VAASAN YLIOPISTO

Filosofinen tiedekunta

Teknisen viestinnän maisteriohjelma

Piia Holmgren

”Pelkästä tietoturvallisuudesta ei välttämättä enää seuraa kyberturvallisuutta”

Käsiteanalyysi kyberturvallisuudesta

Viestintätieteiden pro gradu -tutkielma

Vaasa 2016

SISÄLLYS

TAULUKOT

VAASAN YLIOPISTO
Filosofinen tiedekunta
Tekijä: Piia Holmgren
Pro gradu -tutkielma: ”Pelkästä tietoturvallisuudesta ei välttämättä enää seuraa kyberturvallisuutta”
Käsiteanalyysi kyberturvallisuudesta
Tutkinto: Filosofian maisteri
Koulutusohjelma: Teknisen viestinnän maisteriohjelma
Oppiaine: Viestintätieteet
Valmistumisvuosi: 2016
Työn ohjaaja: Anita Nuopponen

TIIVISTELMÄ:

Tutkimuksen tavoitteena oli selvittää kyberturvallisuuden alan käsitteistöä ja termistöä. Alan käsitteistö ei ole vielä täysin vakiintunutta, jonka vuoksi joillekin käsitteille esiintyy usein eri nimityksiä ja samoja nimityksiä käytetään eri käsitteistä. Tutkimusaineistoksi valittiin suomalaisia alan asiantuntijoiden laatimia tekstejä ja selvityksiä, viranomaisten strategia-asiakirjoja sekä eri tiedotusvälineiden julkaisemia artikkeleita vuosilta 2013–2016. Tutkimusmenetelmänä oli käsiteanalyysi, jonka avulla aineistosta etsittiin alan käsitteistöä ja selvitettiin niiden suhdetta kyberturvallisuuden käsitteeseen.

Tutkimuksen ensimmäisessä vaiheessa selvitettiin ero kyberturvallisuuden ja tietoturvallisuuden käsitteiden välillä. Kyberturvallisuudella tarkoitetaan digitaalisen maailman turvallisuutta, kun taas tietoturvallisuus on kaiken tiedon turvaamista. Tämän jälkeen tutkimuksessa selvitettiin, millaisia käsitteitä kyberturvallisuuteen liittyy. Kyberturvallisuuteen liittyvät käsitteet jaettiin kybermaailmaan, toimijoihin, kyberuhkiin ja kyberturvallisuusstrategian käsitteiden alle. Tutkimuksen lopputuloksena koostettiin alan käsitteistöstä yhtenäinen graafinen esitys, jossa käsitteiden väliset suhteet on eriteltynä.

Tutkimuksessa selvisi myös, että kyberturvallisuuden alan käsitteistö ja termistö on muodostunut eri erikoisalojen, kuten internetkulttuurin, viranomaisten ja poliisien, käytössä olevista käsitteistä ja termeistä. Tämän vuoksi esimerkiksi tiedotusvälineissä käsitteistä saatetaan käyttää erilaisia nimityksiä. Tutkimuksen teon aikana vuosina 2013–2016 kyberturvallisuuteen liittyvien käsitteiden käyttö on kuitenkin lisääntynyt sekä osa käsitteistä ja termeistä ovat vakiintuneet käyttöön. Vakiintumisen myötä alan käsitteistö ja termistö tulevat yhtenäistymään.

AVAINSANAT: kyberturvallisuus, käsiteanalyysi, tietoturvallisuus, terminologia, kyber, tietoyhteiskunta, internet

1 JOHDANTO

Internet on osa jokapäiväistä elämää 2010-luvulla. Sosiaalisessa mediassa vaihdetaan kuulumisia ja mielipiteitä niin läheisten kuin tuntemattomien anonyymien kanssa. Internetissä hoidetaan myös pankkiasiat, opiskelut ja ostokset. Internetin kaupallistamisen myötä 1990-luvulla tuli jokaisen saavutettavaksi. Suomesta tuli 1990-luvulla informaatio- eli tietoyhteiskunta, jolla tarkoitetaan tietoon ja sähköisiin järjestelmiin keskittynyttä yhteiskuntarakennetta. Yhteiskuntien siirtyminen entistä enemmän verkkoon on luonut tarpeen kiinnittää huomiota tiedon ja tietojärjestelmien turvallisuuteen.

Tiedon turvallisuus on siis yksi keskeinen ilmiö nyky-yhteiskunnassa. Suomen ja samalla Euroopan ensimmäinen tietoturvastrategia julkaisiin vuonna 2003 ja sitä päivitettiin viimeksi vuonna 2008. Sen tarkoitukseksi määriteltiin turvallisen arjen luominen tietoyhteiskunnassa, jossa tiedon luottamuksellisuus, eheys ja käytettävyys ovat tärkeässä roolissa. (Tietoturvastrategia 2008: 5) Tietoturvastrategian hyväksymisen jälkeen Suomi on siirtynyt entistä enemmän internetiin, minkä vuoksi yhteiskunnan turvallisuusstrategian yhdeksi kehittämiskohdaksi on luotu erillinen kyberturvallisuusstrategia, joka hyväksyttiin vuonna 2013. Kyberturvallisuusstrategialla tarkoitetaan strategiaa, jolla pyritään digitalisoituneen ympäristön turvallisuuteen.

Tietoturvaan ja tietovuotoihin on alettu kiinnittämään enemmän huomiota sen jälkeen, kun WikiLeaks julkaisi joulukuussa 2007 Yhdysvaltojen armeijan sisäisen 238-sivuisen toimintaohjeen Guantanamon vankileirille. 2010-luvun alun tietovuodot saivat aikaan maailmanlaajuisen kohun, jonka seurauksena internetissä tapahtuva vakoilu ja urkinta ovat puhututtaneet myös Suomessa. Kyberturvallisuuden merkitys on valtioiden tasolla kasvanut niin, että vuonna 2016 Ison-Britannian tiedustelu- ja turvallisuuspalvelu GCHQ järjestää palkallisia kursseja kybertaitojen kehittämiseksi ja kyberuhkien taistelua vastaan (TiVi 2016).

Poliittiset päättäjät ja yhteiskuntien turvallisuusviranomaiset ovat siis havahtuneet digitalisoituneeseen yhteiskuntaan. Pahimmillaan poikkeusolosuhteissa yhteiskunta

lamautui kokonaan, sillä tietoyhteiskunnan toiminnot ovat siirtyneet tietoverkkoihin. Vaikka digitalisoitunut maailma onkin avannut mahdollisuuksia, vahva riippuvuus sen toimivuudesta tarkoittaa myös sitä, että yhteiskuntien ja yritysten toimintaa voidaan hankaloittaa vaikuttamalla sähköisiin järjestelmiin. (Limnéll ym. 2014: 20)

Tietovuotojen ohella myös murrot tietojärjestelmiin ovat viime vuosina pysyneet päivittäisen keskustelun aiheena. Esimerkiksi Helsingin Sanomien internetsivujen arkistossa hakusanalla ”tietomurto” löytyy vuoden 2013 ajalta 44 artikkelia, kun vuodelta 2015 samalla hakusanalla löytyy 63 artikkelia. Tietomurtojen yhteydessä on useimmissa tapauksissa vuodettu käyttäjätietoja internetiin, jossa niitä voidaan käyttää väärin.

Samalla arkistohaulla tulee kiinnittäneeksi käsitteistöön ja termeihin huomiota. Hakusanalla ”tietomurto” löytyy otsikoita, joissa on käytetty termejä *kyberrikollisuus*, *verkkovakoilu*, *tietomurtosarja* ja *hakkerit*, jotka liittyvät jollakin tasolla tietomurtoon. Miten nämä termit sitten liittyvät tietomurtoihin ja ennen kaikkea mitä näillä termeillä tarkoitetaan? Yhdistävänä käsitteenä näille on kyberturvallisuus. Tarvetta alan termien ja käsitteiden tarkemmalle tarkastelulle ja määritelmille olisi. Sanastokeskus TSK julkaisi vuonna 2014 kokonaisturvallisuuden sanaston, jossa ei kuitenkaan otettu tarkemmin kantaa juuri kyberturvallisuuden käsitteistölle.

1.1 Tutkimuksen tavoite

Tutkimukseni tavoitteena on selvittää ja määritellä kyberturvallisuuteen kuuluvaa käsitteistöä. Käytän tutkimuksessani termiä *kyberturvallisuus* kuvastamaan verkon turvallisuutta. Kyberturvallisuudesta ja siihen liittyvistä käsitteistä käytetään erilaisia termejä lähteestä riippuen. Alan käsitteistö ei ole täysin vakiintunutta, joten pyrin selventämään alan käsitteistöä ja laatimaan yhtenäisen käsitejärjestelmän. Käsitejärjestelmän avulla määrittelen ja nimeän kyberturvallisuuden käsitteistöä. Tutkimukseni jakautuu seuraaviin tutkimuskysymyksiin:

1) Mitä kyberturvallisuus on?

Tutkimukseni keskeisin käsite on kyberturvallisuus, joka on vielä vakiintumaton sisällöltään ja siitä käytettävien termien osalta. Selvitän ensimmäisessä vaiheessa yeisellä tasolla sitä, mitä kyberturvallisuus on ja miten se eroaa tietoturvallisuudesta. Näin voin tehdä selkeän rajauksen siitä, mitä kyberturvallisuuden käsitteen alaan kuuluu.

2) Mitä lähikäsitteitä kyberturvallisuuteen liittyy?

Kyberturvallisuuteen liittyy monia eri käsitteitä, jotka esiintyvät pääkäsitteen tavoin ajankohtaisessa keskustelussa. Esimerkkinä tällaisesta käsitteestä on *verkkoturvallisuus*. Pyrin selvittämään näiden käsitepiirteitä, jotta voin vertailla käsitteitä keskenään. Tarkastelen käsitteiden eroja ja yhtäläisyyksiä, jonka jälkeen erottelen ja yhdistän eri termit samaan käsitteeseen.

Tutkimukseni lopputuloksena on ehdotukseni määritelmiksi kyberturvallisuudelle ja sen lähikäsitteille. Esitän ehdotukseni kyberturvallisuuden käsitteistöstä graafisen esityksen avulla.

1.2 Tutkimusaineisto

Tutkimusaineistona käytän Suomen kyberturvallisuusstrategiaa vuodelta 2013, Suomen tietoruvastrategiaa (2008), tiivistä tietoturvasanastoa (2004), kokonaisturvallisuuden sanastoa (2014), Limnéllin ym. (2014) Kyberturvallisuus-kirjaa, periaatepäätöksiä ja toimeenpano-ohjelmia sekä eri tiedotusvälineistä, joista tärkeimpänä lähteenä käytän Helsingin Sanomien verkkoarkistoa. Valitsemani aineisto edustaa kolmea erilaista alaa: valtionhallintoa, ammattilaisten laatimaa sanastoa sekä tiedotusvälineitä, jonka kautta käsitteet ja termit leviävät yleiseen käyttöön.

Suomen kyberturvallisuusstrategia on turvallisuuskomitean laatima ja valtioneuvoston periaatepäätöksellä 24.1.2013 hyväksymä strategia Suomen kyberturvallisuuden parantamisesta ja kehittämisestä. Kyberturvallisuusstrategia on osa yhteiskunnan turvallisuusstrategian toimeenpanosuunnitelmaa. Toimeenpanosuunnitelmalla tarkoitetaan sellaisia sovittuja toimintatapoja, joiden avulla kyberturvallisuusstrategiaan sitoutuneet toimijat, esimerkiksi valtion virastot, pyrkivät kohti kyberturvallista olotilaa. Strategialla kuvatavaan Suomen kybeturvallisuuden visio eli se, millaiseen kyberturvallisuuden tilaan Suomen tulisi pyrkiä, toimintamalli kyberturvallisuuden saavuttamiseksi sekä strategiset linjaukset eli millaisia hankkeita tai muita toimintatapoja sovelletaan kyberturvallisuuteen. Tämän lisäksi valtioneuvoston kanslia laatii erillisen toimeenpano-ohjelman, jossa määritellään toimintatavat, joiden avulla eri hallinnonalat voivat lähteä toteuttamaan kyberturvallisuusstrategiaa. (Kyberturvallisuusstrategia 2013: 2) Viittaan tutkimuksessani aineistoon nimellä *Kyberturvallisuusstrategia 2013*.

Viimeisin kansallinen tietoturvastrategia hyväksyttiin valtioneuvoston päätöksellä vuoona 2008. Tietoturvastrategian avulla on tarkoitus luoda suomalaisille turvallinen arki tietoyhteiskunnassa ja sen visiona on, että suomalaiset voivat luottaa tietojensa turvallisuuteen. Strategian tavoitteena on, että Suomi on tietoturvan edelläkävijänä maailmassa vuonna 2015. (Liikenne- ja viestintäministeriö 2008: 1) Viittaan tutkimuksessani tähän aineistoon nimellä *Tietoturvastrategia 2008.*

Tiivis tietoturvasanasto on Sanastokeskus TSK:n vuonna 2004 julkaisema sanasto tietoturvallisuuden käsitteistä. Sanastossa on koottu termitietueina ja käsitekaavioina 80 tietoturvallisuuteen liittyvää käsitettä. (Sanastokeskus 2004: 3) Koska tietoturvasanasto on ehtinyt 10 vuoden ikään, aineiston käsitteet ovat saattaneet muuttua. Tutkimuksessani käytän aineistosta nimeä *Tietoturvasanasto 2004*.

Näiden lisäksi käytän aineistona eri tiedotusvälineistä poimimiani uutisia ja artikkeleita. Aineistooni kuuluvat artikkelit valitsen vuosien 2013-2016 väliltä. Pääosa tutkimusaineistostani on kerätty Helsingin Sanomien verkkosivuilta. Muiden

tiedotusvälineiden artikkelit ja uutiset olen valinnut siten, että ne täydentävät Helsingin Sanomista artikkeleita.

1.3 Tutkimusmenetelmä ja tutkimuksen eteneminen

Käytän tutkimuksessani terminologisia menetelmiä, joista pääasiallisena käytän systemaattista käsiteanalyysiä ja terminmuodostuksen analyysia. Tutkimuksessani hyödynnän esittämää systemaattista käsiteanalyysiä, joka on yhdistelmä erilaisia terminologisia työkaluja (kts. esim. Nuopponen 2003). Kerron tarkemmin käyttämistäni tutkimusmenetelmistä alaluvussa 1.4. Tutkimuksessani käsiteanalyysi nivoutuu yhteen taustoitus- ja analyysiosien kanssa, jonka vuoksi taustoitus ja analyysi kulkevat rinnakkain tutkimukseni läpi eikä tutkimustani ole jaettu erillisiin taustoitus- ja analyysilukuihin.

Ensiksi määrittelen kyberturvallisuuden käsitteen aineistojen avulla (luku 2). Taustoitan kyberturvallisuuteen liittyviä ilmiöitä eli tietoyhteiskuntaa, internetin historiaa sekä tietoturvallisuutta. Kun olen taustoittanut kyberturvallisuuteen liittyvät ilmiöt ja lähikäsitteet, käyn läpi lähdeaineiston perusteella, millaisia määritelmiä kyberturvallisuuteen liittyy ja millaisia käsitepiirteitä kyberturvallisuus sisältää. Tämän jälkeen vertaan kyberturvallisuuden ja tietoturvallisuuden käsitteitä ja käsitepiirteitä, jonka perusteella annan oman määritelmäni kyberturvallisuudelle ja tietoturvallisuudelle.

Määriteltyäni kyberturvallisuuden käsitteen kartoitan siihen liittyvää käsitteistöä lähdeaineistoni perusteella (luku 3). Jaan kyberturvallisuuden käsitteen neljään osaan: kybermaailmaan (luku 3.1), toimijoihin (luku 3.2), kyberuhkiin (luku 4) ja kyberturvallisuusstrategiaan (luku 5). Selvitettyäni kyberturvallisuuteen liittyvän käsitteistön, muodostan yhteenvedon kyberturvallisuuden käsitteistöstä ja termistöstä (luku 6). Tutkimukseni lopputuloksena on ehdotukseni kyberturvallisuuden alan käsitteistöstä, jonka esitän graafisesti.

1.4 Terminologinen tutkimus

Tässä luvussa kerron tarkemmin tutkimusmenetelmistäni. Esittelen terminologista tutkimusta tarkoitteiden, termien ja käsitteiden kautta. Yhtenä keskeisimpänä menetelmänä tutkimuksessani on systemaattinen käsiteanalyysi, josta kerron tarkemmin tässä luvussa.

1.4.1 Tarkoite, termi ja käsite

Terminologisessa tutkimuksessa keskitytään kolmeen peruselementtiin: tarkoitteisiin, käsitteisiin ja termeihin. Terminologian tutkimuksessa lähtökohtana näistä kolmesta on kuitenkin käsite ja sen analysointi. (Sanastotyön käsikirja 1988: 25)

Tarkoitteet voivat olla joko konkreettisia, kuten ihmiset ja eläimet tai abstrakteja, kuten ominaisuuksia tai prosesseja (Sanastotyön käsikirja 1988: 24). Terminologian sanasto (2006: 10) määrittelee tarkoitteen sellaiseksi olioksi, joka voidaan osoittaa, käsittää tai kuvitella ja joka vastaa jotakin käsitettä. Tällainen esimerkki tarkoitteesta voisi olla se ilmiö, jota kutsutaan kyberturvallisuudeksi.

Käsitteellä tarkoitetaan jostakin asiasta tai esineestä syntyvää mielikuvaa. Käsite on siis tiedon yksikkö, joka muodostuu käsitepiirteiden yhdistelmästä. Käsitteitä käytetään tiedon jäsentämiseen ja ne ovat kielisidonnaisia, joskin yhteiskunta- ja kulttuurierot vaikuttavat erilaiseen käsitejakoon. (Terminologian sanasto 2006: 10) Tutkimani kyberturvallisuuden ala poikkeaa todennäköisesti käsitepiirteiltään toisissa valtioissa ja esimerkiksi englanninkielisestä aineistosta käsitejärjestelmää muodostettaessa lopputulos saattaa olla hyvinkin erilainen. Myös eri ammattikielissä kyberturvallisuuden käsitteistö

Nuopponen ja Pilke (2010: 18) kuvaavat käsitettä mielikuvaksi, jonka intuitiivisesti tunnistetaan liittyvän johonkin esineeseen tai ilmiöön. Sanastotyön käsikirjan (1988: 24) mukaan ihminen muodostaa konkreettisista ja abstrakteista tarkoitteista ajatuskokonaisuuksia, joita kutsutaan käsitteiksi. Sager (1990: 21) puolestaan lähestyy

käsitteitä termien näkökulmasta: Sagerin mukaan käsitteiden tulee tarjota pätevät selitykset terminmuodostusta varten ja tarjota pohja tehokkaammin rakennetuille sanastoille. Käsitettä käsite Sager (1990: 22) ei kuitenkaan määrittele. Käsitteen määritelemiselle löytyy siis monia erilaisia näkökulmia, mutta omassa tutkimuksessani käsite, esimerkiksi kyberturvallisuus, on pikemmin ajatuskokonaisuus tai mielikuva jostakin abstraktista turvallisuuden osa-alueesta.

Käsitteet voidaan jakaa yksilö- ja yleiskäsitteisiin sekä ala- ja yläkäsitteisiin. Yksilökäsite muodostetaan ja nimitetään yhtä tiettyä tarkoitetta, jota ilmaistaan usein erisnimellä, esimerkiksi Tietoturvastrategia 2008. Yleiskäsite syntyy, kun yksilökäsitteiden yhteiset ominaisuudet yhdistetään omaksi abstraktimmaksi käsitteeksi. (Sanastotyön käsikirja 1988: 25-26.) Yleiskäsite vastaa kahta tai useampaa tarkoitetta, joilla on yhtenäisiä ominaisuuksia (Terminologian sanasto 2006: 11).

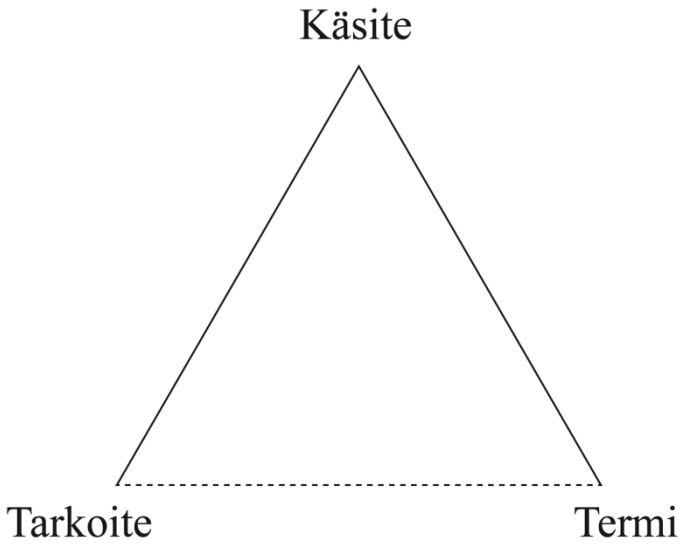
Käsitteet mudostuvat käsitepiirteistä. Käsitepiirteet muodostetaan tarkoitteiden sellaisten ominaisuuksien pohjalta, joita voidaan havaita tai mitata. Käsitepiirteitä käytetään muun muassa käsitteiden luonnehtimiseen, käsitteiden samankaltaisuuden ja erilaisuuden vertailuun sekä termien valinnassa. Omassa analyysissäni käsitteitä erottava tehtävä onkin keskeisessä roolissa. Käsitepiirteet jakautuvat edelleen kahteen luokkaan, sisäisiin ja ulkoisiin käsitepiirteisiin. Sisäiset käsitepiirteet viittaavat tarkoitteissa itsessään havaittuihin ominaisuuksiin, kun taas ulkoiset käsitepiirteet perustuvat tarkoitteiden välisiin suhteisiin, jotka ilmenevät tarkastellessa sitä muihin tarkoitteisiin. Sisäisiä käsitepiirteitä voivat olla esimerkiksi väri, muoto, materiaali ja olomuoto. Ulkoisia käsitepiirteitä ovat suhdepiirteet (esimerkiksi aika), funkiopiirteet (esimekiksi käyttötarkoitus) ja syntypiirteet (esimerkiksi valmistaja). (Sanastotyön käsikirja 1988: 26–27)

Käsitteen määrittelyssä huomioidaan myös käsitteen ala eli ekstensio ja käsitteen sisältö eli intensio, jotka ovat keskenään käänteisessä suhteessa. Käsitteen ala on laajempi kuin käsitteen sisältö eli käsitteen sisältö huomioi vain yksittäistapausten käsitepiirteet. Tämän vuoksi käsitteen määritelmässä tuleekin huomioida vain ne käsitepiirteet, jotka kuuluvat käsitteen alaan. (Kalliokuusi & Seppälä 2014: 11) Esimerkiksi

kyberturvallisuudessa käsitteen alaan lasketaan vain ne käsitepiirteet, jotka kuuluvat jokaisessa tapauksessa kyseiseen käsitteeseen.

