi haktivistiryhmä Anonymous on ilmoittautunut MasterCardin sivustoja vastaan kohdistetun hyökkäyksen tekijäksi sen jälkeen, kun MasterCard päätti estää Wikileaksille osoitettujen lahjoitusten suorittamisen (Burns 2010). Anonymous on myös tehnyt keväällä 2012 hyökkäyksiä eurooppalaisten maiden valtionhallintoa vastaan. Pohjoismaista ainakin Tanskan valtionhallinnon sivusto joutui hyökkäyksen kohteeksi. Anonymous ilmoitti hyökkäyksien olevan protesti, jolla vastustetaan Euroopan unionin maiden osallistumista kansainväliseen väärentämisen vastaiseen ACTA-sopimukseen. Sopimuksessa käsitellään muun muassa Internet-piratismin vastaisia keinoja (Hansen 2012).

Yksi ensimmäisistä laajasti julkisuudessa olleista pohjoismaisista krakkerointitapauksista sattui Ruotsissa syyskuussa 1998, kun eduskuntavaalien alla Ruotsin oikeistopuoleen www-sivustolle murtauduttiin. Sinne ujutettiin linkkejä pornografisiin sivustoihin ja kilpailevan puoleen sivuille (Janczewiski ym. 2009, 3). Pohjoismaisten kyberhyökkäysten määrä on ollut kasvussa, ja kasvu näyttää yhä kiihtyvän. Tämä on osaltaan seurausta Internetin suosion kasvusta: sen käyttäjämäärät ovat nousseet maailmalla vuosien 2000 ja 2010 välillä 1,7 miljardilla (Yhdysvaltain puolustusministeriö 2011, 4).

Norja julkaisi vuonna 2003 kansallisen strategian ICT-järjestelmien suojaamiseksi. Sen seurauksena syntyi kolme organisaatiota: kansallisen tietoturvan koordinointineuvosto (KIS), Norjan CERT-toiminnasta vastaava NorCERT, sekä Norjan tietoturvakeskus (NorSIS). Kuuden ministeriön edustajista koostuva KIS on korkean tason keskustelufoorumi, jolla ei ole virallista päätöksentekovaltaa. Sen sijaan se ohjeistaa ja antaa neuvoja valtion virastoille kriittisen infrastruktuurin suojaamiseksi. NorCERT ylläpitää operaatiokeskusta, joka seuraa

kansallisia kyberuhkia ja tiedottaa niistä. NorSISin tavoite on parantaa yleistä tietoturvatietoisuutta ohjeistuksien ja koulutuksien avulla. (Brunner & Suter 2009, 310-320)

Kriittisen infrastruktuurin suojaamisvastuu Norjassa on Norjan Posti- ja tietoliikennetoimistolla (Norweigian Post and Telecommunication Authority, NPT). Norjalaiset yliopistot ja tutkimuslaitokset muodostavat opetusministeriön rahoittaman UNINNETin, joka tekee tietoturvaloukkausten tutkimustyötä (Brunner ym. 2009, 310, 318).

Ruotsissa on tietotekninen yhteisö (Dataföreningen), johon on liittynyt 32 000 ihmistä. Osana sitä toimii SBA-kokonaisuus (SårBarhetsAnylys), jossa tehdään tietoturva-auditointeja sekä akkreditointeja. Suomen huoltovarmuuskeskusta vastaavaa toimintaa kriittisen infrastruktuurin suojelussa Ruotsissa hoitaa Myndigheten för samhällskydd och beredskap (MSB). Tietotekniikan kannalta MSB:ssä keskeisenä suojattavana kohteena pidetään julkisten sähköisten tiedotuskanavien saatavuuden turvaamista. Kyberterrorismiin ja vakoiluun liittyvissä rikostutkinnoissa Ruotsissa vastuu on turvallisuuspalvelulla (SÄPO). Ruotsin pelastuslaitoksen (Swedish Emergency Management Agency, SEMA) vastuulla on ylemmän tason tietoturvan ohjeistus ja ohjaus. Se järjestää myös seminaareja ja koulutuksia. SEMA on teettänyt tutkimuksia siitä, miten Ruotsi selviytyisi kyberhyökkäyksistä (Brunner ym. 2009, 400-404).

Tanskan kansalliseen tietototurvaan ja kyberhyökkäyksiin liittyvää tilannekuvaa ylläpitää DK-CERT. Muita vastaavia toimijoita Tanskassa ovat MILCERT ja GOVCERT, joiden vastuualueena on puolustusvoimiin, valtionhallintoon sekä tiedustelutoimintaan liittyvät tietoturva-asiat. Pohjoismaissa on myös runsaasti kybersodankäyntiin ja kriittisen infrastruktuurin suojaamiseen liittyvää tutkimustoimintaa. Merkittävimpiä toimijoita on Ruotsin maanpuolustuskorkeakoulun CATS (Center for Assymmetric Threat Studies), joka on laajentanut tutkimustoimintaansa kyberterrorismiin (Brunner ym. 2009, 401).

Pohjoismaiden lainsäädäntö on varsin samankaltainen tietoturvallisuuden osalta, pois lukien Ruotsin FRA-laki, joka antaa Ruotsin puolustusministeriön alaiselle signaalitiedusteluyksikölle FRA:lle (Försvarets radioanstallt) luvan kuunnella kaikkea Ruotsin läpi kulkevaa viestiliikennettä, mukaan lukien Internet-selailu ja sähköpostit. FRA:n työntekijämäärä on noin 700 henkilöä, ja sen tehtäviin sisältyy signaalitiedustelun lisäksi muun muassa yhteiskunnallisesti merkittävien tietoturvaloukkaustapausten tutkiminen (Försvarets radioanstallt 2011).

Pohjoismaissa on lukuisia yliopistoja ja ammattikorkeakouluja, joissa opetetaan tietoturvaa. Ensimmäinen kyberturvallisuuteen liittyvä koulutusohjelma käynnistyy Jyväskylän ammattikorkeakoulussa vuonna 2013. Koulutus sisältää kyberturvallisuuteen liittyvän lainsäädännön ja KATAKRIin perehtymisen lisäksi teoriaa tietoturvan suunnittelu-, salaus- ja tunnistamismene-

telmistä. Opinnoissa harjoitellaan kybersodankäyntiä käytännönläheisessä hyökkäys- ja puolustusharjoituksessa (Rinta 2012).

3.2 Venäjä

Yhdysvaltojen tiedustelu-upseerit eivät pidä Kiinaa pahimpana uhkana maalleen kyberavaruudessa. He ovat esittäneet lausuntoja, joiden mukaan Venäjällä on parempaa osaamista, jonka he arvioivat olevan samaa tasoa kuin Yhdysvalloilla itsellään. Kiina on saanut enemmän huomiota, koska se on jättänyt enemmän jälkiä kyberhyökkäyksistä. Venäjän ei-valtiolliset black hat -hakkerit ja kyberrikollisuuteen keskittyneet yritykset ovat suuri kansainvälinen uhka. Neuvostoliiton turvallisuuspoliisin KGB:n signaalitiedusteluosista muodostettiin vuonna 1991 Neuvostoliiton hajoamisen yhteydessä federaation valtiollisen viestinnän ja informaation virasto, FAPSI. Aluksi se kirjoitti ja mursi koodia, häiritsi viestiliikennettä sekä salakuunteli. Internetin suosion kasvaessa se otti haltuunsa Venäjän suurimman Internet-palvelutarjoajan. Myöhemmin se vaati Venäjän kaikkia Internet-palveluntarjoajia asentamaan valvontajärjestelmiä, joihin ainoastaan FAPSIlla oli pääsy. Vuonna 2003 FAPSI uudelleenorganisoitiin Venäjän nykyiseen tiedustelupalveluun FSB:hen ja yksikön nimi muuttui erikoisviestintä- ja -tiedotuspalveluksi. Voronezhin kaupungissa sillä on yksi suurimmista ja parhaimmista hakkerikouluista maailmassa.(Clarke 2009, 63-64).

Kavkaz Center on verkkosivusto, joka tuottaa propagandaa tšetšeenitaistelijoiden näkökulmasta Kaukasian alueen tilanteesta. Siihen ja tšetšeeniseparatistien chechenpress.com-sivustoon suoritettiin palvelunestohyökkäys vuonna 2002. Kavkaz Center väitti Venäjän liittovaltion turvallisuuspalvelun FSB:n olleen hyökkäysten takana. Kybertaistelut jatkuivat, kun vastaavanlaisia iskuja alettiin tehdä Venäjän uutissivustoja kohtaan. Vuonna 2004 luotu Maslan-A-virus oli räätälöity hyökkäämään Kavkazcenter.com- ja chechenpress.com-sivustoja vastaan. Tietoturvayritys F-Securen mukaan Maslan-A-virus on suunniteltu Venäjällä (Stiennon 2010, 93).

Ensimmäisenä kybersotana pidetään Georgian ja Venäjän välistä sotaa vuonna 2008. Vuonna 2008 Venäjällä ja Georgialla oli erimielisyyksiä Etelä-Ossetian ja Abkhazian itsenäisyydestä. Venäjä tuki niiden itsenäisyyttä, kun taas Georgian mielestä alueet ovat osa Georgiaa. Kyberhyökkäykset käynnistyivät jo kuukausi ennen elokuun seitsemäntenä päivänä käynnistynyttä fyysistä sotilaallista hyökkäystä. ShadowServer-niminen riippumaton tutkimusjärjestö raportoi huolellisesti koordinoidusta hyökkäyksestä Georgian presidentin verkkosivustoa vastaan. Se havaitsi entuudestaan tuntemattoman Machbotiksi kutsutun bottiverkon. Machbot-verkko keskusteli Yhdysvalloissa sijaitsevan hallintapalvelimen kanssa, josta se sai käskyn suorittaa palvelunestohyökkäyksen. Se vastaanotti hallintapalvelimelta kolmea eri komentoa, joiden tarkoitus oli kuormittaa sivustoa kolmen eri tiedonsiirtoprotokollan avulla. Komennoilla saatiin

alasajettua Georgian presidentti Saakašvilin verkkosivut vuorokauden ajaksi. Samalla palvelimella sijaitsi muitakin Georgian valtion sivustoja, jotka myös kärsivät hyökkäyksestä (Stiennon 2010, 95-100).

Elokuun seitsemäntenä päivänä Georgia siirsi joukkojaan Etelä-Ossetian eteläisiin osiin, mikä käynnisti aseellisen konfliktin. Venäjä oli varautunut toimimaan nopeasti, ja jo elokuun kahdeksannen päivän aamuna Venäjän tankit vyöryivät Etelä-Ossetiaan. Tätä olivat kuitenkin jo edeltäneet elokuun seitsemännen päivän iltana käynnistyneet massiiviset hyökkäykset georgialaisia www-sivustoja kohtaan. Hyökkäykset kohdistuivat sivustoihin, joiden avulla Georgian kansalaisia ja maailmaa pidettiin ajan tasalla Georgian tapahtumista. Palvelunestohyökkäyksiä tehtiin myös pankkeja ja ministeriöiden sivustoja kohtaan, ja tietoliikenne Georgiasta ulospäin häiriintyi. Elokuun seitsemännen päivän iltana myös Georgian presidentin www-sivustolle hyökättiin uudestaan. Presidentti Saakašvilistä ja Hitleristä julkaistiin propagandakuvia, joissa he esiintyivät samankaltaisilla eleillä ja ilmeillä. Verkkosivustolla nimeltä StopGeorgia.com julkaistiin ohjeita, kuinka hyökätä 36:tta georgialaista verkkokohdetta vastaan; niiden joukossa olivat muun muassa Yhdysvaltain ja Britannian suurlähetystöt, Georgian eduskunta, korkein oikeus, ulkomaankauppaministeriö sekä useiden uutiskanavien ja sanomalehtien palvelimia (Stiennon 2010, 96-100).

Vaikkakin Venäjän ja Georgian sodan pahin vaihe laantui Venäjän ilmoitettua päättäneensä sotilasoperaationsa elokuun kahdentenatoista päivänä ja tulitaukosopimuksen tultua voimaan elokuun 16. päivänä, taistelut kyberavaruudessa jatkuivat. Elokuun kolmantenatoista päivänä Viron CERT lähetti kyberasiantuntijoita Georgian avuksi. Puola tarjosi apuaan presidentti Saakašvilille tarjoamalla oman presidenttinsä www-sivustolta tilaa uutistiedotteiden julkaisua varten. Georgialaissyntyinen www-hotellipalveluita tarjoavan yrityksen perustaja, joka oli sodan käynnistyessä entisessä kotimaassaan lomailemassa, järjesti Georgian presidentin sivuston siirron oman yrityksensä palvelimille. Samalla hän altisti oman yrityksensä ja sen asiakkaiden sivustot Georgialle tarkoitettujen hyökkäysten kohteeksi. Vielä 27. päivänä elokuuta Georgian ulkoasiainministeriön sivuille tehtiin palvelunestohyökkäys, joka lamautti sivuston. Tämän jälkeen hyökkäykset laantuivat, mutta vuoden päästä sodan vuosipäivänä georgialaista bloggaajaa vastaan hyökättiin yllätyksellisin seurauksin. Nimimerkkiä Cyxumy käyttänyt bloggaaja kannatti kirjoituksissaan voimakkaasti Georgiaa ja kritisoi Venäjää. Hänen käyttämäänsä neljää eri sosiaalisen median julkaisukanavaa vastaan hyökättiin 8.9.2009, ja niiden joukoissa olivat myös Facebook ja Twitter. Hyökkäyksistä kärsivät kaikki hyökkäyksen kohteet, joista Twitterille koitui eniten vahinkoa, kun sen 20 miljoonaa käyttäjää eivät päässeet palveluun kolmeen tuntiin (Stiennon 2010, 101).

Venäjällä työasemista tehtyjen virus- ja haittaohjelmahavaintojen määrä on prosentuaalisesti moninkertainen Suomeen verrattuna, mutta hyvin lähellä kansainvälistä keskiarvoa. Vuonna 2010 Venäjältä löytyi haittaohjelmia noin 10 prosentista työasemista. Yleisimmät havainnot tulivat troijalaisista. Suomeen verrattuna mainosohjelmia havaittiin suhteessa huomattavasti vähemmän (Microsoft 2011, 56-58, 67).

Kimberly Lukin kirjoitti pro gradu -tutkielman vuonna 2007 venäläisten käyttämistä tietoverkkosodankäynnin menetelmistä. Tutkielmassa kerrotaan venäläisten hakkereiden olevan keskimäärin iältään alle 35-vuotiaita. Moskovan kaupunki järjestää vuosittain hakkeritapahtuman, jonka avulla tavoitellaan teknisesti lahjakkaita nuoria. Venäjällä virusten kirjoittaminen ei ole laitonta, mutta niiden levittäminen on. Rikostilastojen mukaan 70 prosentilla venäläisistä kyberrikollisista on korkeakoulututkinto tai he ovat olleet yliopistossa kirjoilla pidätyshetkellä. Lukinin mukaan osa Venäjän valtion ja yliopistojen tutkimusrahoituksesta kertyy harmaasta taloudesta ja lahjakkaita tietotekniikkaopiskelijoita päätyy rikollisjärjestöjen palvelukseen. Kyberrikollisuutta vastaan Moskovassa taistelee hallituksen alainen K-osasto. Lukinin eri lähteiden perusteella laskema pahantahtoisten hakkereiden lukumäärä on noin 2 900 henkilöä. Vaihtelu eri lähteiden välillä tosin oli suuri, mikä johtuu osittain verkkorikollisuuden määrittelyn tavoista. Venäjän tiedustelupalvelut ovat kouluttaneet noin 16 000 henkilöä informaatio- ja tietoverkkosodankäyntiin. Luku sisältää verkonvalvontaan, virusten ja vakoiluohjelmien ohjelmointiin sekä tilannekuvan analysointiin koulutetun henkilöstön. Henkilöluku kasvaisi merkittävästi, jos mukaan otettaisiin lisäksi kryptografian ja matematiikan asiantuntijat. Suoranaisiin tietosodankäynnin puolustus- ja hyökkäysoperaatioihin koulutettuja henkilöitä vuonna 2007 oli arviolta alle 5 000 (Lukin 2007. 33-41).

Vuonna 2008 Venäjän presidentti hyväksyi kaksi tietoturvaan liittyvää asiakirjaa: Venäjän tietoyhteiskunnan kehittämisstrategian sekä ohjeistuksen menetelmistä kansallisen tietoturvan takaamiseksi. Niiden tarkoitus on täydentää vuonna 2000 julkaistua tietoturvallisuuteen liittyvää doktriinia. Julkishallintoon kuuluva Russian Association of Networks and Services (RANS) vastaa tietoturvaan liittyvän lainsäädännön ja ohjeistuksen kehittämisestä. RANSiin kuuluu 122 jäsentä, joihin kuuluu muun muassa yliopistoja, tieteellisiä yhteisöjä, ministeriöitä ja verkko-operaattoreita. Tietoturvahyökkäyksiä Venäjällä valvoo RU-CERT-yksikkö, joka aloitti toimintansa vuonna 1998. (Brunner ym. 2009, 351-354)

3.3 Kiina

Kiina on 1990-luvun lopusta alkaen kehittänyt kyvykkyyttään kybersodankäyntiin. Lähtökohtana Kiinalla on ollut se, että sillä täytyy olla sekä puolustus- että hyökkäyskykyä kyberavaruudessa. Se on kehittänyt hakkeriryhmittymiä, perustanut armeijan kybersodankäyntiyksiköitä ja käynnistänyt kybertiedusteluoperaatioita. Yhdysvalloissa on arvioitu, että Kiinassa on noin 250 hakkeriryhmää, jotka muodostavat Yhdysvalloille kyberuhan (Clarke ym. 2009, 55). Kiinalaiset itse suosivat kybersodankäynnin sijasta termiä informationalisaatio (Kramer ym. 2010, 438). Kiina pyrkii asevoimiensa mukaan uusimaan sodankäyntiä kiinalaisin ominaispiirtein, jonka ytimessä on informationalisaatio (Maanpuolustuskorkeakoulu 2008, 285). Kenraalimajuri Daj Qingmin Kiinan kansanarmeijasta on kertonut, että kybersodankäyntistrategioiden merkitys on noussut keskeiseen asemaan Kiinassa. Daj Qingmin mukaan Kiinan asevoimat ovat panostaneet vahvasti vihollisen tietojärjestelmien sabotoimiseen, sekä vihollisen tiedustelun hämäämiseen (Kramer ym. 2010, 467).

Yksi Kiinan kansanarmeijan johtavista strategeista Li Biyang korostaa, että tulevaisuudessa armeijan lisäksi tulee käyttää siviilien muodostamia tietosodankäyntijoukkoja. Li Biyangin mukaan heikompi maa voi voittaa vihollisensa ylivoimaisella tietosodankäyntikyvykkyydellä. Dai Qingin mukaan Kiinan ei tule käyttää sille perinteistä aktiivista puolustussodankäynnin taktiikkaa, vaan silloin kun kyse on kybersodankäynnistä, on pyrittävä hyökkäyssotaan (Kramer ym. 2010, 467-469).

Vuonna 1999 Kosovossa Yhdysvaltain armeija johti Naton ilmaoperaatiota, jossa tarkoituksena oli pommittaa serbialaista sotilaskohdetta. Väärän tiedustelutiedon takia se pommitti vahingossa kuitenkin Kiinan suurlähetystöä. Pommituksen jälkeen Yhdysvaltojen ja Naton verkkosivustoihin suunnattiin palvelunestohyökkäyksiä. Valtion virastojen työntekijöiden sähköpostit täyttyivät pommitusta protestoivista sähköposteista. Hyökkäyksistä koitui kuitenkin vain vähäisiä haittavaikutuksia, mutta se oli ensimmäinen kerta, kun kiinalaiset käyttivät näkyvästi kyberavaruutta haktivistien protestointikanavana (Clarke 2009, 55).

Vuodesta 2003 alkaen ryhmä kiinalaisia kybervakoojia suoritti lukuisia tietomurtoja Yhdysvaltalaisiin tutkimuslaboratorioihin ja puolustushaarojen esikuntiin. Heillä oli käytössään edistyneitä räätälöityjä työkaluja, joilla he etsivät heikkouksia Yhdysvaltain armeijan verkosta. On arvioitu, että he onnistuivat murtautumaan kymmeniin verkkoihin ja varastamaan valtavan määrään tietoa. Washingtonissa viranomaiset ovat olleet vähäsanaisia siitä, mitä tietoja kiinalaiset onnistuivat varastamaan. He ovat painottaneet sitä, että Yhdysvalloissa salaiseksi luokitellut verkot eivät ole kytköksissä Internetiin ja niihin ei murtauduttu. Kyberasiantuntija Shawn Carpenter oli ensimmäinen, joka sai selville hyökkäysten laajuuden ja tehokkuuden.

Hän onnistui jäljittämään hyökkäysten lähteen, joka sijaitsi Guangdong-nimisessä kiinalaisessa provinssissa. Yhdysvallat syytti Kiinan valtiota vakoilusta, minkä kiinalaiset kiistivät. Carpenter ja useat asiantuntijat ovat yhä sitä mieltä, että hyökkäykset tehnyt Titan Rain -niminen ryhmä on edelleen aktiivisena toimija (Stienning 2010, 3-9) .

Joulukuussa 2010 paljastui Kiinasta lähtöisin oleva laaja verkkohyökkäys, jonka tietoturvayritys McAftee nimesi Operaatio Auroraksi. Hyökkäys kohdistui vähintään 30 suuryritykseen. Se hyödynsi Internet Explorer selaimen sekä Adoben PDF-ohjelmiston haavoittuvuuksia. Adoben ohjelmiston haavoittuvuuden hyödyntämisen onnistumisesta ei tosin ole saatu varmaa näyttöä. Tämän hyökkäyksen lisäksi julkisuudessa on viime vuosina ollut esillä useita suuria verkkohyökkäyksiä, joiden alkuperä viittaa Kiinaan (Linnake 2010).

Zhengzhoussa sijaitseva Kiinan kansanarmeijan tietotekniikkayliopisto on tiettävästi Kiinan suurin tietoverkkosodankäyntiin panostava oppilaitos. Yliopisto työllistää lähes 900 professoria ja tarjoaa 55 koulutusohjelmaa. Ainevalikoimassa on muun muassa rootkitit, tiedon piilottaminen, haittaohjelmien levittäminen ja tunnistus sekä verkkohyökkäykset. Yliopisto julkaisee 150 tietoturvaan liittyvää tutkimusartikkelia vuosittain. Kiinan teollisuusministeriö on käynnistänyt tietoturvan kehityshankkeen 242 (guojia 242 xinxi anquan jihua xiangmu), joka sisältää 242 projektia valtion tietoturvan kehittämiseksi. Kiinan kansanarmeijan yliopiston lisäksi Kiinassa on 46 yliopistoa, joissa opetetaan tietoturvaa. Niistä kymmenen saa rahoitusta kansalliseen s219-tietoturvan soveltamisprojektiin (guojia s219 xinxi anquan yingyong shifan gongcheng), jossa käsitellään tietoturva-alustoja, tunkeutumisenestojärjestelmiä sekä verkkoliikenteen salausratkaisuja. Kiina pyrkii kasvattamaan kykyään kybersodankäyntiin tehostamalla yhteistyötä yliopistojen, armeijan ja yksityissektorin kanssa. Kiinan armeija teettää yliopistoilla useita tutkimuksia ja hyödyntää yliopistoissa kehitettäviä huipputehokkaita supertietokoneita (Krekel & Adams & Bakos 2012. 55-62).

Kiinan kansanarmeijan teknisiä tiedustelutoimistoja on jakautunut seitsemään sotilasalueeseen. Näiden henkilömäärät eivät ole julkisia tietoja, mutta lukumääristä kertoo jotain se, että pelkästään Chengdun sotilasalueella oli vuonna 2005 yli 290 erillistä yksikköä, joiden tehtävinä oli joko elektroninen sodankäynti, verkkosodankäynti tai psykologinen sodankäynti. Kiinan kansanarmeija julkaisi vuonna 2006 strategian, jossa se toi esiin tavoitteen panostaa erityisesti ICT-osaajien rekrytointiin. Omien osaajien lisäksi kansanarmeija on käyttänyt tietoteknisissä sotaharjoituksissa yritysten osaajia muun muassa simuloimaan vihollisen hyökkäystä armeijan johtamisjärjestelmiä vastaan (Krekel ym. 2012, 48-54).

Ylen uutisten mukaan Kiina on palkkaamassa itselleen jopa 200 000 ICT-asiantuntijaa, joita kutsutaan kybersotilaiksi. Heidän tehtävänään on suojata Kiinan omat kriittiset järjestelmät sekä kehittää hyökkäysmenetelmiä ulkomaisiin ympäristöihin (Mäkelä 2012).

3.4 Viro

Neuvostoliiton hajoaminen 1990-luvun alussa käynnisti Virossa informaatioteknologian kehityksen hurjan kasvun. Nykyään Virossa on käytössä yhteensä enemmän matka- ja älypuhelimia kuin siellä on asukkaita. Yli 80 prosenttia virolaisista hoitaa pankkiasiansa Internetin kautta. Tallinnassa on yli 1 200 ilmaista langattomien päätelaitteiden tukiasemaa. Pysäköintimaksut hoidetaan tekstiviestillä, ja käytössä on sähköinen äänestysjärjestelmä (Stiennon 2010, 86).

Virossa kärjistyi sisäinen kriisi huhtikuussa 2007, kun Viro päätti ottaa viron kielen sujuvan osaamisen Viron kansalaisuuden saamisen kriteeriksi. Virossa asuva venäjänkielinen vähemmistö, joka oli asunut Virossa Neuvostoliiton hajoamisesta asti, koki päätöksen vääryydeksi. Konfliktin keskipisteessä oli neuvostoliittolaista sotilasta esittävä pronssipatsas, joka sijaitsi Tallinnan keskustassa. Juhlistaakseen itsenäisyyttään Viro päätti siirtää pronssi-sotilaan kaupungin laidalla sijaitsevalle hautausmaalle. Venäjämieliset kansalaiset käynnistivät vastatoimenpiteenä mellakoita ja ryöstelyjä eri puolilla Tallinnaa. Kun pronssipatsas oli siirretty, käynnistyivät välittömästi massiiviset palvelunestohyökkäykset Viron pankkeja, valtion virastoja sekä tietoliikenneinfrastruktuuria vastaan (Stiennon 2010, 87-89).