Termi on käsitteen kielellinen ilmaus. Käsitteet ovat vain ihmisten mielessä, joten viestinnässä käsitteistä voidaan käyttää vain, jos niille on määritelty termi. Termi ei tarkoita vain yhtä sanaa, vaan termi voi muodostua myös yhdyssanasta, usean sanan sanaliitosta, yksittäisistä kirjaimista, numeroista tai tunnuksista. (Sanastotyön käsikirja 1988: 24; 70)

Sanastotyön käsikirja (1988: 24) esittää pyramidimallin avulla tarkoitteen, käsitteen ja termin suhteita toisiinsa (kuvio 1). Ogdenin ja Richardin kolmiossa kolmion kärjessä oleva käsite sisältää alanurkissa olevista tarkoitteesta ja termistä.



Kuvio 1. Ogdenin ja Richardsin kolmio (Sanastotyön käsikirja 1988: 24)

Kuviossa 1 esiteltyä käsitekolmiota voidaan myös soveltaa käsiteanalyysiin. Nuopponen (2003: 5) kuvaa kuviota 1 kolmelta tasolta: todellisuuden tasolta, käsitteiden tasolta ja ilmaisutasolta. **Todellisuuden tasolla** eli tarkoitteen tasolla tarkastellaan, muokataan ja rakennetaan todellisuutta sekä etsitään ratkaisua jollekin ongelmalle. Käsiteanalyysi onkin kosketus todellisuuteen, jota on tarpeellista jäsentää. **Käsitteiden tasolla**

perehdytään todellisuuteen valmiiden käsitteiden kautta tai jo valmiita käsitteitä muokataan. Tätä kuvaa käsitekolmion kärki, käsitteet**. Ilmaisutasolla** lähtökohtana ovat termit ja teksti. Termien ja tekstien merkitykset ovat lähtökohtana tässä käsiteanalyysin tasossa. (Nuopponen 2003: 5) Tutkimukseni kannalta nämä tasot konkretisoituvat siten, että todellisuuden tasolla jäsentelen vielä vakiintumatonta kyberturvallisuuden käsitteistöä systemaattisen käsiteanalyysin työkalujen avulla. Käsitteiden taso tarkoittaa tutkimuksessani sitä, että selvitän käytössä olevia käsitteitä. Ilmaisutasolla kiinnitän huomiota termeihin: millaisia termejä on käytössä ja kuvaavatko ne ilmiötä.

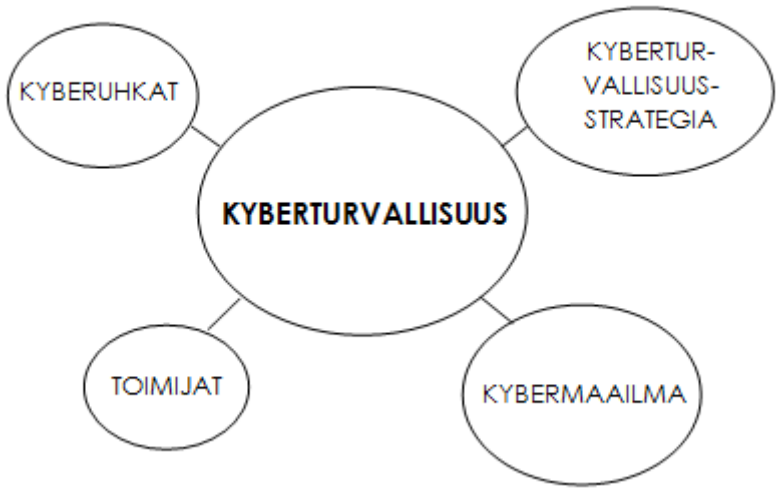
1.4.2 Systemaattinen käsiteanalyysi

Tutkimuksessani sovellan ns. systemaattista käsiteanalyysiä. Systemaattisella käsiteanalyysillä tarkoitetaan menetelmää, jossa alan käsitteistöstä muodostetaan ensin kokonaiskuva, joka selventää alan käsitteiden suhteita toisiinsa. Kokonaiskuva esitetään graafisesti. Tämän jälkeen siirrytään tarkastelemaan pääkäsitteeseen liittyviä ala- ja lähikäsitteitä ja vertailemaan näiden käsitesisältöjä. Lopuksi muodostetaan koko käsitteistöstä yhteneväinen kuva. (Nuopponen 2009)

Käsiteanalyysi voidaan nähdä osana laajempaa terminologista analyysia. Nuopposen ja Pilkkeen (2010: 17) mukaan terminologinen analyysi koostuu käsiteanalyysistä, määritelmien laatimisesta ja termianalyysista. **Käsiteanalyysissä** määritetään käsitepiirteet, selvitetään käsitteiden suhteet ja rakennetaan näiden pohjalta käsitejärjestelmä. Käsiteanalyysi on terminologisista työmenetelmistä tärkein, sillä käsiteanalyysilla saatuja tuloksia käytetään hyväksi esimerkiksi määritelmien kirjoittamisessa ja termien valinnassa (Terminologian sanasto 2006: 6). **Määritelmien laatimisessa** analysoidaan ja koostetaan käsitteitä selventävät käsitepiirteet, valitaan käsitettä kuvaavat käsitepiirteet ja annetaan käsitteelle sisältö. **Termianalyysissä** määritetään käsitteiden ja termien sekä eri termien suhteet, arvioidaan termit ja lopulta muodostetaan termi. (Nuopponen & Pilke 2010: 17) Aion tutkimuksessani käyttää edellä esitettyä mallia terminologisesta analyysistä tutkimuksessani juuri esitetyssä järjestyksessä: ensin teen aineistolleni käsiteanalyysin, jonka jälkeen analysoin

käsitepiirteet ja annan käsitteelle sisällön sekä viimeiseksi valitsen koottujen käsitepiirteitä parhaiten kuvaavan termin.

Käsiteanalyysiä voikin siis kuvailla prosessina, jota jokainen ihminen tekee ajatellessaan (Nuopponen 2003: 1). Koska käsiteanalyysi on osa ihmisen ajattelua, se pitää visualisoida johonkin muotoon. Nuopponen (2011: 5) esittelee yhdeksi tavaksi satelliittimallia. Satelliittimalli on ajatuskartan eli mind mapin kaltainen graafinen esitys käsitteiden keskinäisistä suhteista. Satelliittimallissa keskiöön asetetaan pääkäsite, jonka ympärille voidaan asettaa erilaisia käsitteitä niiden käsitesuhteiden perusteella. Satelliittimallin vahvuutena on sen joustavuus: satelliittimallia on analyysiprosessin edetessä mahdollista laajentaa, muokata ja tarkentaa. (Em. 5) Kuviossa 2 esitän satelliittimallia mukaillen omaa aineistoani:



Kuvio 2. Esimerkki satelliittimallista.

Kuvio 2 on hyvin yksinkertaistettu malli. Satelliittimallissa jokainen käsite linkittyy pääkäsitteeseen käsitteiden välisten suhteiden perusteella. Esimerkissä kyberturvallisuus on keskusnoodi, joka sisältää kaikkien siihen linkittyneiden noodien käsitepiirteet. Linkittyneiden noodien linkitystä kutsutaan käsitesuhteeksi ja käsitesuhteet muodostavat käsitejärjestelmän (Sanastotyön käsikirja 1988: 28). Erilaisia

käsitejärjestelmiä ja käsitesuhteita on useita, mutta omassa tutkimuksessani käytän käsitteiden suhteiden määrittelyyn geneeristä käsitesuhdetta, koostumussuhteista käsitesuhdetta sekä assosiatiivisina funktiosuhteina**.**

Geneerisessä eli hierarkkisessa käsitesuhteessa ylä- ja alakäsitteellä ovat samat käsitepiirteet. Geneerisessä käsitesuhteessa yläkäsitteellä on useita alakäsitteitä ja alakäsitteet ovat toistensa vieruskäsitteitä eli niillä on yhteisten käsitepiirteiden lisäksi jokin erottava lisäpiirre. (Sanastotyön käsikirja 1988: 28) Esimerkiksi tutkimuksessani *murtautujat* ovat yläkäsite, jonka alakäsitteinä ovat *hakkerit* ja *krakkerit*. Molemmilla alakäsitteillä on samat murtautujan käsitepiirteet, mutta niillä on lisäpiirteitä, jotka erottavat vieruskäsitteet toisistaan.

Koostumussuhteissa yläkäsite muodostaa kokonaisuuden, jonka osia alakäsitteet ovat. Niille ei voida määrittää yhtenäisiä kriteerejä kuten geneerisessä käsitesuhteessa. (Sanastotyön käsikirja 1988: 30). Esimerkkinä koostumussuhteisesta käsitejärjestelmästä tutkimuksessani on pääkäsite kyberuhkat, joka jakautuu useampaan eri tyyppiseen kyberuhkaan.

Funktiosuhteissa käsitteillä ei ole yhtenäistä suhdetyyppiä, vaan jokaisella käsitteellä on erilainen suhde pääkäsitteeseen (Sanastotyön käsikirja 1988: 31). Funktiosuhteissa käsitteet liittyvätkin aiheyhteyteen käsitteen tarkoitteiden perusteella (Terminologian sanasto 2006: 17). Suurin osa tutkimukseni käsitesuhteista edustaa funktiosuhteita, sillä pääkäsitteen ja siihen liittyvän käsitteen välille ei ole löydettävissä yhteisiä suhteita, vaan ne liittyvät pääkäsitteeseen asiayhteyden perusteella. Myöskään alan kirjallisuudesta ei löydy nimitystä pääkäsitteeseen suhteessa olevaan käsitteeseen, joten kutsun näitä käsitteitä nimityksellä *lähikäsite*.

2 KYBERTURVALLISUUS

Tässä luvussa pohdin kyberturvallisuutta ilmiönä. Luku jakautuu kyberturvallisuuden määrittelyyn, sen taustoitukseen ja lopuksi teen systemaattisen käsiteanalyysin työkaluja apuna käyttäen analyysin kyberturvallisuuden käsitteistä. Aluksi esittelen ja määrittelen *kyber*-etuliitettä. Tämän jälkeen kerron kyberturvallisuuteen liittyvistä ilmiöistä ja lopuksi määrittelen *kyberturvallisuuden*.

2.1 Kyber-etuliite

Jotta voin ymmärtää kyberturvallisuuden maailmaa, määrittelen ensin kyber-etuliitettä. Sen historia ulottuu 1940-luvun loppuun, jolloin kyberin katsotaan ensiintyvän ensimmäisen kerran Norbert Wienerin teoksessa *Cybernetics: Or Control and Communication in the Animal and the Machine*. Wiener esitti teoksessaan ajatuksen siitä, että tietokoneiden välistä sekä tietokoneen ja ihmisen välistä kommunikaatiota tulisi ymmärtää. Kybernetiikka yhdisti toisiinsa takaisinkytkennän, ihmisten käyttäytymisen ja tiedon muodostaen oman tieteenalansa. Wiener siis loi ajatuksen siitä, että ihminen ja kone voivat kommunkoida sekä toimia yhdessä luonnollisesti. Itse sana *kybernetiikka* juontuu kreikan sanasta *kybernētēs*. (Mindell 2002: 4-5)

Kyber-etuliite nousi esille 1990-luvulla yhteiskunnan siirtyessä yhä enemmän kohti infromaatioyhteiskuntaa, jossa tiedolla ja tiedonvälityksellä on suuri rooli. Erityisesti internetin kehitys toi kyberiä esille. Internetin kehityksen myötä *kyber* viittaa tai on osa tietokoneita, virtuaalitodellisuutta ja internetiä. (Oxford English Dictionaire 2015).

Kyberturvallisuusstrategia 2013 määrittelee kyberin määrittelevästi etuliitteeksi, jonka merkityssisältönä on sähköisen maailman tiedonkäsittely. *Kyber* viittaa tietotekniikkaan, sähköiseen viestintään sekä tieto- ja tietokonejärjestelmiin. (Kyberturvallisuusstrategia 2013: 12) Limnéllin ym. (2014: 29) mukaan *kyberillä* tarkoitetaan digitaalista maailmaa, joka rinnastuu usein kybertoimintaympäristöön ja kyberiä käytetään lähinnä etuliitteenä viittaamaan sähköisen maailman ilmiöihin. Kyber viittaa fyysisen ja digitaalisen maailman rajapintaan, joka on vakiintunut kansainväliseen kielenkäyttöön

(Limnell ym. 2014: 31). Kokonaisturvallisuuden sanastossa (2014: 55) kyber on määriteosa, jonka merkityssisältö liittyy informaation käsittelyyn sähköisessä muodossa ja saakin merkityksensä vasta, kun se esiintyy kokonaisena sanana (esimerkiksi *kyberturvallisuus*).

Kyber-etuliitettä esiintyy siis monissa eri lähteissä eikä sille ole yhtä määritelmää. Kyber-etuliitteen eri määritelmissä yhdistyvät teknologia ja ajatus tilasta tai maailmasta, jossa toimitaan tai joka toimii sähköisesti. Näitä määritemiä yhdistääkin ajatus sähköisestä maailmasta tai tilasta sekä teknologian kehityksestä.

> ***Kyber*** on sähköinen tila, jossa yhdistyy informaatioteknologia ja jossa toimitaan tietoverkkojen välityksellä.

2.2 Tietoturvasta kyberturvallisuuteen

Jotta voin määrittää, mitä kyberturvallisuus on, pohdin myös yhteiskuntaan ja ihmisiin liittyvistä ilmiöistä. Tällaisiksi kyberturvallisuuden alaisiksi ilmiöiksi lasken tietoyhteiskunnan ja sen kehittymisen, internetin sekä tietoturvallisuuden. Katson näiden kuvailevan sitä, millaisessa maailmassa kyberturvallisuus vaikuttaa (**tietoyhteiskunta**), millaisessa ympäristössä kyberturvallisuudesta puhutaan (**internet**) sekä mitä läheisiä teemoja kyberturvallisuuteen liittyy (**tietoturvallisuus**).

2.2.1 Tietoyhteiskunta

2010-luvulla Suomi elää tietoyhteiskunnassa. Tietoyhteiskunta edustaa uudenlaista teollisuusyhteiskunnan jälkeistä vaihetta, jossa tiedolla on suuri merkitys yhteiskunnan toiminnan kannalta. Sitran (1996: 7) raportin mukaan tietoyhteiskunnan määritelmä riippuu tutkijoista ja määritelmä voidaan jakaa informaatioyhteiskuntaan, kommunikaatioyhteiskuntaan, jälkiteolliseen yhteiskuntaan, palveluyhteiskuntaan, asiantuntijayhteiskuntaan, oppimisyhteiskuntaan ja postmoderniin yhteiskuntaan. Näiden perusteella tietoyhteiskunnan määrittelyssä tieto on tärkein asia yhteiskunnassa.

Tieto on tärkeä tuotantovoima ja tavaratuotannosta ollaan siirrytty entistä enemmän tiedon tuottamiseen. Tiedon merkitys taloudessa on myös kasvanut, sillä tieto ja siihen liittyvä infrastruktuuri määräävät ja hallitsevat taloutta. Asiantuntijoiden merkitys yhteiskunnalle on kasvanut ja oppimiskyky on kriittinen kyky tietoyhteiskunnassa selviytymiseen. (Sitra 1996: 7) Tieto onkin merkittävässä osassa nykyistä yhteiskuntaa.

Kehitys teollisesta yhteiskunnasta tietoyhteiskunnaksi ei ole vain suomalainen ilmiö, vaan tietoyhteiskuntakehitystä tapahtuu maailmanlaajuisesti. Suomessa tietoyhteiskunnan kehittämisen suuntaviivat ovat luotu 1990-luvulla, jolloin valtiovarainministeriö julkaisi vuonna 1996 kansalliset linjaukset Suomen kehittämisestä tietoyhteiskunnaksi. Samana vuonna Suomen itsenäisyyden juhlarahasto Sitra julkaisi raporttinsa tietoyhteiskunnan sosiaalisista ja yhteiskunnallisista vaikutuksista sekä vuonna 1998 raportin tietoyhteiskunnan strategisen kehittämisen lähtökohdista. (Sitra 1996: 7)

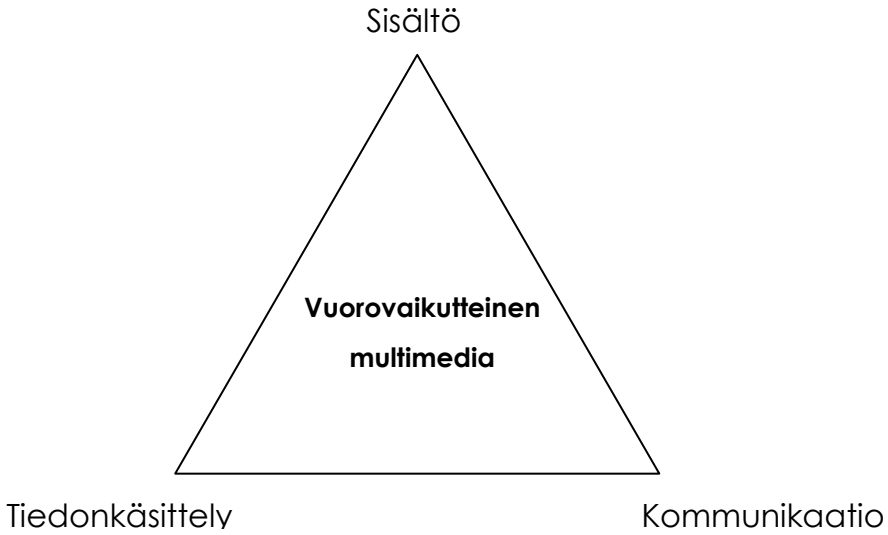
Websterin (2014: 10) mukaan tietoyhteiskuntaa voidaan tarkastella seuraavan viiden kriteerin avulla: teknologia, talous, työelämä, välimatkat ja kulttuuri. Nostan näistä tarkasteluun tutkimukseni kannalta tärkeimmän ilmiön, joka on teknologiat.

Uudet teknologiat ovat paras indikaattori tietoyhteiskunnasta, sillä uusilla teknologisilla innovaatioilla tulee olemaan suuri vaikutus ihmisten sosiaaliseen elämään (Webster 2014: 11). 2010-luvulla uudet teknologiset ratkaisut ovat vaikuttaneet erityisesti ihmisten kommunikaatioon, josta kertoo Facebookin, WhatsAppin, Instagramin ja keskustelufoorumien suosio. Webster jakaa teknologian kehityksen kolmeen aikakauteen.

Ensimmäinen aikakausi 1970-luvun lopulla ja kesti 1980-luvun alkuun. Tällöin uskottiin ”ihmeellisten mikrojen” (eng. *mighty micro's*) eli tietokoneiden muuttavan merkittävästi ihmisten tapaa elää. Toisen aikakauden katsotaan alkaneen 1990-luvun puolivälissä ja kesti vuoteen 2005 saakka, jolloin uskottiin tiedo- ja viestintäteknologian yhdistymisen johtavan uudenlaiseen yhteisöllisyyteen. Tyypillisiä uuden viestintäteknologian tuotoksia olivat tekstiviestit ja tietokoneen välityksellä viestiminen esimerkiksi sähköpostien muodossa. Toisen aikakauden aikana syntyi myös käsite *tiedon valtatiestä* (eng. *information superhighway*), jolla tarkoitetaan tiedon siirtymistä

erilaisiin tietoverkkoihin. Kolmannella aikakaudella sosiaalinen media on keskiössä. Tähän liittyviä teknologisia ilmiöitä ovat esimerkiksi älypuhelimet, taulutietokoneet sekä sosiaalisen median palvelut, kuten Facebook. Avainsanoja kolmannelle aikakaudelle ovat *interaktiivisuus*, *läpinäkyvyys* sekä *joustavuus*. (Webster 2014: 11-12)

Sitran raportin (1996: 8) mukaan tietoyhteiskunnan ytimenä on *vuorovaikutteinen multimedia*. Termi on vuodelta 1996, joka on toki vanha eikä enää yleisesti käytössä. Sen käsitesisältö kuitenkin kuvastaa kuvaamaansa ilmiötä hyvin. Nykyisin samaa ilmiötä kutsutaan *web 2.0*:ksi, joka on vakiintunut kuvastamaan interaktiivista internetiä. Raportissa on kuvattu vuorovaikutteinen multimedia seuraavalla käsitekolmiota muistuttavalla kuviolla:



Kuvio 3. Tietoyhteiskunnan rakenne (Sitra 1996: 8)

Tietoyhteiskunnassa keskiössä on siis Sitran *vuorovaikutteinen multimedia*, joka koostuu sisällöstä, tiedonkäsittelystä sekä kommunikaatiosta. Vuorovaikutteisen median sisältöön kuuluvat tiedon jakelu, julkaisut, mainonta, viihdetuotanto ja tiedon jakelu. Tiedonkäsittelyyn kuuluvat teknologiset välineet eli tietokoneet, ohjelmistot sekä näihin liittyvät palvelut. Kommunikaatiolla tarkoitetaan niitä välineitä, joita kommunikaatiossa tarvitaan: puhelimia, kaapeleita satelliitteja, sekä tv- ja radiolähetyksiin liittyvät laitteistot. (Sitra 1996: 7-8) Koska raportti on vanha, nämä eivät kuvasta kovinkaan

hyvin nykyaikaista tietoyhteiskuntaa. Esimerkiksi kommunikaatiossa nykyisin internet sekä älypuhelimet ovat keskeisemmässä roolissa kuin tv- ja radiolähetykset.

Tästä yhteenvetona määrittelen tietoyhteiskunnan moderniksi yhteiskuntarakenteeksi, jonka piirteinä ovat korostuneet tiedon merkitys, uudet teknologiset innovaatiot sekä internetin tärkeys ihmisten sosiaalisessa kanssakäymisessä.

2.2.2 Internet

Kuten tietoyhteiskunnan määrittelyssä tuli ilmi, tietoyhteiskunnan yksi merkeistä on verkottuminen. Kolmas aikakausi, joka alkoi Websterin (2014: 11-12) määritelmän mukaan vuonna 2005, on entistä enemmän verkossa. Web 2.0 on tuonut erityisesti sosiaalisen median jokapäiväiseen käyttöön niin tietokoneella, kuin älypuhelimilla. Toisin sanoen olemme jatkuvasti saavutettavissa internetin kautta. Kutsun tietokoneita, taulutietokoneita ja älypuhelimia alaluvussa yhteisellä nimellä *päätelaite*, sillä internetiä käytetään erilaisilla laitteilla.

Internet voidaan määritellä itsenäisten verkkojen linkittymäksi, joka näyttäytyy käyttäjälle yhtenäisenä verkkona. Illuusio yhteinäisestä verkosta syntyy standardisoiduista protokollista, joiden avulla käyttäjä liikkuu verkoissa. Toisena tekijänä yhden yhtenäisen verkon illuusiossa ovat verkkoja hoitavat yritykset ja organisaatiot, jotka huolehtivat verkon eri elementtien toiminnasta.

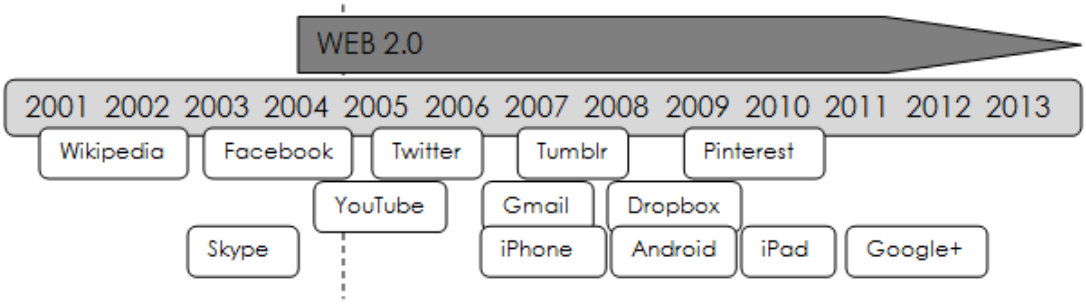
Siitä, mistä internetin historia lähtee, ei ole yhtenäistä käsitystä. Yleisesti internetin historian katsotaan alkavan ARPAnet:stä, jonka julkaisuajankohtana pidetään vuotta 1969. (Peter 2004) Ajatus yhteinäisestä kansallisesta tietoverkosta ulottuu 1950–1960-lukujen kylmään sotaan ja ydinsodan uhkaan Yhdysvalloissa. Silloinen Yhdysvaltojen presidentti J.F. Kennedy halusi ydinsodan kestävän viestintäverkon. (Ryan 2010: 11–13) Siitä, milloin ARPAnet oikeasti perustettiin ja lasketaanko se ensimmäiseksi internetin kaltaiseksi verkoksi, eroaa lähdekirjallisuuden mukaan. Peterin (2004) yhden teorian mukaan ensimmäinen internetiksi laskettava palvelu olisi syntynyt TCI/IP-protokollan myötä vuonna 1978, jolloin otettiin käyttöön ensimmäinen TCI/IPv4-protokolla.

Lasketaan internetin historia sitten ARPAnetistä tai TCI/IP-protokollan käyttöönotosta, kyberturvallisuuden tai peruskäyttäjän kannalta tärkeämpää kertoa HTTP:n ja WWW:stä. Näiden pohjalta on edetty nykyiseen Web 2.0:aan. WWW:n alkuaskelina pidetään Cernissä 1980-luvulla työskennellyttä Tim Berners-Leen sovellusta Enquire. Sovelluksen tarkoituksena oli piirtää yhteyksiä eri ihmisten, ohjelmien ja järjestelmien välillä. Bernes-Lee halusi kehittää hypertekstin ja Xanadun kehittäneen Ted Nelsonin sekä Memexin eli laitteen, joka jäljitti ja yhdisti tietoja tietokorteilta, kehittäneen Vannevar Bushin ideaa eteenpäin. Vuonna 1990 Bernes-Lee aloitti uuden projektin, jonka avulla tutkijat pystyivät vapaasti päättämään tiedostojensa muodosta. Kuvia, tekstiä ja videota kutsuttaisiin yksinkertaisella linkillä. Hypertekstin pohjalta Bernes-Lee kehitti HTML:n, hypertekstin merkkauskielen, joka pohjautui yleisesti käytössä olleeseen SGML-merkkauskieleen. Ensimmäinen HTML-tiedosto luotiin ja katseltiin lokakuussa 1990 ja jouluukuuhun 1990 mennessä Bernes-Lee oli perustanut ensimmäisen palvelimen HTML-tiedostoille sekä kehittänyt ensimmäisen WWW-selaimen tiedostojen tarkasteluun. (Ryans 2010: 105–107)

Internetin suosio kasvoi 1990-luvulla, jolloin ensimmäiset suosituiksi nousseet internet-selaimet julkaistiin. Näistä suosituimmat olivat Netscape Navigator ja Microsoftin ensimmäinen versio Internet Explorer -selaimesta, jonka suosiosta kilpailtiin ”selainten sodassa”. (Ryan 2010: 109) Merkittävä muutos internetin käytössä tuli kuitenkin 2000-luvulla, kun O’Reilly julkaisi käsitteen Web 2.0:sta. (O’Reilly 2005) Siinä, missä aiemmassa versiossa käyttäjillä oli mahdollista ainoastaan lukea ja selata julkaistuja HTML-tiedostoja, Web 2.0 mahdollisti internetin käyttäjien itse osallistua verkossa tiedon luomiseen ja muokkaamiseen. Wikipedia on tästä hyvä esimerkki, joka mahdollisti jo 2000-luvun alussa anonyymien käyttäjien julkaista ja muokata artikkeleita palvelussaan. (Ryan 2010: 137–138)

Internetin muuttuminen mahdollistikin nykyisin käytössä olevien internetpalveluiden synnyn. Tällaisia palveluita ovat jo aiemmin tutkimuksessani mainitut Facebook ja Twitter. Internetin kehittyminen Web 2.0:ksi on tuonut myös kybermaailmaan erilaisia

ilmiöitä. Limnéll ym. (2014: 17) kuvaavat Web 2.0:n kehitystä kuviolla 4. Kuviosta on jätetty pois kyberhyökkäykset.



Kuvio 4. Kybermaailman kehitysaskelia.

Kuvio 4 esittää hyvin sen, miten laajamittainen liiketoiminta ja kaupallistuminen on alkanut vuonna 2005 (Limnéll ym. 2014: 17). Web 2.0:n ja erilaisten sosiaalisen median palveluiden kehittyminen onkin ollut nopeaa. Samoin älylaitteiden kehittyminen näkyy kuviossa, sillä ensimmäinen suosituksi ja jopa ilmiöksi muodostunut iPhone julkaistiin vuonna 2007. Mielestäni kuitenkaan kuvio ei yksiselitteisesti kerro, kuinka kybermaailma on kehittynyt, sillä se keskittyy liiaksi sosiaalisen median eli Web 2.0:n kehitykseen 2000-luvulla. Kuvio 4 kuvastaa kuitenkin hyvin sitä, millaisessa internetissä tavallinen käyttäjä nykyisin viettää aikaansa. Mielestäni internetin kehitys entistä enemmän sosiaaliseksi mediaksi nostaa myös tarvetta ajatella omaa turvallisuuttaan verkossa.

Internet on kehittynyt vuosikymmenten saatossa armeijan tarpeista osaksi ihmisten joka päiväistä elämää. Tietoyhteiskunnassa verkottuminen, tiedon hallinta ja hankinta ovatkin aika pitkälle internetin varassa. Myös kyberturvallisuuden osalta internetillä on tärkeä rooli: kybermaailmalla tarkoitetaan verkossa olevaa ympäristöä ja tässä yhteydessä verkolla tarkoitetaan internetiä.

2.2.3 Tietoturvallisuus

Kyberturvallisuudessa tärkeää on myös tiedon turvallisuus. Jo ennen kybermaailmaan siirtymistä tietoa on pyritty hallitsemaan ja suojaamaan niiltä, jotka eivät ole oikeutettuja tiedon tarkasteluun. Tähän liittyykin käsite tietoturvallisuudesta tai tietoturvasta, jonka ISO/IEC 27000:2009-standardi määrittelee tiedon säilyttämisen luottamuksellisesti, yhtenäisesti ja käytettävästi (ISO/IEC 2009). Myös tietoturvasanasto on samoilla linjoilla määritelmissään: tietoturva on järjestely, jolla pyritään varmistamaan käytettävyys, tiedon eheys ja luottamuksellisuus. Tietoturvaan kuuluu myös aineistojen, laitteiden ja järjestelmien toiminnan varmistaminen. Sen turvallisuutta voidaan vahvistaa esimerkiksi palomuureilla ja virustorjuntaohjelmilla. (Tiivis tietoturvasanasto 2004: 10) Määritelmät tietoturvallisuudesta ovatkin hyvin teknisiä.

Tietoturvallisuuteen liittyy tiedon salaaminen. Aihetta voidaan kuitenkin tarkastella muistakin perspektiiveistä, kuten erilaisten teknisten järjestelmien näkökulmasta. Yksi tällainen näkökulma on tietojärjestelmien turvallisuus (eng. *information system security*), jonka tarkoituksena on määritellä ja kontrolloida järjestelmää, jotta järjestelmän virhetilanteita voidaan ehkäistä sekä estetään luvattomia tietovuotoja, tiedon muokkaamista ja tuhoamista (Slade 2006: 133). Esimerkiksi monet tunnetuista tietovuodoista, kuten vuonna 2006 perustettu ja 2011 julkisuuteen noussut WikiLeaks, ovat mielestäni hyvä esimerkki tietojärjestelmien tietoturvallisuuden heikkouksista. Muun muassa valtioiden arkaluontoista tietoa vuodettiin tietojärjestelmistä WikiLeaksille ja vuodettujen tiedot julkaistiin. Tietojärjestelmien turvallisuus ei siis ole ainoastaan tekniikkaa kuten määritelmät antavat ymmärtää, vaan tietoturva on myös henkilöistä riippuvaa.

Jos tieto on vuodettavissa, tietoturvallisuuteen on liityttävä erilaisia uhkia. Tietoturvasanasto määrittelee tietoturvauhkat sisäisiin ja ulkoisiin uhkiin. Sisäisiä uhkia ovat yrityksen tai organisaation sisällä olevat henkilöt, joiden toiminta muodostaa uhkan. Ulkoisia uhkia ovat yrityksen tai organisaation ulkopuolella olevat tietoturvaa uhkaavat asiat, kuten virukset. (Tiivis tietoturvasanasto 2004: 13) Esimerkiksi WikiLeaks-tapauksessa tietoturvallisuuteen liittyvät vuodot ovat olleet ennemminkin

sisäisiä uhkia. Iso osa tiedosta on kerätty hyvin todennäköisesti organisaatioiden sisältä, jolloin sisäiset uhkat ovat olleet näille organisaatioille suuremmat. Saattaa olla, että tietovuotojen kohteeksi joutuneet organisaatiot ovat varautuneet liiaksi ulkosiin uhkiin, jolloin sisäisiin uhkiin ei ole kiinnitetty riittävästi huomiota.

2.3 Kyberturvallisuuden käsitteen määrittely

Edellisessä alaluvussa tekemäni määritelmä kyberturvallisuudesta ei kuitenkaan riitä määrittämään kyber turvallisuuden käsitettä. Seuraavassa pohdin vielä käsitettä *kyberturvallisuus* lähdeaineiston määritelmien avulla.

Kyberturvallisuusstrategia 2013 määrittelee **kyberturvallisuuden** tavoitetilaksi, jossa *kybertoimintaympäristöön* voidaan luottaa ja se voidaan turvata (Kyberturvallisuusstrategia 2013: 13). Jotta tämä määritelmä avautuisi, *kybertoimintaympäristö* pitäisi myös määritellä. Kyberturvallisuusstrategian 2013 mukaan kybertoimintaympäristö on tiedon käsittelyyn tarkoitettu tietojärjestelmien muodostama toimintaympäristö (Kyberturvallisuusstrategia 2013: 12). Limnéllin ym. (2014: 39) määritelmä kyberturvallisuudesta onkin seuraava:

> ”Kyberturvallisuus tarkoittaa digitaalisen maailman tilaa, jossa vallitsee sekä ymmärryksen myötä tuotettu luottamuksen tunne että käytännön toimenpitein saavutettu kyky ennakoivasti hallita sekä sietää kyberuhkia ja niiden vaikutuksia.”

Limnéll ym. (2014: 39) puhuvat myös kyberturvallisuuden popularisoinnista, jonka avulla käsite tulisi tutuksi jokaiselle yhteiskunnan jäsenelle. Kuitenkaan tämä ei näytä vielä onnistuneen, sillä muualla kuin asiantuntijoiden keskuudessa puhutaan kyberturvallisuudesta muillakin termeillä.

Aineistossani tiedotusvälineitä edustava Helsingin Sanomat eivät määrittele artikkeleissaan termiä *kyberturvallisuus*. Kuitenkin tällä termillä haettaessa aiheesta löytyy 18 artikkelia vuodelta 2014, mutta niiden perusteella on hankala määritellä, mitä Helsingin Sanomat tarkoittaa kirjoittaessa käyttäessään termiä *kyberturvallisuus*. Tällä hakusanalla löytyvissä artikkeleissa käsitellään *kyberturvallisuusharjoitusta*,

verkkohyökkääjiä ja kyberhyökkäyksiä, kybersotaa, verkkorikollisuutta, kybersuurlähettiläitä ja *kyberpoliiseja sekä verkkotiedustelua.* (HS 2014a) Myös *verkkoturvallisuus*- ja *tietoverkkoturvallisuus*-termeillä hakutulokset ovat samankaltaisia. Helsingin Sanomien määritelmänä *kyberturvallisuudelle* näyttäisi olevan, että se on turvallisuutta, johon sisältyy tietoverkoissa esiintyviä ilmiöitä, kuten kyberhyökkäyksiä tai verkossa toimivia henkilöitä ja asioita.

Rantapelkonen & Salminen (2013: 10-12) eivät anna suoraa määritelmää sille, mitä kyberturvallisuus on. Sen mukaan esimerkiksi *kyberturvallisuuden* käsite on moniulotteinen ja tulkinnanvarainen. *Kyberturvallisuus*-käsitteeseen kuitenkin sisältyvät muun muassa **kyberuhkat**. Se on kuitenkin vain osa armeijan monista haasteista, mutta kyberturvallisuuden haasteet ovat ennemminkin esimerkiksi teknologisia tai sosiaalisia. Kuitenkin kyberturvallisuuteen liittyvien ilmiöiden käsitteitä olisi hyvä määritellä tarkemmin. (Rantapelkonen & Salminen 2013: 10-12)

2.4 Kyberturvallisuuden suhde tietoturvallisuuteen

”Pelkästä tietoturvallisuudesta ei välttämättä enää seuraa kyberturvallisuutta” (Turvallisuuskomitea 2014: 9). Vaikka kyberturvallisuudesta puhutaankin ja asiantuntijoiden keskuudessa aineistostani on huomattavissa yhden termin käyttämistä. Kuitenkin aineistoni perusteella samasta asiasta puhutaan seuraavilla termeillä:

- kyberturvallisuus
- verkkoturvallisuus
- tietoverkkoturvallisuus
- digitaalinen turvallisuus
- tietoturvallisuus

Listassa neljän ensimmäisen käsitteen sisällöt ovat kuitenkin hyvin samansuuntaisia. Kun puhutaan *kyberturvallisuudesta, verkkoturvallisuudesta, tietoverkko-turvallisuudesta* tai *digitaalisesta turvallisuudesta*, tarkoitetaan digitaalisen tilan turvallisuutta. Kyberturvallisuutta käsittelevissä artikeleissa vilahtelee kuitenkin myös termi *tietoturvallisuus* ilman sen tarkempaa määrittelyä siitä, miten tietoturvallisuus liittyy kyberturvallisuuteen.

Tietoturvallisuuden ja kyberturvallisuuden suhdetta käsitejärjestelmässä ei ole kovinkaan helppo määritellä, sillä jako tietoturvallisuuden ja kyberturvallisuuden välillä ei ole kovin selkeä. Tietoturvallisuus on tietoturvan järjestelyä, jolla pyritään varmistamaan tiedon eheys, käytettävyys ja luotettavuus. Siihen kuuluvat ne toimet, joilla voidaan taataan esimerkiksi tietojärjestelmien toiminta. (TSK 2004: 10) Tietoturvallisuuden tavoitteena on siis saada ihmiset ja yritykset luottamaan siihen, että heidän tietonsa pystytään turvaamaan tieto- ja viestintäverkoissa sekä niihin liittyvissä palveluissa (Tietoturvastrategia 2008: 1).

Tietoturvallisuuden ja kyberturvallisuuden käsitteissä on jonkin verran yhtäläisyyksiä. Molemmissa pyritään turvaamaan jonkin turvallisuutta. Tietoturvallisuudessa pyritään siihen, että tieto on turvassa ja luotettavaa. Kyberturvallisuudessa puhutaan ennemminkin sähköisen ympäristön turvaamisesta, jossa tieto ja käyttäjät ovat turvassa ja voivat luottaa turvallisuuteen. Toisaalta tietojärjestelmät toimivat nykyisin verkkoympäristöissä, joka voidaan laskea olevan osa kyberturvallisuutta. Tällöin myös tietomurrot voitaisiin laskea osaksi kyberturvallisuutta. Tietovuodolla tarkoitetaan tunkeutumista tietojärjestelmään tai tietoverkkoon (Kokonaisturvallisuuden sanasto 2014: 16).

Tietoturvallisuuden termistö on aiemmin määritelty vuonna 2004 Tietoturvasanastossa, josta on löydettävissä samankaltaisia termejä kyberturvallisuuden kanssa. Samankaltaisia termejä ovat esimerkiksi tietoverkkorikos, tietoturvauhka, palvelunestohyökkäys, tietomurto, hakkeri ja krakkeri sekä haktivisti. Tutkimuksessani vertailen näitä termejä ja käsitteitä muusta aineistostani löytämiin kyberturvallisuuden termeihin ja käsitteisiin.

Keräsin aineistostani seuraavat käsitepiirteet sekä kyberturvallisuudelle että tietoturvallisuudelle (taulukko 1):

Taulukko 1. Kyberturvallisuuden ja tietoturvallisuuden käsitepiirteet.

Kyberturvallisuus	**Tietoturvallisuus**
Sähköisen maailman turvallisuus	Tiedon turvallisuus
Luottamus turvallisuuteen	Luottamus tiedon turvallisuuteen ja eheyteen
Haasteet teknologisia tai sosiaalisia	
Toimii tieto- ja viestintäverkoissa	Kaikki tiedon säilyttäminen, myös sähköinen
Riskeinä mm. kyberuhkat, kyberhyökkäykset, kyber	Riskeinä mm. tietomurrot, tietovuodot, titoturvauhkat

Käsitepiirteitä tarkastelemalla kyberturvallisuuden alustava määritelmä on seuraava:

> ***Kyberturvallisuus*** *on digitalisoituneen maailman turvallisuutta, jossa sen turvallisuuteen. Kyberturvallisuus sijoittuu tieto- ja viestintäverkkoihin ja sen uhkina ovat muun muassa kyberuhkat, joihin kuuluvat kyberhyökkäykset, kybersodat ja kyberterrorismi.*

Määritelmäni tietoturvallisuudelle on:

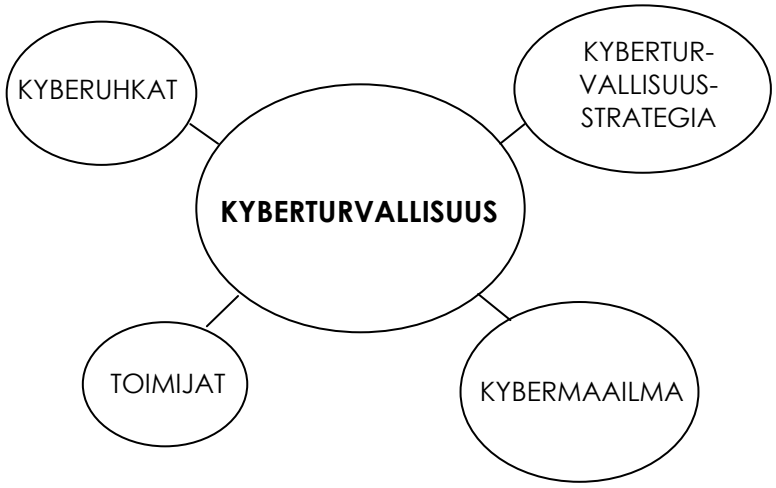
> ***Tietoturvallisuus*** *on tiedon turvallisuutta, jossa tiedon oikeellisuuteen voidaan luottaa ja se voidaan turvata. Tietoturvallisuuden toimintaympäristönä ovat tietojärjestelmät, jotka voivat olla sähköisiä.*

Käsitepiirteitä ja määritelmiä vertailemalla on kuitenkin vaikea päätellä, mikä suhde kyberturvallisuudella ja tietoturvallisuudella. Oma tulkintani käsitteiden suhteista on se, että kyberturvallisuus ja tietoturvallisuus ovat ennemminkin rinnakkaiskäsitteitä ja niillä voi olla samoja alakäsitteitä.

3 KYBERTURVALLISUUDEN KÄSITTEISTÖ

Määrittelin kyberturvallisuuden käsitteen alaluvussa 3.2, jossa totesin kyberturvallisuuden tarkoittavan verkossa tapahtuvaa turvallisuutta. Tässä sekä seuraavassa luvussa selvitän tarkemmin kyberturvallisuuteen liittyviä käsitteitä.

Laadin aineistoni pohjalta seuraavan satelliittimallin, joka havainnollistaa kyberturvallisuuteen liittyviä lähikäsitteitä (kuvio 5).



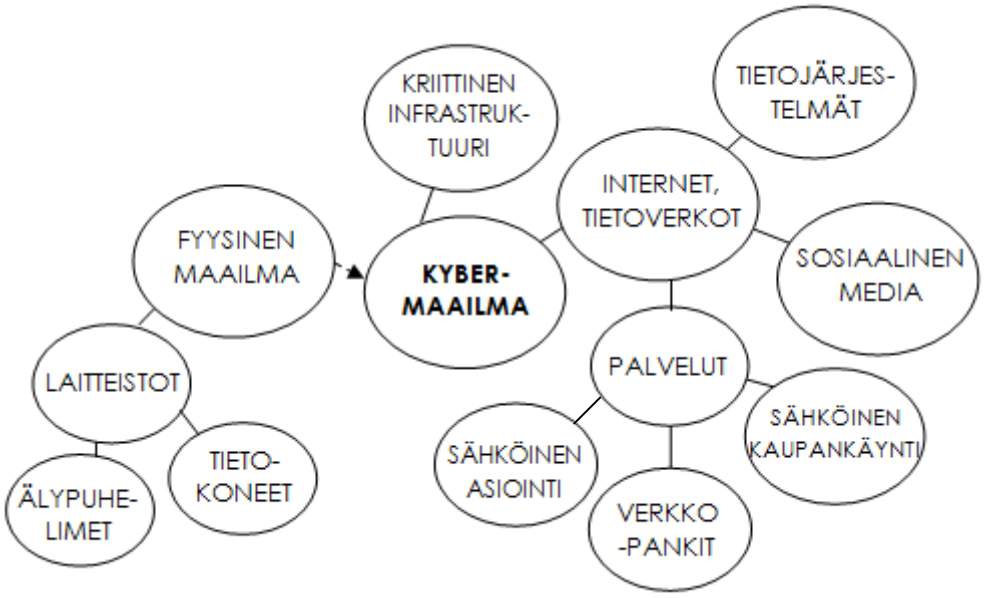
Kuvio 5. Alustava satelliittimalli kyberturvallisuuden käsitteistöstä

Kuten edellä tuli ilmi, kybeturvallisuuden voidaan katsoa olevan osana tietoturvallisuutta. Tutkimuksessani otan tietoturvallisuuden lähikäsitteen mukaan kyberturvallisuuden lähikäsitteiden ja siihen liittyvien käsitteiden vertailuun. Olen kuitenkin jättänyt tästä kuviosta tietoturvallisuuden lähikäsitteen pois, jotta tutkimukseni kannalta satelliittimalli olisi mahdollisimman selkeä.

Alustavaan satelliittimalliin valitsin lähikäsitteiksi kybermaailman, toimijat, kyberuhkat ja kyberturvallissuusstrategian. Jokaisella näistä käsitteistä ona omat ala-, osa- tai lähikäsitteensä, joita selvitän tutkimuksessani seuraavaksi.