Virossa sijaitsevan Swedbankin toimipisteen tietoturvapäällikkö raportoi, että hyökkäyksen lähteiksi tunnistettiin yli 80 000 IP-osoitetta. Viron eduskunnan faksit ja matkapuhelimet tukkeutuivat puheluista, ja hallitusten ja pankkien keskeisimmät palvelimet jumittuivat palvelupyynnöistä. Nämä huhtikuun 27. päivänä käynnistyneet kyberhyökkäykset kestivät useita viikkoja. Venäjänkielisillä keskustelupalstoilla jaettiin työkaluja ja neuvoja kyberhyökkäyksien toteuttamiseen. Hyökkäykset kestivät viikkoja, ja niiden jäljet johtivat Venäjälle. Tapahtumasta käytetään nimitystä ensimmäinen verkkosota, Web War One (Stiennon 2010, 87-88).

Muutaman tunti sen jälkeen, kun palvelunestohyökkäykset olivat alkaneet, Viron tietotekniset avaintoimijat kokoontuivat neuvottelemaan. Kokoukseen osallistui puolustusministeriön, tietoliikenneyritysten, Tarton yliopiston sekä pankkien asiantuntijoita. Heistä muodostui joukko kybertaistelijoita, joiden ensimmäinen tavoite oli saada palvelunestohyökkäykset pysäytettyä. Verkkoliikennettä Viroon alettiin rajoittaa, ja lopulta käytännössä kaikki verkkoliikenne Viron ulkopuolelle katkaistiin. Toimet palauttivat Viron sisäisen pankkiasioinnin sekä tiedotusfoorumien toiminnan. Tämän jälkeen alettiin selvittää syitä, miksi niin monet verkkopalvelut

tukkeutuivat hyökkäyksissä. Syyksi selvisi tietoteknisen arkkitehtuurin heikko suunnittelu (Stiennon 2010, 89-90).

Varsinaiset selaimen esityskerrokselle tietoa julkaisevat verkkopalvelimet kestivät palvelupyyntöjen määrän, mutta viaksi osoittautuivat useimmissa tapauksissa huonosti suunnitellut tietokantaratkaisut, jotka eivät kyenneet käsittelemään suurta määrää yhtäaikaisia palvelupyyntöjä. Nykyisin www-sivustot muodostuvat yleensä dynaamisesti tietokantojen sisällön pohjalta. Tilapäisratkaisuna kriittisimmät sivustot päätettiin rakentaa siten, että ne julkaistiin yksittäisinä staattisina html-sivuina. Näin saatiin noin 72 tunnissa tärkeimmät sivut takaisin näkyville (Stiennon 2010, 90).

Hyökkäykset olivat myös Naton kannalta merkittäviä. Natossa alettiin pohtia, missä vaiheessa Naton on osallistuttava kyberoperaatioihin, jos johonkin sen jäsenmaahan hyökätään. Yhtenä vastauksena oli rakentaa Naton kyberpuolustuskeskus Viroon (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]) Viron armeijaan hylkäämiin tiloihin, jotka sijaitsevat lähellä pronssipatsaan uutta sijoituspaikkaa. Virolla on nyt merkittävä rooli Euroopan unionin kyberpuolustuksessa: se muun muassa järjesti vuonna 2009 EU-ministerien välisen kriittisen infrastruktuurin suojaamiseen liittyvän seminaarin (Stiennon 2010, 90).

Loppuvuodesta 2011 alkoi oikeudenkäynti, jossa kuutta Virossa ja yhtä Venäjällä asuvaa henkilöä syytetään laajasta verkkopetoksesta. Yhdysvaltojen viranomaisten mukaan syytetyt olivat kehittäneet ohjelmiston, jonka avulla he kaappasivat miljoonia tietokoneita ja ohjasivat työasemilla tehtyjä verkkohakuja mainoksiin. Ohjelmisto saastutti noin neljä miljoonaa tietokonetta. Ensimmäisen havainnon niistä teki avaruushallinto-organisaatio Nasa, jonka työasemia saastui haittaohjelmasta (Newell 2012).

3.5 Yhdysvallat

Pohjois-Korea laukaisi useita ohjuksia vuoden 2009 heinäkuussa, Yhdysvaltojen itsenäisyyspäivänä. Vaikka ohjukset upposivat Tyyneen valtamereen, yhdysvaltalaisilta ei jäänyt ajankohta huomaamatta. Samaan aikaan käynnistyi hyökkäys Etelä-Korean ja Yhdysvaltojen verkkosivustoja vastaan. Menetelmänä käytettiin vanhaa MyDoom-nimistä haittaohjelmaa, jota oli muokattu vielä hyökkäystä edeltävänä päivänä. Etelä-Korean turvallisuuspalvelun mukaan haittaohjelmaa julkaistiin ohjelmistojen päivittämiseen käytettävällä palvelimella. Haittaohjelma saastutti alle päivässä 210 000 Windows-konetta, joista puuttuivat viimeisimmät tietoturvapäivitykset. Tämän jälkeen se käynnisti palvelunestohyökkäykset, joiden liikennemäärä oli 39 megatavua sekunnissa hyökkäyskohdetta kohti. Yhdysvalloissa raportoitiin, että useat kohteet, kuten Valkoisen talon ja Yhdysvaltojen ilmailuhallinnon verkkosivustot, tukkeutuivat.

Suuria päivittäisiä käyttäjämääriä käsittelevät sivustot, kuten Amazon.com, kuitenkin selvisivät hyökkäyksistä. Hyökkäykset saivat Yhdysvalloissa enemmän mediahuomiota kuin mikään aiempi kyberhyökkäys. Etelä-Korea väittää Pohjois-Korean olleen hyökkäysten takana. Yhdysvalloilla ei ole vedenpitäviä todisteita Pohjois-Korean osallisuudesta. Hyökkäykset käynnistivät julkisen keskustelun Yhdysvaltojen kyberpuolustus- ja -tiedustelukyvystä (Stiennon 2010, 66-69).

Maaliskuussa 2011 vahvoihin käyttäjätunnistusratkaisuihin erikoistunut RSA Security ilmoitti joutuneensa tietomurron kohteeksi. Tietomurron tekijät saivat varastettua RSA:n SecurID-tuotteen tietoja. Tapahtuman seurauksena RSA ilmoitti joutuvansa korvaamaan miltei kaikki 40 miljoonaa käytössä olevaa SecurID-tuotetta uusilla (CERT.FI 2011). Kolmen yhdysvaltalaisen puolustusteollisuusyrityksen, Lockheed Martinin, L-3 Communicationin ja Northrop Grummanin, on raportoitu joutuneen tietoverkkohyökkäyksen kohteeksi RSA:n tietomurron seurauksena. Hyökkäykset tapahtuivat samoihin aikoihin, kun Pentagon oli ilmoittanut, että toisen maan suorittama kyberhyökkäys voidaan tulkita sodanjulistuksena. Yksi Northrop Grummanin työntekijöistä kertoi tv-haastattelussa, että työnantajan IT-ylläpito oli sulkenut yllättäen etätyöyhteydet ja vaihtanut käyttäjien salasanat. Tästä alkoivat huhut tietomurroista yrityksen tietovarastoihin. Northrop Grummanin tiedotuspäällikkö ei suostunut kommentoimaan tietomurtoa. Myöskään L3-communications ei ole suostunut kommentoimaan mahdollista tietomurtoa (Ragan 2011). Lockheed Martinin julkaiseman tiedotteen mukaan yritys kykeni tunnistamaan hyökkäyksen nopeasti ja ryhtyi välittömästi vastatoimiin, joiden ansiosta hyökkääjät eivät saaneet varastettua yrityksen tietoja. Samana päivänä kun hyökkäys havaittiin, Lockheed Martin päätti estää työntekijöiden etäyhteysmahdollisuudet vähintään viikoksi ja korvata kaikki SecurID-tuotteet uusilla. Lisäksi se käski kaikkien 133 000 työntekijänsä vaihtamaan salasanansa (Schwartz 2011).

Nimimerkkiä Comodohacker käyttävä krakkeri on kertonut olevansa vastuussa heinäkuussa 2011 tapahtuneesta tietomurrosta, joka kohdistui alankomaalaiseen tietoturvavarmenteita julkaisevaan Diginotariin. Hän ilmoitti olevansa iranilainen ja vastustavansa Yhdysvaltojen ulkopolitiikkaa. Tietomurron seurauksena Diginotar julkaisi yli 500 väärennettyä varmennetta suurille organisaatioille, joiden joukkoon kuului Yhdysvaltojen tiedustelupalvelu CIA, Britannian tiedustelupalvelu MI6, Google, Facebook, Microsoft ja Skype. Nimimerkki Comodohacker viittaa samantapaiseen tietomurtoon, joka tapahtui maaliskuussa 2011. Kohteena oli Yhdysvaltalainen Comodo-yritys, joka myös julkaisee varmenteita. Comodo kertoi murtautujan saaneen väärennettyjä varmenteita muun muassa Microsoftin ja Googlen ylläpitämiin verkkopalveluihin. Comodo varoitti verkkoselainten valmistajia, jotka ryhtyivät välittömästi toimiin selainten tietoturvan korjaamiseksi. Yhdessä verkkoselaimessa voi olla jopa 321 luotettua

varmenteen julkaisijaa, joten on ymmärrettävää, että käyttäjän kannalta varmenteiden julkaisijoiden määrä muodostaa melkoisen riskin (McGullagh 2011).

Toukokuussa 2011 tiedotettiin tietomurrosta, jossa Citigroup-yhtiöön kuuluvan pankin 210 000 yhdysvaltalaisen asiakkaan tiedot varastettiin. Krakkerit saivat haltuunsa asiakkaiden nimet, tilinumerot ja osoitetiedot (Whitney 2011).

Yhdysvalloissa armeijassa käsitettä cyber käytetään usein synonyymina tietoverkko-operaatioiden käsitteelle (Computer Network Operations, CNO). Se jakaa tietoverkko-operaatiot kolmeen kokonaisuuteen: tietoverkkohyökkäyksiin (Computer Network Attacks, CNA), tieverkkopuolustukseen (Computer Network Defence, CND) sekä tietoverkkojen hyväksikäyttöön (Computer Network Exploitation, CNE). Tietoverkkojen hyväksikäytöllä tarkoitetaan tietoverkkoihin liittyvää vakoilu- ja tiedustelutoimintaa. CNO sijoittuu informaatio-operaatioiden kokonaisuuden sisälle. Informaatio-operaatioiden kehikossa mainittava Information Assurancen (IA) käsite linkittyy teknisen tietoturvan kannalta vahvasti CNO:iin. Information Assurance sisältää ne menetelmät, joilla tietojärjestelmien luottamuksellisuus, eheys ja käytettävyys taataan. Siihen sisältyvät kyvykkyydet hyökkäyksiltä suojaamiseen, hyökkäysten tunnistamiseen sekä hyökkäyksiin reagointiin. Käytännössä IA liittyy enemmän tietoturvaratkaisuiden rakentamiseen ja ylläpitoon, kun taas CNO sisältää varsinaisten tietoverkko-operaatioiden suunnittelun ja toteuttamisen (Andress & Winterfeld 2011, 37-38).

Yhdysvaltojen ydinaseisiin liittyviin järjestelmiin kohdistuu päivittäin 10 miljoonaa tapahtumaa, jotka luokitellaan kyberhyökkäyksiksi. Niistä alle tuhat saa aikaiseksi jotain haittaa. Ydinaseiden suojausjärjestelmistä vastaava National Nuclear Security Administration (NNSA) haluaa nostaa suojaukseen käytettävää budjettia 126 miljoonalla dollarilla yhteensä 155 miljoonaan dollariin. NNSA pitää epätodennäköisenä, että ydinohjusten laukaisujärjestelmiin kyettäisiin murtautumaan, koska ne toimivat suljetuissa ympäristöissä. Sillä ei ole myöskään tiedossa yhtään virusta tai haittaohjelmaa, joka olisi räätälöity ydinohjusten laukaisemiseksi. Se pitää räätälöityjä viruksia kuitenkin mahdollisena uhkana (Koebler 2012).

Yhdysvaltojen puolustusministeriö julkaisi vuonna 2006 doktriinin nimeltä Joint doctrine for Cyber. Doktriinin ongelmana on, että valtaosa sen tietosisällöstä on salaista. Lisäksi Yhdysvalloissa maavoimat sekä ilmavoimat käyttävät informaatio-operaatioiden yhteydessä eri käsitteistöä (Andress 2011, 38).

Kenraali Keith Alexander nimitettiin vuonna 2009 johtamaan U.S. CYBERCOM -yksikköä, joka vastaa Yhdysvaltojen sotilaallisista kyberoperaatioista. Hänen mukaansa Yhdysvaltojen puolustusministeriön verkkoihin kohdistuu joka tunti noin 250 000 kyselyä. Kenraali Alexander on määrittänyt, että U. S. CYBERCOMilla on viisi periaatetta: muistaa, että kyberavaruus on yksi

suojattava toimintaympäristö, tehdä puolustamisesta aktiivista, laajentaa puolustus kriittiseen infrastruktuuriin, edistää yhteistä puolustuskykyä ja kehittää Yhdysvaltojen teknistä etulyöntiasemaa (Andress 2011, 40).

Yhdysvaltojen ilmavoimien komentaja, kenraalimajuri Richard E. Webber on ilmoittanut, että hänen tärkeimpänä tehtävänään on kehittää kyberavaruuden tilannekuvan muodostamista. Ilmavoimiin on hänen johdollaan perustettu Cyber Operations Liason Element (COLE), jossa yhteysupseerit toimivat tiedonvaihdon linkkinä kyberoperaatioiden ja perinteisten operaatioiden suunnittelussa. Merivoimat on suunnitellut kybersodankäyntikykynsä tavoitetilan ja organisoinut uudelleen tiedustelu- ja johtamisjärjestelmäosastojaan integroimalla niiden toimintoja(Andress 2011, 41).

Yhdysvaltojen armeijan maavoimissa on suunniteltu konsepti, miten ne harjoittavat kyberoperaatioita vuosina 2016–2028. Konseptiin liittyy kyberverkko-operaatiokehikko (CYNETOPS), jossa kybertilannekuvaa muodostetaan omista, vihollisen ja erikseen määritettyjen toimijoiden kyvykkyyksistä sekä toiminnasta. Yhdysvaltojen puolustusministeriö on julkaissut INFOCON-ohjeistuksen, joka määrittää viisi eri valmiustasoa tietojärjestelmien puolustamiseen. Ohjeistus määrittää jokaiselle valmiustasolle omat toimintamenetelmät, joita tulee noudattaa. Korkein taso INFOCON 1 sisältää maksimaalisen valmiuden toimet ja INFOCON 5 tason normaalin toiminnan ohjeistuksen (Andress 2011, 42).

Yhdysvallat avasi kesäkuussa 2011 kybersodankäynnin tiedustelukeskuksen (Cyber Warfare Intelligence Center). Sen päätoimipiste sijaitsee Teksasissa ilmavoimien tukikohdassa, jossa työskentelee 400 henkilöä. Kaiken kaikkiaan kybersodankäynnin tiedustelukeskuksen palkkalistoilla on lähes tuhat työntekijää. Keskuksen välittömässä läheisyydessä toimii Yhdysvaltojen kansallisen tietoturvaviranomaisen kryptologiakeskus (NSATCC) sekä ilmavoimien tiedustelukeskus (Yhdysvaltojen ilmavoimat 2010).

Yhdysvaltojen kriittisen infrastruktuurin suojaamisesta vastaa National Cyber Security Division (NCSD). NCSD:llä on kaksi päätavoitetta: rakentaa kansallinen järjestelmä, jolla kyetään vastaamaan kyberuhkiin, sekä kyberriskien hallintaohjelma kriittisen infrastruktuurin suojaamiseksi. US-CERT on yksi NCSD:n rahoittajista; NCSD työllistää noin 380 asiantuntijaa. Yhdysvalloissa on meneillään useita suuria kyberturvallisuuteen liittyviä hankkeita, joista yksi suurimmista on poliisien kyberportaali (Cyber Cop Portal). Portaalissa on edistyneitä työkaluja kyberrikosten tutkimiseen. Sitä käyttää maailmanlaajuisesti noin 5 300 tutkijaa (U.S Deparment of homeland security 2012).

3.6 Lähi-itä

Kesäkuussa 2010 Iranin ydinlaitoksia vastaan hyökättiin uudenlaisella tietokonemadolla, joka oli tehty teollisuusjärjestelmien vakoiluun ja uudelleenohjelmointiin. Se sai nimekseen Stuxnet. Stuxnet pääsi tunkeutumaan Iranin ydinlaitoksiin saastuneen USB-tikun kautta, ja paikalla toimineita venäläisiä ydinvoimateknikoita epäiltiin tikun liittämisestä järjestelmään. Mato sekoitti Siemensin toimittaman sentrifugien ohjauslogiikkajärjestelmän, joka lähetti eteenpäin virheellisiä arvoja suomalaisen Vacon-yrityksen valmistamille taajuusmuuntimille ja sabotoi siten sentrifugit pyörimään väärällä toimintanopeudella. Madon toinen päätoiminto oli nauhoittaa sentrifugien normaalitoimintaa ja lähettää sitä takaisin hämäystarkoituksessa varsinaisen sabotaasin aikana. Kansainväliset ydinvoimatarkkailijat raportoivat, että hyökkäyksellä oli merkittäviä haittavaikutuksia Iranin ydinvoimaohjelmaan. Iranin presidentti Mahmoud Ahmandinejad syytti hyökkäyksestä Israelia ja Yhdysvaltoja, mutta väitti sillä olleen vain vähäisiä vaikutuksia. Suuri joukko tietokoneasiantuntijoita, ydinvoimaeksperttejä ja entisiä viranomaisia on sitä mieltä, että Stuxnet luotiin israelilaisten ja yhdysvaltalaisten yhteisprojektina, jossa oli mahdollisesti osapuolina myös britannialaisia ja saksalaisia. Tietoturva-asiantuntijat pitävät Stuxnetia niin monimutkaisena, että valtiolliset toimijat ovat olleet sen takana (Broad & Markoff & Sanger 2011). F-Securen arvion mukaan Stuxnetin laatiminen on vaatinut noin 10 henkilötyövuoden panostuksen. Stuxnet on kooltaan noin 10 kertaa suurempi kuin virukset yleensä, ja se on ohjelmoitu entuudestaan tuntemattomalla ohjelmointikielellä (F-Secure 2011).

Stuxnet hyödynsi useita Windowsin haavoittuvuuksia, ja se pystyi levittäytymään USB-liitännän, verkkojaon, RPC-haavoittuvuuden sekä tulostuspalvelun (print spooler) haavoittuvuuden kautta. Haittaohjelman rootkit-tiedostot oli digitaalisesti allekirjoitettu piirilevyjä valmistavan JMicron Technology Corpin sekä Realtek Semiconductor -puolijohdevalmistajan aidoilla varmenteilla (Matrosov 2011).

Lähi-idän maiden välillä on suuria eroja valtion harjoittamassa Internet-sensuurissa. Iranin 38 miljoonan Internetin käyttäjän joukossa ei ole sensuurin ansiosta esimerkiksi Facebookin käyttäjiä. Naapurimaassa Jordaniassa valtaosa Internetin käyttäjistä taas käyttää myös Facebookia. Lähi-idässä Israel on vahva toimija tietoturvan ja kybersodankäynnin alueilla, mutta se on myös suosittu kyberhyökkäysten kohde. Israelin lisäksi Turkki on panostanut vahvasti kyberuhkien torjumiseen. Turkki on organisoinut armeijansa kybertoiminnot Yhdysvaltojen Cyber Commandin toimintaa vastaaviksi (Vavuz 2011).

Wordpress.comissa julkaistaan blogia nimeltä Middle East Cyber War Timeline. Blogista ilmenee, että Lähi-idän alueella tapahtuu jatkuvasti kyberhyökkäyksiä. Hyökkäykset ovat usein Israelia vastaan tai Israelin suorittamia. Palvelunestohyökkäykset, luottokorttitietojen varastaminen sekä www-sivustojen sisällön sabotointi ovat yleisimpiä hyökkääjien suorittamia tekoja. Lähi-idän kybertoimijat poikkeavat muusta maailmasta siten, että motiivit ovat usein poliittisia tai uskonnollisia. Tämä ilmenee jo pelkästään hyökkääjien käyttämistä nimistä, kuten Islamic Ghosts Team, GaZa HackeR TeaM, IDF Team Israel Defence Force (Passeri 2012).

3.7 Muu maailma

Vaikka opinnäytteeseen on poimittu lähinnä julkisuudessa esillä olleita suuria hyökkäyksiä maittain, maailmalla on useita muita maita, joiden suorituskyky kyberavaruudessa on merkittävä. Sellaisissa maissa kuin Intia ja Brasilia on valtavasti ohjelmoinnin ja kryptologian osaamista. Kriittisen infrastruktuurin suojaamiseen ja kyberturvallisuuteen panostetaan vahvasti Kanadassa, Australiassa, Britanniassa, Japanissa ja Ranskassa. Pohjois-Korean ja Etelä-Korean välillä on ollut useita tapahtumia, jotka voidaan luokitella kyberhyökkäyksiksi (Andress 2011, 64-69).

4 Hyökkäysmenetelmät

Ensimmäiset tietojärjestelmähyökkäykset 1980- ja 1990-luvuilla olivat yksinomaan asiantuntijoiden suorittamia. Nykyään lähes kuka tahansa pystyy tekemään hyökkäyksiä valmisohjelmistojen avulla. Useimmiten valmisohjelmia käyttävät kokeilunhaluiset nuoret tietokoneharrastajat, mutta myös rikolliset käyttävät niitä taloudellisien intressien saavuttamisen välineenä. Hienostuneet räätälöidyt ohjelmistot on usein suunniteltu tiettyä käyttötarkoitusta varten, ja niiden takana voivat olla valtiolliset toimijat ja kyberterroristit (Janczwewski ym. 2009, 262-263). Hyökkäyksen ensimmäinen vaihe käynnistyy tiedustelulla. Hyökkääjä pyrkii keräämään mahdollisimman paljon tietoa kohdeorganisaatiosta. Tiedustelutietoa kerätään teknisillä menetelmillä esimerkiksi organisaation www-sivuilta tai muista avoimista lähteistä. Tietoa voidaan kerätä myös sosiaalisilla menetelmillä, esimerkiksi lähestymällä organisaation tietohallintoa kysymyksillä (Valtiovarainministeriö 2009, 18). Tämän jälkeen aloitetaana varsinaisen hyökkäyksen huolellinen suunnittelu analysoitujen tietojen perusteella. Toiseen vaiheeseen sisältyy myös työkalujen ja hyökkäysmenetelmien valinta. Hyökkäyksen kolmannessa vaiheessa skannataan kohteen verkkolaitteiden, työasemien ja palvelimien tietoja mahdollisten haavoittuvuuksien löytämiseksi. Verkkoskannauksella pyritään selvittämään verkon rakennetta. Porttiskannauksen avulla etsitään avoimia portteja, joiden kautta voidaan suorittaa murtautuminen. Porttiskannauksella voidaan myös selvittää, mitä ohjelmia ja protokollia kohdejärjestelmässä on käytössä, jotta voidaan hyödyntää niihin liittyviä haavoittuvuuksia. Ohjelmis-

tojen haavoittuvuusskannauksen tavoitteena on saada selville käyttöjärjestelmä- ja sovellusversiotietoja. Niitä verrataan haavoittuvuustietokantaan mahdollisten tietoturva-aukkojen löytämiseksi. Kolmannen vaiheen tuloksena saadaan siten luettelo niistä keinoista, joiden avulla järjestelmään murtautuminen on mahdollista (Heinonen 2003, 12-15).

Haittaohjelmat jaetaan usein kahteen osaan: lataajaan ja varsinaiseen haittakoodiin. Lataaja on usein pieni ja huomaamaton, ja sen ainoa tehtävä on noutaa haittakoodia sisältävä ohjelma verkosta. Lataaja voidaan konfiguroida käynnistymään ajastetusti, millä pyritään peittämään jälkiä. Hyökkäyksen neljännessä vaiheessa lataaja aktivoituu ja hakee haittaohjelman siihen kovakoodatusta osoitteesta tai ohjauspalvelimellaan sijaitsevan konfiguraatiotiedoston tietojen perusteella (Valtiovarainministeriö 2009, 18-19).

Viides vaihe eli murtautumisvaihe käynnistyy, kun haittaohjelma aktivoituu. Murtautumisvaiheessa haittaohjelma pyrkii saamaan järjestelmänvalvojan oikeudet tai muut riittävät oikeudet hyökkäyksen suorittamiseksi. Hyökkäyksen tavoitteena voi olla aiheuttaa tuhoa kohdejärjestelmään, hyödyntää sitä jatkohyökkäyksiin tai varastaa tietoa kohteesta. Viimeisessä vaiheessa peitetään jäljet; vaihe sisältää lokitietojen sotkemista tai tietojen tuhoamista käyttöjärjestelmien, sovellusten ja verkkolaitteiden lokeista (Valtiovarainministeriö 2009, 19).

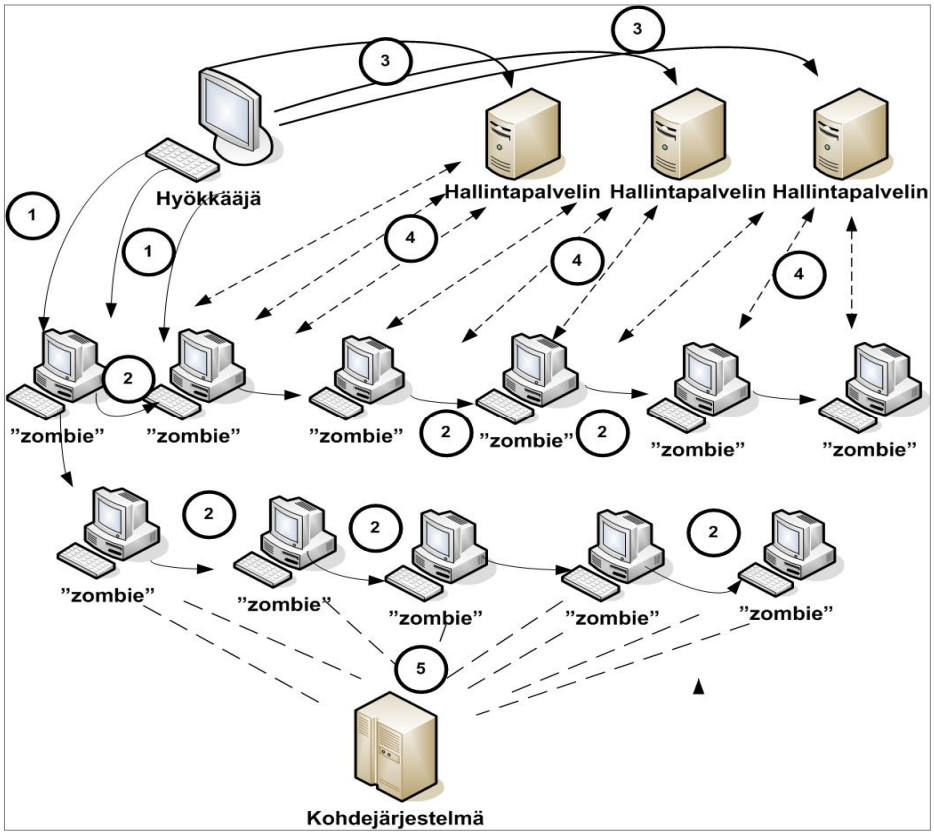
4.1 Palvelunestohyökkäykset

Yksinkertaisimpia palvelunestohyökkäyksiä (Denial of Service, DoS) voidaan toteuttaa lähettämällä suuria määriä ping-paketteja kohdepalvelimelle. Menetelmällä kuormitetaan palvelimen toimintaa siten, että palvelut eivät ole enää saatavilla. Tätä kutsutaan ping-floodaukseksi. Nykyään tämän tyyppinen hyökkäys onnistuu harvoin, koska kohteen resurssit yleensä ovat merkittävästi tehokkaammat kuin hyökkääjän. Lähinnä suurien sähköpostiviestimäärien lähettäminen on tätä menetelmää hyödyntäen nykyään merkittävä haittatekijä. Sähköpostipalvelimen levyresurssien täytyttyä palveluiden saatavuus estyy.

Vuosituhannen vaihteessa hyökkääjät alkoivat valjastaa useita verkkoresursseja, joita kutsutaan bottiverkoiksi (botnet). Bottiverkkoja käytetään hajautettuihin palvelunestohyökkäyksiin (Distributed Denial of Service, DDoS). Tavallisten käyttäjien työasemista muodostetaan usein bottiverkkoja heidän tietämättään. Tällaista työasemaa kutsutaan kaapatuksi tietokoneeksi (engl. zombie). Tyypillisesti hyökkäyksen apuna käytettävistä kaapatuista tietokoneista etsitään tietoturva-aukkoja, joita hyödyntäen niihin asennetaan haittakoodia. Haittaohjelmassa voi olla kovakoodattuna hyökkäyksen ajankohta ja kohde. Kohdetta sekä ajankohtaa voidaan muuttaa myös dynaamisesti. Internetissä käytettävä TCP/IP-protokollaperhe (Transmission Control Protocol / Internet Protocol) mahdollistaa pakettien lä-

hettämisen siten, että niiden lähdeosoite on väärennetty. Hyökkääjät käyttävät tätä keinoa jälkiensä peittämiseen. Lähettääkseen komentoja kaapatuille tietokoneille hyökkääjät voivat käyttää useita eri protokollia, kuten TCP, UDP (User Datagram Protocol) tai korkeamman tason protokollia, kuten Telnet ja IRC (Internet Relay Chat). Kohteiden skannaus ja saastuttaminen suoritetaan yleensä automatisoiduilla skripteillä.

Kuvassa 3 esitetään yksi esimerkki, miten tavallisten käyttäjien koneet kyetään valjastamaan bottiverkoksi, joka suorittaa palvelunestohyökkäyksen hyökkääjän valitsemaan kohteeseen. Hyökkääjä hyödyntää käyttäjien työasemissa olevia haavoittuvuuksia ja ujuttaa työasemiin haittaohjelman (kuva 3, vaihe 1). Käyttäjän työasemasta tulee kaapattu tietokone, joka suorittaa käyttäjän tietämättä toimintoja, kuten haittaohjelman levittämistä edelleen muihin työasemiin (kuva 3, vaihe 2). Hyökkääjä etsii verkosta sellaisia palvelimia tai reitittimiä, jotka kykenevät käsittelemään suuria määriä palvelupyyntöjä, ja asentaa niihin bottiverkon hallintaohjelman (kuva 3, vaihe 3). Kaapattujen tietokoneiden työasemissa olevaa haitta-ohjelmaa käskytetään hallintapalvelimen avulla; hallintapalvelin havaitsee, mitkä työasemat ovat käynnissä, ja se kykenee myös päivittämään työasemissa olevan haittaohjelman uudempaan versioon. Hyökkääjä käynnistää palvelunestohyökkäyksen antamalla hyökkäyskäskyn hallintapalvelimen kautta kaapatuille tietokoneille (kuva 3, vaihe 4). Kohdejärjestelmän resurssit ylikuormittuvat lukuisista lähteistä tulevista palvelupyynnöistä, mikä aiheuttaa palvelun jumiutumisen (kuva 3, vaihe 5).(Spect & Lee, 1-2).



Kuva 3: Hajautettu palvelunestohyökkäys

4.2 Virukset ja haittaohjelmat

Ensimmäinen PC-tietokoneelle luotu virus oli nimeltään Brain. Sen ohjelmoivat pakistanilaiset veljekset Basit ja Amjad Alvi. Brain luotiin ohjelmoijiensa mukaan kostoksi, koska veljesten ohjelmoimia tuotteita myytiin piraattikopioina. Virus levittäytyi kirjoittamalla haittakoodia levykkeiden käynnistyssektorille, kun levykkeestä tehtiin kopio. Tätä ennen tosin Applen käyttöjärjestelmälle oli tehty jo vuonna 1982 Elk Cloner -niminen virus, joka toimi samankaltaisella periaatteella (Antivirusware 2012).

Ensimmäinen tunnettu Internetissä leviävä haittaohjelma oli Morris-mato, joka saastutti vuonna 1988 arviolta 10 prosenttia Internetiin kytketyistä tietokoneista. Morris levittäytyi kopioimalla itseään, ja se hyödynsi Unix-järjestelmissä olevissa suosituissa sendmail- ja finger-työkaluissa olleita haavoittuvuuksia. Mato käytännössä lamautti Internetin useaksi päiväksi ja pakotti useat organisaatiot irrottamaan tietokoneensa Internetistä. Madon kirjoittanut Robert Tappan Morris tuomittiin myöhemmin ensimmäisenä Internet-petoksesta. Tämän jälkeen haittaohjelmat alkoivat hiljalleen yleistyä. Muita tunnetuimpia matoja ovat SQL-Slammer, Melissa ja Code Red (Marsan 2008).

Haittaohjelmat ja virukset voidaan jakaa yleisimpiin päätyyppeihin niiden tekniikan mukaan, joita ovat madot, makrot tai skriptit, troijalaiset, rootkitit, polymorfiset virukset, muistinvaraiset virukset sekä aikapommit. Troijalainen voi vaikuttaa tavalliselta ohjelmalta, mutta se suorittaa salaa toimintoja, jotka eivät näy käyttäjälle. Troijalaiset eivät tyypillisesti levittäydy tai kopioidu itsestään, mutta ne aiheuttavat valittuun kohdejärjestelmään vahinkoa. Ne voivat tuhota tiedostoja ja mahdollistaa kohdekoneen etähallinnan, ja niitä voidaan käyttää tietojen varastamiseen. Madot pyrkivät monistamaan itseään ja leviämään siten mahdollisimman laajalle. Yleisiä menetelmiä matojen levittämiseen ovat ohjelmistohaavoittuvuudet ja sähköpostin liitetiedostot. Käynnistyslohkovirukset, kuten aiemmin mainittu Brain, ovat nykyään harvinaisia, koska levykkeet ovat poistuneet käytöstä ja tiedostoja siirretään usein muistitikuilla. Kuten Stuxnet-tapaus osoittaa, muistitikuista on tullut merkittävä uhka varsinkin myös järjestelmille, jotka eivät ole kiinni tietoverkoissa.

Takaoviksi kutsutaan ohjelmia, jotka mahdollistavat ulkopuolisen murtautumisen kohteeseen ohittamalla tietoturvakontrollit. Takaovet voivat asentua haittaohjelman avulla, tai ne voivat olla jo valmiiksi koodattuna ohjelmassa. Aikapommit on nimensä mukaisesti suunniteltu aktivoitumaan tiettynä ajankohtana. Ne voivat käynnistyä maan itsenäisyyspäivänä, uskonnollisena juhlapyhänä tai vaikkapa työntekijän työsuhteen päättyessä (Top Choice Reviews 2010).

Polymorfiseksi kutsutaan sellaista virusta, joka ei ainoastaan monista itseään, vaan sen digitaalinen allekirjoitus muuttuu jokaiseen kopioon. Tällä vaikeutetaan virustorjuntaohjelmistojen virushavainnointikykyä. Toinen tapa hämätä virustorjuntaohjelmistoja on viruksen kryptaaminen, mutta koska virus sisältää myös salakirjoituksen purkukoodin, virustorjuntaohjelmistot tunnistavat usein tämän tyyppiset virukset. Teknisten toimintatapojen lisäksi haittaohjelmia voidaan luokitella niiden toiminnallisuuksien mukaan. Tyypillisiä toiminnallisuuteen viittaavia termejä ovat Adware, Malware, Ransomware, Riskware, Spyware ja Stealware (Laaksonen 2010. 8, 23). Rootkiteillä on ominaispiirteitä, joita voidaan käyttää sekä hyökkäykseen että puolustukseen. Rootkitejä käsitellään hiukan tarkemmin kohdassa 4.2.1.

Saksalaisen NETPilot GmbH - tietoturvayrityksen julkaisemien tilastojen mukaan Yhdysvalloissa sijaitsee ylivoimaisesti suurin määrä haittaohjelmia levittävistä www-sivustoista maailmassa (NETPilot GmbH 2012).

4.3 Rootkit

Rootkitit yleistyivät 1990-luvulla Unix-pohjaisissa laitteissa. Ne pyrkivät tyypillisesti asentumaan itse käyttöjärjestelmään ja piilottamaan itsensä. Rootkitit hyödyntävät kohteensa haavoittuvuuksia. Niiden tyypillisiä ominaisuuksia on kohteen etähallinta, tartuntajälkien tuhoaminen sekä haitallisten prosessien ja verkkoyhteyksien peittäminen.

Rootkit-käsite viittasi alun perin kokoelmaan työkaluja, joilla voidaan saada pääkäyttäjän (root) oikeudet Unix-käyttöjärjestelmässä. Rootkitejä voi kuitenkin olla missä tahansa käyttöjärjestelmässä. Kaikki rootkitit eivät kuitenkaan ole vaarallisia: niitä voidaan käyttää esimerkiksi DVD-levyjen kopiointiohjelmissa tai jopa virustorjuntaohjelmistoissa. Siten rootkitejä ei voida luokitella pelkäksi hyökkäysmenetelmäksi (Symantec 2012).

Yksinkertaisimmat hyökkäystarkoitukseen tehdyt rootkitit ovat vain piilotettuja takaoviohjelmia, jotka jättävät tietyn tietoliikenneportin auki. Rootkitejä on kuitenkin usean tyyppisiä, mutta yleisesti ne sisältävät työkaluja tai menetelmiä hyökkäyksen peittämiseen. Yksi tapa on korvata järjestelmänvalvojan (root, administrator) sellaiset yleisesti käyttämät komennot, jolla hyökkäys voisi paljastua. Esimerkiksi jos järjestelmänvalvoja käyttää käynnissä olevia prosesseja luettelevaa ps-komentoa Linux-järjestelmässä, hyökkääjä voi yrittää korvata ps-komennon aidolta vaikuttavalta ps-komennolla, joka piilottaa järjestelmään ujutetut haitalliset prosessit. Siten järjestelmänvalvoja ei havaitse mitään normaalista poikkeavia prosesseja. Rootkitit voivat sisältää järjestelmälokia sotkevia toimintoja hyökkäyksen jälkien haihduttamiseksi. Jotkin edistyneemmät rootkitit eivät ainoastaan korvaa käyttöjärjestelmän tiedostoja, vaan päivittävät käyttöjärjestelmän kerneliä. Tunkeutumisenestojärjestelmät tark-

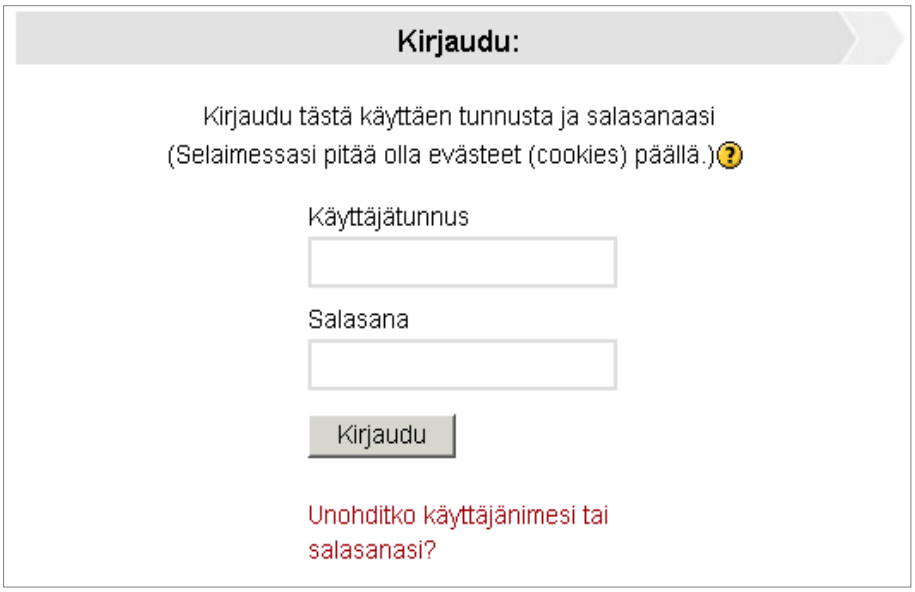
kailevat useimmiten tiedostoihin kohdistuneita muutoksia, mutta eivät välttämättä kerneliä (Harris 2008, 643-644).

4.4 SQL-injektio

Valtaosa relaatiotietokannoista hyödyntää vuonna 1986 standardoitua SQL-kyselykieltä (Sturcutred Query Language). SQL-kielen avulla tietokantaan voidaan tehdä tiedonhakuja, muokkauksia, lisäyksiä ja poistoja. Erityisesti www-pohjaiset sovellukset ovat alttiita SQL-injektioiksi kutsutuille hyökkäysmenetelmille. SQL-injektioiden avulla kohdesovellukseen voidaan syöttää haitallisia SQL-lauseita. Verkkosovellukset on toteutettu yleensä dynaamisilla skriptauskielillä, kuten ASP (Active Server Pages), PHP (Pre Hypertext Prosessor) ja JSP (Java Server Pages). SQL-injektio tehdään useimmiten hyödyntäen sovelluksen ohjelmistokoodin, www-palvelinohjelmiston tai skriptauskielen haavoittuvuuksia. Sovellusten ohjelmoijat ketjuttavat monesti SQL-komentoja käyttäjien www-sovelluksella syöttämiin arvoihin. Hyökkääjän kannalta se mahdollistaa haitallisten SQL-lauseiden ujuttamisen syötteiden joukkoon (Janczwewski ym. 2009, 162).

4.4.1 Hyökkäykset verkkolomakkeiden avulla

Yksi tapa suorittaa SQL-injektio on käyttää verkkosovelluksen lomaketta. Seuraavassa kuvataan yksinkertaisen SQL-injektion suorittaminen www-sivuston kirjautumislomakkeella.



Kuva 4: Tyypillinen kirjautumissivu.

Kirjautumissivu voidaan luoda esimerkiksi ASP-skriptauskielellä, jossa kirjautumiseen liittyvän ohjelmistokoodin pätkä voisi näyttää esimerkiksi seuraavalta:

```
<%
Dim username, password;
kayttajatunnus = Request.form(”text_kayttajatunnus);
salasana = Request.form(”text_salasana);
’ käyttäjätunnus- ja salasanamuuttujien kohdistaminen web-sivun lomakekenttiin’

var yhteys = Server.CreateObject(“ADODB.Connection”);
var objekti = Server.CreateObject(“ADODB.Recordset”);
‘ tietokannan käsittelyn asetuksia’

var sql_kysely = ”select * from USERS where kayttajatunnus=’”+ text_kayttajatunnus+ ”’
and salasana=’”+ text_salasana’”’;”;
’kirjautumislomakekenttiin liittyvä SQL-kysely joka kohdistetaan tietokantaan’

objekti.open(sql_kysely, yhteys);
if (objekti.eof) then
response.write”kirjautuminen epäonnistui.”
else
response.write ”tervetuloa www-palveluun x!”;
%>
```

Kuva 5: Esimerkki ASP-koodista, joka käsittelee www-palveluun kirjautumista.

Listauksen 1 osalta oleellinen kohta ohjelmakoodia murtautujan kannalta on

var sql_kysely = ”select * from USERS where kayttajatunnus=’”+ text_kayttajatunnus+ ”’ and salasana=’”+ text_salasana’”’;”;

Käytännössä tämä pätkä koodia muodostaa USERS-nimiseen tietokantatauluun kyselyn, jossa on mukana käyttäjän syöttämä käyttäjätunnus ja salasana. Esimerkiksi syöttämällä lomakkeeseen käyttäjätunnukseksi Martti ja salasanaksi Atk-2012! syntyy tietokantaan kohdistuva SQL-kysely, jonka sisältö on

select * from USERS where username = ’Martti’ and salasana = ’Atk-2012!’:

Mikäli tämä käyttäjätunnuksen ja salasanan yhdistelmä on oikea, kirjautuminen sovellukseen onnistuu. Käyttäjä pääsee sovelluksen niihin osioihin, joihin hänen oikeutensa edellyttävät. Hyökkääjä voi sen sijaan yrittää syöttää tekstikenttiin vääriä ennalta-arvaamattomia arvoja, esimerkiksi seuraavasti:

käyttäjätunnus: Martti
salasana: jotakin’ or ’1’ = ’1’;

SQL-lauseeseen sisältyvä ehto ’1’ = ’1’ palauttaa OR-komennon yhteydessä aina vastauksen tosi (true). Mikäli sovelluksen ohjelmointi on toteutettu huolimattomasti, ohjelma voi tulkita, että käyttäjätunnus Martti ja salasana jotakin ovat kelvollinen yhdistelmä. Pahimmassa tapauksessa tällä menetelmällä voidaan saada ohjelma palauttamaan kaikki käyttäjätunnukset ja salasanat. Mikäli hyökkääjä tietää ennakolta käyttäjätunnuksen ja sovelluksessa hyödynnettävän tietokantaohjelmiston, hän voi hyödyntää tietokantaohjelmiston ominaisuuksia tietomurron apuna. Esimerkiksi huolimattomasti toteutetussa SQL Server -tietokantaohjelmistoa käyttävässä ohjelmassa kirjautuminen voisi onnistua ilman salasanaa syöttämällä seuraavat arvot www-lomakkeen kenttiin:

Käyttäjätunnus: joku ’or kayttajatunnus = ’admin’; –-
salasana:

Tämä johtuu siitä, että Microsoftin SQL Serverin käyttämä Transact-SQL-laajennus tulkitsee merkkiyhdistelmän –- kommentiksi, jonka jälkeen tulevia SQL-lauseosioita ei suoriteta. Muita vastaavanlaisia ehtolauseiden yhdistelmiä hyödyntäen hyökkääjä voi tuhota tietokannan sisällön, sammuttaa tietokannan tai lähettää sen sisällön toiselle palvelimelle. Käytännössä hyökkääjä kykenee tekemään mitä tahansa, minkä mahdollistavat ne oikeudet, jotka hän on sovelluksen avulla onnistunut hankkimaan (Janczewski ym. 2009, 164).

4.4.2 Selaimen osoitekentän manipulointi

Toinen yleinen tapa toteuttaa SQL-injektioita on selaimen URL-osoitekentän (Universal Resource Locator) manipulointi (URL-poisoning). Seuraavassa esitetään yksinkertainen esimerkki, miten kyberrikollinen voi murtautua kuvitteelliseen verkkokauppaan. SQL-kyselyn suorittava ohjelmakoodirivi verkkokaupassa voisi olla

```
sql_kysely= " SELECT TuoteNimi, TuoteKuvaus FROM Tuotteet WHERE TuoteNumero = " &
Request.QueryString("TuoteNro")
```

Tässä yhteydessä arvo TuoteNro saadaan kyselyyn verkkokaupan sivuston URL-parametristä: http://www.esimerkkikauppa.com/tuotteet/tuotteet.asp?tuotenro=123. Tämän URL-osoitteen lähettämisen tuloksena syntyy SQL-kysely

```
SELECT TuoteNimi, TuoteKuvaus FROM Tuotteet WHERE TuoteNumero = 123
```

Käytännössä haetaan siis tuote-nimisestä tietokantataulusta tuotteen numero 123 nimi sekä tuotekuvaus. Vastaavasti kuin aiemmassa esimerkissä, voitaisiin ketjuttaa kyselyyn lisäksi OR 1=1 syöttämällä URL-osoitteeksi

http://www.esimerkkikauppa.com/tuotteet/tuotteet.asp?tuotenro=123 or 1=1

Tällöin tuloksena saataisiin kaikkien tuotteiden listaus tuotekuvauksineen. Vastaavasti tuotetaulu voitaisiin tuhota komennolla

http://www.esimerkkikauppa.com/tuotteet/tuotteet.asp?tuotenro=123; DROP TABLE tuotteet

4.4.3 Muut menetelmät

Hyökkääjä ei aina saa verkkosovelluksesta sellaista vastetta, josta hän pystyisi päättelemään, onko kohde haavoittuvainen vai ei. Menetelmää, jossa hyökkäys pyritään tekemään näkemättä sovelluksen antamia vasteita, kutsutaan Blind SQL -injektioksi. Tietoa saadaan koostettua kohdetietokannasta hakemalla useilla tosiehtolauseilla vastaukseksi yksittäistä merkkiä tai bittiä. Tietokannan antamien ”true”- tai ”false”-vastausten perusteella saadaan koostettua tietoa. Kyselyillä voidaan hakea esimerkiksi, alkaako käyttäjätunnuksen salasana tietyllä kirjaimella, ja kun vastaukseksi saadaan ”true”, tiedetään käyttäjätunnuksen ensimmäinen kirjain. Tämän jälkeen edetään seuraavaan kirjaimeen ja niin edelleen. Mikäli vastauksena saadaan tyhjä sivu vakiomuotoisen virheilmoitussivun sijasta, voidaan päätellä, että kysely onnistui. Mikäli järjestelmä on suojattu tätä menetelmää vastaan, voidaan toteuttaa aikaperusteinen Blind SQL -injektio (Time Based Blind SQL-Injection). Kyselyn ehdoksi voidaan asettaa pitkä viive, jolloin kyetään päättelemään kyselyn läpimenoajasta, oliko vastaus ”true” vai ”false”. Aikaperusteisista Blind SQL -injektioista on olemassa monimutkaisempi, mutta tehokkaampi muunnelma, jota kutsutaan Deep Blind -injektioksi. Se perustuu vaihtelevien aikaviipeiden käyttöön (Matuna 2008, 2). Erilaisten SQL-injektioiden tekoon on useita valmisohjelmistoja. Edistyneet työkalut, kuten BSQL-hacker, soveltuvat sekä aloittelijoille että asiantuntijoille. Työkaluissa on valmiita hyökkäysskriptejä, automaatio-toimintoja, helppokäyttöisiä käyttöliittymiä ja tuki suosituimmille tietokantaohjelmistoille.

4.5 Web 2.0 -sovellusten haavoittuvuudet

Web 2.0 -termiä käytetään usein viime vuosien sisällä kehitetyistä uusista verkkotekniikoista ja palveluista. Web 2.0:sta ei ole olemassa tarkkaa määritystä, mutta useimmiten se liitetään vähintäänkin seuraaviin tekniikoihin ja niiden avulla rakennettuihin palveluihin: Ajax, Mashups, Widgets, SOAP, REST, XML-RPC, RSS, Atom, JSON. Mikäli näillä tekniikoilla rakennettujen palveluiden takana on käytössä tietokantaohjelmisto, hyökkääjä voi yrittää hyödyntää SQL-injektioita, mutta tekniikoita vastaan on kehitetty omia hyökkäysmenetelmiä.

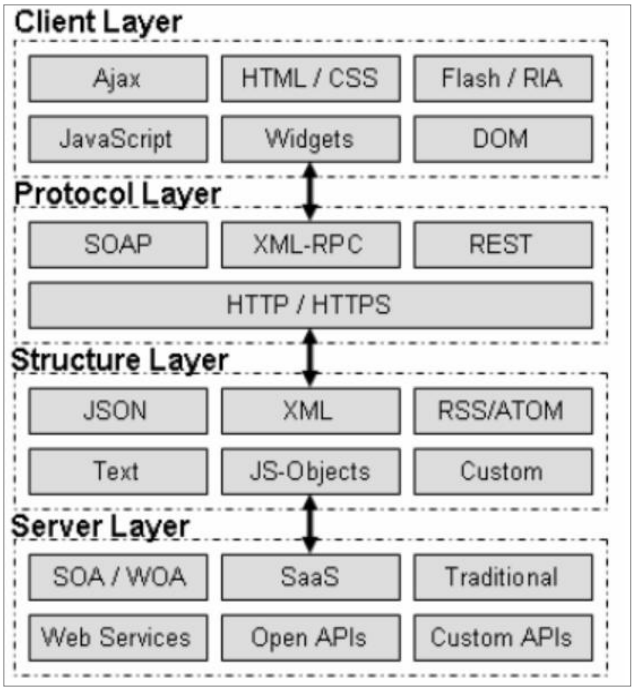
Esityskerroksella toimiva Asynchronous Javascript And Xml (Ajax) tarjoaa asynkronisen kommunikointimenetelmänsä ansiosta nopeammat vasteajat selainpohjaisen sovelluksen käyttäjälle. Ajaxin avulla selaimeen saadaan rakennettua entistä näyttävämpiä käyttöliittymiä, jolloin muiden client-ohjelmistojen tarve vähenee. Termiä Rich Internet Applications (RIA) käytetään Flashista ja muista tekniikoista, jotka mahdollistavat näyttävien käyttöliittymien rakentamisen verkkosovelluksiin. Widgetit (pienoisohjelmat, pienohjelmat) ovat pieniä sovelluksia, joita voi sijoittaa sovelluksiin, verkkosivuille tai tietokoneen työpöydälle. Tyypillisiä widgetejä ovat kellot sekä uutis- ja säätietoja näyttävät ohjelmanpätkät. Mashup (koostesovellus) on widgetiä laajempi käsite, joka tarkoittaa verkkopohjaisia palveluja ja palvelurajapintoja, joita yhdistelemällä voidaan luoda uusia palvelukokonaisuuksia (Shah 2007, 28).