3.1 Kybermaailma

Yksi kyberturvallisuuteen liittyvistä keskeisistä käsitteistä on se tila, missä verkossa toimitaan. Lähteestä riippuen siihen voidaan viitata termeillä *kybermaailma*, *kyberturvallinen toimintaympäristö* tai *kybertoimintaympäristö*. Näistä *kybermaailma* kuvaa tätä käsitettä, sillä kaksi edellä esitettyä termiä eivät esimerkiksi kata kyberturvallisuuden toimijoita. *Kybertoimintaympäristö* esiintyy tutkimusaineistossa Kyberturvallisuusstrategiassa 2013, jolloin on luontevampaa käyttää kyseistä termiä strategian yhteydessä.



Kuvio 6. Kybermaailma

Kybermaailma on ei ole ainoastaan läsnä verkossa, sillä yksiselitteistä jakoa fyysisen ja bittien maailman välille ei voida tehdä (Limnéll ym. 2014: 14). Esimerkiksi sodankäynti on siirtynyt verkkoon, jolloin rajanvetoa kybermaailman ja fyysisen maailman välille voi olla vaikea vetää. Tämän perusteella olen laittanut satelliittimalliini myös fyysisen maailman, jonka alle lasketaan kuuluvaksi laitteet, joilla voidaan olla yhteydessä kybermaailmaan. Tällaisia ovat tietokoneet ja älypuhelimet.

Kybermaailmaan kuuluvat laitteistojen lisäksi myös internet ja tietoverkot. Nämä jakautuvat aineistoni perusteella tietojärjestelmiin, sosiaaliseen mediaan sekä sähköisiin

palveluihin, joita voivat olla sähköinen kaupankäynti, verkkopankit ja sähköinen asiointi (esimerkiksi KELA:n asiointipalvelu verkossa).

Kybermaailmasta puhuttaessa aineistossa nousee esille vahvasti **kriittisen infrastruktuurin** käsite. Tällä tarkoitetaan yhteiskunnan tärkempiä toimintoja, joiden avulla jokapäiväinen elämä yhteiskunnassa mahdollistetaan. Esimerkiksi Suomessa kriittiseen infrastruktuuriin kuuluvat yhteiskunnan tekniset perusrakenteet (esimerkiksi joukkoviestintä, tietoliikenne, vesihuolto ja kunnalliset peruspalvelut), kuljetus-, varastointi- ja jakelujärjestelmät, elintarvikehuolto, energiahuolto, sosiaali- ja terveyshuolto sekä sotilaallista maanpuolustusta tukeva tuotanto ja ylläpito. (Hagelstam 2005: 14; 60) Kriittisen infrastruktuurin toiminnot ovat nykyään pitkältä kiinni sähköisissä tietojärjestelmissä, jolloin tämän käsitteen ottaminen mukaan kyberturvallisuuden käsitettä tutkittaessa on välttämätöntä.

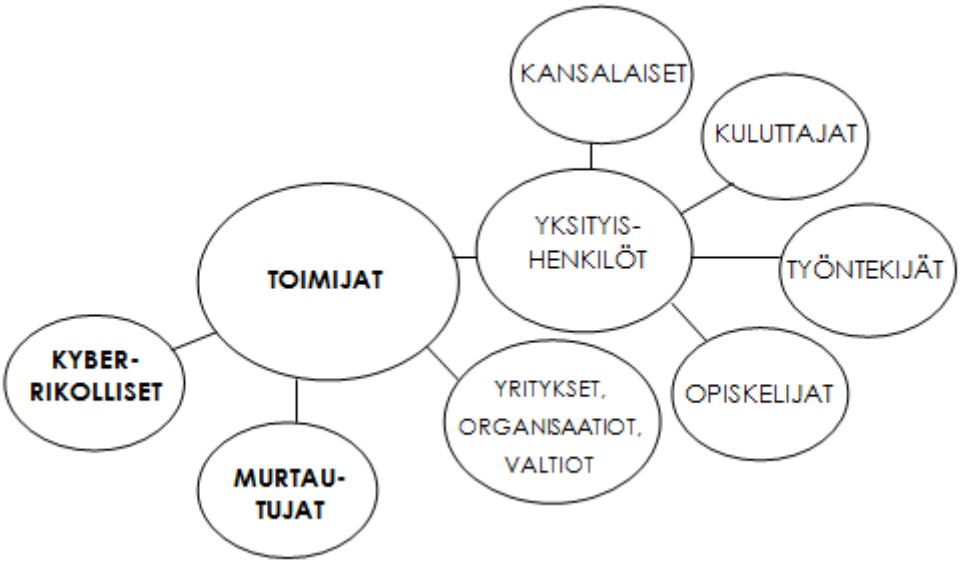
Kokonaisturvallisuuden sanastossa (2014: 55) käytetään kybermaailmasta termiä *kyberympäristö*. Tällä tarkoitetaan yhden tai useamman sähköisessä muodossa olevan informaation käsittelyä niille tarkoitetuista tietojärjestelmistä. Tämä määritelmä rajaa pois muun kybermaailmassa tapahtuvan toiminnan, jonka vuoksi kyberympäristö ei yksinään riitä kuvaamaan digitaalisen maailman ympäristöä.

> ***Kybermaailma*** *on siis digitaalinen ympäristö, jossa tiedon siirto ja käsittely tapahtuu. Kybermaailmaan liittyy sekä fyysisen maailman että digitaalisen ympäristön toimintoja, jolloin se voi toimia myös rajapintana kahden erilaisen tilan välillä.*

3.2 Kybermaailman toimijat

Kybeturvallisuuteen liittyy siis olennaisena osana verkossa toimijat. Näitä toimijoita ovat jokainen verkon käyttäjä. Tarkemmin kybermaailmassa asioivat henkilöt voidaan jakaa sen perusteella, millä asialla he kybermaailmassa ovat. Tähän kuuluvat yksityishenkilöt, valtiolliset toimijat, yritykset ja organisaatiot, murtautujat ja rikolliset. Kyberrikolliset esittelen luvussa 5, sillä kyberrikollisiin liittyy vahvasti **kyberrikollisuuden** käsite ja se saa käsitesisältönsä kyseiseltä käsitteeltä ollen näin

kyberrikollisuuden tekijä. Kuitenkin tässä jaottelussa tulee huomioida, että toimijoita löytyy myös muista kyberturvallisuuteen liittyviä käsitteistä, jolloin ei voida sanoa, että kaikki kybermaailman toimijat ovat jaettavissa esitetysti.



Kuvio 7. Kyberturvallisuuden toimijat.

Kuviossa **yksityishenkilöillä** tarkoitetaan tavallisia käyttäjiä. Kybermaailmassa toimiminen esimerkiksi verkkopankkien, verkkokauppojen ja viestinnän kautta on arkipäivää lähes jokaiselle yksityishenkilölle. Yksilöön vaikuttaa myös välillisesti yhteiskunnan toiminta kybermaailmassa, sillä monet ns. kriittisen infrastruktuurin toiminnot ovat nykyisin sähköisessä ympäristössä. (Limnéll ym. 2014: 49)

Yksityishenkilöt voidaankin siis jakaa sen mukaan, mitä ryhmää he kulloinkin edustavat. Näitä ryhmiä voivat olla kuluttajat, työntekijät, opiskelijat ja kansalaiset. Jokainen yksityishenkilö on siis tilanteen mukaan eri toimijana kybermaailmassa.

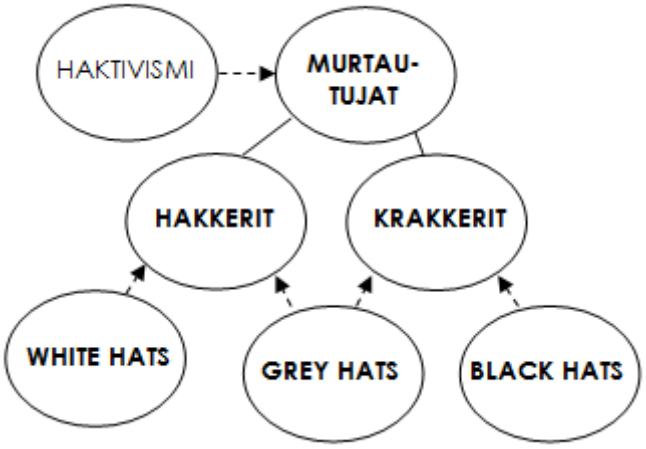
Kybermaailma vaikuttaa yksilöiden viestintään ja yhteydenpitoon. Näihin voidaa laskea sosiaalinen media, sähköposti, pikaviestimet, internetpuhelut sekä muut uudet tekniset ratkaisut. Myös opiskelu on nykyisin mahdollista verkossa sekä kouluun liittyy monia sähköisiä palveluita, kuten sähköiset reissuvihkot, e-kirjat ja e-lehdet. Kuitenkaan kybermaailmaa ei pystytä täysin hyödyntämään opinnoissa, sillä usein

oppilaat ja opiskelijat ovat opettajia edellä tietotekniikkataidoissa (Limnéll ym. 2014: 54).

Limnéll ym. (2014: 50–52) määrittelevät yksityishenkilölle perusperiaatteet, joilla yksityishenkilö voi huolehtia omasta kyberturvallisuudestaan. Nämä perusperiaatteet ovat varmuuskopiointi, salasanat, jotka jakautuvat riittävän vahvoihin ja erilaisiin salasanoihin, epäilyttävien kohteiden (sähköpostilinkkien ja liitteiden) avaamatta jättäminen, epäilyttävien laitteiden kokeilemattomuus, laitteiden suojaaminen, tietojen jakamainen, ohjelmistopäivitykset, sähköpostihuijaukset sekä järkeen ja valppauteen.

3.2.1 Murtautujat

Murtautujat ovat niitä kybermaailman toimijoita, jotka toimivat kybermaailmassa murtautuen tietojärjestelmiin, ohjelmiin tai verkkosivuille. Heitä erottavat tarkoitusperät, jotka voivat olla laillisia, laittomia tai näiden väliltä. Olen nimennyt nämä murtutujiksi, sillä eri tyyppisille murtautujille ei näyttänyt olevan yhtenäistä nimitystä.



Kuvio 8. Murtautujat

Hakkereilla on lähteestä riippuen eri määritelmiä ja käsitettä käytetään hyvin eri tavoin. *Hakkereilla* (engl. *hacker*) voidaan tarkoittaa henkilöitä, jotka murtautuvat eli hakkeroivat eri tietojärjestelmiin. Hakkeri voi myös tunkeutua tietokoneelle tai sen

ulkopuolelta. (Limnéll ym. 2014: 236) Toisaalta Rouskun (2001) mukaan hakkereiksi ei pitäisi kutsua niitä henkilöitä, jotka murtautuvat tietojärjestelmiin. Tutkimusaineiston pohjalta vaikuttaa siltä, että hakkerin käsitesisältöön kuuluu nimenomaisesti tietojärjestelmään murtautuminen, jolloin hakkerien toimintaan tarkoitusperistä huolimatta kuuluu tietojärjestelmään murtautuminen eli *hakkerointi*.

Järjestelmään murtauduttaessa murtautuja pääsee tarkastelemaan sen sisältämää tietoa ja halutessaan muuttamaan, kopioimaan tai poistamaan sen sisältämää tietoa. *Hakkerointi* mahdollistaa myös laittoman käytön esimerkiksi oman propagandan levittämiseen. (Limnéll ym. 2014: 236) Murtautuja tunkeutuu siis tietoverkkoon tai -järjestelmään luvattomasti. Murtautuja saattaa käyttää tietojärjestelmiä käyttöoikeuden vastaiseksi. Käytössä on myös termi *krakkeri* (engl. *cracker*) tällaiselle murtautujalle, joka käyttää näitä oikeuksia väärin. (Tiivis tietoturvasanasto 2004: 16) Vaikka nykyisin *hakkeri* ja *krakkeri* vaikuttavat olevan synonyymeja keskenään, näiden käsitesisältö eroaa toisistaan juuri tarkoitusperien perusteella. Puhuttaessa murtautujista olisikin hyvä tehdä selkeämpi ero sille, kenestä käytetään nimitystä *hakkeri* ja *krakkeri*.

Murtautujat voidaan kuitenkin jakaa heidän tarkoitusperien mukaan omiin kategorioihinsa. Tällaisia jaotteluja ovat *white hats* (valkohatut) ja *black hats* (mustahatut), toisaalta eri tarkoitusperien mukaan hakkereita voidaan kutsua joko *hakkereiksi* tai *krakkereiksi*. *White hatilla* ja *hakkereilla* viitataan sellaisiin toimijoihin, joiden toiminta ei tähtää rikolliseen tai laittomuuksiin. Heidän toimintaansa voidaan myös kutsua *eettiseksi hakkeroinniksi*, jonka tavoitteena on testata järjestelmien kriittisiä vikoja ja raportoida niistä eteenpäin. (Limnéll ym 2014: 236; Saarelainen 2013: 22–24)

Tietomurtoihin tai muihin rikolliseen toimintaan erikoistuneita hakkereita tulisikin kutsua *krakkereiksi* tai *black hateiksi*. Näiden välimaastoon sijoittuu ns. *grey hat* -hakkerit, jotka toimivat laillisen ja laittoman toiminnan välimaastosssa. (Limnéll ym. 2014: 236) Toisin kuin hakkeri, krakkeri käyttää osaamistaan tietomurtoihin (Rousku 2001). Krakkerien toiminta on näkynyt tiedotusvälineissä. Esimerkiksi lokakuussa 2014 tietomurron tehneet krakkerit yhdysvaltalaiseen pankkiin veivät 83 miljoonan asiakkaan tiedot. (HS 2014b)

Hakkereita ja krakkereita yhdistää käsite *haktivismista*. **Haktivismilla** tarkoitetaan hakkerien poliittista tai sosiaalista toimintaa (Limnéll ym. 2014: 236; HS 2014c). Poliittisessa toiminnassa valtio voi ulkoistaa verkkohyökkäysten teon hakkeriryhmälle ja näin irtisanoutua itse hyökkäyksestä. Toisaalta poliittisessa haktivismissa voidaan myös vastustaa valtion poliittista linjaa. (HS 2014c) Haktivismi onkin eräänlaista aktivismia verkossa, jonka työkaluina käytetään tietojärjestelmiin murtautumista ja murtaudutuissa tietojärjestelmissä tietojen muokkaamista, poistamista tai julkaisemista (Limnéll ym. 2014).

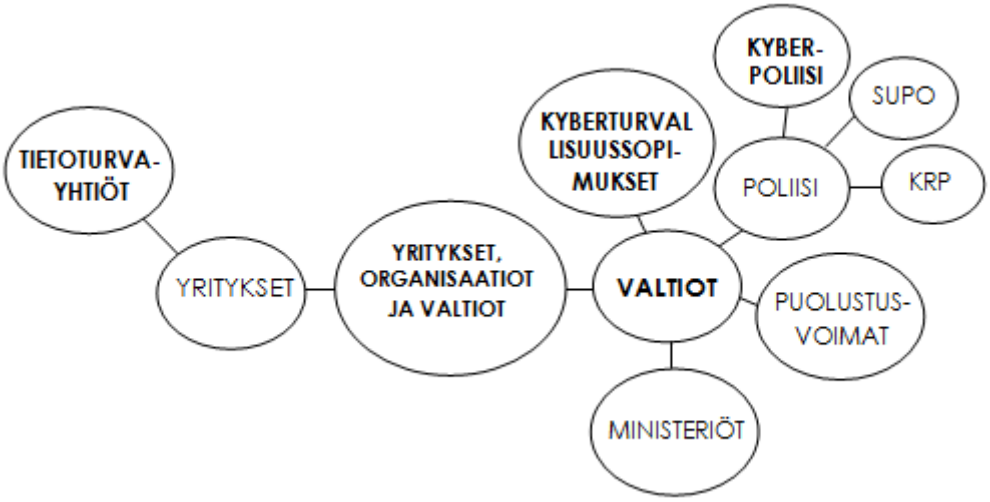
Hakkerit voivat myös jakautua hakkeriryhmiin. Tällaisia ryhmiä ovat esimerkiksi *Anonymous* ja *LulzSec*. Kyseiset ryhmät ovat esimerkiksi murtautuneet organisaatioiden ja yritysten tietojärjestelmiin. (Rantapelkonen & Salminen 2013: 2) Hakkeriryhmät noudattavatkin jonkinlaista haktivismia. Esimerkiksi Anonymous-ryhmää Limnéll ym. (2014: 233) kuvailevat löyhäksi hakkeri- ja aktivismiryhmäksi, joka toimii omien arvojensa ja toimintatapojensa mukaan. Heidän toimintatapojaan ovat hakkerointioperaatiot, kampanjat, tietopaljastukset ja pilailu. (Limnéll ym. 2014: 233)

Käsitepiirteiden perusteella hakkerista ja krakkerista voidaankin tehdä seuraavat määritelmät:

> ***Hakkeri*** *on henkilö, jolla on laaja tietotekninen osaaminen. Hakkeri ei käytä tietoteknistä osaamistaan rikolliseen toimintaan.*
>
> ***Krakkeri*** *on henkilö, joka käyttää tietoteknistä osaamistaan rikolliseen ja laittomaan toimintaan, kuten tietojärjestelmiin murtautumiseen.*

3.2.2 Yritykset ja valtiot

Kybermaailmassa toimii yksityishenkilöiden, *kyberrikollisten* ja murtautujien lisäksi myös valtiot, organisaatiot ja yritykset. Tutkimusaineiston perusteella yritykset, organisaatiot valtiot jakautuvat yrityksiin sekä valtiollisiin toimijoihin (kuvio 9).



Kuvio 9. Yritykset, organisaatiot ja valtiot

Tutkimusaineistossa korostuu valtiot, joiden osuus kybermaailman ja kyberturvallisuuden takaamisessa on yrityksiä ja organisaatioita isommassa roolissa. **Valtiollisten tekijöihin** voidaan laskea ministeriöt, puolustusvoimat ja poliisi. Aineistoni uutisartikkeleissa puhutaan muun muassa *kyberpoliiseista* ja *kybersotilaista*, joilla on valmiudet toimia kybermaailmassa – heillä on siis **kybertaitoja**. Valtioiden sisällä voi olla myös muita yksittäisiä tekijöitä. Esimerkiksi Suomeen on perustettu virka **kybersuurlähettiläälle,** jonka tehtävänä on käydä **kyberdialogia** eli esimerkiksi kyberturvallisuuteen, ihmisoikeuksiin ja internetin hallintoon liittyvää keskustelua niin kansainvälisessä, kuin alueellisesti (IT-Viikko 2014).

Valtioiden välillä voidaan myös tehdä kyberturvallisuussopimuksia, joissa sovitaan **kyberkonflikteihin** liittyvistä suhtautumistavoista. Esimerkiksi Venäjä ja Yhdysvallat ovat solmineet tällaisen sopimuksen (HS 2014d).

Poliisi toimii kybermaailmassa paikallisten poliisien, suojelupoliisin eli SUPOn ja keskusrikospoliisin eli KRP:n välityksellä. Uusimpana toimijana poliisin kentässä ovat suunnitteilla olevat **kyberpoliisit.** Tässä tulee kuitenkin huomata **kyberpoliisin** ja **nettipoliisin** ero, vaikka aineistossani näiden käsitteitä ja termejä ei sekoitetakaan toisiinsa. Aineistossani kuitenkin ilmenee usein *netti*- ja *kyber*-etuliitteiden käyttämistä synonyymeinä. **Nettipoliisi** on Helsingin poliisilaitoksessa toimiva poliisi, jonka

tarkoituksena on näkyä internetissä ja näin pyrkiä ennaltaehkäisemään rikoksia, madaltamaan kynnystä yhteydenottoon sekä puuttua verkossa tapahtuviin rikoksiin (Helsingin poliisi 2015). **Kyberpoliisit** taas ovat kybermaailmaan perehtyneitä poliiseja, jotka tutkivat etenkin vakavaa kyberrikollisuutta verkossa (HS 2014e). Nettipoliisi on siis enemmän esimerkiksi sosiaalisessa mediassa helposti lähestyttävä poliisi, kun taas kyberpoliisi keskittyy verkossa tapahtuviin rikoksiin.

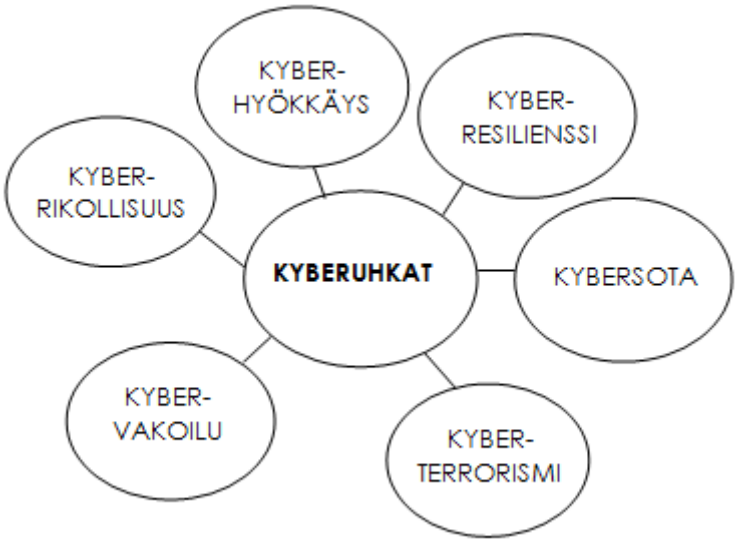
Puolustusvoimien toiminta kybermaailmassa jakautuu kybersotaan ja siihen liittyviin toimiin. Lyhyesti määriteltynä kybersodalla tarkoitetaan sotatoimia kybermaailmassa. Määrittelen kybersodan käsitettä tarkemmin luvussa 5.1. Aineistosta nousee esille myös **kybersotilaan** käsite, mutta varsinaista määritelmää sille, mikä on kybersotilas, ei löydy. Kybersotilaista puhuttaessa viitataan tiedusteluun kybermaailmassa ja kyberhyökkäyksiin. Kybersotilaille opetettaisiin **kybertaitoja** tai heillä olevia kybertaitojaan pyrittäisiin hyödyntämään esimerkiksi asepalveluksessa. (HS 2014f)

Ministeriöiden toiminta kybermaailmassa on lähinnä lainsäädäntöön ja strategioihin liittyvät tehtävät. Ministeriöt ja niiden alaisuudessa toimivat virastot eivät siten ole samalla tavalla toimijoita kybermaailmassa kuin esimerkiksi poliisi toimii.

Myös **yritykset** ovat yhtenä osana kybermaailmaa. Kybermaailmassa yritysten roolina on joko tarjota palveluilta tai suojautua itse kybermaailman vaaroilta. Palveluntarjoajista ovat esimerkiksi tietoturvayhtiöt, kuten maailmanlaajuisesti tunnettu F-Secure, joka tarjoaa palveluita niin yksityiseen kuin muiden yritysten ja organisaatioiden käyttöön (F-Secure 2015).

4 KYBERMAAILMAN UHKAT

Kyberturvallisuuteen liittyy tiiviisti erilaiset uhkat. **Kyberuhkilla** tarkoitetaan niitä uhkia, jotka esiintyvät digitaalisessa ympäristössä ja jotka uhkaavat turvallista toimintaa kybermaailmassa. Tässä luvussa tarkastelen kyberuhkiin liittyviä käsitteitä. Olen jakanut kyberuhkat viiteen erilaiseen uhkaan: **kyberhyökkäyksiin**, **kybersotaan**, **kyberterrorismiin, kybervakoiluun** ja **kyberrikollisuuteen** sekä kyberuhkiin liittyvään sietokykyyn eli **kyberresilienssiin**.