Protokollakerroksella käytettävä Simple Object Access Protocol (SOAP) on erittäin suosittu palvelukeskeisessä arkkitehtuurissa (Service Oriented Architecture). SOAP pohjautuu XML-kieleen, ja sitä käytetään pääasiassa HTTP-protokollan yli. SOAP-dokumentin rakenne on tarkasti määritelty palveluiden välistä tiedonvaihtoa ajatellen (Shah 2007, 29-30). Remote Procedure Call (RPC) eli etäkutsu on vanha menetelmä prosessien etäkäynnistykseen. Etäkutsuja voidaan käynnistää saman koneen käyttöjärjestelmän prosessien välillä tai verkon yli. Käyttöjärjestelmiä on yhä enemmän alettu suojata siten, että lähinnä ainoastaan HTTP-liikenne on sallittu. Tästä syystä kehitettiin HTTP:n päällä toimiva XML-RPC–etäkutsumenetelmä. Kuten nimestä ilmenee, niin XML-RPC on SOAPin tavoin XML-pohjainen. Verkkopalveluissa suosittu Representational State Transfer (REST) on verkkopalveluissa suosittu arkkitehtuurityyli. Kuten XML-RPC ja SOAP, se pohjautuu XML:ään ja HTTP:n hyödyntämiseen. Lukuisat verkkokaupat on rakennettu RESTiä hyödyntäen, koska se on erityisen käytännöllinen tilatietojen välittämiseen, kun käyttäjä liikkuu verkkokaupassa sivulta toiselle (Shah 2007, 33-34).

JavaScript Object Notation (JSON) on kevyt tiedonsiirtomuoto. Se on yksinkertaisempi merkintäkieli kuin XML. Nimestään huolimatta JSON ei rajoitu JavaScriptiin vaan on ohjelmointi kielestä riippumaton. JSONia käytetään usein Ajax-sovelluksissa (Harju 2008, 24).

Real Simple Syndication- (RSS) ja Atom-syötteet ovat toimintaperiaatteeltaan ja käyttötarkoitukseltaan samankaltaisia. Niitä käytetään pääasiallisesti blogi- ja uutisvirtojen kokoamiseen. Syötteet ovat XML-tiedostoja, jotka lukijaohjelman avulla muunnetaan helposti ymmärrettävään muotoon (Kurki 2008, 22).

Kuvassa 6 on Web 2.0:n tietoturva-asiantuntija Shreejay Shahin esittämä näkemys siitä, miten Web 2.0 -tekniikoiden arkkitehtuurikerrokset jakautuvat.



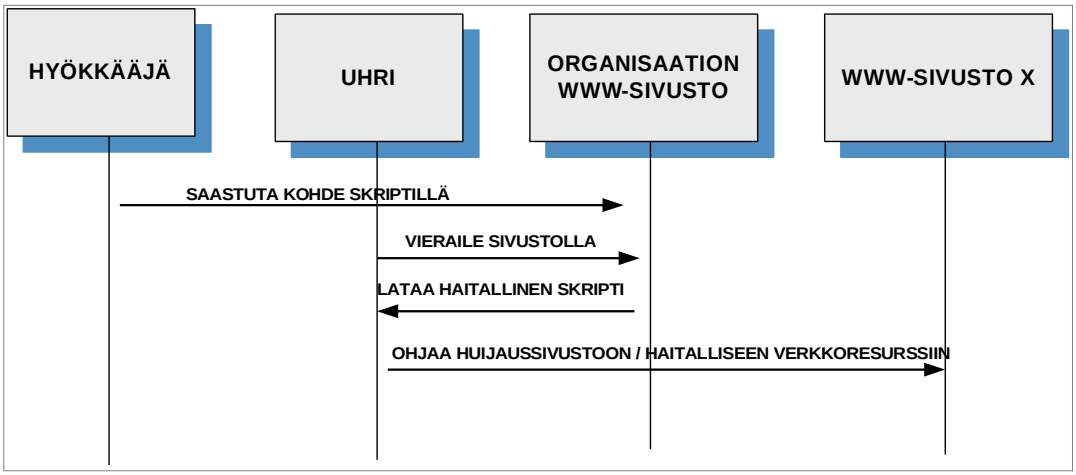
Kuva 6: Web 2.0 -kerrokset .

4.6 Cross-site scripting -hyökkäys

Cross-site scripting (XSS) -hyökkäys voidaan kohdistaa käyttäjän selainohjelmistoon tai palvelimella sijaitsevaan verkkosivustoon. XSS-haavoittuvuuksia käytetään myös paljon haittaohjelmien levittämiseen. Web 2.0 -sovellukset käyttävät RSS-syötteitä, widgetejä ja JavaScript-pohjaista koodia, jotka kaikki ovat alttiita XSS-hyökkäyksille. Document Object Model (DOM) on ohjelmointirajapinta (API), joka on käyttöjärjestelmästä riippumaton. Se mahdollistaa dokumenttien muokkauksen ja sitä käytetään JavaScriptin kanssa dynaamisten verkkosivujen luomiseen. DOMin manipulointi XSS-injektion avulla on yksi suosittu hyökkäysmenetelmä.

Yleinen tapa suorittaa XSS-hyökkäys on manipuloida asiakasohjelmistossa suoritettavaa koodia hyökkääjän haluamalla tavalla. Hyökkääjä lataa haittakoodin osaksi palvelimella sijaitsevaa verkkosivua. Haittakoodi suoritetaan joka kerta, kun käyttäjät selaavat sivua (Shaah 2007, 33-34). Käyttäjä voidaan esimerkiksi johdattaa oikean verkkopankin sijasta toiselle sivustolle,

joka näyttää samalta verkkopankilta. Seuraavassa on yksinkertaistettu kuva XSS-hyökkäyksen perusperiaatteesta:



Kuva 7: XSS-hyökkäyksen periaate.

Evästeissä (cookie) käsitellään käyttäjien istuntoon liittyviä tietoja, joihin lukeutuvat käyttäjän istunnon tunnistaminen, seuraaminen ja käyttäjäasetusten personointi. Hyökkääjä voi pyrkiä varastamaan käyttäjän evästeen ujuttamalla seuraavan koodinpätkän verkkosivulle:

<script> document.location= 'http://xss.esimerkkisivusto.com varastacookie.php?
'+document.cookie </script>

Koodista näkyy, että käyttäjän tullessa sivulle hänet ohjataan toiselle sivustolle, jossa sijaitsee skripti nimeltä varastacookie.php, joka kerää evästeessä olevan tiedon. Erilaisia XSS-hyökkäysmenetelmiä on paljon. Ne vaihtelevat hyökkääjän tavoitteiden mukaisesti. Yleisimpiä tavoitteita ovat identiteettivarkaudet, tietoaineiston varastaminen, käyttäjän selailutottumusten vakoilu ja huijaussivustolle ohjaaminen (Guillaumier J. 2012).

4.6.1 XML-pohjaiset hyökkäysmenetelmät

Vaikka tässä käsitellään yksinkertaisin esimerkein, miten SOAP-protokollaa voidaan väärinkäyttää, samankaltaisia hyökkäysmenetelmiä on mahdollista hyödyntää XML-RPC:n ja REST:n kohdalla.

XML-pohjaiseen SOAP-viestiin voidaan tehdä SQL-injektio manipuloimalla XML-tiedostoa seuraavalla tavalla:

```
<? xml version=”1.0” encoding=”utf-8”?>
<soap:Envelope xmlns:soap=”http://schemas.xmlsoap.org/soap/envelope/”
                    xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
                     xmlns:xsd”http://www.w3.org/2001/XMLSchema
<soap:Body>
<getProductInfo xmlns=”http://esimerkkikauppa.fi/”>
<id> 1 or 1=1 </id>
</soap:envelope>
```

Koodissa lihavoituna esitetty <id> 1 or 1=1 </id> on lisätty muutoin normaaliin SOAP-viestiin, jolloin tuloksena voi olla, se että saadaan lueteltua kaikki tämän kuvitteellisen verkkokaupan tuotteet yhden sijasta. Mikäli tämä menetelmä onnistuu, niin voidaan yrittää hyödyntää muita vastaavia SQL-injektiomenetelmiä, joita käsiteltiin aiemmin opinnäytetyössä.

Myös käyttöjärjestelmän komentotasolle voidaan yrittää murtautua manipuloimalla SOAP-viestiä. Seuraavassa on kuvattu yksinkertainen esimerkki, kuinka SOAP-viestiin putkitetaan käyttäjätunnuksen syötön perään hakemistolistauskomento.

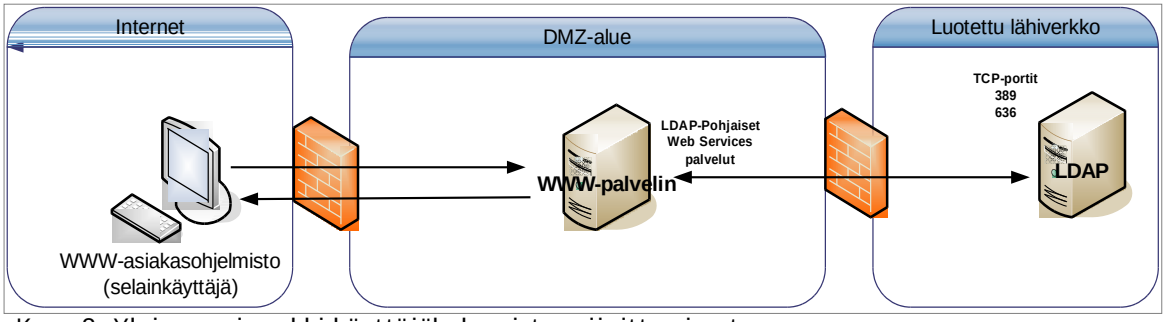
```
<? xml version=”1.0” encoding=”utf-8”?>
<soap:Envelope xmlns:soap=”http://schemas.xmlsoap.org/soap/envelope/”
                    xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
                     xmlns:xsd”http://www.w3.org/2001/XMLSchema

<soap:Body>
<getUserPrefFile xmlns=http://esimerkkikauppa.com/”>
<user>Martti | dir c:\</user>
</getUserPrefFile>
</soap:Body>
</soap:Envelope>
```

Edellä olevassa listauksessa on lisätty SOAP-viestiin komento ”| dir C:\”. Onnistuneen hyökkäyksen tuloksena saadaan lueteltua kaikki C-aseman juuressa olevat tiedostot. Mikäli oikeudet, joilla päästään käskyttämään komentokehotetta, ovat riittävän vahvat, voidaan ajaa palvelin alas tai tuhota sen kiintolevyjen sisältö.

XPATH on kieli, jolla XML-dokumenteista haetaan tietoa. Monet verkkopalvelut prosessoivat XML-dokumenttaja XPATHin avulla. XML-sanomaa voidaan manipuloida tekemällä XPATH-injektio. Muita tehokkaita hyökkäystapoja ovat sanakirjahyökkäykset ja LDAP-injektiot. Sanakirjahyökkäyksen tekoon on olemassa helppokäyttöisiä työkaluja, joihin voidaan ladata tiedosto, joka sisältää pitkän luettelon käyttäjätunnuksia ja salasanoja, joita kohdepalveluun murtautumiseen voidaan yrittää (Shah 2007, 258, 278).

Lightweight directory access protocol (LDAP) on laajasti käytetty verkkoprotokolla käyttäjähakemistojen käsittelyyn. Sen avulla voidaan lukea, muokata ja luoda tietoa. Palvelukeskeisessä SOA-arkkitehtuurissa suosituissa Web Services -palveluissa on mahdollisuus LDAP-integraatioon. LDAP-injektio on yksi keino murtautua Internetin kautta organisaation sisäverkkoon. LDAP käyttää TCP-porttia 389 ja SSL-suojattuna porttia 646. Organisaatiot sijoittavat usein LDAP-palvelimensa suojattuun sisäverkkoon ja WWW-palvelimensa niin kutsutulle DMZ-alueelle (Demilitarized Zone). Oheisessa kuvassa on esitetty perusarkkitehtuuri LDAP:n sijoittelusta verkkoympäristössä.



Kuva 8: Yleinen esimerkki käyttäjähakemiston sijoittamisesta.

Internetin kautta voidaan suorittaa LDAP-injektio manipuloimalla SOAP-viestin sisällä olevia LDAP-kyselyjä. Murtautuja ei ainoastaan pääse aiheuttamaan vahinkoa DMZ-alueella olevalle verkkosivustolle, vaan myös käyttäjähakemistolle, jota usein käytetään myös käyttäjähakemistona useille luotetussa sisäverkossa oleville järjestelmille.

4.7 Salasanan murtaminen

Väsytysmenetelmällä (brute force) tarkoitetaan kohteen suojauksen murtamista käymällä systemaattisesti läpi kaikki mahdolliset vastaukset. Menetelmän hyvä puoli on se, että se johtaa lopulta aina haluttuun lopputulokseen. Parhaimmat suojausalgoritmit ovat kuitenkin niin vahvoja, ettei tämä menetelmä ole välttämättä ajallisesti järkevä hyökkääjän kannalta (Nurminen 2002, 1-2). Ellei hyökkääjällä ole käytössään esimerkiksi pilvipalveluna hankitun klusterin prosessointitehoa tai bottiverkkoa, väsytysmenetelmää tehokkaampi tapa on toteuttaa sanakirjahyökkäys. Ihmisten tapana on luoda salasanoja, jotka muodostuvat sanoista ja mahdollisesti niihin liitetyistä numeroista ja erikoismerkeistä. Internetistä on saatavilla useita valmiita salasanalistoja, joita voi käyttää sanakirjahyökkäyksiin. Hyökkäyksessä käytettäviin salasanoihin lisätään ohjelmallisesti numeroita ja erikoismerkkejä salasanojen alkuun ja loppuun. Tämä parantaa hyökkäyksen onnistumismahdollisuutta, mutta toisaalta myös hidastaa hyökkäystä. Sanakirjahyökkäystä muistuttavassa rainbow table -hyökkäyksessä käytetään valmiiksi laskettuja taulukkoja kryptauksen murtamiseksi. 40-bittisessä salauksessa on yli triljoona avainta. Mikäli yksi tietokone pystyy käsittelemään noin 500 000 avainta sekunnissa, siltä veisi noin 25 päivää käydä kaikki vaihtoehdot läpi. Rainbow table -hyökkäyksessä, jossa vaihtoehdot ovat jo valmiiksi laskettuja, tietomurto toteutuu minuuteissa viikkojen sijasta. (AccessData 2006, 3)

Mikäli hyökkääjä pääsee Unix- tai Windows-pohjaiseen työasemaan käsiksi, hän pystyy murtautumaan järjestelmään pääkäyttäjän oikeuksilla helposti. Varsinkin Windows-käyttöjärjestelmiin on olemassa monenlaisia helppokäyttöisiä työkaluja salasanojen murtamiseen (Drave 2010, 3-4).

Yksi menetelmä murtautua Linux-järjestelmään on käyttää BackTrack-ohjelmistoa. Murtautuminen on varsin yksinkertaista:

1. Käynnistetään BackTrack-ohjelmisto CD-levyltä.
2. Siirrytään hakemistoon komennolla cd /usr/local/john.
3. Annetaan komento unshadow etc/passwd etc/shadow > saltedpasswords.
4. Annetaan komento john saltedpasswords.

Edellä oleva esimerkki murtaa CD-levyllä sijaitsevat salasanat. Kiintolevyllä sijaitsevien salasanojen murtaminen toimii samalla tavalla ja vaatii vain pari lisäkomentoa. Mikäli hyökkääjä pääsee fyysisesti käsiksi työasemiin tai palvelimiin, hän voi asentaa koneeseen rautapohjaisen keylogger-tuotteen. Rautapohjainen keylogger sijoitetaan tyypillisesti koneen takana sijaitseviin liittimiin. Se on käyttöjärjestelmästä riippumaton, eivätkä haittaohjelmatorjuntaohjel-

mistot havaitse sitä. Keyloggerin avulla on mahdollista kerätä käyttäjien näppäimistöllä kirjoittamia salasanoja.

Muita potentiaalisia kohteita salasanojen murtamiseen ovat verkkolaitteet ja tietokantaohjelmistot. Helpoimmillaan reitittimiin ja kytkimiin pääsee käsiksi niiden valmistajakohtaisilla oletussalasanoilla, mikäli niitä ei ole vaihdettu. Salasanamurto-ohjelmiin on saatavilla verkkolaitekohtaisia kirjastoja, joilla hyödynnetään laitteen mahdollisia tietoturva-aukkoja. Tietokantaohjelmistoihin on rakennettu sanakirjahyökkäystyökaluja ja muita ohjelmistokohtaisia apuvälineitä, jotka mahdollistavat heikosti suojattuihin tietokantoihin murtautumisen (Drave 2010, 26).

4.8 Man in the middle

Man in the middle (MITM) -hyökkäys perustuu siihen, että hyökkääjä on keksinyt tavan lukea ja muokata kahden osapuolen välisiä viestejä osapuolten huomaamatta. Esimerkiksi jos Martti ja Pertti vaihtavat julkisia salausavaimia keskenään, skenaario voi edetä seuraavasti: Martti lähettää Pertille julkisen avaimensa ja hyökkääjä sieppaa avaimen. Hyökkääjä ei lähetä Martin julkista avainta, vaan lähettää tilalla oman julkisen avaimensa Pertille. Kun Pertti lähettää oman julkisen avaimensa, hyökkääjä korvaa avaimen omallansa ja lähettää sen eteenpäin Martille. Tämän jälkeen hyökkääjä voi seurata ja muokata osapuolien välistä viestiliikennettä. (Tuominen 2005, 28-29). Julkisen avaimen menetelmästä kerrotaan lisää luvussa 5.5.

Man in the middle -hyökkäyksiä voidaan käyttää moniin tarkoituksiin. Viestintävirasto varoittaa avoimiin WLAN-tukiasemiin liittyvistä riskeistä, koska niitä hallinnoiva taho voi helposti suorittaa MITM-hyökkäyksen. Syyskuussa 2011 F-Secure varoitti Man in the middle -hyökkäyksistä, joissa hyökkääjä pyrki ohjaamaan suomalaisten verkkopankkien asiakkaat huijaussivustoille. Keväällä 2011 Facebook poisti sivultaan Syyrian kyberarmeija -fanisivuston. Syyrian viranomaiset käynnistivät sen jälkeen MITM-hyökkäyksen estääkseen kansalaistensa pääsyn Facebookiin (Ungerleider 2011). Nämä ja aiemmin esitetty Diginotarin sertifikaattien murtotapaus ovat vain yksiä monista variaatioista toteuttaa man in the middle -hyökkäys.

5 Puolustusmenetelmät

Kriittisten tietojärjestelmien suojaamiseen ei ole käytettävissä sen erikoisempia teknisiä menetelmiä kuin muidenkaan tietojärjestelmien suojaamiseen. Sen sijaan kriittisten järjestelmien suojaamisessa tulisi suunnitella, miten yleisiä tietoturvaan liittyviä tekniikoita implementoidaan ottaen huomioon järjestelmän erityispiirteet. Organisaatio voi säästää muiden järjestelmien tietoturvaan liittyvissä kustannuksissa ja työmäärässä, mutta kriittisissä tietojärjestelmissä ei tulisi säästää. Tässä luvussa käydään ensin lyhyesti läpi ne tekniset dokumentit, joiden pohjalta kriittisten järjestelmien tietoturvaa voidaan rakentaa. Tämän jälkeen esitellään tunnettuja suojaustekniikoita, joiden käytännön hyödyntämistapojen tulee perustua teknisten määrittelydokumenttien rajaamiin ehtoihin.

5.1 Tekniset dokumentit

Ennen tietojärjestelmän siirtymistä tuotantokäyttöön teknisen tietoturvan kannalta merkittävien asioiden tulee olla dokumentoitu. Tässä opinnäytetyössä ehdotetaan, että kun rakennetaan kriittistä järjestelmää vähintäänkin tietoturvan vaatimusmäärittely, toipumisuunnitelma ja tietoturva-arkkitehtuurin kuvaus tulee olla tehtynä. Ennen tietojärjestelmän siirtämistä tuotantokäyttöön on toteutettava väärinkäyttömallinnus, ja tietoturva-auditointi.

5.1.1 Tietoturvan vaatimusmäärittely

Jokaisen tietojärjestelmähankinnan perustana tulee olla vaatimusmäärittely. Tietoturvan vaatimusmäärittely voi olla osana järjestelmän yleistä vaatimusmäärittelyä tai omana dokumenttinaan. Tietoturvavaatimuksia on monenlaisia, esimerkiksi tapahtumien jäljitettävyys, varmuuskopiointi ja palautukset, salausmenetelmät, käyttäjän tunnistus ja palvelutaso. (Relator Oy 2009, 2)

Kriittisten järjestelmien vaatimusmäärittelyssä on erityisen tärkeää panostaa korkean käytettävyyden (high availability) ja niin sanotun taistelunkeston vaatimuksiin. Tietojärjestelmien palveluiden käytettävyys määrittyy siitä, kuinka hyvin palvelut ovat olleet käytettävissä kuluneella ajanjaksolla. Organisaatio voi itse määrittää korkean käytettävyytensä rajat. Esimerkiksi Hewlett Packardin johto määritti vuonna 1998 korkean käytettävyyden rajaksi 99,999%, joka tarkoittaa että kyseinen järjestelmä voi vuositasolla olla korkeintaan yhteensä viisi minuuttia poissa käytössä. Korkeaa käytettävyyttä tavoitellaan tyypillisesti monentamalla laitteet, niiden komponentit sekä ohjelmistot. Mikäli jokin laite vikaantuu, palvelun toiminnan

jatkuvuus varmistetaan varalaitteella. Kuormantasaajia (load balancer) käytetään laiteresurssien tasapuoliseen jakamiseen sellaisissa ympäristöissä, joissa käyttäjämäärät ovat suuria tai järjestelmäkokonaisuus edellyttää suurta laskentatehoa. (Salovaara 2007, 2)

Taistelunkesto-termiä käytetään erityisesti maanpuolustuksen kannalta kriittisissä tietojärjestelmissä. Se käsittää joitain korkean käytettävyyden vaatimuksia laajentavia erityispiirteitä, kuten palveluiden maantieteellinen monistaminen sekä sähkömagneettisilta pulsseilta (elecgtromagnetic pulse, EMP) suojautumisen. Huoltovarmuuskeskus käyttää kansallisesti kriittisten tietojärjestelmien osalta taistelunkestosta käsitettä huoltovarmuus. Lisäksi se asettaa huoltovarmuuden vaatimukseksi sen, että kriittisten tietojärjestelmien tietovarantojen on sijaittava Suomessa; samoin järjestelmien tuki- ja ylläpito-osaamisen tulee olla Suomessa (Kuparinen 2010, 20).

5.1.2 Riskien hallinta ja arviointi

Riskien arviointi sisältää riskien tunnistamisen, analysoinnin sekä luokittelun. Riskien tunnistamisvaiheessa luetellaan kaikki mahdolliset riskit. Tunnistamisvaihe vaatii paljon eri vaihtoehtojen miettimistä, mutta kun se on kerran tehty yhdelle tietojärjestelmälle, saatuja tuloksia voidaan hyödyntää lähtöaineistoina muiden tietojärjestelmien riskien tunnistamiseen. Riskeihin voi sisältyä kaikkea palvelinhuoneen ilman lämpötilan vaihteluiden ja tahallisten tietoturvahyökkäysten väliltä. Analysoinnissa riskiä voidaan kuvata joko kvantitatiivisesti tai kvalitatiivisesti. Kvantitatiivinen kuvaus on tyypillisesti prosenttilukema, joka kertoo arvion siitä, kuinka todennäköinen uhka on. Kvalitatiivisesti uhka voidaan esittää siten, että rakennetaan riskimatriisi, joka kuvaa uhkaa sanallisesti. Kvalitatiivinen uhkamatriisi voi olla työläs rakentaa, mutta standardit, kuten BSI Standard 100-1, tarjoavat valmiita työvälineitä siihen. Analysoinnin toinen keskeinen osa on arvioida riskin toteutumisen vaikutukset. Luokitteluvaiheessa riskit järjestellään vakavuusjärjestykseen analyysistä saatujen tietojen perusteella (BSI Standard 100-1, 35-37) .

Riskien hallinta on toinen riskeihin liittyvä osa-alue, jonka prosessi tulee suunnitella ennen järjestelmän siirtämistä tuotantokäyttöön. Riskien hallintaan sisältyy riskien seuranta, ratkaisu sekä jälkiseuranta. Riskien seurannan ensimmäinen vaihe on tilanteen hahmottaminen. Tapahtuma tai tapahtumaketju käydään läpi kokonaisuudessaan ja kirjataan ylös kaikki merkittävät havaitut tapahtumat aikajärjestyksessä. Riskien ratkaisu sisältää kaikki ne toimet, joilla järjestelmän tila saadaan palautettua normaaliksi. Riskien jälkiseurannassa käydään koko tapahtumahistoria läpi ja suunnitellaan ne toimet, joilla pyritään minimoimaan riskin toteutumisen uusiutuminen (Laitonen 2010, 47-49).

Tietojärjestelmien suojaamisessa riskien hallinta voidaan suunnitella myös jatkuvuus- ja toipumissuunnitelmien avulla. Dokumentit sisältävät kirjalliset ohjeet toimista, joilla ongelmatilanne saadaan ratkaistua. Jatkuvuussuunnitelmassa määritetään keinot, joilla poikkeustilanteisiin varaudutaan ja se, miten poikkeustilanteista selvitään. Toipumissuunnitelma sisältää tärkeysjärjestyksessä ne toimet, joilla järjestelmä saadaan takaisin toimintakuntoon. Mikäli järjestelmäkokonaisuus sisältää vähän kriittisiä osia, joiden toiminnan palauttaminen voidaan jättää myöhemmäksi, tieto asiasta on määritetty toipumissuunnitelmassa. Toipumissuunnitelman säännöllinen käytännön testaaminen on tärkeä toimenpide kriittisten järjestelmien kohdalla. (Laakso 2012)

5.1.3 Tietoturva-arkkitehtuuri ja väärinkäyttömallinnus

Tietoturva-arkkitehtuuri on osa organisaation tietoteknistä kokonaisarkkitehtuuria. Arkkitehtuuri tarjoaa kehitysprojekteja ohjaavan tietoturvakehikon. Siinä määritellään tietoturvapolitiikat ja organisaatiossa tehdyt tietoturvaan liittyvät tuotevalinnat sekä kuvataan organisaation tietoturva-arkkitehtuurin nykytila ja tulevaisuuden tavoitetila. (Petterson 2007, 4). Perinteisesti tietojärjestelmien arkkitehtuurikuvaukset suunnitellaan siten, että ensin kuvataan toiminnallinen arkkitehtuuri ja sen jälkeen sitä vastaava tekninen arkkitehtuuri. Tietoturva-arkkitehtuurin suunnittelu noudattaa myös samoja periaatteita. Toiminnallinen vaatimus voi olla esimerkiksi, että kaikki tietoaineisto tulee säilyttää salatussa muodossa. Teknisessä arkkitehtuurissa taas kuvataan tehdyt salaustuotevalinnat sekä mallinnetaan niitten käyttö mallinnuskielellä. Tunnetuin tietojärjestelmien mallinnuskieli on Unified Modeling Language (UML). Useat arkkitehtuurien mallinnustyökalut tukevat UML:a, johon on vuonna 2002 julkaistu myös UMLsec-laajennus. Se on kehitetty erityisesti tietoturva-arkkitehtuurin mallinnusta varten (Jürsens 2002, 3).

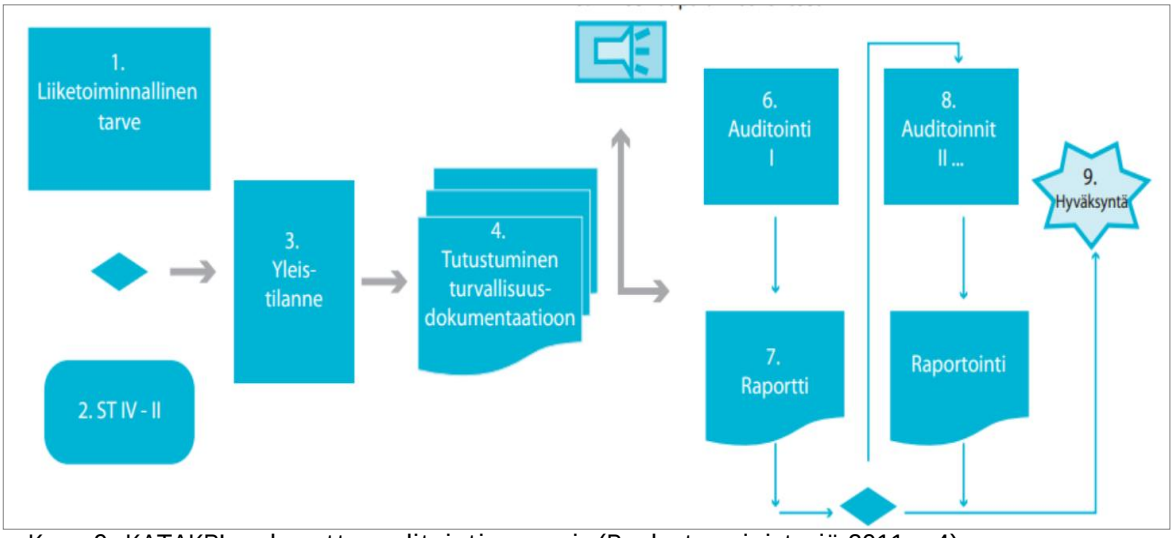
Väärinkäyttömallinnuksella (misuse case modeling) tuetaan tietoturva-arkkitehtuurin suunnittelua sekä riskien arviointia ja uhkakartoitusta. Väärinkäyttömallinnus aloitetaan selvittämällä käyttäjät, heidän roolinsa ja tehtävänkuvansa. Haastattelemalla käyttäjiä saadaan selville, miten he tyypillisesti käyttävät tietojärjestelmää (mikäli kyseessä on jo olemassa oleva tietojärjestelmä). Saadut tiedot auttavat ymmärtämään käyttäjän toimintamalleja käyttötapauksien mallintamista ajatellen. Tämän jälkeen suunnitellaan tietojärjestelmän käyttötapaukset, jollei niitä ole jo laadittu. Seuraava vaihe on varsinaisten väärinkäyttötapausten suunnittelu. Väärinkäyttötapaukset sisältävät useita tavallisia käyttötapauksia vastaan muodostettuja uhkaskenaarioita. Lopuksi mallinnetaan muut uhkaskenaariot, joita hyökkääjä voi pyrkiä toteuttamaan. Väärinkäyttömallinnuksessa syntyneitä tuloksia voidaan peilata tietoturva-arkkitehtuurissa kuvattuihin tietoturvaan vaikuttaviin komponentteihin ja suunnitella niihin

tarvittaessa muutoksia. Suunniteltuja käyttötapauksia voidaan hyödyntää penetraatiotestauksessa (Xu & Pauli 2005, 2-3).

5.1.4 Tietojärjestelmän auditointi

Kansallisen turvallisuusauditointikriteeristön (KATAKRI) ensimmäinen versio ilmestyi vuonna 2009 ja toinen versio vuonna 2011. Sen päätavoitteisiin kuuluu yhdenmukaistaa viranomaistoimintoja tietoturvatarkastuksiin liittyvissä toimintamenetelmissä. KATAKRIa voidaan käyttää yritysten, yhteisöjen sekä viranomaisten ja niiden sidosryhmien oman sisäisen turvallisuuden kehittämisessä (Rajamäki 2011, 9).

KATAKRI sisältää neljä osa-aluetta: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Näille kaikille osa-alueilla esitetään KATAKRIssa joukko kysymyksiä, jotka auditoinneissa tarkistetaan. Kysymyksiä peilataan vaatimuksiin, jotka vaihtelevat perustason viranomaisvaatimusten (suojaustaso IV) ja korotetun tason (suojaustaso II) välillä. Vaatimuksia täydentävät elinkeinoelämän suositukset. Suojaustasot vastaavat kansainvälisiä käsitteitä RESTRICTED, CONFIDENTIAL ja SECRET. Kriteeristö ei ota kantaa suojaustason I (erittäin salainen) vaatimuksiin. Kriteeristö on kansallisesti velvoittava, kun suomalaisen yrityksen tietoturvataso todennetaan kansainvälisen viranomaispyynnön pohjalta. KATAKRIn toinen päätavoite on auttaa organisaatioita omassa sisäisessä turvallisuustoiminnassa (Puolustusministeriö 2011a, 1-4)



Kuva 9: KATAKRIssa kuvattu auditointiprosessi. (Puolustusministeriö 2011a, 4)

Edellä olevassa kuvassa on kuvattu turvallisuusauditointiprosessin tekninen suoritus. Prosessi alkaa auditointitarpeen tunnistamisella. Tarve voi olla organisaation määrittämä käytäntö tietojärjestelmien auditoinneista tai perustua kansainvälisiin vaatimuksiin. Tavoitetaso määritellään välille ST IV – ST II yleensä järjestelmässä käsiteltävän tiedon luokituksen pohjalta.

Perusteet auditoinnin käynnistämiselle saadaan, kun hahmotetaan järjestelmäkokonaisuus sekä se, mihin muihin järjestelmiin tai tietoverkkoihin se on kytköksissä ja kun hahmotetaan lisäksi järjestelmän omistajuus ja ylläpitovastuut sekä elinkaarivaihe. Tämän jälkeen käydään läpi kaikki turvallisuuteen liittyvä dokumentaatio, jota tietoturvallisuudesta on käsitelty aiemmin tässä luvussa. Mikäli dokumentaatiossa on puutteita tai sen perusteella on havaittavissa ilmiselviä parannusvaatimuksia, niistä voidaan tiedottaa ennen varsinaista auditointia. Auditointi suoritetaan KATAKRIn vaatimuksiin peilaten ja siitä laaditaan raportti. Raportista ilmenevät täyttyneet vaatimukset, havaitut turvallisuuspoikkeamat ja poikkeamien vakavuus. Mikäli raportista ilmenee tarvetta korjaustoimille, järjestelmä auditoidaan uudelleen, kun korjaustoimet on tehty. Auditointeja toistetaan, kunnes järjestelmästä voidaan antaa hyväksyntä. Akkreditointilausunnosta ilmenee, millä suojaustasolla järjestelmää saa käyttää, milloin järjestelmä on auditoitava uudestaan sekä muut mahdolliset reunaehdot (Puolustusministeriö 2011a 4-5).

5.2 Penetraatiotestaus

Penetraatiotestaus voidaan määritellä lailliseksi ja luvalliseksi menetelmäksi etsiä tietojärjestelmistä ja verkkolaitteista teknisiä heikkouksia. Testien tavoitteena on tehdä testattavasta kohteesta turvallisempi. Prosessiin sisältyy heikkouksien etsiminen kohteesta sekä usein myös hyökkäykset, joilla havaittu tietoturva-aukko voidaan todentaa. Penetraatiotestauksesta käytetään joskus myös nimityksiä ethical hacking sekä white hat hacking. Haavoittuvuuksien arviointi (vulnerability assessment) sekoitetaan välillä penetraatiotestaukseen, vaikka se on järjestelmien ja prosessien tietoturvan arviointia. Se ei sisällä käytännön teknisten työkalujen hyödyntämistä haavoittuvuuksien kartoitukseen eikä niiden todentamista hyökkäyksillä. Haavoittuvuuksien arviointi sekä penetraatiotestaus kuuluvat molemmat tietoturva-auditoinnissa tehtäviin toimiin (Broad 2011, 1).

Penetraatiotestaus suoritetaan kokoelmalla erilaisia työkaluja, joita löytyy esimerkiksi suositusta Backtrack Linux -jakelusta. Pahantahtoiset tahot käyttävät työkaluja myös oikeiden hyökkäysten tekoon. Osa käytettävistä testausmenetelmistä soveltuu myös hyökkäysmenetelmiksi, joista on jo kirjoitettu aiemmassa luvussa. Oikeastaan suurimpana erona hyökkäyksiin verrattuna on se, että hyökkäyksen viimeistä vaihetta eli varsinaista vahingontekoa ei suoriteta kuin korkeintaan demonstraationomaisesti.

5.3 Honeypots ja honeynets

Ympäristöjä, joiden tarkoitus on hämätä hyökkääjää ja tarkkailla heidän toimintaansa, kutsutaan termeillä honeypots ja honeynets. Käsitteellisesti ne tarkoittavat samaa asiaa sillä erotuksella, että honeynetit sisältävät useita honeypot-verkkopalveluita. Ne on rakennettu siten, että ne muistuttavat oikeata verkkopalvelua, jolla ei todellisuudessa ole lainkaan käyttäjiä ylläpitäjää lukuun ottamatta. Seuraamalla hyökkääjää voidaan selvittää, mitä tietoa hän mahdollisesti etsii tai mitkä hänen tavoitteensa ovat. Honeypots-ympäristöissä korostuu seuranta- ja lokitusmenetelmien tärkeys. Niitä voidaan hyödyntää myöhemmin tehtävässä syvemmässä analyysissa. Honeypots on yksi harvoista menetelmistä saada tietoa uusista haavoittuvuuksista (zero-day). (Janczwewski ym. 2009, 98).

Honeypotsit ja honeynetit voivat olla interaktiivisia tai tarjota vain vähän interaktiivisia toimintoja. Interaktiiviset ympäristöt tarjoavat mahdollisuuden kirjautua useisiin verkkopalveluihin, kun taas vähemmän interaktiiviset ympäristöt simuloivat esimerkiksi vain www-palvelun etusivun näkymän. Vähemmän interaktiivisten ympäristöjen etuna on, että hyökkääjälle voidaan helposti luoda lukuisia haavoittuvilta näyttäviä kohteita hämäystarkoituksessa. Yksi tunnetuimmista tähän tarkoitukseen tehdyistä avoimeen lähdekoodiin perustuvista ohjelmista on nimeltään Honeyd. Vaikka ympäristössä olisi todellisuudessa vain muutama palvelin, Honeydin kaltaisten ohjelmistojen avulla voidaan ajaa virtuaalikoneita, jotka saavat ympäristön näyttämään siltä kuin palvelimia olisi useita satoja. Vastaavasti yksi tunnetuimmista korkean interaktiivisuuden työkaluista on nimeltään Sebek. Sen asentaminen ja hyödyntäminen on monimutkaisempaa, mutta Sebekin etuna on, että sen avulla saadaan kerättyä ja analysoitua enemmän tietoa hyökkääjän aikeista (Andrés & Kenyon 2004, 441-443; Janczwewski ym. 2009, 98).

Vähentääkseen kiinnijoutumisen riskiä sekä hyökkäysmenetelmiensä paljastumista hyökkääjät etsivät kohdeympäristöstä poikkeamia, jotka paljastavat ympäristön olevan rakennettu hämäystarkoitukseen. Poikkeamat voivat olla esimerkiksi tilastollisia poikkeamia tiedostojen päivämäärissä, ko'oissa tai tiedostotyypeissä. Siksi honeypotsin rakentamisessa on tärkeää luoda satunnaisuutta tietosisältöön sekä eroavaisuuksia kohdepalvelimien välille, mikäli niitä on useita. Edistyneemmissä honeypots-ohjelmistoissa on mukana menetelmiä, jotka peittävät merkkejä ohjelmistosta, jolla ympäristö on rakennettu. Käyttöjärjestelmästä piilotetaan honeypots-ohjelmistoon liittyvät tiedostot sekä lokitiedostot, joilla seurataan hyökkääjän toimia. Ohjelmistoissa voi olla käytössä myös viivästystoimintoja, joilla voidaan hämätä hyökkääjää siten, että hyökkääjä voi kuvitella onnistuneensa toteuttamaan palvelunestohyökkäyksen. Hämäystarkoitukseen rakennettuun ympäristöön voi olla asennettu myös haitta- ja vakoiluohjelmia, joiden avulla hyökkääjä voidaan jäljittää (Janczwewski ym. 2009, 146).

Honeypots-ympäristön käyttötarkoitus voi olla myös disinformaation jakaminen. Sotilaallisessa käytössä voidaan jakaa hyökkääjälle väärää tiedustelutietoa. Tieto voi muun muassa sisältää vääriä operaatiosuunnitelmia, käskyjä, joukko- tai kalustotietoja. Vastaavasti honeynetsien avulla voidaan myös hämätä hyökkääjää luulemaan, että kohteella on valtavat tietotekniset resurssit (Janczwewski ym. 2009, 146).

5.4 Vahva tunnistus ja pääsynhallinta

Luotettava tunnistaminen voidaan toteuttaa laitteelle, ohjelmistolle tai henkilölle. Roolipohjaisella pääsynhallinnalla varmistetaan, että tunnistettu kohde pääsee käsiksi vain tarvittaviin resursseihin. Yleisiä tapoja tunnistaa henkilö on PIN-koodi, salasana tai kirjautumisfraasi. Nämä eivät sellaisenaan ole vahvoja tapoja toteuttaa tunnistamista, koska paljastuttuaan ne menettävät hyötynsä. Biometriikkaa, jolla henkilö tunnistetaan fyysisen ominaisuuden, kuten sormenjäljen tai silmän värikalvon avulla, käytetään vähemmän. Menetelmänä myöskään biometriikka ei ole aukoton, vaan biometrisiä tunnistamismenetelmiä voidaan huijata (Linden 2012. 12-13; Andress 2011, 70).

Salasanan tai PIN-koodin lisäksi voidaan tietoturvan tekijöitä lisätä yhdistämällä ne fyysiseen elementtiin, kuten pankkikorttiin, toimikorttiin, matkapuhelimeen tai USB-tokeniin. Siten jos järjestelmässä ei ole tietoturva-aukkoja, hyökkääjän on periaatteessa saatava haltuunsa fyysinen elementti sekä siihen liittyvä salasana tai PIN-koodi. Hyökkääjällä voi olla laitteesta, toimikortista tai niiden sisältämästä varmenteesta oleva kopio, jolla hän kykenee tunkeutumaan järjestelmään. Kuitenkin fyysinen laite tai kortti vaikeuttavat huomattavasti murtautumista pelkkään salasanaan tai PIN-koodiin verrattuna. (Harris 2008, 161; Linden 2012. 12-13; Andress 2011, 70)

Pääsynhallinnalla kontrolloidaan sitä, pääseekö kohde (joka voi olla henkilö, prosessi tai toinen tietokone) suorittamaan halutun toiminnon järjestelmän tarjoamassa resurssissa. Tyypillisiä toimintoja ovat luku-, poisto-, kirjoitus-, suoritus- ja hakutoiminnot. Pääsynhallinta on kenties keskeisin tietoturvamekanismi, kun päämääränä on saavuttaa tiedon luottamuksellisuus, eheys sekä saatavuus (Andress 2011, 71).

Pääsylista (Access Control List, ACL) on yksinkertainen tapa toteuttaa pääsynhallintaa. Lista muodostuu taulusta, joka määrittää yksittäisen käyttäjän tai ryhmän oikeudet tiettyyn tiedostojärjestelmän resurssiin. Jokainen objekti sisältää tunnisteen, joka viittaa siihen liittyvään pääsylistaan. Käyttäjä voi käsitellä objektia pääsylistassa määritettyjen oikeuksien mukaisesti. Verkkopohjaisissa pääsylistoissa pääsyä rajoitetaan tyypillisesti IP-osoitteiden, MAC-osoitteiden tai tietoliikenneporttien rajauksilla. Pääsylistoja voidaan konfiguroida myös suodattamaan osia tietoliikenteen sisällöstä (Harris 2008, 220-222).

Harkinnanvarainen pääsynhallinta (Discretionary Access Control, DAC) on pääsynhallintamalli, jossa resurssin omistaja hallinnoi resurssin oikeuksia. Resurssin omistaja voi päättää, kuka saa käsitellä resurssia ja miten. Pakollisen pääsynhallinnan mallissa (Mandatory Access Control, MAC) omistaja ei pääse päättämään resurssin oikeuksista, vaan oikeudet määrittää ryhmä tai henkilö, jonka tehtäviin kuuluu hallinnoida oikeuksia. Pakollinen pääsynhallinnan malli suunniteltiin erityisesti sotilaalliseen ja muun valtionhallinnan käyttöön. Sen tarkoituksena oli määrittää pääsyoikeuksia tiedon suojaustason mukaan. Suojaustasolla määritellään, onko tieto salaista, julkista, luottamuksellista tai erittäin salaista (Linden 2012, 33; Harris 2008, 211).

Roolipohjaisen pääsynhallinnan mallissa (Role-Based Access Control, RBAC) oikeuksia ei sidota käyttäjään tai ryhmään vaan rooliin. Rooli on joko henkilön tehtävänimike tai tietty tehtävä organisaatiossa. RBAC suunniteltiin erityisesti suurten kaupallisten organisaatioiden käyttöön, joissa DAC:n ja MAC:n käyttö oli liian työlästä ja monimutkaista. Myöhemmin sen on havaittu toimivan hyvin myös ei-kaupallisissa organisaatiossa, joissa on paljon käyttäjiä ja monimutkaisia käyttöympäristöjä. Ominaisuuksiin perustuvan pääsynhallinnan mallissa (Attribute-Based Access Control, ABAC) keskitytään henkilön, resurssin tai ympäristön ominaisuuksiin. Yksinkertaistettuna esimerkkinä voidaan käyttää klassista huvipuiston vaatimusta: päästäksesi tähän laitteeseen sinun on oltava vähintään näin pitkä. Yleisesti ABACia hyödynnetään verkkosovelluksissa, joissa esimerkiksi katsotaan, täyttääkö selain tietyt vaatimukset (Andress 2011, 74; Linden 2012, 33, Harris 2008 214-216).

Edellä mainittujen pääsynhallintamallien lisäksi on rakennettu malleja hyvinkin spesifisiin käyttötarkoituksiin. Biba-malli keskittyy tiedon eheyden suojaamiseen, jopa tiedon luottamuksellisuuden menettämisen uhalla. Niin sanottu Kiinan muurin malli (Chinese Wall) on suunniteltu estämään eturistiriitojen syntymisen. Se soveltuu erityisesti lakisovelluksiin.

Monitasotietoturvalla (Multilevel Security, MLS tai Content-based Information Security, CBIS) tarkoitetaan karkeasti ottaen oikeuksien määrittämistä siten, että henkilöllä on näkymä vain niihin tietoihin, joihin hänen oikeutensa riittävät. Tähän liittyy kiinteästi tiedon rakenteisuus – esimerkiksi yhdessä asiakirjassa voi olla useita eri käyttöoikeuksia sisältäviä rakenneosia. Monitasotietoturva voi tarkoittaa käyttäjien näkökulmasta esimerkiksi sitä, että käyttäjä, jolla on laajemmat käyttöoikeudet, näkee dokumentin sisällöstä kaiken, kun rajallisemmat käyttöoikeudet omistava henkilö näkee vain johdannon. Monitasotietoturva voi myös itse tietosisällön rajoittamisen lisäksi rajata tietoon kohdistuvia toimia, kuten tulostamista. Kun tieto itsessään on jo suojattu sisäisesti roolien tai käyttäjäkohtaisten oikeuksien mukaisesti, ei tiedon väärinkäyttö onnistu niin helposti, koska tiedoston haltuun saaminen ei vielä tarkoita, että koko tiedoston sisältö on automaattisesti nähtävissä (Relator Oy 2009, 4).

5.5 Salausmenetelmät

Kryptografia on tietoaineiston sisällön salaamiseen keskittynyt tiede. Sen tavoitteena on mahdollistaa tiedon siirtäminen tai säilyttäminen salattuna siten, että ainoastaan luvitettu taho pystyy tulkitsemaan salatun tiedon. Salausmenetelmät voivat pohjautua ohjelmisto- tai laitteistopohjaiseen salaukseen. Salauksen murtamiseen keskittynyttä toimintaa kutsutaan kryptoanalyysiksi. Kryptologia-termillä tarkoitetaan kryptografiaan ja kryptoanalyysiin liittyvää tutkimusta (Harris 2008, 670).

Auguste Kerckhoff julkaisi vuonna 1883 tutkimuksen, jonka mukaan salausmenetelmän ainoan salaisen osion tulisi olla salausavain. Hän esitti, että salausalgoritmin tulisi olla yleisessä tiedossa. Väittely aiheesta on edelleen ajankohtainen. Toisten mielestä salausalgoritmi on turvallisempi, kun usea henkilö kykenee tutkimaan sitä. Toisaalta useat valtiot ympäri maailmaa ovat suunnitelleet omia algoritmejaan, jotka eivät ole julkisia. Heidän näkemyksensä on, että mitä harvempi ihminen tuntee algoritmin, sitä vaikeampi se on murtaa. Salausmenetelmän vahvuus koostuu algoritmista, salausavaimesta, avaimen pituudesta ja käynnistysvektoreista sekä siitä, miten ne kaikki toimivat yhteen (Harris 2008, 668).

5.5.1 Salausavaimet

Yhdessä salausalgoritmissa voi olla käytössä tietyn pituisia avaimia, esimerkiksi 128- tai 256-bittisiä. Algoritmin mahdollisten avainten joukkoa kutsutaan algoritmin avainavaruudeksi. Käytettävä avain pyritään valitsemaan satunnaisesti avainavaruudesta avaingeneraattorilla. Mikäli valinta ei ole satunnainen vaan ennustettavissa, hyökkääjä voi murtaa salauksen arvaamalla avaimen. Mikäli algoritmin avainpituus olisi 2 bittiä, sen avainavaruus olisi 4, joka vastaisi erilaisten avainten maksimilukumäärää. Nykyään käytetään useimmiten 128-, 256- tai 512-bittisiä avainpituuksia. 512-bittinen avainpituus mahdollistaa avainavaruuden, jonka koko ~ laajuus on 2^{51}. Avaingeneraattorin tulisi käyttää koko avainavaruus ja valita avaimen tekoon tarvittavat arvot mahdollisimman satunnaisesti (Harris 2008, 669).

5.5.2 Symmetrisen salauksen algoritmit

Symmetrisessä algoritmissa on käytössä yksi salainen avain, joka on sekä lähettäjällä että vastaanottajalla. Lohkosalain ottaa ennalta määrätyn bittimäärän eli lohkon selväkielisestä viestistä ja salaa sen. Jonosalain salaa jokaisen yksittäisen bitin erikseen. Lohkosalain voi myös toimia kuten jonosalain, jos se asettaa lohkon pituudeksi yhden bitin. Nykyisin suurin osa algoritmeista perustuu lohkosalaukseen. Koska lohkosalaimet käsittelevät kerrallaan suurempaa osaa salattavasta tiedosta, ne yleensä ovat hitaampia ja vaativat enemmän resursseja. Ne ovat myös alttiimpia virheille, koska yksittäinen virhe jonosalauksessa vaikuttaa vain yhteen bittiin kerrallaan, kun taas lohkosalaimessa se vaikuttaa koko lohkoon. Lohkosalaimet soveltuvat yleensä paremmin sellaisen tiedon salaamisen, jossa tiedoston koko on valmiiksi tiedossa, kuten tiedostojen tai sähköpostiviestien salaamiseen. Jonosalaimet soveltuvat paremmin tietomassan salaamiseen, jonka määrä on ennalta tuntematon. Tällaista tietoaineistoa voivat olla esimerkiksi videoneuvottelut tai puhelut (Andress 2011, 70).