Kuvio 10. Kyberuhkat

Rantapelkosen & Salmelan (2013) mukaan kaikki uhkat eivät liity ainoastaan teknologioihin, vaan kyberuhkat ovat myös sosiaalisia ja humaaneja ja jolloin ne myös vaikuttavat moninaisesti eri maihin, organisaatioihin, yhtiöihin ja yksilöihin. Kyberuhkat eivät siis ole eristäytyneitä muista uhkista, vaan niitä pitäisi tarkastella yhdessä niiden uhkien kanssa, joissa kybermaailmalla on merkittävä rooli. (Em.)

Kyberuhkat kohdistuvat siis yhteiskunnan kannalta kriittisiin kohteisiin. Tällaisiksi kohteiksi voidaan laskea kaikki ns. kriittisen infrastruktuurin kohteet, joita ovat esimerkiksi sähkön-, veden- tai tiedonjakelu. Kriittiset infrastruktuurit ovat siis

sähköisiä tai fyysisiä rakenteita, jotka ovat välttämättömiä yhteiskunnan toiminnalle. (HS 2014f; Kyberturvallisuusstrategia 2013: 12)

Kyberuhkille tulee myös määritellä termit, sillä kuten muissakin käsitteissä on tullut ilmi, termit vaihtelevat jopa saman tekstin sisällä. Esimerkiksi lokakuussa 2014 järjestetyssä Pirkka 14 -harjoituksessa käytettiin termiä tietoverkkouhka, jossa kyberhyökkäyksellä lamautettiin kuntien tietojärjestelmiä ja vaikeuttin kriittisen infrastruktuurin toimintaa. Myös nettihakkeri teki nettihyökkäyksen Valkeakosken ammattiopiston verkkosivuille. (Länsi- ja Sisä-Suomen aluehallintovirasto 2014a; Länsi- ja Sisä-Suomen aluehallintovirasto 2014b)

Limnéll ym. (2014: 113) ovat jakaneet kyberuhkat niin sanottuun uhkajaotteluun, johon kuuluvat **kybersota**, **kyberterrorismi**, **kybervakoilu**, **kyberrikollisuus** sekä **haktvismi ja hakkerointi**. Näitä arvioidaan motivaation, toimijoiden ja kohteiden näkökulmasta.

Taulukko 2. Kyberuhkajaottelu (Limnéll ym. 2014: 113).

	Motivaatio	Toimijat	Kohde
Kybersota	Poliittinen / sotilaallinen hallinta	Valtiot	Kriittinen infra ja muut strategiset kohteet
Kyberterrorismi	Poliittinen muutos, pelko	Terroristit	Infra, voimavarat ja julkiset kohteet
Kybervakoilu	Tiedon varastaminen	Valtiot ja yritykset	Hallitukset, yritykset, yksilöt
Kyberrikollisuus	Taloudellinen hyötyminen	Rikolliset	Yritykset ja yksilöt
Haktivismi, hakkerointi	Poliittinen muutos, egoismi	Aktivistit, haktivistit ja yksilöt	Hallitukset, yritykset, yksilöt

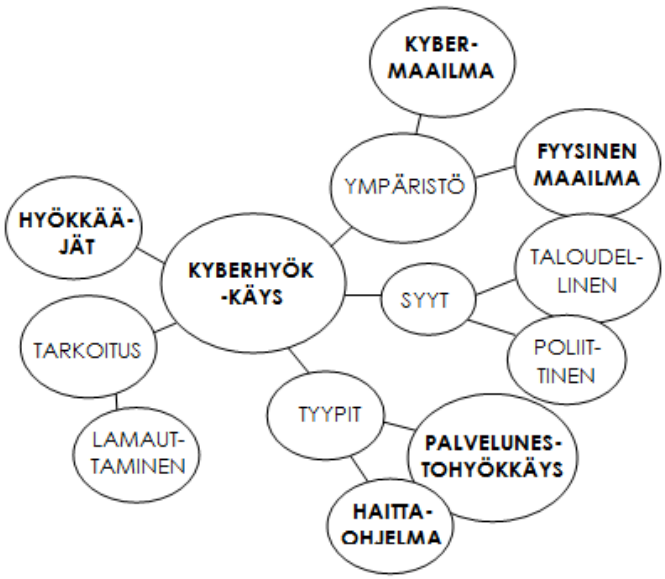
Kyberuhkajaottelun mukaisia uhkia toistuu myös muussa aineistossa, joskin jaottelu uhkista. Esimeriksi Limnéllin ym. (2014) esittämään jaotteluun kyberhyökkäykset

esiintyy erillisenä uhkana. Kyberuhkajaottelussa kyberhyökkäykset ovat osa kyberterrorismia, mutta kyberhyökkäyksiä esiintyy myös muiden kyberuhkissa. Esimerkiksi krakkerit hyödyntävät erilaisia kyberhyökkäyksiä. Samoin kybervakoilun voisi nähdä olevan haktivismia tai kyberrikollisuutta.

Esimerkiksi kyberhyökkäys muodostaa häiriötilanteen ja tätä häiriötilannetta voidaan kutsua **kyberhäiriöksi**. Kyberuhkan käsitteeseen ei liity ainoastaan uhkiksi koetut tekijät, joita vastaan pitää puolustautua, vaan kyberuhkia varten on hyvä mitoittaa sietokyky. Kyberuhkien sietokykyyn eli kyberresilienssiin liittyy varautumis- ja ennakoinkikyky, toimintakyky häiriötilanteessa sekä häiriötilanteen jälkeinen toipumis- ja palautumiskyky. (Kyberturvallisuusstrategia 2013: 4)

4.1 Kyberhyökkäykset

Kyberhyökkäykset ovat kybermaailmassa tapahtuvia tekoja, joila pyritään tuottamaan haittaa tai vahinkoa toiselle osapuolelle. Kyberhyökkäyksen käsitteeseen liittyvät siis ympäristö, syyt, hyökkäysten tyypit, hyökkäysten tarkoitukset ja hyökkääjät.



Kuvio 11. Kyberhyökkäykset

Lyhyesti kyberhyökkäyksen määritelmä voisi olla seuraava: kybermaailmassa tapahtuva hyökkäys, jolla voidaan tuottaa haittaa, vahinkoa tai tuhoa. Hyökkäyksen kohde voi olla joko kybermaailmassa tai se voi kohdistua fyysisen maailmaan, kuten jonkin kriittisen infrastruktuurin kohde. (Limnéll ym. 2014: 240) Kyberhyökkäyksillä voidaan pahimmillaan lamauttaa kriittisen infrastruktuurin ja yhteiskunnan toimintoja (Kyberturvallisuusstrategia 2013: 17). Toisaalta Helsingin Sanomien (HS 2015a) määritelmän mukaan verkkohyökkäyksien tarkoituksena on estää pääsy jollekin verkkosivulle kohdistamalla verkkoliikennettä niin paljon, että palvelimen suorituskyky ei riitä vastaamaan kaikkiin lähetettyihin kutsuihin.

Helsingin Sanomien artikkelista nousee esille tarve määritellä kyberhyökkäyksen käsite tarkemmin. Helsingin Sanomien määritelmä vastaa ennemmin **palvelunestohyökkäyksen** määritelmää eivätkä kaikki kyberhyökkäykset ole palvelunestohyökkäyksiä. Myös samassa uutisessa puhutaan samasta pankkeihin kohdistuneesta kyberhyökkäyksestä joko termillä *verkkohyökkäys* tai *palvelunestohyökkäys*.

> ”Toimitusjohtaja Mikko S. Niemelä tietoturvayhtiö Silverskin Information Securitystä arvioi, että verkkohyökkäykset pankkeja kohtaan on tehty rahan ja huomion takia. - - Niemelä ei usko, että palvelunestohyökkäykset aiheuttavat vahinkoja pankkien järjestelmälle. Hyökkäykset vain ruuhkauttavat verkkoliikenteen ja estävät palvelujen normaalin käytön.” (HS 2015a)

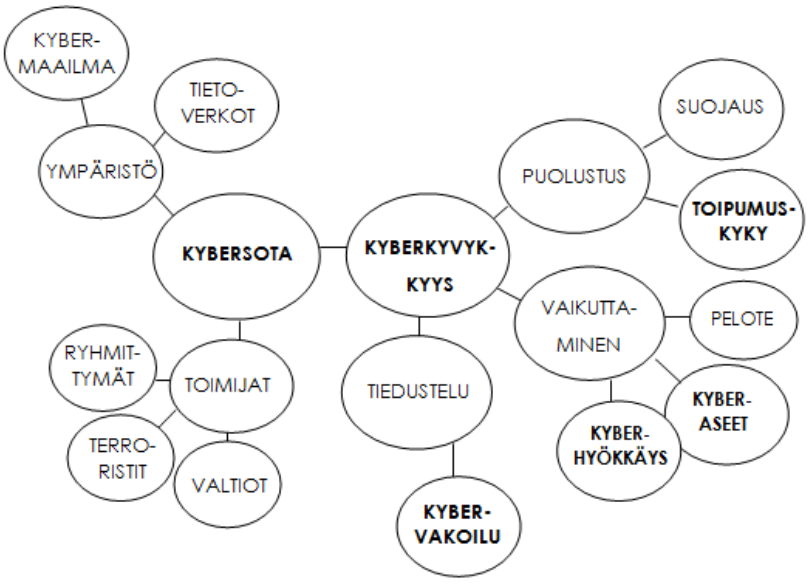
Kyberhyökkäyksien syyt voidaan jakaa poliittisiin ja taloudellisiin. Toisaalta Kyberturvallisuuskeskus (2015: 7) syyt altistaviin ja mahdollistaviin syihin. Näistä hyökkäyksille altistavia syitä ovat kiinnostava informaatio ja merkittävät yhteistyökumppanit. Mahdollistavia syitä ovat järjestelmien ja verkon tarjoamat mahdollisuudet sekä puutteet havainnointi- ja reagointikyvyssä. (Em. 7) Satelliittimalliin jaoin syyt näihin neljään kategoriaan: poliittisiin, taloudellisiin, altistaviin ja mahdollistaviin, joista kaksi viimeistä jakautuu vielä kiinnostukseen ja yhteistyöhön sekä tekniikkaan ja valmiuksiin.

Kyberhyökkäykset voivat kohdistua niin yksilöihin, yrityksiin ja organisaatioihin sekä valtioihin. Kuitenkaan kyberuhkat eivät ole samanlaisia esimerkiksi yksilölle kuin valtiolle. Valtioon kohdistuvia hyökkäyksiä voivat olla vakoilu ja tiedustelu, kun yksilöihin kohdistuvissa kyberhyökkäyksissä on usein urkinnasta ja sen myötä tunnusten joutumisesta kyberrikollisille. (Rantapelkonen & Salminen 2013: 7; Rantapelkonen & Kantola 2013: 27)

> ***Kyberhyökkäys*** *on kybermaailmassa tapahtuva hyökkäys, jonka tarkoituksena on esimerkiksi lamauttaa yhteiskunnan toimintaa. Sen tarkoitus voi olla poliittinen tai taloudellinen ja sen vaikutukset voivat kohdistua joko kybermaailmaan tai fyysiseen maailmaan.*

4.2 Kybersota

Kybersota on sotatieteissä esiintyvä termi, jolla viitataan kyberympäristössä toimivan organisoidun vihollisen toimintaa (Ahvenainen 2013: 154). Kybersota voi olla myös digitaalisessa maailmassa tapahtuvaa internetliikenteen häirintää ja vakoilua, jolla muun muassa pyritään vaikeuttamaan viestintää (HS 24.1.2013).



Kuvio 12. Kybersota

Kybersota on kokonaisuutena laaja käsite ja sotatieteissä kohtalaisen tutkittu aihe, jonka vuoksi tässä tutkimuksessa ei perehdytä kybersodan eri muotoihin. Tutkimusaineistostani nousee esille kuviossa 12.

Tutkimusaineiston perusteella *kybersota* sisäiltäisikin myös **kybervakoilun** käsitteen. Toisaalta kybervakoilu ei aina liity sodankäyntiin, joten kybervakoilu ei voi olla kybersodan alakäsite. Samoin kybersotaan liitetään puolustautumisen lisäksi **kyberhyökkäykset,** mutta **kyberrikolliset** ja **krakkerit** saattavat myös hyödyntää kyberhyökkäyksiä. Limnéll ym. (2014: 144) luettelevat nämä käsitteet **kyberkyvykkyyden** käsitteen alle, joka jakautuu tiedusteluun, vaikuttamiseen ja puolustukseen.

Tiedustelutoimintaan liittyykin edellä mainittu **kybervakoilu**, jossa hyödynnetään vakoilun keinoja kybermaailmassa. Vaikuttamisen alta aiemmassa alaluvussa käsitellyn kyberhyökkäyksen lisäksi **kyberaseet.** Kuten muukin kybermaailmassa, kyberaseilla tarkoitetaan kybermaailmassa eli digitaalisessa ympäristössä käytettäviä aseita. Verrattuna fyysiseen aseeseen kyberase on useimmiten ohjelmistopohjainen. Toisaalta myös fyysinen ase saattaa sisältää siruja, joiden avulla aseita voidaan ohjata tietokoneiden välityksellä. (Hanska 2013: 170–171) Tässä tutkimuksessa *kyberase* kuitenkin rajataan tarkoittamaan kybermaailmassa toimivaa asetta.

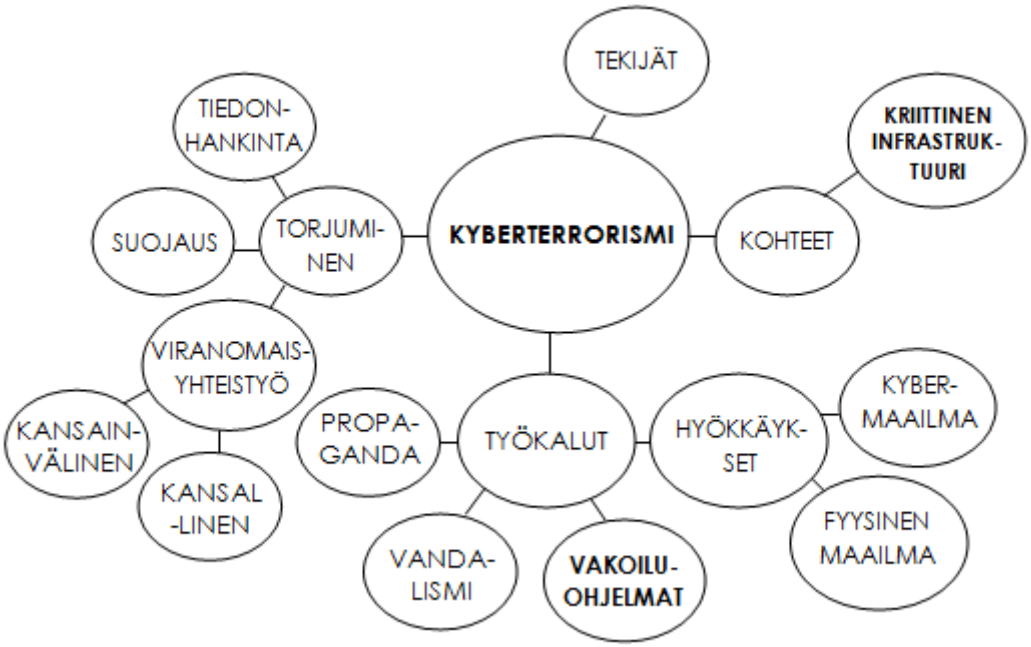
Kybersotaan liittyvät myös valtiot, jotka pyrkivät joko puolustautumaan tai hyökkäämään kybersodalta. Kybersotaan liittyviksi valtioiksi voidaan laskea muun muassa Yhdysvallat, Venäjä, Kiina, Israel, Pohjois-Korea ja Syyria. (HS 2013b). Terroristit ja kybermaailmassa toimivat haktivistit voidan laskea myös mukaan kybersodan toimijoihin.

Kybersodassa erityisesti tietoturva ja tiedon varmuus ovat keskeisessä roolissa, kun tarkastellaan kybersodan ympäristöä. Jos tietoturvasta ei huolehdita ja vastapuoli pystyy havaitsemaan haavoittuvuuksia tietojärjestelmistä, kybersota saatetaan hävitä. Myös käyttäjien tietämättömyys voidaan nähdä yhtenä kybersodan ympäristöön liittyvinä uhkina, sillä jos käyttäjät eivät itse tiedä toimistaan kyberympäristössä, käyttäjien tietämättömyys voi aiheuttaa suurta haittaa kybersodankäynnissä. (Palokangas 2013: 151). Kybersodan voisikin määritellä seuraavasti:

> ***Kybersota*** *toimii siis kybermaailmassa, jossa erityisesti kybersodan hyökkäykset tehdään tietoverkkoihin. Tietoverkkoihin kohdistetuissa iskuissa on tarkoitus lamauttaa joko viestintää tai vahingoittaa kriittistä infrastruktuuria.*

4.3 Kyberterrorismi

Terrorismi on poliittisesti motivoitunutta toimintaa, jolla pyritään vaikuttamaan yleisöön ja joka kohdistuu yleensä siviiliväestöön tai sotatoimiin osallistumattomiin henkilöihin (Ruby 2002: 10). Myös kybermaailmassa on terrorismia, joskin iskut eivät kohdistu ainoastaan digitaaliseen ympäristöön, vaan iskujen kohteena voi olla kriittinen infrastruktuuri eli esimerkiksi sähkölaitokset. Kyberterrorismi jakautuu työkaluihin, tekijöihin, tavoitteisiin, syyt ja kohteet.



Kuvio 13. Kyberterrorismi.

Limnéll ym. (2014: 131) määrittelevät **kyberterrorismin** ennalta suunnitelluiksi iskuiksi, joiden tarkoitukset ovat poliittisia, ideologisia, sosiaalisia tai uskonnollisia ja niiden on tarkoituksena on kiinnittää huomio johonkin asiaan, levittää pelkoa tai

vaikuttaa väestöön ja päätöksentekoon. Kyberterrorismissa siis hyödynnetään kybermaailmaa ja sen tarjoamia mahdollisuuksia.

Viranomaiset määrittelevät kyberterrorismin toiminnan kautta. Kyberterrorismiin liittyvät **kyberiskut**, jotka kohdistuvat kriittisen infrastruktuuriin. Näihin kyberiskuihin saattaa liittyä myös tiedustelutoimintaa. Iskuilla pyritään vaikuttamaan mielipiteisiin ja päätöksentekoon. Viranomaisyhteistyöllä varmistetaan kyberterrorismin torjuntaan liittyvät valtuudet ja toimintakyky. (Sisäasiainministeriö 2014: 5; 17–18)

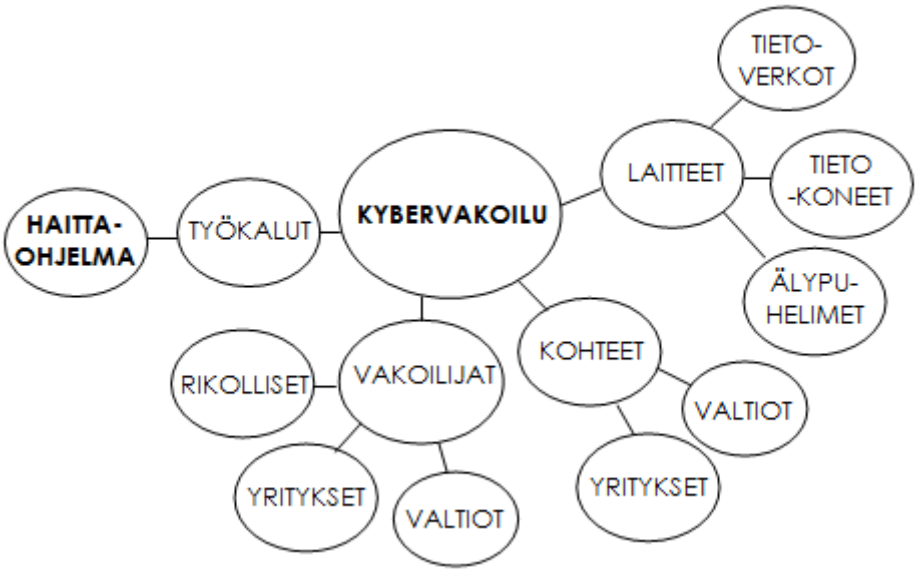
Kyberterrorismin työkaluja ovat propagandan levittäminen, vandalismi, palvelunestohyökkäykset, vakoiluohjelmat, ohjelmien tai ohjelmistojen käskyjen muuttaminen, kyberhyökkäykset sekä fyysiset hyökkäykset keskeisiä laitteistoja kohtaan (Limnéll ym. 2014: 135).

Propagandan levittämisellä tarkoitetaan kyberterroristien luomaa sisältöä, jota jaetaan verkossa. Usein propagandan levittäminen tapahtuu multimedian muodossa, jotta voidaan vaikuttaa suureen määrään ihmisiä, tehostetaan rekrytointia ja motivoidaan muita ihmisiä osallistumaan terroritekoihin. Vandalismi on usein yhteydessä palvelunestohyökkäyksiin: kybermaailmassa vandalismi on esimerkiksi verkkosivuille murtautumista ja niiden sisältöjen muuttamista valheelliseksi. Palvelunestohyökkäyksissä pyritään estämään esimerkiksi verkkosivuille pääsy. Vakoiluohjelmat varastavat tietoa, kun taas ohjelmien ja ohjelmistojen käskyjen muuttamisella pyritään vahingoittamaan esimerkiksi infrastruktuurin kriittisiä järjestelmiä. Laitteistoihin saattaa kohdistua myös fyysisiä iskuja. Kriittisen infrastruktuurin järjestelmät ovat usein keskitettyjen valvomo-ohjelmistojen varassa, jolloin yhdellä iskulla voidaan lamauttaa tai ottaa haltuun koko järjestelmä (Limnéll ym. 2014: 135–136).

5.4 Kybervakoilu

Yksi turvallisuuteen liittyvä uhka on vakoilu. Kybermaailmassa yksi suuri uhka on joutua vakoilun kohteeksi, jolloin vakoileva osapuoli pyrkii saamaan tietoa vakoilun

kohteena olevasta osapuolesta. **Kybervakoilu** jakautuu laitteisiin, kohteisiin, vakoilijoihin sekä työkaluihin.



Kuvio 14. Kybervakoilu

Limnéll ym. (2014: 130) pitää kybervakoilua yhtenä vakavimmista kyberturvallisuuteen liittyvistä uhkista. Vakoilu itsessään on vanha ilmiö. **Kybertiedustelua**, joka on kybervakoiluun läheisesti liittyvä käsite, Limnéll ym. (2014: 128) kuvaa tiedon keräämiseen prosessiksi, jossa tietoa pyritään keräämään kaikin mahdollisin keinoin, analysoidaan kerätty tieto ja jaetaan tieto päätöksentekoa varten. (Limnéll ym. 2014: 130). Kyberturvallisuuskeskus (2015: 29) taas määrittelee kybervakoilun tietovekkojen välityksellä tapahtuvaksi luvattomaksi tiedustelutoiminnaksi. Kybermaailmaan liitettynä tiedustelu ja vakoilu tapahtuvat siis sähköisesti.