Tunnettuja lohkosalausalgoritmeja ovat DES, 3DES, ja AES. Näistä DES onnistuttiin murtamaan vuonna 1999 testissä, joka kesti vain noin 22 tuntia. Tämä johtuu DES:n pienestä avainpituudesta, jota pyrittiin paikkaamaan 3DES-algoritmilla. Se on käytännössä sama DES-algoritmi, joka salakirjoittaa joka lohkon kolmesti eri salausavaimella. Tunnetuimmista algoritmeista AES on se, johon luotetaan eniten; sitä ei tiettävästi ole onnistuttu murtamaan täydellisesti koskaan. AES käyttää kolmea salakirjoitusmenetelmää: vaihtoehtoina ovat 128-bittiset, 192-bittiset tai 256-bittiset salausavaimet, joissa kaikissa lohkon pituus on 128 bittiä. Muita tunnettuja lohkosalausalgoritmeja ovat Twofish, Serpent, CAST5, RC6 ja IDEA. Tunnetuimpia jonosalausalgoritmeja ovat RC4, RC5, ORYX, sekä SEAL (Andress 2011, 71).

5.5.3 Epäsymmetrisen salauksen menetelmät

Symmetrisen salauksen menetelmä käyttää vain yhtä avainta, kun taas epäsymmetrisen salauksen menetelmässä käytetään kahta avainta: julkista ja salaista. Julkisella avaimella salakirjoitetaan tieto, ja julkista avainta voidaan jakaa eteenpäin. Salaista avainta käytetään salatun tiedon avaamiseen, ja avainta säilytetään suojatusti eikä jaeta eteenpäin. Sähköpostin salaaminen on yleinen epäsymmetrisen salauksen käyttötapaus. Viesti salataan vastaanottajan julkisella avaimella, jolloin vastaanottaja kykenee purkamaan salauksen salaisella avaimellaan. Kolmas osapuoli ei siten voi purkaa salattua viestiä. Julkiset ja salaiset avaimet luodaan monimutkaisten matemaattisten operaatioiden avulla. Epäsymmetrisen salauksen menetelmän esittelivät ensimmäistä kertaa vuonna 1976 Martin Hellman ja Whitfield Diffie. Suurin etu verrattuna symmetriseen salaukseen on avainten jakelussa. Symmetrisen salauksen menetelmässä avaimen jakelun prosessin tulee olla huolellisesti suunniteltu ja toteutettu ja se voi viedä paljon aikaa. Avain voidaan esimerkiksi joutua toimittamaan henkilökohtaisesti vas-

taanottajille, kun taas epäsymmetrisen salauksen menetelmällä luotua julkista avainta on mahdollista jaella vapaasti (Harris 2008, 681-684; Andress 2011, 72).

Epäsymmetriset menetelmät perustuvat johonkin vaikeana pidettyyn matemaattiseen ongelmaan. Esimerkiksi Ron Rivestin, Adi Shamirin ja Lenoard Adlemanin mukaan nimetty RSA-algoritmi perustuu suurten lukujen tekijöiden jaon vaikeuteen. Se on tunnettu asymmetrinen algoritmi ja sitä käytetään myös Secure Socets Layer (SSL) -protokollassa, joka on suosittu erityisesti verkkosivustojen kirjautumistietojen salauksen yhteydessä. Elliptisillä käyrillä on useita etuja verrattuina muunlaisiin algoritmeihin. Ne tarjoavat vahvemman suojauksen lyhyillä avainpituuksilla ja ne ovat nopeita ja tehokkaita. Niitä on myös helpompi hyödyntää mobiililaitteissa (Andress 2011, 72).

5.5.4 Tiivistefunktiot

Symmetristen ja epäsymmetristen salausmenetelmien lisäksi tiivistefunktiot (hash functions) ovat oma salausmenetelmänsä. Niitä kutsutaan myös nimillä yksisuuntaiset funktiot tai hajautusfunktiot. Tiiviste luodaan tiivistefunktion avulla laskemalla mielivaltaisen pitkästä syötteestä lyhyt vakiomittainen merkkijono. Tiivistefunktioita hyödynnetään sähköpostiviestien digitaalisessa allekirjoittamisessa. Tiivisteistä ei voida päätellä mitään viestien sisällöstä, vaan niiden avulla voidaan todentaa, ettei viesti ole muuttunut matkalla. Tiivistefunktioita käytetään myös pääteyhteyksien sekä useiden Unix-pohjaisten käyttöjärjestelmien salasanojen suojaamiseen. Message Digest 5 (MD5) on yksi käytetyimmistä algoritmeista (Andress 2011, 73; Harris 2008, 714-715).

Esimerkkinä MD-5-tiivisteen toimivuudesta voidaan vertailla kahta lausetta, jotka eroavat vain yhdellä merkillä. Lause: ”Tee työtä jolla on tarkoitus.” tuottaa MD5-tiivisteen: ”84aff96d5a466a05b9f6ac8ccd336ecc”. Sen sijaan lause: ”Tee työtä jolla on tarkoitus!” tuottaa MD5-tiivisteen ”b432ec8a2bd0d5db68c9102d35f30bee”. Lähes samasta lauseesta muodostuu siten täysin erilainen tiiviste.

Korkeampaa tietoturvaa vaativissa ympäristöissä käytetään nykyään 128-bittisen MD5:n sijasta Secure Hash Algorithm 2:ta (SHA-2). SHA-2 sisältää neljä eri tiivistefunktiota, jotka ovat 224-, 256-, 384- sekä 512-bittisiä. Lähitulevaisuudessa julkaistaan SHA-2:n seuraaja SHA-3 (Harris 2008, 719-720).

5.5.5 Varmenteet

Varmenteita eli sertifikaatteja käytetään henkilöiden, palveluiden sekä laitteiden tunnistamiseen. Varmentaja (Certificate Authority, CA) on varmenteita myöntävä taho, jonka tehtävä on varmentaa se, että taho, jolle varmenne myönnetään, on se, joka hän väittää olevansa. Varmenteita myöntäviä yrityksiä on lukuisia, kuten Verisign ja Diginotar (Andress 2011, 74). Suomessa virallinen varmenteiden myöntäjä on Väestörekisterikeskus. Kaikkien Suomen kansalaisten on mahdollista hakea Väestörekisterikeskuksesta henkilökohtainen kansalaisvarmenne. Lisäksi Väestörekisterikeskus myöntää palvelinvarmenteita sekä organisaatiovarmenteita (Väestörekisterikeskus 2012). Luvussa 3.5. esiteltiin yksi käytännön esimerkki varmenteisiin liittyvistä riskeistä Diginotarin tietomurron yhteydessä. Mikäli varmentajan järjestelmään onnistutaan murtautumaan, menettävät varmenteet luotettavuutensa. Tästä syystä kriittisten järjestelmien varmenteita luodessa tulisi harkita, käytetäänkö julkisesti tunnetun varmentajan sijasta organisaation itse allekirjoittamia varmenteita (Self-Signed Certificates) varsinkin, jos kriittisen järjestelmän omistavalla organisaatiolla on käytössään oma julkisten avainten hallintajärjestelmä (Public Key Infrastructure, PKI).

PKI-järjestelemä koostuu laitteista, ohjelmistoista, prosesseista, toimijoista ja käytännöistä. PKI:n avulla luodaan, hallitaan, hyödynnetään ja suljetaan varmenteita. Sulkulistaksi (Certificate Revocation List) kutsutaan luetteloa, johon varmentaja sulkee ne varmenteet, joita on väärinkäytetty tai jotka eivät ole enää käytössä. Sulkulistan läpikäymisen lisäksi ohjelma voi tarkistaa yksittäisen varmenteen voimassaolon ja käytettävyyden tarkistamispalvelusta (Online Certificate Status Protocol). Viestintäviraston CERT-FI-yksikkö on julkaisut 28.11.2011 tietoturvakatsauksen, jossa käsitellään varmenteisiin kohdistuvia riskejä sekä teknisiä ratkaisuja riskien vähentämiseksi. Tekniset suojausratkaisut on jaettu katsauksessa neljään eri ryhmään: nimipalvelintietoihin perustuvat ratkaisut, palvelupään ratkaisut, sovelluspään ratkaisut sekä keskitetyt ratkaisut (CERT-FI 2012). Opinnäytetyön liitteessä 2 on Viestintäviraston julkaisema taulukko teknologiavaihtoehtojen tarjoamasta suojasta eri tilanteisiin.

5.6 Tietoliikenteen keskeiset suojaustekniikat

Pelkästään tietoliikenteen suojaukseen liittyvillä menetelmillä voidaan saavuttaa auttava suojataso tietojärjestelmille. Tämä johtuu siitä, että tietoliikenteen suojaumenetelmillä voidaan suojata käyttöjärjestelmää, sovellusta, sekä varsinaista tietoa. Siinä missä salatut tietoliikenneyhteydet suojaavat tietosisältöä, sovellusta ja käyttöjärjestelmää kyetään suojaamaan palomuureilla ja tunkeutumisen estojärjestelmillä. Seuraavissa alikappaleisssa käsitellään yleisempiä tietoliikenteen suojaustekniikoita.

5.6.1 Palomuurit ja VPN

Yleisin komponentti tietojärjestelmien suojaamiseen verkkohyökkäyksiltä on palomuuri. Ensimmäinen kaupallinen palomuuri tuli myyntiin vuonna 1992. Palomuuri sijoitetaan verkossa yleensä sellaiseen kohtaan, jossa verkkoliikenteen sisällön luotettavuuden taso muuttuu. Palomuurilla voidaan rajata myös luotetun sisäverkon liikennettä siten, että vain tarpeelliset palvelut ja niiden luvitetut käyttäjät pystyvät kommunikoimaan keskenään. Pakettisuodatus on palomuurien keskeisin perustoiminto. Verkkoliikenteestä suodatetaan yksittäisiä paketteja IP-osoitteiden, protokollien sekä porttien perusteella. Käytännössä tämä tarkoittaa, että suunnitellaan palomuureille säännöt siten, että tietyt protokollat, IP-osoitteet ja tietoliikenneportit ovat joko kiellettyjä tai sallittuja. Turvalliseksi mielletty tapa on aluksi määrittää kaikki arvot kielletyiksi ja sen jälkeen sallia ainoastaan tarvittava tietoliikenne. Pakettien suodatus voidaan toteuttaa joko tilallisena tai tilattomana palomuurin ominaisuuksien mukaan (Andress 2011, 118).

Tilaton pakettien suodatus voi tarkastella vain yksittäistä pakettia. Tilallinen pakettien suodatus mahdollistaa liikenteen tarkemman valvonnan. Tilallinen palomuuri pitää yhteyskohtaisesti kirjaa TCP- ja UDP-yhteyksistä ja sallii vain yhteyteen kuuluvat paketit. Jokaisesta paketista tarkistetaan, kuuluuko se johonkin olemassa olevaan yhteyteen. Ainoastaan olemassa oleviin tai uusin yhteyksiin liittyvät paketit päästetään läpi. Kun yhteys avataan, tutkitaan, onko se sallittu palomuurin säännöissä. Palomuurin yhteyslistaan (state table) lisätään hyväksytyn yhteyden tiedot ja jatkossa kyseiseen yhteyteen liittyvät paketit päästetään läpi. Yhteyden sulkeutuessa yhteyslistalta poistetaan yhteyteen liittyvät tiedot. Palomuureissa voi olla myös sisällön suodatusominaisuuksia (deep packet inspection), joiden avulla voidaan tietoliikenteen sisällön perusteella päättää, sallitaanko yhteys vai ei (Harris 2008, 551-552).

Palomuuri ei voi suodattaa paketteja salattujen VPN-tunnelin (Virtual Private Network) sisältä, joten salattu VPN-yhteys puretaan, ennen kuin tietoliikenne suodatetaan palomuurin läpi.

Nykyään usein tästä syystä käytetään VPN-palomuuria, joka hoitaa VPN:n ja palomuurien toiminnallisuuden. VPN mahdollistaa salatun tietoliikenteen sellaisen verkon läpi, johon ei luoteta. VPN eli näennäisesti yksityinen verkko voidaan muodostaa yhdistämällä julkisen verkon läpi kaksi tai useampia yrityksen verkkoja. Toinen yleinen VPN:n käyttötapaus on suojatun tietoliikenneyhteyden muodostaminen Internet-koneelta yrityksen sisäverkossa sijaitseviin palveluihin. Suuremmat organisaatiot käyttävät myös suljetuissa sisäverkoissaan VPN-tekniikoita tietoturvan parantamiseksi (Harris 2008, 609).

VPN-yhteyttä kutsutaan usein VPN-tunneliksi, jossa tieto liikkuu salattuna kahden pisteen välillä. Standardoituja tunnelointiprotokollia ovat IPsec, L2TP, L2F, sekä PPTP. L2TP-tunnelointiprotokollaa voidaan hyödyntää etäkäyttötarkoituksessa; se ei sisällä omaa salausta, vaan sen yhteydessä käytetään IPsec-protokollan salausta. L2F-tunnelointiprotokollaa käytetään ainoastaan verkkojen yhdistämiseen; se hyödyntää poin to point (PPP) encryption -protokollaa (ECP) tiedon salaukseen. PPTP on Microsoftin etäkäyttöä varten kehittämä tunnelointiprotokolla, joka hyödyntää Microsoftin MMPE-protokollaa salaukseen (Andress 2011, 158)

5.6.2 Tunkeutumisen havaitsemis- ja estojärjestelmät

Tunkeutumisen estojärjestelmällä (IPS, Intrusion Prevention System) tarkoitetaan tavallisesti uudemman sukupolven järjestelmää verrattuna tunkeutumisen havaitsemisjärjestelmään (IDS, Intrusion Detection System). Yksinkertaistettuna erona IDS-järjestelmä hälyttää tunkeutumisyrityksestä, kun taas IPS-järjestelmä estää hyökkääjän etenemisen. Tuotekuvauksissa käytetään lyhenteitä IDS/IPS tai IDPS kuvaamaan, että tuote sisältää havaitsemis- ja torjuntaominaisuuksia. Tunkeutumisen estojärjestelmää alettiin kehittää 1990-luvun loppupuolella. Sen merkittävä parannus palomuureihin nähden on, että IPS suorittaa pääsynhallintaa ohjelmakohtaisesti eikä IP-osoitteiden tai porttien perusteella. Tunkeutumisen estojärjestelmä voi toimia myös laitteen sisäisesti käyttöjärjestelmän tasolla verkkotason lisäksi. (Sillberg 2008, 14-15).

Yhdysvaltojen puolustusministeriö perusti 1980-luvun lopussa projekteja, joissa luotiin malleja tunkeutumisen havaitsemiseksi. Nykyiset tunkeutumisen havaitsemisjärjestelmät pohjautuvat kyseisistä projekteista luotuihin malleihin (Anderson 2006, 25). IDS-järjestelmä havaitsee normaalista poikkeavat ei-toivotut muutosyritykset järjestelmässä. Havaitsemisjärjestelmä tarkkailee muun muassa hyökkäyksiä, jotka kohdistuvat haavoittuviin palveluihin, luvattomia kirjautumisyrityksiä, pääsyä arkaluontoisiin tiedostoihin, ohjelmien puskuriylivuotoja ja mahdollisia haittaohjelmia. IDS/IPS-järjestelmä koostuu sensoreista, konsolista sekä palvelimesta tai useista palvelimista. Sensoreita käytetään hyökkäyksien havaitsemiseen. Konsolilla hallitaan sensoreita sekä valvotaan hälytyksiä. Palvelimella olevaan tietokantaan tallennetaan

hälytykset, ja lisäksi palvelinohjelmisto välittää sensoreilta saadut hälytykset konsolille (Sillberg 2008, 16).

Yksi tunnetuimmista avoimeen lähdekoodiin pohjautuvista IDS/IPS-ohjelmistoista on SNORT, joka tarjoaa yli 14 000 tunkeutumissormenjälkeä. Sormenjälkiä käytetään erilaisten tunkeutumisyritysten havaitsemiseen. Suurimpia kaupallisia toimijoita IDS/IPS-markkinoilla ovat Cisco, IBM, McAffee, Juniper Networks, sekä Sourcefire (Kibirkstis 2009).

5.7 Työasemien suojaaminen

Virustorjuntaohjelmistot ovat suosittuja erityisesti Windows-ympäristöissä. Ne tekevät reaaliaikaista tarkastuksia sekä ajastettuja tiedostojärjestelmän sekä prosessien skannauksia. Havaitessaan viruksen tai haittaohjelman virustorjuntaohjelmisto pyrkii yleensä sammuttamaan siihen liittyvät prosessit, poistamaan haittaohjelman tai asettamaan sen karanteeniin. Virustorjuntaohjelmisto tunnistaa virukset ja haittaohjelmat sormenjälkitiedoston perusteella. Sormenjälkiä julkaistaan tyypillisesti usean kerran päivässä. Internet-yhteydessä olevien työasemien ja palvelimien haittaohjelmatunnisteet päivittyvät nopeasti sormenjälkien julkaisun jälkeen. Sen sijaan järjestelmille, joilla ei ole Internet-yhteyttä, on suunniteltava omat päivitysmenetelmät. Sisäverkkoon voidaan sijoittaa oma palvelin, joka jakelee uusia virustunnisteita. Vaihtoehtoisesti voidaan päivittää yksittäisiä koneita manuaalisesti siirrettävän muistivälineen avulla. Virustorjuntaohjelmistoista on saatavilla räätälöityjä versioita, joissa on esimerkiksi lisäksi saatavilla palomuuritoimintoja ja verkkoliikenteen haittaohjelmatarkistusta. Palvelinkäyttöön on räätälöityjä virustorjuntaohjelmia palvelimen käyttötarkoituksen mukaan. Esimerkiksi sähköpostipalvelimille, tiedostopalvelimille ja sovelluspalvelimille on tarjolla omat ohjelmistot (Andress 2011, 138).

Virustorjunnan lisäksi työasemien ja palvelinten suojaamisessa keskeisessä asemassa on käyttöjärjestelmään liittyvien tietoturvapäivitysten ajantasaisuus. Internet-yhteydessä olevat käyttöjärjestelmät kykenevät noutamaan tietoturvapäivityksensä heti, kun päivitys julkaistaan. Verkkoihin, jotka eivät ole Internet-yhteydessä, voidaan rakentaa omia päivityspalvelimia. Päivitysten testaaminen ennen niiden asentamista on olennaista, koska niillä voi olla vaikutusta tietojärjestelmän tai sovelluksen toimintaan. Työasemien vakioinnin avulla varmistetaan, että työasemissa on tietoturvallisuuden kannalta sama lähtötaso. Vakiointi mahdollistaa myös työasemasertifikaatin sekä muiden tunnisteiden sijoittamisen työasemaan. Tunnistetietojen pohjalta voidaan joko sallia tai kieltää työaseman liikennöinti verkossa. Työasemassa ajettavien palveluiden määrä kasvattaa hyökkäysrajapintaa, joten työasemavakio pyritään tekemään siten, että ainoastaan tarpeelliset palvelut ovat käytössä. Windows-pohjaisissa käyttöjärjestelmissä on käytössä työasemiin ja palvelimiin liittyviä käytäntöjä (policies), joiden määrittelyyn on kiinnitettävä erityistä huomiota. Käytäntöjen avulla voidaan säätää asioi-

ta, kuten salasanan monimutkaisuusvaatimuksia tai työaseman lukkiutumisaika. Palvelimien ja työasemien tiedostojärjestelmien salaamiseen on saatavilla useita ohjelmistoja. Varsinkin kannettavien tietokoneiden tiedostojärjestelmien salaaminen on yleinen tietoturvakäytäntö yrityksissä (Texasin yliopisto 2009).

Viruksia ja haittaohjelmia voi tulla siirrettävien muistivälineiden kautta sellaisiinkin verkkoihin, joissa ei ole Internet-yhteyttä. Erityisesti USB-laitteiden suosion kasvun myötä työasemia ja palvelimia on alettu suojata työasemiin kytkettävien laitteiden muodostamilta uhkilta. Ohjelmilla, kuten EndPoint Security tai DeviceLock, voidaan hallita siirrettäviä muistivälineitä sekä muita työasemiin kytkettäviä oheislaitteita. Tämän tyyppisten ohjelmistojen avulla voidaan sallia vain tiettyjen luvitettujen USB-laitteiden kytkeminen tietokoneisiin tai estää kokonaan DVD-asemien, USB-, infrapuna- tai sarjaporttien käyttö.

6 Suojausmalli

Suomessa on herätty panostamaan voimakkaasti kyberturvallisuuteen. Valmisteilla oleva kyberstrategia tähtää siihen, että Suomi on tietoturvan johtomaita vuonna 2016. Paljon on kuitenkin tehtävää yhteiskunnan kriittisten järjestelmien suojaamisessa. Tässä luvussa esitetään suosituksia kriittisten järjestelmien suojaamiseksi. Suositukset pohjautuvat tehtyihin havaintoihin aiheeseen liittyvästä lainsäädännöstä ja ohjeistuksista, tapauksista maailmalta sekä tietoturvatekniikoista.

6.1 Suosituksia lainsäädäntöön ja vastuujakoon

Suomessa on voimassa useita lakeja, jotka käsittelevät tietoturvaa ja yhteiskunnan turvallisuutta. Lait eivät kuitenkaan ole kattavia: esimerkiksi yhteiskunnan kriittisten järjestelmien suojaamisen vastuut ovat epäselviä. Vaikka huoltovarmuuslaki asettaa korkealla tasolla vastuun kriittisten järjestelmien suojaamisesta, ei yhteiskunnan kriittisiä järjestelmiä ole tiettävästi kokonaisuudessaan tunnistettu ja yksilöity. Laeissa ei mainita käsitettä kyber ja muita siitä johdettavissa olevia sanoja. Asiasanana kyber on kuitenkin kansainvälisesti yleinen, ja sen päivittämisestä lainsäädäntöön voitaisiin saada hyötyä. Kyberterroristilla saattaa olla samankaltaiset motiivit ja tavoitteet kuin henkilöllä, jonka me käsitämme terroristiksi. Terroriiskujen keinovalikoimat kuitenkin poikkeavat niin paljon, että termien erottaminen toisistaan voi olla perusteltua.

Suomessa on käyty keskustelua siitä, salliiko laki virus- ja haittaohjelmien kirjoittamisen, sekä pitäisikö kansallisten intressien suojaamiseksi kehittää niin sanottuja kyberaseita. Kuten useissa muissakin maissa, Suomessa laitonta ei ole virusten kirjoittaminen sinänsä, vaan nii-

den levittäminen. Laki ei myöskään määritä, kuka saa käyttää kyberaseita ja missä tilanteessa. Nykyiset ase- ja johtamisjärjestelmät pohjautuvat pitkälti tietotekniikkaan, joten puolustusvoimat on kybersodankäynnin luonteva toimija erityisesti hyökkäysten kannalta. Kansallinen tietotekninen osaaminen on kuitenkin niin jakaantunut, että puolustusvoimien tulisi miettiä, mistä tahoista sen kyberarmeijan reservi muodostuisi. Tietotekniikan kasvava merkitys sodankäynnissä pitäisi huomioida myös varusmieskoulutuksessa.

Ylätasolla yhteiskunnan kriittiset toiminnot on määritelty yhteiskunnan turvallisuusstrategiassa. Seuraavan vaiheen tulisi olla käsitteiden yhdistäminen yksittäisiin tietojärjestelmiin. Huoltovarmuuskeskus ei voi organisaationa yksin tehdä määrittelyä, siihen tarvitaan tietojärjestelmän omistajien panostusta. Heti kun kriittiset tietojärjestelmät on saatu tunnistettua, tulee käynnistää niiden tietoturva-auditointi.

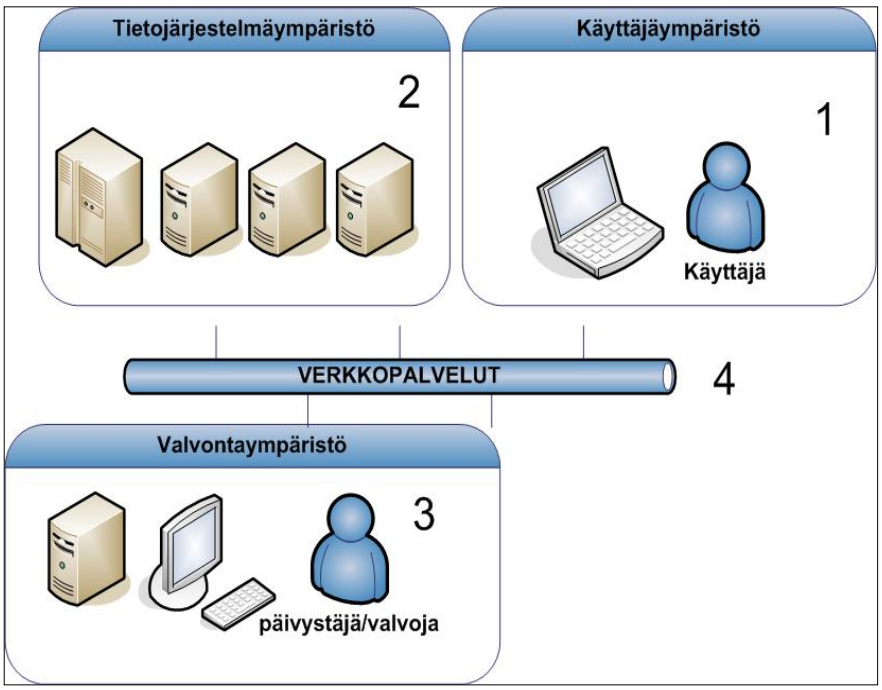
Yhtenä osana kriittisten järjestelmien suojaamisessa voitaisiin ottaa mallia Yhdysvaltojen INFOCON-valmiustasoista. Kun järjestelmiin kohdistuu uhkia tai hyökkäyksiä, merkittävältä kriisiltä voidaan parhaimmillaan välttyä, jos toimintamallit suunnitellaan eri valmiustasoille.

KATAKRI- ja VAHTI-ohjeistukset antavat hyvän pohjan auditointityölle. VAHTI-ohjeissa on käsitelty valtionhallinnon kriittisten järjestelmien suojaamista. KATAKRI sisältää kattavan ohjeistuksen kaikkiin muihin suojaustasoihin paitsi suojaustasoon I (erittäin salainen). Opinnäytteen yhtenä suosituksena ehdotetaan, että yhteiskunnan kriittisille tietojärjestelmille tulisi asettaa oma auditointikriteeristö. Kyseinen kriteeristö voisi olla osana VAHTI-ohjeistusta tai KATAKRIa. Kriteeristön ei kuitenkaan tulisi pohjautua ainoastaan järjestelmän tiedon suojaustasoon. Yhteiskunnalle kriittinen järjestelmä voi olla esimerkiksi ohjausjärjestelmä tai julkinen tiedotuskanava, jolloin järjestelmän sisältämän tiedon salattavuusasteella ei ole merkitystä. Kriittisten järjestelmien auditointikriteeristö voisi sisältää esimerkiksi KATAKRIn Suojaustason II vaatimukset soveltuvin tarkennuksin. Tarkennuksiin voisi lukeutua sellaisia asioita kuin vaatimukset väärinkäyttömallinnukselle, järjestelmän kotimaiselle ylläpidolle ja kehitystyölle sekä lähdekoodin katselmoinnille. Kriittisten järjestelmien erikoispiirteiden vuoksi voi olla tarpeellista luoda KATAKRIsta ja muista standardeista yhdistetty järjestelmäkohtainen auditointikriteeristö. Tietoturva-auditoinnissa on tarpeen mukaan käytettävä järjestelmän omistavan tai ylläpitävän tahon erikoisosaamista, mutta kansallisen turvallisuusviranomaisen tulee tehdä kriittisten järjestelmien akkreditointi.

Honeynets-ympäristöjen rakentamista kriittisten järjestelmiin kohdistuvien uhkien tunnistamiseksi tulisi kehittää. Erityisesti hyötyä voitaisiin saada sellaisten järjestelmien suojaamisen osalta, joissa käsitellään salaista tietoa. Rakentamalla salaista tietoa sisältäviä järjestelmiä muistuttavia ympäristöjä, voitaisiin mahdollisesti saada selville mistä tiedosta tunkeutuja on kiinnostunut, mitä menetelmiä hän käyttää sekä hänen motiivinsa.

6.2 Havaintoja suojaus- ja hyökkäysmenetelmistä

Merkittävä osa viime vuosina paljon julkisuutta saaneista tietoturvahyökkäyksistä on ollut palvelunestohyökkäyksiä. Palvelunestohyökkäykset ovat usein kohdistuneet www-palvelimiin, jotka toimivat tiedotuskanavina. Tietomurrot sen sijaan ovat kohdistuneet henkilö- ja asiakasrekistereihin sekä sähköpostipalvelimiin. Virukset ja vakoiluohjelmat leviävät suljettuihin ympäristöihin siirrettävien muistivälineiden avulla. Ohjelmat, kuten Stuxnet ja Duqu, viittaavat valtiolliseen toimintaan virusten tehtailussa. Suojausmenetelmiä kehitetään jatkuvasti; puute ei usein ole suojauskeinojen saatavuudessa vaan niiden oikeaoppisessa käytössä. Suojauksen rakentaminen tulee aloittaa määrittämällä tunnistettavat uhkat ennen teknisten menetelmien ja suojaustuotteiden valintaa. Kriittisten järjestelmien suojauksen tulee perustua kerrosajatteluun siten, että yhden tietoturvakontrollin pettäessä järjestelmäkokonaisuuden seuraava suojauskerros estää hyökkäyksen. Oheisessa kuvassa on jaoteltu tekniset suojausmenetelmät neljään tasoon niiden sijoituspaikan mukaan.



kuva 10: Suojausmenetelmien sijoittelupaikkoja.

1. Käyttäjäympäristössä eli loppukäyttäjän työasemassa olevia suojausmenetelmiä ovat virustorjuntaohjelmisto, VPN-Client, ohjelmistopalomuuri, työaseman kovennukset,

valvonta- ja hallinta-agentit, tiedostojen salaamis- ja tuhoamisohjelmistot sekä työasema- ja käyttäjävarmenteet.

2. Tietojärjestelmäympäristön eli palvelinympäristön suojausmenetelmiä ovat virustorjuntaohjelmistot, palvelinten kovennus, käyttäjähakemiston suojaukset, pääsynhallinta, tiedostosuojaukset, tietokantojen suojaukset, varmistusjärjestelmät, lokipalvelimet, palvelujen monistaminen, turvallinen ohjelmakoodi sekä palvelinvarmenteet.

3. Valvontaympäristön tarjoamia suojausmenetelmiä ovat siirrettävien muistivälineiden hallinta, virustorjunnan valvonta, järjestelmän toiminnan valvonta, lokien valvonta sekä verkkolaitteiden valvonta.

4. Tietoliikennekerroksessa suojautuminen voidaan toteuttaa palomuureilla, liikenteen suodatuksella, tunkeutumisenestojärjestelmillä, tietoliikenteen salauspalveluilla, virusten tunnistamisella, kuormantasauksella, verkkolaitteiden koventamisella ja monistamisella.

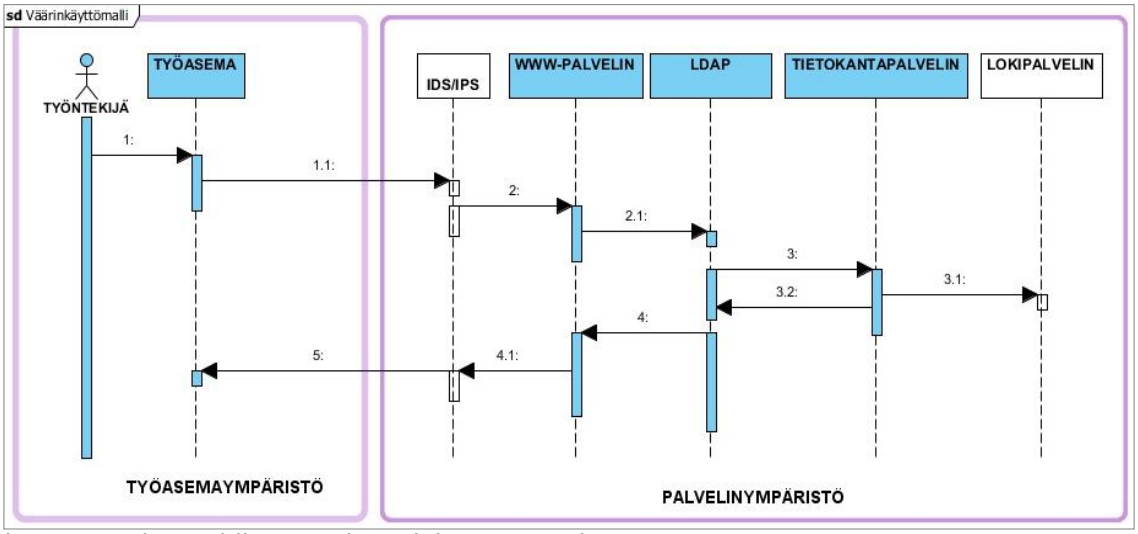
6.3 Artefakti

Maailmalla tapahtuneita tietoturvahyökkäyksiä seuraamalla voidaan tehdä johtopäätöksiä siitä, mitkä ovat todennäköisimmät suojattavaan järjestelmään kohdistuvat uhkat. Julkisissa verkkopalveluissa on perusteltua panostaa palvelunestohyökkäyksiltä suojaamiseen. Suljetussa ympäristössä uhka tulee todennäköisemmin siirrettävästä mediasta viruksena tai vakoiluohjelmana. Vähemmän kriittisen järjestelmän suojaaminen ainoastaan todennäköisimmiltä uhkilta voi olla joskus perusteltua, mutta kriittisen järjestelmän suojaaminen vaatii enemmän.

Tässä opinnäytetyössä esitetään kolmijakoinen malli kriittisten tietojärjestelmien suojaamiseen. Mallin ensimmäinen osa sisältää uhkilta suojautumisen tehdyn väärinkäyttömallinnuksen pohjalta. Toinen osa mallista on uhka-analyysilista valtiollisille ja ei-valtiollisille toimijoille. Viimeinen osa mallista on kriittisen järjestelmän tietoturvan tilannekuvan valvonta.

6.3.1 Uhkilta suojautuminen väärinkäyttömallinnuksen pohjalta

Taulukko 5 toimii esimerkkinä työkalusta, jonka avulla kriittiseen järjestelmään tarvittavia suojausmekanismeja voidaan luoda. Taulukon oletuksena on, että ennen taulukon luomista tietojärjestelmän suojaamiseen liittyvät väärinkäyttötapaukset (misuse case) on tunnistettu ja mallinnettu. Esimerkkinä mallinnuksen teosta toimii taulukon ensimmäinen väärinkäyttötapaus, joka on mallinnettu seuraavana olevassa UML-kuvassa.



kuva 11: Sekvenssidiagrammi väärinkäyttötapauksesta.

Kuvan 11 diagrammissa on kuvattu väärinkäyttötapaus, jossa oma työntekijä tekee tietomurron tietokannassa sijaitsevaan aineistoon. Kuvan perusteella voidaan suunnitella suojautumismenetelmiä kyseisen väärinkäyttötapauksen toteutumisen estämiseksi. Diagrammista ilmenee vaiheistettuna ne tekniset komponentit, joihin tapaus liittyy. Tämä mallinnustapa auttaa havainnollistamaan hyökkäykseen liittyvät osatekijät, mikä puolestaan auttaa suojausmenetelmien suunnittelussa.

Väärinkäyttömallinnusta käytetään hyvin harvoin tietojärjestelmien kehitysprojekteissa. Syynä siihen on väärinkäyttömallinnuksesta muodostuvat työmäärät ja kustannukset. Kriittisten järjestelmien suojaamisessa ne eivät kuitenkaan saa olla perusteita. Tyypillisesti kriittisten järjestelmien rakentamiseen käytetään niin paljon rahaa ja henkilöresursseja, että väärinkäyttömallinnus toisi vain murto-osan lisäkustannuksia projektiin. Johtuen siitä, että väärinkäyttömallinnusta tehdään niin harvoin, ei ole vielä tiedossa kattavaa tutkimustietoa siitä, kuinka paljon väärinkäyttömallinnus parantaa tietojärjestelmien tietoturvaa. On kuitenkin selvää, että väärinkäyttömallinnus tuo yhden merkittävän lisätason kriittisten järjestelmien tietoturvaan.

VÄÄRINKÄYTTÖTAPAUS	SUOJAUSMENETELMÄT
Oma työntekijä murtautuu tietoon, johon hänellä ei ole käyttöoikeuksia	Vahva tunnistautuminen, tiedostojen salaaminen, tietokantojen salaaminen, käyttöoikeuksien hallinta, käyttäjähakemiston salaaminen, lokien hallinta ja valvonta, tietokantapalvelimen ja tiedostopalvelimen kovennukset, IDS/IPS-ohjelmistojen käyttöönotto
Ulkoverkosta suoritetaan palvelunestohyökkäys verkkopalvelimeen	Www-palvelimen ja tietokantapalvelimen kovennukset, kuormantasaus, palvelin- sekä verkkolaitteistojen monistaminen, hälytysarvojen määrittäminen ja valvonta, IDS/IPS-ohjelmistot , palomuurien ja verkkolaitteiden konfiguraatiot, verkonvalvonta, www-ohjelmiston turvallinen lähdekoodi
USB-tikulta siirtyy vakoiluohjelma työasemaan, jolla tietojärjestelmää käytetään	ajantasaiset virustorjuntaohjelmistot työasemissa ja palvelimissa, USB-laitteiden hallintaohjelmisto, työaseman kovennukset, IDS/IPS-toteutukset, työasemapalomuuri, verkkolaitteiden konfiguroiminen siten, ettei vakoiluohjelma pääse lähettämään tietoa paluuliikenteenä, ajantasaiset työaseman tietoturvapäivitykset
Tietokantaan suoritetaan SQL-injektio verkkopalvelimen kautta	turvallinen ohjelmakoodi, tietokantaohjelmiston tietoturva-asetukset, verkkopalvelimen konfiguraatio, käyttöoikeuksien rajaaminen, erikoismerkkien ja epävalidien arvojen syöttämisen estäminen

Taulukko 5: Väärinkäyttömallinnukseen pohjautuva suojautuminen.

Väärinkäyttötapausten suunnitteluun voitaisiin hyödyntää kansainvälisiltä CERT-viranomaisilta saatavaa tietoa. Keräämällä tietoa hyökkäyksistä, jotka on tehty toiminnallisuudeltaan, tai tekniseltä toteutukselta omaa suojattavaa järjestelmää vastaavaa järjestelmää kohtaan säästytään siltä, että väärinkäyttötapaukset jouduttaisiin suunnittelemaan täysin tyhjältä pöydältä.

6.3.2 Uhka-analyysi kyberavaruuden toimijoista

Inhimillisen erehdyksen ja järjestelmävian lisäksi valtiolliset ja ei-valtiolliset toimijat voivat olla uhka kriittisille järjestelmille. Suomen poliittisen ja sotilaspoliittisen aseman pohjalta voidaan tehdä oletus, että ei-valtiolliset toimijat ovat näistä suurempi uhka kansallisille kriittisille järjestelmille. Tapaukset maailmalta osoittavat, että valtiollisista toimijoista suurin uhka ovat tiedustelupalveluiden keinot tietomurtoihin. Suoranainen vahingonteko Suomen kansallisesti kriittisiä järjestelmiä kohtaan muussa kuin tiedonhankintatarkoituksessa on rauhan aikana epätodennäköistä. Ei-valtiolliset toimijat ovat huomattavasti arvaamattomampia. Niiden motiivit voivat olla esimerkiksi uskonnollisia, taloudellisia, poliittisia tai perustua pelkästään henkilökohtaiseen kyvykkyyteen aiheuttaa vahinkoa.

Opinnäytetyössä esitetään, että sekä valtiollisia että ei-valtiollisia toimijoita tulisi seurata. Ehdotus perustuu siihen, että tuntemalla eri toimijoiden muuttuvat toimintamallit, ja hyökkäysmenetelmät, ne osataan ottaa huomioon kriittisten järjestelmien suojaamisessa. Toimijoiden kyvykkyyksistä ja aktiivisuudesta voidaan ylläpitää tilannekuvaa ja niitä voidaan analysoida. Valtiollisten toimijoiden seurannasta voidaan tuottaa harvemmin – esimerkiksi neljännesvuosittain – analysoituun tietoon perustuva tilannekatsaus. Ei-valtiollisten toimijoiden seurannan tulisi olla jatkuvaa ja uhkatrendien ja kyvykkyyksien analysointi tiiviimpää. Tämä johtuu siitä, että ei-valtiolliset toimijat kykenevät paljon nopeampiin liikkeisiin kuin valtiolliset toimijat.

Taulukossa 6 on kuvattu kuvitteellinen esimerkki analysoituun tietoon pohjautuvasta valtiollisten toimijoiden seurannasta.

Valtio	Hyökkäyskyky (1-10)	Puolustuskyky (1-10)	Infrastruktuurin toimivuuden riippuvuus tietotekniikasta (miinus 1-5)	Kokonaissuorituskyky (0-19)	Uhkatodennäköisyys valtiollinen hyökkäys	Ajankohtaista
Yhdysvallat	8	4	4	8	0 %	Yhdysvallat kouluttaa kybersotilaita Israelin kanssa
Venäjä	7	6	3	10	2 %	Venäjä käynnistänyt kybersodan Viroa vastaan
Kiina	5	6	2	9	1 %	Epäiltyjä hyökkäyksiä Yhdysvaltojen ilmavoimien verkkoihin
Färsaaret	9	7	1	15	94 %	Färsaaret perustaa kyberhyökkäyksiin keskittyvän 8000 henkilön vahvuisen joukko-osaston

Taulukko 6: Valtiollisten toimijoiden kuvitteellinen analyysitaulukko.

Taulukkoa voi käyttää yksinkertaisena valtioiden muodostaman uhkan seurantatyökaluna. Vaikka Suomi tuskin lähivuosina suorittaa kyberhyökkäyksiä muita valtioita kohtaan, taulukossa on huomioitu myös eri maiden infrastruktuurin riippuvuus tietotekniikasta. Mikäli maan kriittinen infrastruktuuri ei ole riippuvainen tietotekniikasta, kyberhyökkäyksillä kyseistä maata kohtaan tuskin on kovin suurta vaikutusta. Taulukko pohjautuu kuvitteellisen analyysin pohjalta muodostettuihin arvoihin siten, että maan kybersodankäynnin suorituskyvyn arvo muodostetaan laskemalla yhteen hyökkäyskyky ja puolustuskyky. Saadusta summasta vähennetään lukuarvo, joka kuvaa maan infrastruktuurin riippuvuutta tietotekniikasta, jolloin saadaan lopputulokseksi kokonaissuorituskykyä kuvaava arvo. Lisäksi taulukossa on sarake, joka kuvaa valtiollisen hyökkäyksen todennäköisyyttä maittain, sekä sarake, joka kuvaa merkittävää ajankohtaista valtiollista aktiviteettia. Taulukko on työkaluna erittäin pelkistetty, mutta se antaa perusajatuksen laajemman sovelluksen suunnittelun pohjakasi. Sovellus, jonka tietokannassa olisi kattavat tiedot maiden tietoteknisistä toimijoista, koulutusohjelmista, panos-

tuksesta kybersodankäyntiin, aiheeseen liittyvästä lainsäädännöstä sekä hyökkäystapauksista, tarjoaisi hyvän pohjan analyysien ja raporttien laatimiseen. Kuten tämä opinnäytetyö osoittaa, pelkästään julkisista lähteistä on koostettavissa helposti tietoa analyysin lähtöaineistoksi.

Ei-valtiollisiin toimijoihin voidaan laskea kaikki muut toimijat alkaen omista työntekijöistä. Eri toimijoiden tilanneseurannan kannalta kuitenkin lähinnä erilaisten aktivisti- ja kyberrikollisryhmien seuraaminen on järkevää. Ryhmien lisäksi yksittäisten ryhmiin kuulumattomien tai osana ryhmää toimivien henkilöiden erillisseuranta voi olla perusteltua. Taulukossa 7 on otettu esille tiettyjä ei-valtiollisten toimijoiden asioita, joita seurataan. Taulukossa esitetyt tiedot ovat kuvitteellisia. Haktivistiryhmittymillä on vaihtelevasti tapana ilmoittaa etukäteen hyökkäysaikeistaan. Vertaamalla toteutuneita hyökkäyksiä suoritettuihin uhkauksiin voidaan arvioida kyseisen toimijan uskottavuutta ja uhkapotentiaalia. Hyökkäysten lukumäärä antaa kuvaa ryhmittymän koosta ja aktiivisuudesta. Hyökkääjän kyvykkyyttä voidaan arvioida tutkimalla tarkemmin aiemmin toteutuneita hyökkäyksiä. Arvioimalla hyökkääjän motiiveja voidaan päätellä mahdollisen tulevan hyökkäyksen kohde. Esimerkiksi haktivisti voi pyrkiä murtautumaan verkkopalveluun sanomansa julkaisemiseksi, sen sijaan taloudellista etua tavoitteleva taho voi pyrkiä kiristämään tietomurron avulla saatujen tietojen avulla.

Ryhmä / Henkilö	Suoritetut hyökkäykset (lkm)	Uhatut / toteuneet hyökkäykset %	Kyvykkyysarvio (1-10)	Motiivit	Uhkatodennäköisyys	Ajankohtaista / muuta tietoa
LulzSec	42	82 %	7	"huvin vuoksi"	12 %	havaittu myös toimintaa Suomessa
AnonFinland	7	3 %	2	aktivismi, "huvin vuoksi"	2 %	arviolta ryhmä koostuu vain muutamasta teinistä
Al-Jihad Hackers	12	70 %	6	uskonnollis-poliittiset	4 %	kiinnostus Suomea kohtaan voi kasvaa
Jie Dong	3	ei ennakko-uhkauksia	8	taloudelliset	3 %	uhka lähinnä maksuliikennejärjestelmiin liittyen

Taulukko 7: Ei-Valtiollisten toimijoiden kuvitteellinen analyysitaulukko.

6.3.3 Kriittisen järjestelmän tilannekuva

Järjestelmän toimintakyvyn tarkkailun lisäksi tässä työssä esitetään, että kriittisen järjestelmän tietoturvasta on ylläpidettävä tilannekuvaa. Järjestelmän omistajan kannalta on hyödyllistä nähdä oman järjestelmän tietoturvan tilannekuva, mutta kaikkien yhteiskunnan kannalta kriittisten järjestelmien kannalta on hyödyllistä koostaa lisäksi keskitettyä tilannekuvaa. Mikäli yhtä kriittiseksi luokiteltua järjestelmää vastaan hyökätään, on mahdollista, että hyökkäykset laajenevat koskemaan muita järjestelmiä. Sopiva paikka tällaiselle korkean tason tilannekuvalle saattaisi olla esimerkiksi valtioneuvoston tilannekeskus (VNTIKE).

Taulukolla 8 simuloidaan työvälinettä, joka esittää kriittisten järjestelmien tilannekuvaa. Taulukossa oleva sarake, joka kuvastaa järjestelmän toimintakykyä, ei välttämättä korreloi yksi yhteen järjestelmän tietoturvan kanssa, mutta järjestelmän toimintakyvyn heikkeneminen voi olla merkki tietoturvahyökkäyksestä. Kriittisten järjestelmien haavoittuvuuksien todennäköisyyttä voidaan arvioida useilla eri tavoilla. Mikäli järjestelmä on kytketty julkiseen Internetiin tai se tarjoaa muita avoimia hyökkäysrajapintoja, se voi olla haavoittuvampi kuin suljettu järjestelmä. Haavoittuvuuteen voivat vaikuttaa monet muutkin seikat, kuten järjestelmän käyttäjämäärät, sen rakentamisvaiheessa tehdyt tietoturvapanostukset tai järjestelmän tekniset ratkaisut. Hyökkäyksen todennäköisyydet voivat vaihdella olosuhteiden mukaan: esimerkiksi puhelinoperaattoria vastaan tehtävän hyökkäyksen todennäköisyys saattaa kasvaa, kun operaattori ilmoittaa irtisanovansa henkilöstöä. Hyökkäysmenetelmä- ja tilanteen kuvaus -sarakkeissa on kuvattu järjestelmään kohdistuneen hyökkäyksen tapaa, siitä aiheutuvaa haittaa sekä korjaustoimia.

Suojattava järjestelmä	Hyökkäyksen todennäköisyys %	Haavoittuvuuden todennäköisyys %	Järjestelmän toimintakyky %	Värikoodi	Hyökkäysmenetelmä/ Vian syy	Tilanteen kuvaus
Järjestelmä 1 ("sähkönjakelu")	**3** % (erittäin epätodennäköinen, 1 % – 5 %)	**3** % (erittäin epätodennäköinen, 1% – 5 %)	**100**% (täysin toimintakuntoinen)		ei tiedossa olevaa hyökkäystä	Normaali
Järjestelmä 2 ("teleliikenneverkko")	**15** % (mahdollinen, 6 % – 39 %)	**15** % (mahdollinen, 6 % – 39 %)	**83**% (ydinpalvelut toimivat, 99-65%)		ohjelmistovirhe	Ohjelmistovirhe toissijaisissa palveluissa, korjaus käynnistetty
Järjestelmä 3 ("hätätiedotussivustot")	**55** % (todennäköinen, 40 % – 69 %)	**55** % (todennäköinen, 40 % – 69 %)	**40**% (osa ydinpalveluista toimii 64%-30%)		palvelunestohyökkäys	Verkkosivustot toimivat, mutta hitaasti
Järjestelmä 4 ("ilmatilannekuva")	**82** % (erittäin todennäköinen 70 % – 100 %)	**82** % (erittäin todennäköinen 70% –100 %)	**20**% (ydinpalvelut toimintakyvyttömiä tai kriittistä tietoa menetetty)		tietomurto	Hyökkääjä syöttää väärää tietoa tutkakuvaan

Taulukko 8: Kriittisten järjestelmien tilannekuvan seuraaminen.

Keskitetyn kriittisten järjestelmien tilannekuvasovelluksen hyödynnettävyys on täysin riippuvainen niistä lähteistä, joista tilannekuvaa koostetaan. Tilannekuvasovellusta voidaan aloittaa kehittämään vasta, kun kriittiset tietojärjestelmät on tunnistettu. Tämän lisäksi täytyy suunnitella prosessit ja menetelmät joilla tietoa välitetään yksittäisestä tietojärjestelmä keskitet-

tyyn tilannekuvaan. Valmis tilannekuvasovellus parantaa mahdollisuuksia reagoida kyberhyökkäyksiin. Ottamalla käyttöön INFOCONin tapaiset toimenpideohjeet hyökkäysten varalta, sovelluksen hyödyntäminen tehostuisi entisestään.

7 Yhteenveto ja opinnäytetyöprosessin arviointi

Tutkimusmenetelmäosiossa käsiteltiin Hevnerin seitsemää ohjetta. Työn lähtökohta oli etsiä ratkaisu johonkin ongelmaan. Työn pääkysymys oli, kuinka kriittisiä tietojärjestelmiä voitaisiin suojata nykyistä paremmin. Kysymykseen haettiin vastausta tutkimalla, mitkä ovat keskeiset kansalliset toimijat kriittisten järjestelmien osalta, mikä on aiheeseen liittyvä lainsäädäntö sekä ohjeistus Suomessa sekä mihin yhteiskunnan toimintoihin kriittiset järjestelmät liittyvät. Vastauksena saatiin suosituksia lainsäädännön ja vastuujaon selkiyttämiseksi sekä tietoturva-auditoinnin kehittämiseksi. Varsinaisena artefaktina luotiin kolmiosainen suojausmalli, josta on mahdollista kehittää edelleen kriittisten järjestelmien suojaamista tehostava sovellus. Artefaktin luomisen vaiheet kuvattiin kuvassa 2, pohjautuen Hevnerin ryhmän oppeihin.

Aihealueina tietoturva ja siihen liittyvä kyberulottuvuus ovat todella laajoja, joten tutkimusprosessiin liittyneiden lähteiden määrästä ei ollut pulaa. Hyödyllisten lähteiden suodattaminen ja oleellisen tiedon omaksuminen asettivat siten työlle lisähaasteita. Niin kutsutuista hyökkäys- ja suojausmenetelmistä täytyi poimia vain keskeisimmät. Samoin kun kuvattiin maailmalla tehtyjen suurimpien tai kiinnostavimpien kyberhyökkäyksien taustoja, jouduttiin tekemään valintoja lukuisten vaihtoehtojen kesken.