Kybervakoilussa ei ole useinkaan tavoitteena näkyviä muutoksia vakoilun kohteena oleviin tietojärjestelmiin tai laitteisiin, vaan vakoilussa pyritään pitkäaikaiseen ja huomaamattomaan läsnäoloon. Näin esimerkiksi organisaation toimintaa voidaan seurata ja tiedon eheyttä rikkoa. (Kyberturvallisuuskeskus 2015: 3)

Tiedotusvälineissä kybervakoilu liittyy usein valtioon kohdistuvaan tiedusteluun ja -vakoiluun. Esimerkiksi Ilta-Sanomat uutisoi 13.1.2016 kybervakoilusta:

> ”Tietoturvayritys Kaspersky Labin mukaan Suomen ulkoministeriöön kohdistuneessa verkkovakoilussa kaikki viittaa siihen, että verkkovakoiluryhmä Turla sai valtion tukea. Verkkovakoojat tunkeutuivat Suomen ulkoministeriöön vuonna 2013. Paljastuneen laajan verkkovakoilun takana on ollut venäläinen verkkovakoiluryhmä Turla. Tämän vahvistaa arvionaan tietoturvayritys Kaspersky Lab Ilta-Sanomille.”

Kybervakoilun nähdäänkin olevan tällä hetkellä yksi suurimmista uhkista Suomelle, sillä kybervakoilun avulla kerätään arkaluontoista tietoa, jonka avulla voidaan tuottaa huomattavaa vahinkoa maanpuolustukselle, turvallisuudelle, taloudelle ja ulkomaansuhteille. Myös uskottavuus kyberosaamisen alalla voi heikentyä. (Kyberturvallisuuskeskus 2015: 6)

Kybervakoiluun syyllistyvät kaikki toimijat, jotka vakoilevat fyysisessä maailmassa. Vakoiluun syyllistyvät kansainväliset yritykset, rikolliset sekä valtiolliset toimijat. Näiden motiivit kybervakoiluun kuitenkin vaihtelevat, sillä valtiollisia toimijoita kiinnostaa saada tietoonsa valtionsalaisuuksia, kun rikolliset pyrkivät ansaitsemaan rahaa vakoilulla. (MTV 2014)

Helsingin Sanomien (2013a) uutisoimaa laajaa kybervakoiluun käytettyä haittaohjelmistoa alettiin kutsua *Punaiseksi Lokakuuksi* (engl. *Red October*) tai lyhyemmin *Rocraciksi* ja sen avulla kerättiin tietoa tietoverkoista, tietokoneista sekä älypuhelimista.

Kybervakoilun työkalut ovat hyvin pitkälti samoja kuin kyberhyökkäyksissä, joskin haittaohjelmat korostuvat aineistosta. Kuviossa 14 olen listannut kybervakoilun työkaluihin ainoastaan haittaohjelmat, sillä muita kyberhyökkäyksien työkaluista ei aineistosta ole selkeästi nostettavissa kyseiseen kuvioon.

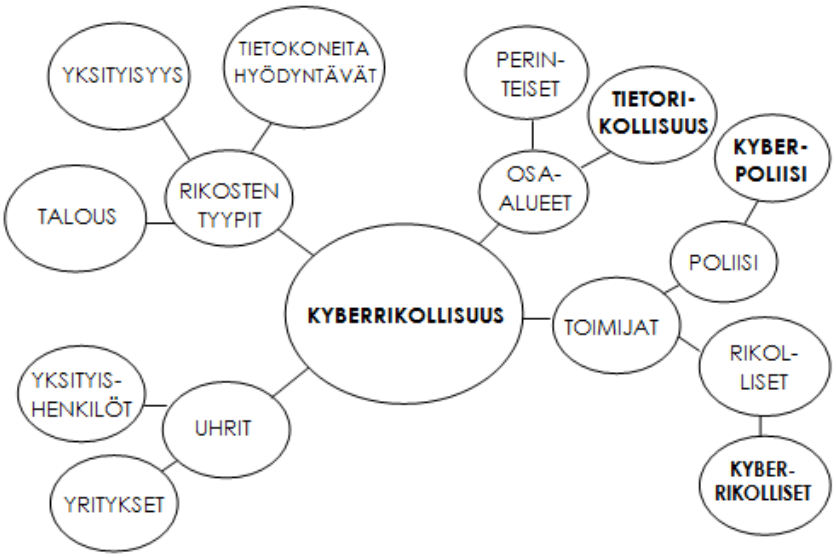
Vaikka kybervakoilun käsite onkin aineiston mukaan suhteellisen yhtenäinen, eri termejä samalle käsitteelle ja määritelmälle on löydettävissä. Helsingin Sanomat käyttää tässäkin yhteydessä *verkko*-etuliitettä *kyber*-etuliitteen sijaan. Helsingin Sanomat

(2014g) kertoi heinäkuussa 2014 Suomen ulkoministeriöön kohdistuneista tietomurroista ja verkkovakoilusta, jossa kaksi eri valtiota vakoili kahden erillisen verkkohyökkäyksen avulla. Näkisin, että yhdenmukaisuuden vuoksi tätä käsitettä tulisi kutsua *kybervakoiluksi***,** sillä kaksi rinnakkaista termiä samasta käsitteestä hankaloittaa kyseisen ilmiön ymmärtämistä. Samalla voidaan myös verrata tietoturvasanastosta löytyvää verkkotiedustelun määritelmää muualta löytyvään kybertiedustelun määritelmään. Tietoturvasanaston (2004: 16) mukaan verkkotiedustelulla tarkoitetaan tietoverkoissa tapahtuvaa tiedustelua.

> ***Kybervakoilu*** *on tietoverkoissa tapahtuvaa vakoilua ja tiedustelua. Kybervakoilu voi kohdistua niin valtiollisiin tekijöihin, organisaatioihin ja yrityksiin. Kybervakoilun työkaluja ovat kyberhyökkäykset, joista erityisesti haittaohjelmien avulla vakoilu.*

4.5 Kyberrikollisuus

Rikolliset ovat löytäneet myös kybermaailmaan, jossa rikoksen uhreiksi joutuvat niin yritykset kuin yksityiset henkilöt. Kyberrikollisuuden käsite jakaantuu rikosten eri osa-alueisiin, toimijoihin, uhreihin ja rikosten tyyppeihin.



Kuvio 15. Kyberrikollisuus

Kyberrikollisuudella tarkoitetaan niitä rikoksia, jotka kohdistuvat tietokoneisiin tai verkossa tehtyyn rikokseen. Kyberrikoksessa verkot tai tietokoneet ovat toiminnan välineitä, kohteita tai rikoksen tekemisen paikka. Euroopan unionin määritelmän mukaan kyberrikollisuutta ovat tiedon tai tietojärjestelmien luottamusta, eheyttä tai saatavuutta vaarantavat toimet. Toisaalta kyberrikollisuuteen voidaan laskea kuuluvaksi myös elokuvien ja musiikin laiton lataaminen, joka fyysisessä maailmassa laskettaisiin varkaudeksi. Kyberrikollisuus on ennemminkin tietoinen toimintatapa kuin yksittäinen teko, ja kyberrikollisuudessa voidaan hyödyntää monia eri keinoja ja se voi kohdistua eri kybermaailman toimijoihin. (Limnéll ym. 2014: 120–121)

Euroopan unioni on useammassa eri yhteydessä luokitellut ja määritellyt kyberrikollisuutta. Budapestin sopimuksessa vuonna 2001 määriteltiin neljä pääkategoriaa kyberrikollisuudelle ja vuonna 2007 listattiin kolme osa-aluetta. EU:n lainsäädäntö tuntee myös kyberrikoksia. Nämä yhdistämällä voidaankin saada aikaiseksi seuraava listaus kyberrikollisuuden osa-alueista:

- tiedon ja tietojärjestelmien luottamuksellisuutta vastaan tehdyt hyökkäykset
- tietokoneita hyödyntävät rikokset
- sisällöltään rikolliset toimet
- kopiosuojaa tai tuotemerkkiä loukkaavat rikokset
- yksityisyyden loukkaukset
- talousrikokset, ulkopuolinen pääsy ja sabotaasi. (Limnéll ym. 2014: 125–126)

Käsiteanalyysiä hyödyntäen yllä luetellut kyberrikollisuus voidaankin jakaa taloudellisiin, yksityisyyteen ja tietokoneita hyödyntäviin rikoksiin. Taloudellisiin rikoksiin voidaan luokitella talousrikokset ja kopiosuojaa tai tuotemerkkiä loukkaavat rikokset, kuten musiikin laiton lataaminen. Yksityisyyteen kuuluvat yksityisyyttä ja sisällösesti rikollista toimintaa kuuluvat rikokset. Tietokoneita hyödyntäviin rikoksiin kuuluvat loput luetelluista rikoksista. Kyberrikollisuus voidaan jakaa myös poliisin tavalla, jossa kyberrikollisuus on joko tietoverkkoja hyödyntävää perinteitä rikollisuutta sekä puhtaaksi tietorikollisuudeksi, jossa rikoksen kohteena ovat tietokeskittymät (HS 2013b).

Limnéllin ym. (2014: 121) mukaan kyberrikokselle lienee turha etsiä yhtä käsitettä, vaikka tämänkin käsitteen määritteleminen olisi olennaista. Kyberrikollisuuden rinnalla

esiintyy myös termi *verkkorikollisuus*. Kuitenkaan tarkkaa määritelmää verkkorikollisuudelle ei löydy. Esimerkiksi Helsingin Sanomien uutisessa 16.2.2014 verkkorikollisuudesta puhutaan seuraavasti:

> ”Keskusrikospoliisiin aiotaan luoda verkkorikoksiin erikoistunut keskus, joka vastaa vaativimpien juttujen tutkimisesta. Sellaisia ovat esimerkiksi rikosepäilyt, joilla on yhteys kansainväliseen tai järjestäytyneeseen rikollisuuteen -- Yhteyspisteen kautta kulkisivat kansainvälisiin tietoverkkorikoksiin liittyvät virka-apupyynnöt. Sen keskeinen tehtävä on käynnistää esitutkintatoimet viivytyksettä, jotta poliisi ehtii saada rikoksia koskevan näytön eli datan talteen.” (HS 2014e)

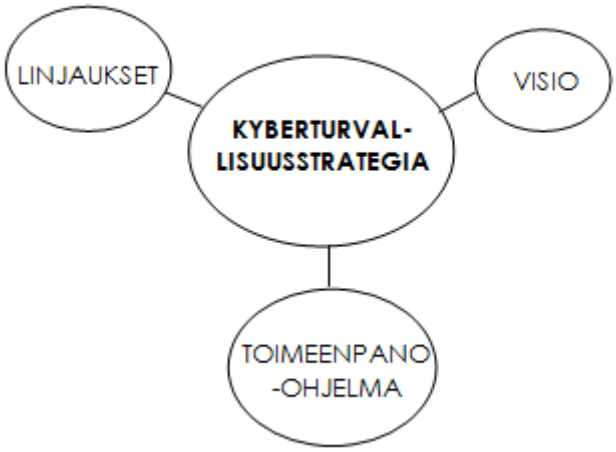
Helsingin Sanomien verkkosivuilla tunnisteella ”verkkorikollisuus” on listattu uutisia, joissa käsitellään verkossa tapahtuneita rikoksia. ”Verkkorikollisuus”-tunnisteen alle on listattu Applen iCloud -palvelusta vuodetut julkisuuden henkilöiden alastonkuvat, tietovuotoihin liittyviä uutisia, verkkotunnusten urkintayritykset ja kyberpoliisien palkkaamista koskeva uutinen. Koska verkkorikollisuudesta ei tarkempaa määritelmää löydy, tämän perusteella verkkorikollisuus olisi siis verkossa tapahtuvaa rikollisuutta. Uutisessa vilahtaa myös termi tietoverkkorikokset, jotka ilmeisesti viittaavat samaan käsitteeseen: rikoksiin, jotka tapahtuvat (tieto)verkossa.

5 KYBERTURVALLISUUSSTRATEGIA

Kyberturvallisen tilan toteuttamiseksi esimerkiksi valtion tai organisaation tasolla voidaan luoda siihen tarkoitettu strategia. Strategialla tarkoitetaan esimerkiksi organisaation tulevaisuuden suuntaa ja niitä keinoja sekä menetelmiä, joiden avulla haluttuun päämäärään päästään. Strategiaan kuuluu myös käsite visiosta eli halutusta tavoitetilasta. (Business Dictionary 2015) Strategiat perustuvat ympäristöön koskeviin analyyseihin ja ne ovat tulevaisuuteen suuntautuvia (Viitala & Jylhä 2006: 71).

Tarkastelen tässä luvussa Suomen Kyberturvallisuusstrategiaa 2013 sekä Tietoturvastrategiaa 2008. Muodostan aluksi eri määritelmistä satelliittimallit, jotka yhdistän yhdeksi yhteiseksi satelliittimalliksi, sillä eri lähteistä on muuten vaikea muodostaa yhtä yhteistä satelliittimallia. Eri strategiat eroavat käsitteiltään ja sisällöltään niin paljon, ettei ilman tarkempaa erittelyä voi muodostaa yhtenäistä mallia kyberturvallisuusstrategian käsitteistöstä.

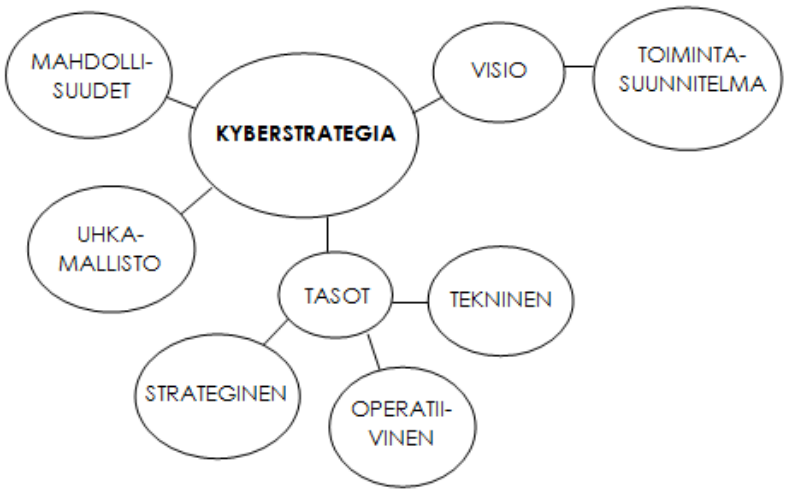
Kyberturvallisuusstrategia 2013 on osa vuonna 2010 laadittua Yhteiskunnan turvallisuusstrategian toimeenpanoa. Se noudattaa yleisen turvallisuusstrategian periaatteita ja määritelmiä. Kyberturvallisuusstrategia jakautuu kyberturvallisuuden visioon, toimintamalliin ja strategisiin linjauksiin. Tämän lisäksi valmisteilla on kyberturvallisuusstrategian toimeenpano-ohjelma, jonka tarkoituksena on määritellä eri hallintoalojen vastuulle tulevat käytännön toimenpiteet. Näillä toimenpiteillä on tarkoitus luoda edellytykset toteuttaa kyberturvallisuusstrategiaa. (Kyberturvallisuusstrategia 2013: 2)



Kuvio 16. Kyberturvallisuusstrategia 2013

Limnéll ym. (2014: 157) käyttävät samasta strategiasta termiä kyberstrategia. Muihin strategioihin verrattuna Limnéll ym. keskittyvät yritysten kyberstrategian suunnitteluun. Kyberstrategiassa muutetaan abstrakti visio operatiivisen eli toiminnallisen tason toimintasuunnitelmaksi, jota toteutetaan suorittavalla tasolla ja näin ulottuu koko yrityksen tai organisaation toimintaan. Kyberstrategia tulisikin toteuttaa yrityksessä yhteistyössä, jotta kaikkien osaaminen voidaan valjastaa ongelmien ratkomiseen.

Keskeisintä kyberstrategian laatimisessa on kommunikaatio kaikkien organisaation toimijoiden välillä. Strategiaa varten kyberturvallisuutta voidaan tarkastella kolmella tasolla: strategisella, operatiivisella ja teknisellä. Myös kyberturvallisuuden mahdollisuudet sekä uhkamalliston luominen kuuluvat osana strategian laadintaa. (Em. 157-160) Limnéllin ym. määritelmän mukaan kyberstrategiasta muodostuu hieman kuviota 16 eroava satelliittimalli:



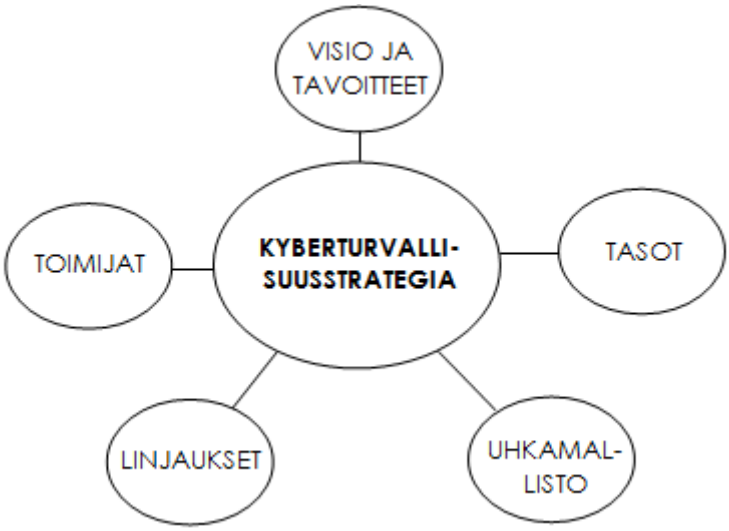
Kuvio 17. Kyberstrategia

Ennen kyberturvallisuusstrategian tai yhteiskunnan turvallisuusstrategian luomista Valtioneuvoston kanslia on jukaissut tietoturvastrategian vuonna 2008. Tietoturvastrategian visiona on se, että suomalaiset voivat luottaa tietojensa turvallisuuteen erilaisissa tieto- ja viestintäverkoissa sekä niissä toimivissa palveluissa. Myös tietoturvaosaamisen pitäisi olla korkealla tasolla.

Strategian tavoitteena myös eri tietojärjestelmien ja -verkkojen toimintavarmuuden varmistaminen. Strategia jakautuu kolmeen tavoitteeseen: perustaitoihin, riskien hallintaan ja toimintavarmuuteen sekä kilpailukykyyn ja kansainväliseen verkostoyhteistyöhön. Tärkeimpänä on luottamus, jonka katsotaan ulottuvan palveluiden helppokäyttöisyyteen, kuluttajansuojaan, sisältöjen aitouteen sekä yksityisyyden ja muidem etujen suojeluun Tietoturvastrategiaan liittyy myös toimintapano-ohjelma, jonka avulla visio voidaan saavuttaa. (Tietoturvastrategia 2008: 2; 8)

Kuvio 18. Tietoturvastrategia

Vertailemalla näitä kolmea satellittimallia yhteisiksi käsitteiksi nousevat visio ja sen alakäsite toimeenpano-ohjelma. Myös linjaukset ja toimitamallit voidaan laskea löytyvän jokaisesta satelliittimallista, joskin määritelmissä näiden sisällöt hieman eroavat toisistaan. Oma satelliittimalli kyberturvallisuusstrategiasta onkin seuraava:



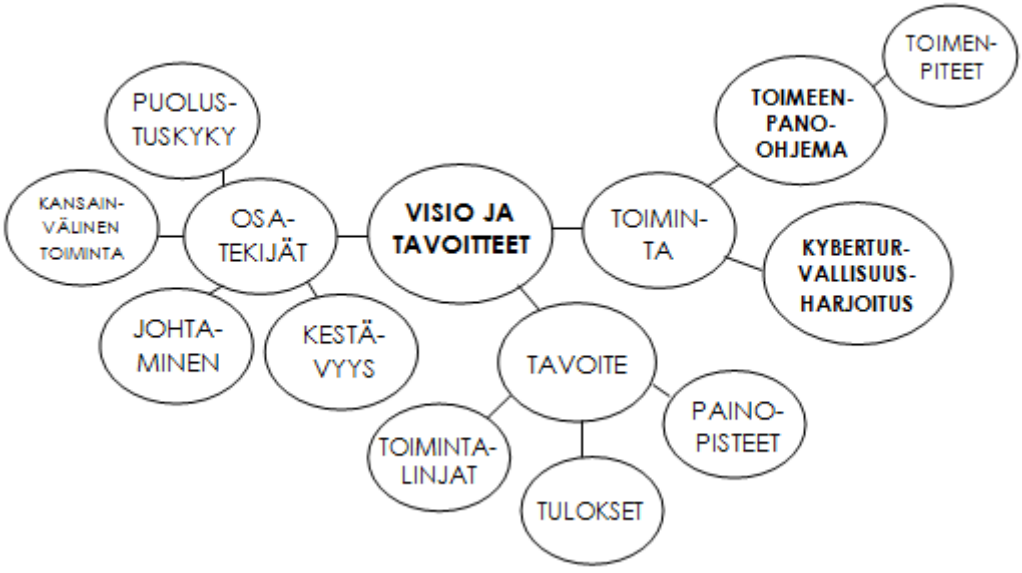
Kuvio 19. Kyberturvallisuusstrategian lähikäsitteiden jaottelu

Tässä kyberturvallisuusstrategian satelliittimallissa tulee huomioida se, että lähden määrittelemään kyberturvallisuusstrategian käsitettä valtiohallinnon näkökulmasta.

Esimerkiksi Limnéll ym. (2014: 161–164) esittää teoksessaan mallin, jolla yritys voi luoda kyberstrategian. Tällöin kyberturvallisuusstrategian käsitesisältökin muuttuu, jos huomioisin myös yritysten strategioita. Haluan kuitenkin keskittyä Suomen valtioneuvoston laatimaan kyberturvallisuusstrategiaan 2013 ja Turvallisuuskomiten (2014) siihen laatimaan toimeenpano-ohjelmaan.

5.1 Visio ja tavoitteet

Visio on käsitteenä yleisemmin tunnettu liiketoiminnassa. Visiolla tarkoitetaan yrityksen tulevaisuudenkuvaa. Se on tahtotila, johon strategian avulla pyritään ja toimii suunnannäyttäjänä. (Viitala & Jylhä 2006: 70) Kyberturvallisuusstrategian käsitteessä **visiolla** tarkoitetaan tahtotilaa, johon strategian avulla halutaan saavuttaa eli digitaalisen maailman turvallisuutta.



Kuvio 20. Kyberturvallisuusstrategian visio ja tavoitteet

Kyberturvallisuusstrategian visio jakautuu toimintaan ja osatekijöihin. Vision toiminnalla tarkoitetaan niitä toimia, joiden avulla kyberturvallisuusstrategiassa määritelty tavoitetila saavutetaan. Osatekijät ovat taas niitä vision alueita, jotka

määrittelemällä voidaan päästä haluttuun tavoitetilaan. Vision toimintaan on aineistosta löydettävissä kaksi selkeää lähikäsitettä, **toimeepano-ohjelma** ja **kyberturvallisuusharjoitus**.