Suomessa on tehty useita tietoturvaan liittyviä tutkimuksia. Tämä opinnäytetyö laajentaa tietoturvan katsontakulmaa yhteiskunnalle kriittisiin järjestelmiin ja kyberuhkiin, joita ei tiettävästi Suomessa ole opinnäytetöissä käsitelty. Aihe on varsin ajankohtainen, kun Suomessa laaditaan vuoden 2012 aikana kyberstrategia ja vuonna 2013 käynnistyy ensimmäinen kyberturvallisuuteen keskittyvä ammattikorkeakoulupohjainen koulutusohjelma.

Tiettyyn hyökkäysmenetelmään tai valtiolliseen toimijaan keskittyvä yksityiskohtainen jatkotutkimus toisi aiheesta arvokasta lisätietoa. Työn varsinaisille hyödyntäjille eli valtionhallinnon eri toimijoille ja kriittisten järjestelmien omistajille työn toivotaan antavan varsinaisten suositusten ja suojausmallin lisäksi aiheeseen liittyvää taustatietoa, ja sen toivotaan herättävän uusia ajatuksia. Tutkimusmenetelmästä voidaan todeta, että suunnittelututkimus soveltuu hyvin teknisten järjestelmien mallintamiseen ja kehittämiseen.

7.1 Opinnäytetyöprosessin arviointi

Laureassa opinnäytetyö aloitetaan valitsemalla aiheeseen sopiva tutkimusmenetelmä, ja kuvaamalla se. Tutkimusmenetelmään liittyvä työmäärä tämän opinnäytetyön osalta oli noin 15 prosenttia kokonaistyömäärästä. Opinnäytetyön sitomisella tiettyyn tutkimusmenetelmään saavutetaan tietynlaista automaattista ohjausta opinnäytetyön etenemiselle oikeaan suuntaan. Oletettavasti myös opinnäytetöiden arvioiminen helpottuu yhdenmukaisten tutkimusmenetelmien myötä. Tämän opinnäytetyön puitteissa koettiin, että tutkimusmenetelmään liittyvä työ oli pois varsinaisen substanssin kirjoittamiselta. Lisäksi opinnäytetyön varsinaisia hyödyntäjiä ei kiinnostane niinkään työn tutkimusmenetelmäosio, vaan muu sisältö. Laureassa on YAMK-tutkintoon yhdistetty tutkimusmenetelmiä käsitteleviä opintoja, joihin yhtenä kehitysehdotuksena voitaisiin suunnitella yhdistettävän myös opinnäytetyön tutkimusmenetelmän raportoiminen. Siten tutkimusmenetelmä olisi yhä mukana, mutta ei esillä niin vahvasti varsinaisessa opinnäytetyön kirjallisessa julkaisussa.

Opinnäytetyötä kirjoitettaessa pyrittiin löytämään esitetylle tiedolle lähde myös silloin, kun työn kirjoittajalla oli kokemuspohjaista tietoa esitetystä asiasta. Tämä johti valitettavan usein Internetistä löydettyjen lähteiden käyttöön, joiden taso oli hyvin vaihteleva. Laureassa ylempään amk-tutkintoon sisältyvien opinnäytetöiden on oltava julkisia. Tämän opinnäytetyön puitteissa julkisen aineiston kerääminen ei ollut ongelma. Sen sijaan ongelmaksi muodostui analyysin muodostaminen kootusta aineistosta, joka olisi voinut pakottaa työn salaiseksi. Tästä syystä suojausmalli- ja johtopäätösosiot jäivät tavoitteita suppeammiksi. Opinnäytetyöstä jätettiin myös tarkoituksellisesti yhdistämättä tiettyjä julkisista lähteistä kerättyjä tietoja yhteen, koska myös siten olisi kokonaisuudeksi muodostunut ei-julkista tietoa.

Yhtenä työn tavoitteista oli kuvata eri maissa tapahtuneita hyökkäyksiä, sekä maiden varautumista hyökkäyksiin. Hyökkäystapahtumien perusteella pyrittiin valitsemaan keskeisimmät hyökkäysmenetelmät, ja niihin liittyvät suojausmenetelmät. Eri maiden varautumista kriittisten järjestelmien suojaamiseen sen sijaan kuvattiin hiukan tarkemmin ainoastaan Pohjoismaiden osalta. Jälkikäteen ajateltuna työstä olisi voitu rajata pois tekniset hyökkäys- ja suojausmenetelmät. Keskittyminen eri maiden kybervalmiuksiin olisi johtanut selkeämpään kokonaisuuteen. Toisaalta opinnäytetyön kirjoittajan oman teknisen osaamisen kehittämisen kannalta, teknisiin menetelmiin perehtyminen oli hyödyllistä.

Kokonaisuutena opinnäytetyön kirjoittaminen oli mielenkiintoisen aihevalinnan ansiosta antoisaa. Mikäli aika ja työn julkisuusvaatimukset olisivat mahdollistaneet, työhön olisi tehty lisäyksiä erityisesti eri maiden kybersodankäynnin suorituskykyyn, sekä johtopäätöksiin liittyen.

7.1.1 Käytetyt lähteet

Työssä hyödynnetyt lähteet jakautuivat siten, että noin kolmasosa niistä oli kirjalliseksi lähteiksi luokiteltavia, kolmasosa julkaisemattomia lähteitä ja loput sähköisiä lähteitä. Yhteensä erilaista lähdemateriaalia kerättiin noin 180 kappaletta, joista käytettiin noin sataa. Useat kirjalliset teokset sisälsivät niin paljon sivuja, että teosten sisältä pyritettiin ainoastaan etsimään keskeiset kohdat. Joitain hyödylliseksi tunnistettuja kirjoja jouduttiin jättämään kokonaan pois aikataulusyistä johtuen.

Tutkimusmenetelmäosiossa käytettiin pääsääntöisesti Laurean opintojaksojen yhteydessä käsiteltyjä lähteitä. Merkittäviin kyberhyökkäystapauksiin tutustuttiin kirjojen avulla, ja tapauksiin etsittiin täydentävää tietoa Internetistä. Jotkin hyökkäystapauksista olivat kirjoitushetkellä niin tuoreita, ettei niistä ollut saatavilla kirjallisia lähteitä. Teknisiin hyökkäys-, ja suojausmenetelmiin oli hyvin saatavilla kirjallisia lähteitä. Hyökkäysmenetelmät pyrittiin valitsemaan perustuen luvussa kolme esiteltyihin hyökkäystapauksiin. Tästä syystä Web-pohjaisia hyökkäyksiä käsiteltiin hiukan yksityiskohtaisemmin.

7.1.2 Suojausmallin taustat

Opinnäytteen tavoitteena oli parantaa uuden innovaation kautta kriittisten järjestelmien suojaamista. Tutustumalla eri tutkimusmetodeihin havaittiin, että ainoa sopiva tutkimusote opinnäytteelle oli suunnittelututkimus. Hevnerin ryhmän suunnittelema ohjeistus on kehitetty teknisten tutkimusten avuksi osana suunnittelututkimuksen kokonaisuutta. Valitsemalla Hevnerin ryhmän ohjeet suojausmallin rakentamisen pohjaksi saatiin selkeä perusajatus sille, kuinka opinnäytetyöprosessi viedään läpi. Hevnerin ryhmän ohjeiden avulla opinnäytetyön rakenne oli hahmoteltavissa melko vaivattomasti.

Aluksi oli tutustuttava taustoihin: kansallisiin toimijoihin, ohjeisiin, standardeihin ja lainsäädäntöön. Tuntematta taustoja, kuten aiheeseen liittyvää lainsäädäntöä, artefaktiin oltaisiin voitu periaatteessa laatia esimerkiksi lainvastaista kyvykkyyttä vastahyökkäyksiin. Näiden asioiden jälkeen tutustuttiin niihin hyökkäyksiin, joilta ollaan suojautumassa, sekä sivuttiin miten muissa maissa varaudutaan kyberuhkien varalta. Seuraavaksi käsiteltiin teknisiä hyökkäys,

-ja puolustuskeinoja. Lopulta artefaktin luomiselle saatiin riittävät perusteet, kun kaikki edellä mainittuihin asioihin oli perehdytty.

Suojausmallin ensimmäisessä vaiheessa esiteltiin tarve määrittää ne mahdolliset menetelmät, joilla tietojärjestelmää voitaisiin väärinkäyttää. Tällöin mahdollisiin väärinkäyttötapauksiin voidaan varautua rakentamalla torjuntamekanismit. Onnistunut tietojärjestelmäprojekti edellyttää, että ennen järjestelmän rakentamista on määriteltävä järjestelmän käyttötapaukset. Tästä syntyi ajatus siitä, että käyttötapausten lisäksi tulisi määrittää mahdolliset väärinkäyttötapaukset. Etsiessä väärinkäyttömallinnukseen liittyviä lähteitä havaittiin, että niitä on saatavilla melko vähän. Jo tästä syystä voidaan olettaa, että väärinkäyttömallinnusta käytetään hyvin harvoin tietojärjestelmäprojekteissa. Siten voidaan tehdä jatkopäätelmiä siitä, että tietojärjestelmiin liittyviä tietoturvaratkaisuja rakennetaan usein pohtimatta kunnolla niitä uhkia, joilla kyseisillä ratkaisulla haetaan tietoturvaa.

Toisessa vaiheessa esiteltiin uhka-analyysi valtiollisista, ja ei-valtiollisista toimijoista. Tuntemalla eri toimijat ja heidän menetelmänsä, kyetään rakentamaan tarvittavia uusia suojausmekanismeja, tai kehittämään vanhoja. Ymmärtämällä se, että valtiollisten ja ei-valtiollisten toimijoiden keinot, resurssit, osaaminen sekä motiivit voivat poiketa toisistaan osataan uhkia vastaan suojautua tehokkaammin. Perusteet uhka-analyysin tarpeelle syntyivät kappaleessa kolme esitetyistä hyökkäystapauksista.

Viimeisenä kokonaisuutena ehdotettiin tilannekuvaohjelmiston rakentamista kriittisten järjestelmien valvontaan. Seuraamalla keskitetysti kriittisten järjestelmien tilannetta, kyetään reagoimaan tehostetusti niistä löydettyihin vikoihin, sekä järjestelmiin kohdistuviin hyökkäyksiin. Keskitetty tilannekuva mahdollistaa myös tilanteen raportoinnin tarvittaville tahoille. Organisaatioilla on tyypillisesti käytössä heidän omia tietojärjestelmiä ja niiden tietoturvaa valvovia ohjelmistoja, varsinkin ydinjärjestelmien osalta. Ajatus keskitetystä kriittisten järjestelmien tilannekuvasta pohjautuu tarpeeseen hyödyntää nykyisistä valvontajärjestelmistä saatavia tietoja yhteiskunnan turvallisuuden näkökulmasta.

7.1.3 Loppusanat

Haluan vielä lopuksi kiittää Miia Hermeliniä opinnäytetyöhön liittyvistä neuvoista. Kiitos myös kaikille luonnosversioon perehtyneille tietoturva-asiantuntijoille, jotka kommentoivat työtä, ja antoivat Laurealle oman lausuntonsa. Palaan todennäköisesti vielä aihealueeseen laatimalla siitä ei-julkisen raportin.

Lähteet

Kirjalliset lähteet

Aho, H. 1999. Tiede, tutkimus ja tutkielma. Johdatus tutkielman maailmaan. 3. painos. Porvoo: WSOY.

Andrés, S. Kenyon B. 2004. Security Sage's guide to Hardening the Network Infrastructure. Yhdysvallat: Syngress Publishing.

Andress, J. & Winterfeld, S. 2011. Cyber Warfare Techniques, Tactics and Tools for Security Pratctitioners. Waltham, Yhdysvallat: Syngress Publishing.

Alter, S. 2008. Defining information systems as work systems: implication for the IS field. European Journal of Information Systems vol. 17/2008.

Brown, H. & Cook, R. Gabel, M. 2011. Environmental Design Science Primer. New Haven, Yhdysvallat: Advocate Press.

Brunner, E. & Suter, M. 2009. International CIIP Handbook 2008/2009. Zürich, Sveitsi. ETH Zürich.

Carr, J. 2011. Cyber Warfare: Mapping the Cyber Underworld. Washington, Yhdysvallat. O'Reilly.

Cederberg, A. 2011. Suomen Turvallisuusvuosikirja 2011 – 2012: Artikkeli: Yhteiskunnan turvallisuusstrategia (YTS) torjuu uhkia. Forssa: Forssa Print.

Clarke, R. & Knake, R. 2010. Cyber War. New York, Yhdysvallat: HarperCollins Publishers.

Dunn, M & Mauer, V. 2006. International CIIP Handbook 2006 Vol II. Zürich, Sveitsi: ETH Zürich.

Hagestam, A. 2005. CIP – kriittisen infrastruktuurin turvaaminen, käsiteanalyysi ja kansainvälinen vertailu. Helsinki: Huoltovarmuuskeskuksen julkaisuja.

Harris S. 2008. CISSP All-In-One Exam Guide. 4. painos. New York, Yhdysvallat: McGraw-Hill.

Hevner, A. & March S. & Park ,J. & Ram, S. 2004. Design Sciens in Information Systems Research. MIS Quarterly Vol. 28.

Kramer, D. & Starr, S. Wentz, L. 2009. Cyberpower and National Security. Virginia, Yhdysvallat: Potomac Books.

Kurki, M. 2008. Tulevaisuuden verkkopalvelut. Haaga-Helia julkaisusarja. Helsinki: Haaga-Helia Ammattikorkeakoulu.

Janczewski, L. & Collard, A. 2009. Cyberwarfare and Cyber Terrorism. 2. painos. Herheys Yhdysvallat: IGI Global.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Opinpajan kirja.

Kotilainen, T. & Lehto, S. 2011. Kybersodan etulinjassa. Tietokonelehti 9/2011. Helsinki: Sanoma Magazines Finland.

Krekel, B. & Adams, B. & Bakos G. 2012. Chinese Capabilities for Computer Network Operations and Cybe Espionage. North Grumman Corp.

Maanpuolustuskorkeakoulu 2008. Sota Kiinalaisin erityispiirtein – Sodan kuva Kiinassa 2000-luvulla. Julkaisusarja 1, Strategian tutkimuksia No 24. Helsinki: Maanpuolustuskorkeakoulun julkaisut.

March, S. & Smith, G. 1995. Design and natural science research on information technology. Minnesota Yhdysvallat: University of Minnesota.

Relator Oy 2009. Tietoturvan huomioon ottaminen järjestelmähankinnassa. White Paper.

Shah, S. 2007. Web 2.0 Security Defending AJAX RIA and SOA. Yhdysvallat. Charles River Media.

Stiennon, R. 2010. Surviving Cyberwar. Plymouth Iso-Britannia: Government Institutes.

Puolustusministeriö 2011a. Kansallinen turvallisuusauditointikriteeristö versio II. Helsinki: Puolustusministeriö.

Puolustusministeriö 2011b. Yhteiskunnan turvallisuusstrategia. Vammala: Vammalan kirjapaino.

Puolustustaloudellinen suunnittelukunta 2000. Tietojärjestelmien tietoturvallisuuden hallinnolliset järjestelyt. Helsinki: Huoltovarmuuskeskuksen julkaisuja.

Valkoinen talo (the White House) 2011. The National Strategy to Secure Cyberspace.

Valtiovarainministeriö 2006. Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2008. Helsinki: VM-julkaisutiimi.

Valtiovarainministeriö 2009. Kohdistetut hyökkäykset, VAHTI 6/2009. Helsinki:

VM-julkaisutiimi.

Valtiovarainministeriö 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010. Helsinki: VM-julkaisutiimi.

Viestintävirasto 2010. Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje. Helsinki: Viestintävirasto.

Yhdysvaltojen puolustusministeriö (Department of Defense) 2011. Strategy for Operating in Cyberspace. Yhdysvallat: Department of Defense.

Julkaisemattomat lähteet

Access Data 2006. Rainbow Tables. Sovelluksen käyttöopas. Access Data.

Andersson M. 2006. IPS-järjestelmien tukeminen Netflown avulla. Jyväskylän yliopisto. Jyväskylä. 2006.

Drave, J. 2010. Cracking Passwords. White Paper.

Harju, S. 2008. Ajax sovelluksen suunnittelu ja toteutus. Tampereen ammattikorkeakoulu. Tampere. Opinnäytetyö.

Heinonen, A. 2003. Verkkohyökkäysinformaation keskitetty analysointi. Tekninen korkeakoulu. Espoo. Diplomityö.

Huhtakangas, T. 2011. Tietoturvapäällikkön haastattelu 18.11.2011. Pääesikunta. Helsinki.

Huopana,V. 2011. Puolustusvoimien johtamisrakenteen ja logistiikkastrategian yhteydet. Maanpuolustuskorkeakoulu. Tuusula. Tutkielma.

Lucas, L. & Necesal, L. 2011. Measures for Critical Information Systems protection. International Journal of mathematical models and methods in applied sciences. Artikkeli.

Kuparinen, V. 2010. Huoltovarmuus ja tietoyhteiskunta. Helsinki: Huoltovarmuuskeskuksen julkaisuja.

Laaksonen, J. 2010. Kotikäyttäjän tietoturva. Haaga Helian AMK. Helsinki. Opinnäytetyö.

Lukin, K. 2007. Venäläisten käyttämät tietoverkkosodankäynnin menetelmät. Turun yliopisto. Pro Gradu -tutkielma.

Linden, M. 2012. Identiteetin- ja pääsynhallinta. Tampereen Yliopisto. Luentomateriaali.

Matrosov, A. & Rodionov, & E. Harley, D. & Malcho, J. 2012. Stuxnet under the Microscope. ESET. White Paper.

Mavituna, F. 2008. Deep Blind SQL-Injection. White Paper.

Microsoft 2011. Microsoft Security Intelligence Report 2011. Microsoftin julkaisut.

Nurminen, J. 2002. Password Crackers. Lappeenrannan yliopisto. Lappeenranta. Seminaarityö.

Rajamäki M. 2011. Pätevyysmalli turva-auditoijan tutkintokoulutukselle. Laurea. Espoo. Opinnäytetyö (YAMK).

Salovaara, J. 2007. Korkean käytettävyyden klusterivertailu. Helsingin yliopisto. Helsinki. Pro Gradu -tutkielma.

Sillberg, R. 2008. Tietoverkkoon tunkeutumisen havaitseminen SNORT:in avulla. Satakunnan ammattikorkeakoulu. Pori. Opinnäytetyö.

Spect, M. & Lee, R. Distributed Denial Service Taxonomies of Attacks, Tools and countermeasures. Princeton University. Tutkielma.

Symantec Security Response 2012. Windows rootkit overview. White Paper.

Tuominen, T. 2005. WLAN Tietoturva. Tampereen ammattikorkeakoulu. Tampere. Opinnäytetyö.

Sähköiset lähteet

Antivirus Ware 2011. History of computer viruses. Viitattu 12.11.2011. http://www.antivirusware.com/articles/history-computer-viruses.htm

Berglund, N. 2011. Military fends off major cyber attack. Viitattu 20.9.2011 http://www.newsinenglish.no/2011/05/19/military-fends-off-major-cyber-attack/

Broad, Markoff, Sanger 2011. Stuxnet. Viitattu 22.2.2012. http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html

Burns J. 2010. Hackers attact those seen as Wikileaks enemies. Viitattu 22.11.2011. http://www.nytimes.com/2010/12/09/world/09wiki.html?_r=1

CERT.FI 2011. Tietoturvakatsaus 3/2011. Viitattu 27.1.2012.
http://www.cert.fi/katsaukset/2011/tietoturvakatsaus3b2011.html

CERT.FI 2012. Vuosikatsaus 2011. Viitattu 5.2.2012
http://www.cert.fi/attachments/tietoturvakatsaukset/6565qcnq0/CERT-FI_tietoturvakatsaus_4_2011_julkinen.pdf

F-Secure 2011. Computer invaders. Viitattu 4.2.2012.
http://www.fsecure.com/weblog/archives/00002124.html

Försvarets radioanstallt 2011. Försvarets radioanstallt organisation. Viitattu 26.11.2011.
http://www.fra.se/hem.11.html

Guillaumier J. 2012. Is your Website hackable? Viitattu 23.2.2012.
http://www.acunetix.com/websitesecurity/xss.htm

Hansen, T. 2012. Dansk Anonymous Celle: Vi har hacket statsforvaltningen.dk. Viitattu 4.5.2012. http://www.version2.dk/artikel/dansk-anonymous-celle-vi-har-hacket-statsforvaltningendk-44713?

Holmes, D. 2011. Reuters 2011. Viitattu 5.1.2012
http://www.reuters.com/article/2011/12/28/us-trains-security-idUSTRE7BR0C520111228

Huoltovarmuuskeskus 2011. CIIP-käsite. Viitattu 12.11.2011.
http://www.huoltovarmuus.fi/toimialat/tietoyhteiskunta/ciip-kasite/

Huoltovarmuuskeskus 2011b. Huoltovarmuuskeskus. Viitattu 10.11.2011.
http://www.huoltovarmuus.fi/organisaatio/huoltovarmuuskeskus/

Kerkkänen, T. 2011. Armeija palkkaa väkeä kybertaisteluihin. Viitattu 4.12.2011.
http://yle.fi/uutiset/armeija_palkkaa_vakea_kybertaisteluihin/5444616

Kibirkstis, A. 2009. Instrusion Detection FAQ. Viitattu 11.2.2012.
http://www.sans.org/security-resources/idfaq/top-selling-ids-ips.php

Koebler, J. 2012. U.S nukes face up to 10 million attacks daily. Viitattu 12.4.2012.
http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily

Laakso, M. 2012. Jatkuvuus- ja toipumissuunnitelma. Viitattu 9.3.2012.
http://www.tietojesiturvaksi.fi/content/jatkuvuus-ja-toipumissuunnitelma

Linnake T. 2010. Google hyökkääjät saattoivat iskeä yli sataan yritykseen. Viitattu 12.10.2011. http://www.itviikko.fi/tietoturva/2010/03/01/google-hyokkaajat-saattoivat-iskea-yli-sataan-yritykseen/20103034/7

Marsan M. 2008. Morris worm turns 20. Viitattu 25.11.2011.
http://www.networkworld.com/news/2008/103008-morris-worm.html

McGarry, M. 2008. Norbert Wieners Cybernetic Theory and Parental Control. Viitattu 3.9.2011. http://www.colorado.edu/communication/meta-discourses/Papers/App_Papers/McGarry.htm

McGullagh D. 2011. Comodo hacker says he's protesting U.S policy. Viitattu 11.12.2011. http://news.cnet.com/8301-31921_3-20050581-281.html

Mäkelä J. 2012. Verkkojen mukana kaatuu koko yhteiskunta. Viitattu 24.4.2012. http://yle.fi/uutiset/verkkojen_mukana_kaatuu_koko_yhteiskunta/5095956

NetPilot GmbH 2012. Clean Mx Realtime Database. Viitattu 7.2.2012. http://support.clean-mx.de/clean-mx/virusesstats

Newell J. 2012. Estonia to excradite high flying cyber crime suspect to US. Viitattu 12.4.2012. http://au.news.yahoo.com/world/a/-/world/13181609/estonia-to-extradite-high-flying-cyber-crime-suspect-to-us/

Passeri P. 2012. Middle East Cyber War Timeline. Viitattu 4.4.2012. http://hackmageddon.com/tag/hamas/

Pohjonen V. 2011. Keskusrikospoliisi tutkii epäiltyä tietomurtoa. Viitattu 20.12.2011. http://www.sss.fi/uutiset/277415.html

Ragan S. 2011. The military contractors linked to post-RSA attacks. Viitattu 5.2.2012. http://www.thetechherald.com/articles/Three-military-contractors-linked-to-post-RSA-attacks/13697/

Rinta N. 2012. Kyberuhkatutkinto päättyy Jyväskylässä loppusotaan. Viitattu 4.5.2012. http://www.tietoviikko.fi/kaikki_uutiset/kyberuhkatutkinto+paattyy+jyvaskylassa+quotloppusotaanquot/a794007

Schwartz M. 2011. Locheed Martin suffers massive Cyberattack. Viitattu 9.12.2011. http://www.informationweek.com/news/government/security/229700151

Texasin yliopisto 2009. Windows 2003 Server Hardening Checklist. Viitattu 12.3.2012. http://security.utexas.edu/admin/win2003.html

Top Choice Reviews 2009. Types of viruses. Viitattu 27.9.2011. http://antivirus-software.topchoicereviews.com/types-of-viruses.html

Ungerleider 2011. Syria's Facebook Wars. Viitattu 13.12.2012. http://www.fastcompany.com/1752528/syrias-facebook-wars

U.S. Department of Homeland Security 2012. National Cyber Security Division. Viitattu 5.3.2012. http://www.dhs.gov/xabout/structure/editorial_0839.shtm

Vavuz E. 2011. Turkey to mobilize against cyber-terrorism. Viitattu 29.1.2012. http://www.todayszaman.com/newsDetail_getNewsById.action?<newsId=233913http://www.todayszaman.com/newsDetail_getNewsById.action?newsId=233913

Väestörekisterikeskus 2012. Sähköinen henkilöllisyys ja varmenteet. Viitattu 5.2.2012. http://www.vrk.fi/default.aspx?id=134

Vänskä, O. 2012. Tuore laki remonttiin - ”tekisi tietomurtojen tutkinnasta mahdotonta”. Viitattu 15.4.2012. http://www.tietoviikko.fi/kaikki_uutiset/article793656.ece

Whitney L. 2011. Citigroup ups number of accounts breached in attack. Viitattu 10.10.2011 http://news.cnet.com/8301-1009_3-20071622-83/citigroup-ups-number-of-accounts-breached-in-attack/http://news.cnet.com/8301-1009_3-20071622-83/citigroup-ups-number-of-accounts-breached-in-attack/

Yhdysvaltojen ilmavoimat 2010. Construction begins on first cyber warfare intelligence center. Viitattu 3.3.2012. http://www.af.mil/news/story.asp?id=123204543

Yleisradio 2012. Tässä on Suomen Pahin uhkakuva: Viiden minuutin sota. Viitattu 25.3.2012 http://yle.fi/uutiset/tassa_on_suomen_pahin_uhkakuva_viiden_minuutin_sota/5082446

Kuvat

Taulukot