Vision osatekijöinä ovat puolustuskyky, kansainvälinen toiminta, johtaminen ja kestävyys, joka jakautuu kriisinkestävyyteen, talouteen ja infrastruktuuriin. Kyberturvallisuusstrategian pohjalta laaditussa toimeenpano-ohjelmassa (Turvallisuuskomitea 2014: 2) toimeenpano-ohjelma määritellään ympäripyöreästi keskeisimmiksi toimenpiteiksi, joilla saavutetaan aiemmin laaditussa strategiassa määritellyt tavoitteet. Näitä toimenpiteitä luetellaan kyseisessä toimeenpano-ohjelmassa 74. Tähän satelliittimalliin näitä toimenpiteitä ei ole erikseen listattu niiden määrän vuoksi ja toisaalta kaikki toimeenpano-ohjelmat eivät välttämättä sisällä samoja toimenpiteitä. Nämä voidaan myös jakaa keskeisiksi kehittämiskohteiksi, joita Kyberturvallisuusstrategian 2013 toimeenpano-ohjelmassa on lueteltu seuraavat:

- kyberturvallisuuskeskuksen perustaminen
- valtion ympärivuorokautinen tietoturvatoiminta
- SA-TU-hanke: salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke
- poliisin toimintakyvyn kehittminen kyberrikollisuuden torjunnassa
- lainsäädännön kehittäminen
- tutkimus- ja koulutusohjelmat sekä muu osaamisen vahvistaminen.

Satelliittimallista löytyy kaksi määriteltävää käsitettä, jotka ovat toimeenpano-ohjelma ja kyberturvallisuusharjoitus. Kyberturvallisuusharjoitukselle löytyy aineistosta myös kaksi muuta termiä: *kyberturvaharjoitus* ja *kyberharjoitus*. Helsingin Sanomat (HS2014h) käyttää uutisensa otsikossa termiä kyberturvaharjoitus, mutta varsinaisessa uutisessa samasta harjoituksesta käytetään termiä kyberturvallisuusharjoitus. TiVi (2013) uutisoi puolustusvoimien ja Jyväskylän ammattikorkeakoulun yhdessä järjestämästä kyberharjoituksesta.

Kyberturvallisuusstrategialla on tavoitteita, joihin se pyrkii vastaamaan. Tavoitteet voidaan jakaa sen mukaan. Nostan tavoitteisiin vielä Limnéllin ym. (2014: 224) kyberstrategiaprosessin tulokset, sillä tavoitteiden ja tulosten välillä on syy-

seuraussuhde toisiinsa. Tavoitteet on jaettu painopisteisiin, toimintalinjoihin ja tuloksiin.

Tietoturvastrategiassa 2008 tavoite on pyrkiä luomaan suomalaisille eli kansalaisille, yrityksille, viranomaisille ja muille toimijoille turvallinen arki tietoyhteiskunnassa. Tavoite on jaettu kolmeen eri painospisteeseen, jotka ovat ”perustaidot arjen tietoyhteiskunnassa, tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä kilpailukyky ja kansainvälinen verkostoyhteistyö”. (Tietoturvastrategia 2008: 4) Vaikka nämä painopisteet onkin jo edellisessä alaluvussa käsitelty, näen tarpeelliseksi nostaa painopisteet myö osaksi tavoitetta. Suoranaista eroa sille, ovatko painopisteet linjauksia vai tavoitteita, ei tietoturvastrategiassa tehdä, joten katson niiden liittyvän näihin molempiin.

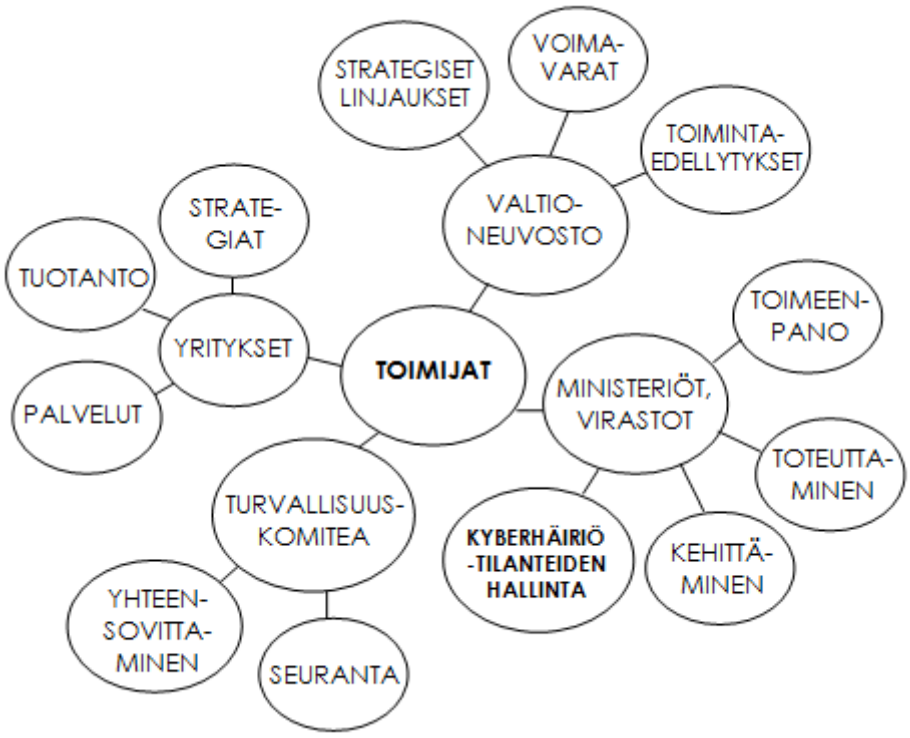
Kyberturvallisuusstrategian 2013 tavoitteena on se, että Suomi kykenee halitsemaan kybermaailman haittavaikutuksia. Kyberturvallisuusstrategian 2013 taustamuistiolle määritellään vielä erillinen tavoite:

> ”Taustamuistion keskeinen tavoite on lisätä kyberturvallisuuden toimijoiden ymmärrystä kybertoimintaympäristöstä ja sen myötä auttaa heitä oman kyberturvallisuutensa kehittämisessä.” (Em. 17)

Nämä tavoitteet voidaan yhdistää yhdeksi tavoitteeksi, jossa pyritään hallitsemaan kybermaailman haittavaikutuksia, lisätä kyberturvallisuuden toimijoiden ymmärrystä sekä auttaa eri toimijoita kyberturvallisuuden kehittämisessä.

5.2 Toimijat

Kyberturvallisuusstrategiassa toimijoiksi aineiston perusteella olen laskenut kuuluvaksi valtioneuvoston, ministeriöt ja virastot, turvallisuuskomitean sekä yritykset. Näiden lisäksi jokaiselle toimijalle on lueteltu ne tehtävät, jotka niille kuuluvat kyberturvallisuusstrategioiden mukaan.



Kuvio 21. Toimijat kyberturvallisuusstrategiassa

Tässä jaottelussa korostuvat erityisesti valtiolliset toimijat. Aineistoni pohjautuu tältä osin enimmäkseen julkishallinnon strategioihin, jolloin yksityissektorin toimijat esiintyvät ainoastaan strategian toimeenpanovaiheessa. Kuitenkin tulee huomioida, että jokaisella toimijalla on erilainen rooli strategiaa suunniteltaessa ja myöhemmin toteutettaessa.

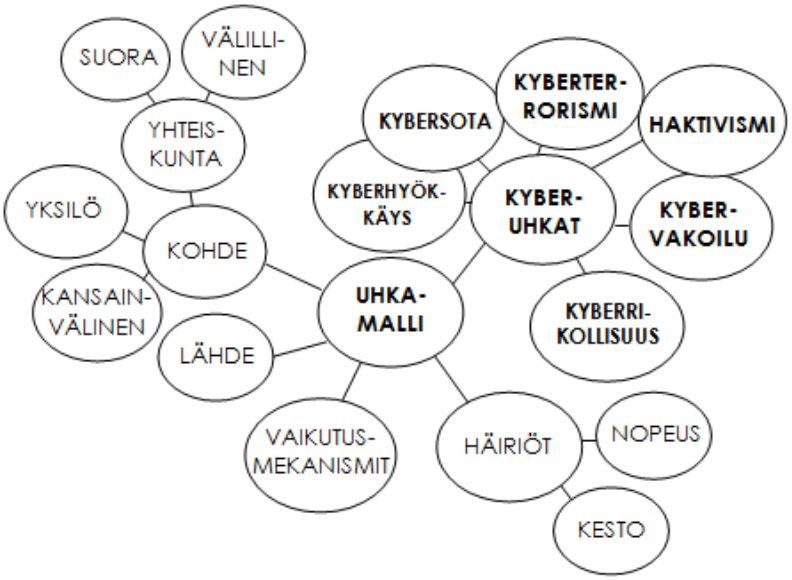
Kun kyberturvallisuusstrategiaa lähdetään kehittämään, ensimmäisenä toimijana aktivoituu valtioneuvosto. Kyberturvallisuusstrategiassa (2013: 19) määritellään valtioneuvoston tehtäviksi strategiset linjaukset, tarvittavien voimavarojen luominen sekä mahdollistaa muiden toimijoiden edellytykset toteuttaa kyberturvallisuusstrategiaa. Kuitenkaan valtioneuvosto ei itse luo strategiaa, vaan strategiatyöhön otetaan mukaan muita toimijoita.

Toisena valtiollisena toimijana kyberturvallisuusstrategiassa ovat eri **ministeriöt** ja niiden alaisuudessa olevat **virastot**. Näiden toimijoiden tehtävänä ovat valtioneuvoston kokoaman työryhmän laatiman strategian toteuttaminen käytännössä. Näihin käytännön tehtäviin kuuluvat toimeenpano-ohjelman laatiminen ja sen noudattaminen, kyberturvallisen toiminnan kehittäminen omalla toimialallaan sekä kyberhäiriötilanteiden hallinta.

Kyberturvallisuusstrategian toteuttamista sekä kybertoimintaympäristön kehitystä seuraa valtioneuvoston nimittämä **turvallisuuskomitea**. Valtiollisilla toimijoilla ei yksin ole riittävää mahdollisuutta toteuttaa kyberturvallisuusstrategiaa. Tällöin mukaan otetaan myös eri yritykset ja niiden tarjoamat palvelut. Toisaalta myös jokainen yritys vastaa itse omasta kyberturvallisuudesta ja tarvittaessa laatii oman suunnitelmansa.

5.3 Uhkamalli

Uhkamalliston käsite jakautuu kyberuhkiin, häiriöihin, vaikutusmekanismeihin, lähteeseen ja kohteeseen. Kuviossa 22 esitetyt kyberuhkat ovat aiemmin määritelty luvussa 4.

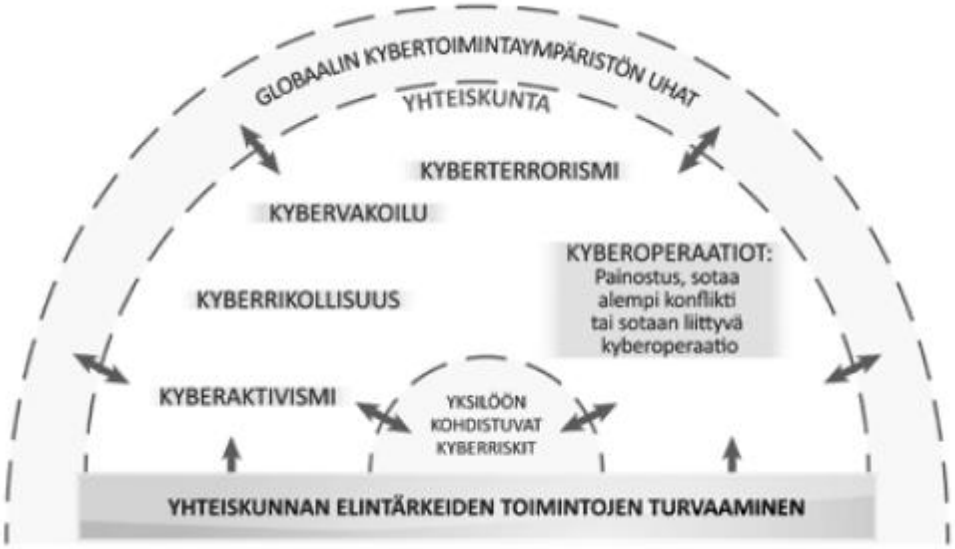


Kuvio 22. Uhkamalli

Uhkamallissa huomioidaan häiriöt, joilla tarkoitetaan esimerkiksi kriittiseen infrastruktuuriin kohdistuvia hyökkäyksen aiheuttamia häiriöitä, kuten sähkönjakelun häiriöt. Häiriöitä analysoidessa tulee myös huomioida niiden ajallinen kesto sekä se, kuinka nopeasti häiriö ilmenee.

Uhkamallissa esiintyy myös kohteet, joita ovat yhteiskunta, yksilöt ja kansainvälinen taso. **Yhteiskuntaan häiriöt** voivat vaikuttaa suoraan tai välillisesti sekä ne voivat esiintyä itsenäisinä, samanaikaisesti tai toistensa jatkumoina. (Kyberturvallisuusstrategia 2013: 19)

Uhkamallilla siis tarkoitetaan kuvausta esimerkiksi yhteiskuntaan kohdistuvista uhkista. Näissä pyritään huomioimaan satelliittimallissa esiintyvät tekijät. Kyberturvallisuusstrategiassa 2013 uhkamalli on jaoteltu toisin kuin oma satelliittimallini. Tässä strategiassa esitetyssä mallissa kyberuhkat ovat jaoteltu sen mukaan, mihin kohteeseen ne kohdistuvat.



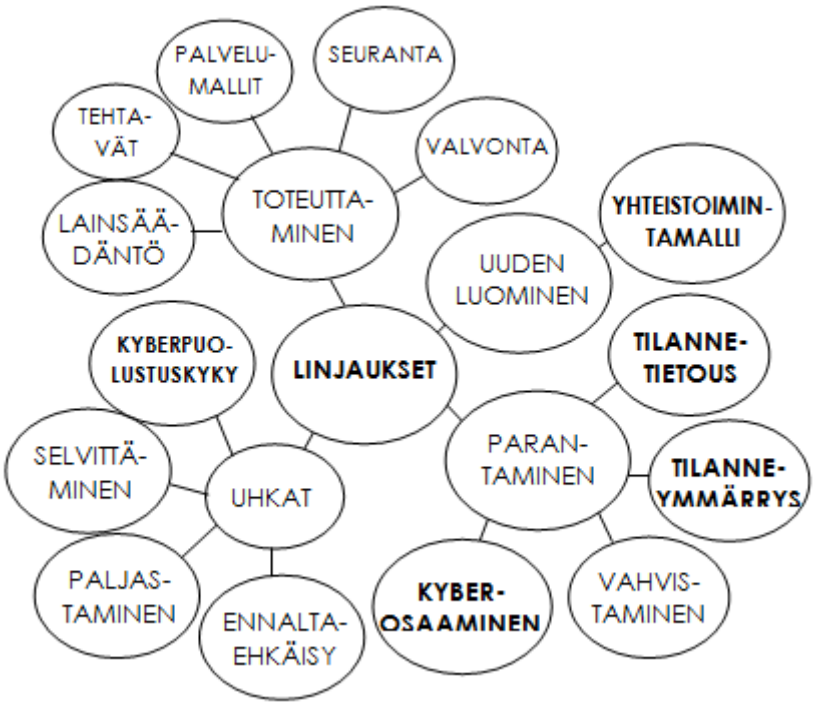
Kuvio 23. Kyberturvallisuusstrategian 2013 kyberuhkamalli (2013: 19).

Kuvio 23 kertoo siis ennemmin kyberuhkamallin käsitteen toiminnalliset suhteet kuin sen, mitä käsitepiirteitä kyberuhkamalli pitää sisällään. Limnéllin ym. (2014: 113)

esittelemä ja omassa tutkimuksessani luvussa 4 kyberuhkajaottelu (taulukko 2, s. 42) tukee paremmin omaa jaotteluani kyberuhkamallini määritelmää.

5.4 Linjaukset

Linjaukset-satelliittimalli ovat muodostettu pitkälti Kyberturvallisuusstrategian 2013 yhdeksän strategisen linjauksen perusteella, jotka olen jakanut neljään kokonaisuuteen: uuden luomiseen, parantamiseen, uhkiin ja toteuttamiseen. Tietoturvastrategiassa 2008 linjaukset ovat määritelty kolmeen painopisteeseen: perustaitoihin, riskien hallintaan ja toimintavarmuuteen sekä kilpailukyky ja verkostoyhteistyö. Nämä painopisteet ovat jaettavissa näihin neljään alaan, jossa perustaidot kuuluvat parantamisen alle, riskien hallinta ja toimintavarmuus uhkiin sekä kilpailukyky ja verkostoyhteistyö ovat linjausten toteuttamista.



Kuvio 24. Kyberturvallisuusstrategian linjaukset

Linjauksilla tarkoitetaan strategiassa niitä toimenpiteitä, joilla esimerkiksi kyberturvallisuutta parannetaan. Ne ovatkin edellytyksenä sille, että strategian visio voidaan toteuttaa. Linjaukset toteutetaan **toimeenpano-ohjelmalla**, jossa määritellään tarkemmin keinot saavuttaa strategian visio esimerkiksi määritellystä kyberturvallisuuden tilasta. (Kyberturvallisuusstrategia 2013: 4)

Uuden luominen -noodin alle on kerätty ne löydettävät linjaukset, joissa pyritään luomaan jotain uutta. Kyberturvallisuusstrategia 2013 esittelee tällaiseksi linjaukseksi yhteistoimintamallia, jossa muun muassa lisätään eri toimijoiden välistä yhteistyötä, tavoitellaan jaettua tilannetietoisuutta ja torjutaan tehokkaasti kyberuhkia. (Kyberturvallisuusstrategia 2013: 7) Tietoturvastrategiasta 2008 ei löydy tähän alanoodiin sopivia linjauksia.

Linjauksissa pyritään parantamaan jo olevia asioita, kuten tilannetietoisuutta, tilanneymmärrystä, vahvistamaan eri toimijoiden välistä yhteistyötä ja parannetaan kyberosaamista. Perustaitojen parannus koskee taas kaikkia toimijoita, kun taas Kyberturvallisuusstrategiassa 2013 mainitut parannusta vaativat kohteet ovat ennemmin viranomaislähtöisiä.

Uhkissa pyritään tekemään toimenpiteitä, joilla kyberuhkia ennaltaehkäistään ja paljastetaan, niitä selvitetään ja kehitetään kyberpuolustuskykyä. Tietoturvastrategian 2008 riskien hallinta ja toimintavarmuuden kehittäminen ovat myös laskettavissa tähän noodiin.

Viimeisenä noodina ovat toteuttamiseen liittyvät linjaukset. Näitä ovat lainsäädännön muuttaminen niin, että strategian visio voidaan saavuttaa, määritellään jokaisen toimijan tehtävät ja luodaan palvelumalli sekä strategian toimeenpanoa valvotaan ja toteutumista seurataan.

6 KOKONAISKUVA KYBERTURVALLISUUDESTA

Aloitin kyberturvallisuuden käsitteen tarkastelun esittelemällä siihen liittyviä ilmiöitä sekä vertailin **kyberturvallisuuden** ja **tietoturvallisuuden** käsitteitä (luku 3). Tämän jälkeen tutkin kyberturvallisuuteen liittyviä käsitteitä luvuissa 4, 5 ja 6. Tässä luvussa koostan yhteen kyberturvallisuuden käsitteistön kokonaisuudessaan ja esittelen kyberturvallisuuden alan keskeisimmät käsitteet. Liiteeseen 1 olen koonnut graafisen esityksen kyberturvallisuuden alan käsitteistä. Kuvion keskellä on pääkäsite kyberturvallisuus, jonka ympärille muu käsitteistö muodostuu.

Jaoin kyberturvallisuuden käsitteistön neljään luokkaan: **kybermaailmaan, toimijoihin, kyberuhkiin** ja **kyberturvallisuusstrategiaan**. Nostin nämä tärkeimmiksi käsitteiksi, sillä tutkimusaineiston perusteella kyberturvallisuuden käsitteet liittyivät näihin luokkiin. Ainoan poikkeuksen tästä tekee toimijat, jotka sisältyvät muihinkin ala- ja lähikäsitteisiin. Toimijoilla oli erilaisia käsitesisältöjä riippuen siitä, minkä käsitteen yhteydessä ne esiintyivät. Kyberturvallisuudessa toimijat ovatkin keskeisessä roolissa.

Kyberturvallisuus on digitalisoituneen maailman turvallisuutta, jossa sen turvallisuuteen. Kyberturvallisuus sijoittuu tieto- ja viestintäverkkoihin ja sen uhkina ovat muun muassa **kyberuhkat**, joihin kuuluvat **kyberhyökkäykset, kybersodat** ja **kyberterrorismi**.

Kybermaailmalla tarkoitetaan digitaalisen maailman tilaa, jossa kyberturvallisuus esiintyy. Se ei ole täysin itsenäinen tila, vaan siihen liittyy myös **fyysinen maailma**, kuten esimerkiksi älypuhelimet ja tietokoneet. Kybermaailman ja fyysisen maailman rajapinnassa on **kriittinen infrastruktuuri**, jolla tarkoitetaan yhteiskunnan välttämättömiä toimintoja (esimerkiksi sähkölaitokset). Kybermaailmaan liittyvät internetissä ja tietoverkoissa olevat palvelut, tietojärjestelmät sekä sosiaalinen media.

Toimijat ovat henkilöitä tai organisaatioita, jotka ovat osa kyberturvallisuuden toteutumista. Nämä ovat jaettavissa yksityishenkilöihin, yrityksiin, organisaatioihin ja

valtioihin, murtautujiin sekä kyberrikollisiin. Murtautujissa esiintyy laillisissa tarkoituksissa toimivia **hakkereita**, laittomissa tarkoituksessa toimivia **krakkereita** sekä näiden väliin sijoittuvia murtautujia. Käytössä ovat myös termit *white hat* (hakkerit), *black hat* (krakkerit) sekä *grey hat* (näiden väliin sijoittuvat). Käyttöön on kuitenkin vakiintunut termi *hakkeri* kuvaamaan kaikkia tietojärjestelmiin murtautuvia tahoja. Selkeyden vuoksi olisikin hyvä käyttää eri termiä näistä murtautujista.

Kyberturvallisuuteen liittyy erilaisilta uhkilta suojautuminen. Näistä käytetään termiä **kyberuhkat,** joka jakautuu **kyberresilienssiin, kyberhyökkäyksiin, kybersotaan, kyberterrorismiin** ja **kyberrikollisuuteen. Kyberresilienssi** on varautumis- ja ennakoinkikykyä, toimintakykyä häiriötilanteessa sekä häiriötilanteen jälkeinen toipumis- ja palautumiskykyä (Kyberturvallisuusstrategia 2013: 4).

Kyberhyökkäykset ovat taloudellisista tai poliittisista syistä tehtyjä iskuja, jotka kohdistuvat kybermaailmaan (esimerkiksi tietojärjestelmiin) tai fyysisen maailman kohteisiin (esimerkiksi kriittisen infrastruktuuri). Hyökkäykset voivat olla **palvelunestohyökkäyksiä,** joilla estetään esimerkiksi verkkosivuille pääseminen tai **haittaohjelmia**, joilla pyritään estämään järjestelmän toimintaa. Hyökkääjät ovat esimerkiksi **kyberterroristeja** tai **krakkereita**.

Kybersota on tietoverkkojen välityksellä tapahtuvaa sodankäyntiä. Kybersotaan osallistuu valtiot, terroristit sekä muut ryhmittymät ja se sijoittuu joko kybermaailmaan tai sen kohteena voivat olla fyysisen maailman kohteet. **Kybersotilaat** ovat toimijoita, jotka osallistuvat kybersotaan valtion toimesta. **Kyberaseita** voivat olla joko digitaalisessa maailmassa käytettävät aseet tai fyysisissä aseissa saattaa olla siru, jolla voidaan etäohjata aseen toimintaa. Kybersotaan liittyy myös **kyberkyvykkyys**, jolla tarkoitetaan toimintavalmiutta. Se jakautuu puolustamiseen, vaikuttamiseen ja tiedusteluun.

Kyberterrorismi on poliittista vaikuttamista, joka kohdistuu kybersodan ulkopuolisiin henkilöihin ja ryhmiin. Sen kohteena on kriittinen infrastruktuuri ja kyberterrorismissa hyödynnetään kyberhyökkäyksiä, kuten **vakoiluohjelmia**. Muita kyberterrorismin

työkaluja ovat propagandan levittäminen ja vandalismi. Viranomaisyhteistyöllä pyritään ehkäisemään terrorismia.

Kybervakoilu on tiedonhankintaa digitaalisessa maailmassa. Se kohdistuu yrityksiin ja valtioihin. Yritykset ja valtiot osallistuvat myös vakoiluun, jonka lisäksi rikolliset pyrkivät vakoilemaan saadakseen tietoa. Tietoa hankitaan vakoiluohjelmilla, joiden kohteina ovat älypuhelimet, tietokoneet ja tietoverkot.

Kyberrikollisuudella tarkoitetaan laitonta toimintaa, joka kohdistuu yksityisiin henkilöihin tai yrityksiin. Kyberrikollisuus jakautuu perinteiseen rikollisuuteen sekä tietorikollisuuteen, jossa kohteena ovat tietokeskittymät kuten tietojärjestelmät. Kyberrikollisuutta torjuvat poliisit ja kybermaailmaan koulutetut **kyberpoliisit**, jotka selvittävät **kyberrikollisten** tekemiä rikoksia.

Kyberturvallisuuden varmistamiseksi valtiot ja yritykset laativat **kyberturvallisuusstrategioita.** Kyberturvallisuusstrategioiden osa-alueet ovat visio ja tavoitteet, toimijat, uhkamalli ja linjaukset.

Visio on tavoitetila, johon tulevaisuudessa pyritään (Viitala & Jylhä 2006). Sen osatekijöitä on puolustuskyky, kestävyys, johtaminen ja kansainvälinen toiminta. Visio muutetaan toiminnaksi toimeenpano-ohjelman, määriteltävien toimenpiteiden ja kyberturvallisuusharjoitusten avulla. Kyberturvallisuusstrategian **tavoitteessa** määritellään painopisteet, joihin pyritään, tulokset ja toimintalinjat, joilla tavoite saavutetaan.

Kyberturvallisuusstrategiassa **toimijat** jaetaan valtioneuvostoon, ministeriöön ja virastoihin, turvallisuuskomiteaan ja yrityksiin. Jokaisella toimijalla on oma roolinsa kyberturvallisuusstrategian suunnittelussa ja toimeenpanossa. **Valtioneuvosto** tekee strategiset linjaukset sekä tarjoaa voimavarat ja toimintaedellytykset muille toimijoille. **Ministeriöt ja virastot** toteuttavat ja toimeenpanevat strategian käytäntöön, kehittää kyberturvallisuuteen liittyvää toimintaa sekä **kyberhäiriötilanteiden hallinta** on viranomaisten vastuulla. Kyberhäiriötilanteet ovat kybermaailmassa olevia

häiriötilanteita, joka vaarantaa kybermaailmassa olevia toimintoja. **Turvallisuuskomitea** on viranomaisista ja yrityksistä koostuva toimija, jonka vastuulla on seurata kyberturvallisuusstrategian toteuttamista ja yhteensovittaa eri toimijoiden toimintaa. **Yritykset** laativat omat kyberturvallisuusstrategiansa, tarjoavat kyberturvallisuuteen liittyviä palveluita ja osallistuvat kyberturvallisuusstrategian toteuttamiseen.

Kyberturvallisuusstrategian keskiössä on **uhkamalli**, jossa määritellään turvallisuusuhkat. Siihen liittyvät **kyberuhkat**, joita ovat kyberhyökkäys, kybersota, kyberterrorismi, kybervakoilu, haktivismi ja kyberrikollisuus. Siinä määritellään myös häiriöt, joiden kestoa ja nopeutta arvioidaan.

Linjauksilla pyritään luomaan viranomaisille toimintamallit, parantamaan kyberturvallisuutta, kehittämään uhkiin liittyvää toimintaa ja mahdollistaa kyberturvallisuusstrategian toteuttaminen.

7 PÄÄTELMÄT

Tutkimuksen tavoitteena oli selvittää ja määritellä kyberturvallisuuteen kuuluvaa käsitteistöä. Alan käsitteistö on tutkimuksen teon aikana vuosina 2013–2016 hiljalleen vakiintunut, mutta käsitteitä ja termejä käytetään edelleen epäjohdonmukaisesti ja sekoitetaan usein tietoturvallisuuden käsitteistöön. Tutkimukseni pääkäsitteeksi valitsin kyberturvallisuuden, joka jakautui useampaan ala- ja lähikäsitteeseen.

Tutkimusmenetelmäksi valitsin systemaattisen käsiteanalyysin, jonka avulla tutkin kyberturvallisuuteen liittyviä käsitteitä ja niiden käsitesisältöjä. Lopuksi muodostin käsitteistä yhteinäisen kuvan. Tutkimuksessani etsin tutkimusaineistostani käsitteitä, joiden suhdetta selvensin graafisella esityksellä eli satelliittimallilla. Lopuksi kokosin jokaisesta käsitteestä yhtenäisen satelliittimallin kyberturvallisuuden alan käsitteistöstä. Aineistona käytin Limnéllin ym. (2014) teosta Kyberturvallisuus, valtiohallinnon laatimia strategioita, termistöjä, Helsingin Sanomien uutisartikkeleita sekä muiden julkaisemia uutisartikkeleita, tiedotteita ja periaatepäätöksiä sekä muita yksittäisiä artikkeleita eri tiedotusvälineistä ja aikakausilehdistä.

Tutkimukseni jakautui kahteen tutkimuskysymykseen. Ensiksi selvitin, mitä kyberturvallisuus on ja miten se eroaa tietoturvallisuudesta. *Kyber*-etuliitteellä viitataan digitaaliseen tilaan, jossa yhdistyy informaatioteknologia ja jossa toimitaan tietoverkkojen välityksellä. Eri aineistoja tarkastelemalla selvisi, että kyberturvallisuus ja tietoturvallisuus eivät kuvaa samaa ilmiötä, vaan **kyberturvallisuudella** viitataan yleisemmin digitaalisen maailman eli tietoverkoissa tapahtuvan toiminnan turvallisuuteen. Se kuvaakin laajemmin tietoverkkoihin kohdistuvia uhkia ja turvaamista. **Tietoturvallisuus** on sen sijaan tiedon luotettavuutta ja turvaamista. Siinä missä kyberturvallisuus liittyy aina digitaaliseen ympäristöön, tiedon eheys ja luotettavuus eivät esiinny ainoastaan tietoverkoissa. Myöskään kyberturvallisuus ei ole tietoturvallisuuden alakäsite, vaan ovat toistensa lähikäsitteitä. Näiden kahden yläkäsitteeksi nousi **kokonaisturvallisuus**. Kokonaisturvallisuudella tarkoitetaan yhteiskunnan tilaa, jossa ”elintärkeisiin toimintoihin kohdistuvat uhkat ja riskit ovat hallittavissa” (Kokonaisturvallisuuden sanasto 2014: 22).

Toiseksi selvitin kyberturvallisuuden alan käsitteistöä laajemmin. Poimin tutkimusaineistostani kyberturvallisuuteen liittyviä käsitteitä ja muodostin ensin suppean kokonaiskuvan. **Kyberturvallisuuteen** liittyy neljä käsitekokonaisuutta: kybermaailma, toimijat, kyberuhkat ja kyberturvallisuusstrategia. Muodostin jokaisesta neljästä isommasta käsitteestä omat satelliittimallit, joihin kokosin jokaiseen käsitteeseen liittyviä lähikäsitteitä. Usealla käsitteellä saattoi olla useampi eri termi tai samalla termillä saatettiin viitata eri käsittesiin, jolloin tein oman ehdotukseni käytettävästä termistä. Esimerkiksi termillä *hakkeri* viitattiin kaikkiin tietojärjestelmiin murtautujiin tai vain laillisissa tarkoituksissa toimiviin murtautujiin, minkä takia sopiva termi yläkäsitteelle on murtautujat ja laillisissa tarkoituksissa murtautuville termi *hakkeri*. Kuitenkin *hakkeri*-termi on vakiintumassa tarkoittamaan kaikkea tietojärjestelmään murtautumista, jolloin erityyppisille murtautujille olisi hyvä muodostaa omat nimityksenä.

Tutkimukseni lopputuloksena muodostin yhteinäisen satelliittimallin, johon kokosin kaikki tutkimusaineistostani löytämäni käsitteet. Kyberturvallisuuden alan käsitteistö on tällä hetkellä laaja. Se on monialainen erikoisala, joka vielä hakee rajojaan. Kyberturvallisuuden erikoisalan käsitteistössä on tällä hetkellä käsitteitä ja termejä, jotka ovat aiemmin esiintyneet poliisien (esimerkiksi rikollisuus), puolustusvoimien (sotaan ja terrorismiin liittyvät), viranomaisten ja yritysten (strategia) sekä internetkulttuurin (hakkerit) erikoisaloilla. Tämä selittänee sen, miksei tiedotusvälineissä vielä käytetä käsitteitä ja termejä yhteneväisesti.

Osa tutkimusaineiston pohjalta nostetuista käsitteistä esiintyivät myös **tietoturvallisuuden** käsitteen alla. Nostin näistä käsitteistä kuvaavimmat ja kyberturvallisuuteen selkeimmin liittyvät omaan satelliittimalliini. Tutkimusaineiston vuoksi satelliittimalli kuvastaa lähinnä vuosina 2013–2015 ollutta käsitteistöä, jolloin käsitteiden määrään ja termeihin on voinut tulla muutoksia tutkimuksen valmistumisvuonna 2016.

Koska kyberturvallisuusalan käsitteistö on kohtalaisen uutta, tutkimuksen teon aikana vuosina 2013-2016 käsitteet ovat vakiintuneet alkutilanteeseen nähden. Esimerkiksi Sanastokeskus TSK julkaisi joulukuussa 2014 oman kokonaisturvallisuuden alan sanaston, jossa on määritelty tutkimuksessani esiintyviä käsitteitä. Otin Sanastokeskuksen laatiman sanaston osaksi tutkimusaineistoani juurikin käsitteiden vakiintumisen vuoksi. Tästä huolimatta erityisesti tiedotusvälineissä käsitteiden käyttö on vasta vakiintumassa, jonka vuoksi aihetta kannattaa vielä jatkossa tutkia.

Keskityin tutkimuksessani suomalaiseen aineistoon, sillä halusin selvittää suomalaisten käytössä olevaa käsitteistöä. Kyberturvallisuus on kuitenkin yleismaailmallinen ilmiö, jonka vuoksi selvää rajausta ei voi tehdä suomalaisen ja ulkomaalaisen käsitteistön välillä. Jatkossa kyberturvallisuuden käsitteistön tutkimusta voisi laajentaa ulkomaalaiseen aineistoon ja esimerkiksi verrata sitä, miten käsitteistö eroaa esimerkiksi suomalaisessa ja yhdysvaltalaisessa aineistossa. Suomenkielisessä käsitteistössä tapahtuu vakiintumista, joten esimerkiksi muutaman vuoden kuluttua käsitteistön muutosta voisi tutkia ja verrata 2010-luvun alussa käytössä olleisiin käsitteisiin.

LÄHTEET

Business Dictionary (2015). *Strategic vision*. [Lainattu 29.3.2015] Saatavana: http://www.businessdictionary.com/definition/strategic-vision.html

F-Secure (2016). *Who we are. F-Secure at a glace*. [Lainattu 20.1.2016] Saatavilla: https://www.f-secure.com/en/web/about_global/about-us

Hagelstam, Alex (2005). *CIP – kriittisen infrastruktuurin turvaaminen.* Käsiteanalyysi ja kansainvälinen vertailu. Helsinki: Huoltovarmuuskeskus.

Hanska, Jan (2013). The Emperor's Digital Clothes: Cyberwar and the Application of Classical Theories of War. Teoksessa: *The Fog of Cyber Defence*. Toim. Rantapelkonen Jari & Mirva Salminen. Helsinki: Maanpuolustuskorkeakoulu.

Helsingin Sanomat (2013a). *Laaja kybervakoilu paljastui* [Lainattu 15.1.2015] Saatavilla: http://www.hs.fi/paivanlehti/kotimaa/Laaja+kybervakoilu+paljastui/a1358137665361

Helsingin Sanomat (2014a). Arkistohaku hakusanalla kyberturvallisuus. [Lainattu 12.2.2015] Saatavilla: http://www.hs.fi/haku/?haku=kyberturvallisuus

Helsingin Sanomat (2014b). *Tietomurto Yhdysvaltojen suurimpaan pankkiin vei 83 miljoonan asiakastiedot.* [Lainattu 10.2.2015] Saatavilla: http://www.hs.fi/a1305881364549

Helsingin Sanomat (2014c). *Kyberaika muuttaa sotia ja konflikteja*. [Lainattu 10.1.2015] Saatavilla: http://www.hs.fi/kotimaa/a1405826705250

Helsingin Sanomat (2014d). *Venäjä ja Kiina allekirjoittamassa sopimuksen verkkosodan välttämisestä* [Lainattu 10.1.2015] Saatavilla: www.hs.fi/ulkomaat/a1305891567367

Helsingin Sanomat (2014e). *Kyberpoliisit tulevat Suomeen*. [Lainattu 10.1.2015] Saatavilla: http://www.hs.fi/kotimaa/a1392435533996

Helsingin Sanomat (2014f). *Puolustusvoimien komentaja: Kyber-taitojen opettaminen varusmiehille selvitetään jo tänä vuonna*. [Lainattu 10.1.2015] Saatavilla: http://www.hs.fi/kotimaa/a1411641881547

Helsingin Sanomat (2014g). *Supo: Ulkoministeriötä vakoili kaksi eri valtiota – "materiaalia on viety runsaasti"*. [Lainattu 10.1.2015] Saatavilla: http://www.hs.fi/kotimaa/a1404264100388

Helsingin Sanomat (2014h). *Kansallinen kyberturvaharjoitus käynnissä Jyväskylässä*. [Lainattu 10.1.2015] Saatavilla: http://www.hs.fi/kotimaa/a1402377051452

Helsingin Sanomat (2015). *Kyberhyökkäys voi uhata yhteiskuntarauhaa.* [Lainattu

10.1.2015] Saatavilla: www.hs.fi/kotimaa/a1420258381241

Helsingin poliisilaitos (2015). *Poliisi sosiaalisessa mediassa*. [Lainattu 15.1.2015] Saatavilla: https://www.poliisi.fi/nettipoliisi

Ilta-Sanomat (2016). *Tietoturvayritys Kaspersky Lab vahvistaa Ilta-Sanomille: venäläinen Turla vakoili valtion tuella.* [Lainattu 10.2.2016] Saatavilla: http://www.iltasanomat.fi/digi/art-2000001065486.html

ISO/IEC (2009). *ISO/IEC 2700:2009. Information technolog. Security techniques. Information security management systems. Overview and vocabulary.* Sveitsi: ISO/IEC.

IT-viikko (2014). *Suomeen uusi virka: kybersuurlähettiläs*. [Lainattu 15.1.2015] Saatavilla: http://www.itviikko.fi/uutiset/2014/09/01/suomeen-uusi-virka-kybersuurlahettilas/201412076/7

Kalliokuusi Virpi & Katri Seppälä (2014*).* Terminologisen käsiteanalyysin rooli käsitemallinnuksessa. *Terminfo,* 2014: 4.

Kokonaisturvallisuuden sanasto (2014). Sanastokeskus TSK. Helsinki: Suomen Pelastusalan Keskusjärjestö SPEK.

Kyberturvallisuuskeskus (2015). *Kyberturvallisuuskeskuksen vuosikatsaus. Vuosi 2014.* Helsinki: Viestintävirasto.

Kyberturvallisuusstrategia (2013). Helsinki: Turvallisuuskomitean sihteeristö

Liikenne- ja viestintäministeriö (2008). *Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi*. Helsinki: Liikenne- ja viestintäministeriö.

Limnéll, Jarmo, Klaus Majewski & Mirva Salminen (2014). *Kyberturvallisuus*. Jyväskylä: Docendo.

Länsi- ja Sisä-Suomen aluehallintovirasto (2014a). *Pirkka 14 -valmiusharjoitus alkaa*. [Lainattu 10.10.2014] Saatavana: https://www.avi.fi/web/avi/-/pirkka-14-valmiusharjoitus-alkaa-lansi-ja-sisa-suomi-

Länsi- ja Sisä-Suomen aluehallintovirasto (2014b). *Pirkka 14 -valmiusharjoitus todisti: kunnat ja viranomaiset kaikki riippuvaisia toisistaan.* [Lainattu 1.12.2014] Saatavana: http://www.avi.fi/web/avi/-/pirkka-14-valmiusharjoitus-todisti-kunnat-ja-viranomaiset-kaikki-riippuvaisia-toisistaan-lansi-ja-sisa-suomi-

Mindell, David A. (2002). *Between Human and Machine: Feedback, Control, and Computing Before Cybernetics.* Baltimore: The Johns Hopkins University Press.

MTV Uutiset (2014). *Asiantuntija vastaa: Tällaista on kybervakoilu Suomessa*. [Lainattu 12.2.2015] Saatavana: http://www.mtv.fi/uutiset/kotimaa/artikkeli/asiantuntija-vastaa-tallaista-on-kybervakoilu-suomessa/4386560

National Research Council Staff, Committee on the Internet in the Evolving Information Infrastructure (2001). *Internet's Coming of Age*. Washington D.C: National Academies Press.

Nuopponen, Anita (2003). Käsiteanalyysi asiantuntijan työvälineenä. Teoksessa: *Kieli ja asiantuntijuus*. AfinLA-vuosikirja, 13-24. Toim. Merja Koskela & Nina Pilke. Jyväskylä: Suomen soveltavan kielitieteen yhdistys.

Nuopponen, Anita (2009). Käsiteanalyysia käsiteanalyysistä – kohti systemaattista käsiteananalyysia. Teoksessa: *XXIV Vakki-Symposiumi*. Toim. Mona Enel-Nilsson ja Niina Nissilä. Vaasa: Vaasan yliopisto

Nuopponen, Anita (2011). Methods of concept analysis – tools for systematic concept analysis. *The LSP Journal - Language for special purposes, professional communication, knowledge management and cognition*. Vol 2, 4-15.

Nuopponen, Anita & Nina Pilke (2010). *Ordning och reda*. Terminologilära i teori och praktik. Stockholm: Nordstedts.

O'Reilly, Tim (2005). *What is Web 2.0. Design Patterns and Business Models for Next Generation of Software*. [online] [Lainattu 16.2.2016] Saatavana: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

Oxford Dictionaires (2014). *Cyber*. [online] [Lainattu 10.10.2014] Saatavana: http://www.oxforddictionaries.com/definition/english/cyber

Palokangas, Tero (2013). Cyberwar: Another Revolution in Military Affairs? Teoksessa: *The Fog of Cyber Defence*. Toim. Rantapelkonen Jari & Mirva Salminen. Helsinki: Maanpuolustuskorkeakoulu.

Peter, Ian (2004). *So, who really did invent the Internet?* [Lainattu 15.10.2014] Saatavana: http://www.nethistory.info/History%20of%20the%20Internet/origins.html

Rantapelkonen Jari & Harry Kantola (2013). Insights into Cyberspace, Cyber Security, and Cyberwar in the Nordic Countries. Teoksessa: *The Fog of Cyber Defence*. Toim. Rantapelkonen Jari & Mirva Salminen. Helsinki: Maanpuolustuskorkeakoulu.

Rantapelkonen Jari & Mirva Salminen (2013). Summary. Teoksessa: *The Fog of Cyber Defence*. Toim. Rantapelkonen Jari & Mirva Salminen. Helsinki: Maanpuolustuskorkeakoulu.

Ruby, Charles L (2002). The Definition of Terrorism. *Analyses of Social Issues and Public Policy*. Volume 2: Issue 1.

Ryan, Johnny (2010). *History of Internet and Digital Culture*. Lontoo: Reaktion Book.

Saarelainen, Ari (2013). *Kybersodan aseet.* Tietokone, 2013: 9. Helsinki: Sanoma Magazines.

Sager, Juan C (1990). *A practical course in terminology processing.* Amsterdam: Benjamins.

Sanastotyön käsikirja (1988). Tekniikan sanastokeskus. Jyväskylä: Gummerus

Sisäasiainministeriö (2014). *Valtioneuvoston periaatepäätös kansalliseksi terrorismin torjunnan strategiaksi 2014-2017*.

Sitra (1996). *Suomi teollisen ja tietoyhteiskunnan murroksessa*. Tietoyhteiskunnan sosiaaliset ja yhteiskunnalliset vaikutukset. Toim. Antti Hautamäki. Helsinki: Suomen itsenäisyyden juhlarahaston Sitra.

Slade, Rob (2006). *Dictionary of Information Security*. Syngress Publishing.

Terminologian sanasto (2006). Sanastokeskus TSK. Helsinki: Sanastokeskus TSK.

Tiivis tietoturvasanasto (2004). Sanastokeskus TSK. Helsinki: Sanastokeskus TSK.

TiVi (2013). *Puolustusvoimat järjestää viisipäiväisen kyberharjoituksen*. [Lainattu 20.1.2015] Saatavana: http://www.tivi.fi/Arkisto/2013-05-10/Puolustusvoimat-j%C3%A4rjest%C3%A4%C3%A4-viisip%C3%A4iv%C3%A4isen-kyberharjoituksen-3200779.html

TiVi (2016). Vakoiluvirasto järjestää kesäkursseja – maksaa opiskelijoille. [Lainattu 18.2.2016]. Saatavana: http://www.tivi.fi/Kaikki_uutiset/ vakoiluvirasto-jarjestaa-kesakursseja-maksaa-opiskelijoille-6246360

Turvallisuuskomitea (2014). Kyberturvallisuusstrategian toimeenpano-ohjelma. Helsinki.

Viitala, Riitta & Eila Jylhä (2006). *Liiketoimintaosaaminen: menestyvän yritystoiminnan perusta*. Helsinki: Edita.

Webster Frank (2014). *Theories of the Information Society*. 4. painos. New York: Routledge.

LIITTEET

Liite 1. Kyberturvallisuuden alan käsitteistö