Sähkötekniikan korkeakoulu

Kyber rantautui Suomeen

Jarno Limnéll

Aalto-yliopisto

TIEDE + TEKNOLOGIA

TYÖPAPERIT

Aalto-yliopiston julkaisusarja
TIEDE + **TEKNOLOGIA** 12/2014

Kyber rantautui Suomeen

Jarno Limnéll

Aalto-yliopisto
Sähkötekniikan korkeakoulu
School of Electrical Engineering

Jarno Limnéll
Professor
Cyber Security
Aalto University
Department of Communications and Networking
P.O. BOX 13000
00076 AALTO
FINLAND
Tel: +358-(0)40-5276173
Twitter: @JarnoLim
email: jarno.limnell@aalto.fi

Aalto-yliopiston julkaisusarja
TIEDE + **TEKNOLOGIA** 12/2014

ISBN 978-952-60-6021-7 (painettu)
ISBN 978-952-60-6022-4 (pdf)
ISSN-L 1799-487X
ISSN 1799-487X (painettu)
ISSN 1799-4888 (pdf)
http://urn.fi/URN:ISBN:978-952-60-6022-4

Unigrafia Oy
Helsinki
2014

441 697
Painotuote

Alkusanat

Kyber-alkuiset sanat ovat vakiintumassa osaksi suomen kieltä ja kulttuuria. Puhumme jo varsin sujuvasti kyberturvallisuudesta, kyberuhkista ja esimerkiksi kybertoimintaympäristöstä. Suomalaisesta yhteiskunnasta ja yrityselämästä löytyy useita tehtävänimikkeitä, kuten kyberturvallisuusasiantuntija ja kybersuurlähettiläs, joissa etuliitteenä on ”kyber.” Suomeen on hiljattain perustettu Kyberturvallisuuskeskus, luotu kyberturvallisuusstrategia, perustettu kyberturvayhtiöitä ja voimme vierailla kyberturvallisuusmessuilla. Kyber on rantautunut Suomeen.

Tämän tutkimuksen tarkoituksena oli selvittää miten ja erityisesti milloin kyber-käsitteet ovat ilmestyneet suomalaiseen hallinnolliseen turvallisuusajatteluun. Milloin valtionhallinnon ja tämän tutkimuksen kannalta sen keskeisimpien virastojen asiakirjoissa alettiin käyttää kyber-käsitteitä ja minkälaisia merkityssisältöjä käsitteille on annettu?

Kyber-käsite ei ole ilmestynyt Suomeen tyhjästä ja siksi on merkityksellistä tutkia, että milloin ja millaisten annettujen merkityssisältöjen kautta kyber-käsite on hallinnolliseen turvallisuusajatteluun rantautunut. Selvyyden vuoksi todetaan, että tutkimuksen tavoitteena ei ollut määritellä kyber-sanaa tai siihen yhdistettäviä lisämääreitä.

Espoo, 26 Marraskuu 2014
Jarno Limnéll

Sisältö

1. Johdanto[1]

Kyber-alkuiset sanat ovat vakiintumassa osaksi suomen kieltä ja kulttuuria. Puhumme jo varsin sujuvasti kyberturvallisuudesta, kyberuhkista ja esimerkiksi kybertoimintaympäristöstä. Suomalaisesta yhteiskunnasta ja yrityselämästä löytyy useita tehtävänimikkeitä, kuten kyberturvallisuusasiantuntija ja kybersuurlähettiläs, joissa etuliitteenä on ”kyber.” Suomeen on hiljattain perustettu Kyberturvallisuuskeskus, luotu kyberturvallisuusstrategia, perustettu kyberturvayhtiöitä ja voimme vierailla kyberturvallisuusmessuilla. Kyber on rantautunut Suomeen.

Ajalle ominaista on, että kyber jakaa käsitteenä varsin voimallisesti ihmisten mielipiteitä niin yhteiskunnallisesti kuin akateemisesti. Käsitteenmäärittely on parhaillaan käynnissä, eikä selkeää vakiintunutta määrittelyä kyberistä suomen kielessä ole.

Sanana kyber tulee kreikan kielen sanasta kybereo[2] – ohjata, opastaa, hallita. Kyberin alkulähteitä tutkittaessa viitataan usein kybernetiikkaan, jonka juuret johdetaan Norbert Wienerin vuonna 1948 julkaisemaan teokseen Cybernetics[3], jossa Wiener tutki ohjaamisen ja valvonnan suhdetta viestintään. Kyborgeista[4] on puhuttu 1960-luvulta lähtien ja kyberavaruuden -käsite (cyberspace) on ollut kansainvälisesti käytössä ainakin 1980-luvun puolivälistä alkaen. Suomen kielen kyber pohjautuu englanninkieliseen sanaa ”cyber”, mikä Oxfordin sanakirjan mukaan yhdistyy tietokoneiden kulttuuriin, informaatioteknologiaan ja virtuaaliseen todellisuuteen. [5]

Suomen kielessä kyber-sanaa harvoin käytetään yksinään vaan se esiintyy lähes poikkeuksetta yhdyssanan määriteosana. Tällöin on huomioitava, että esimerkiksi sanoissa kyberturvallisuus tai kyberterrorismi on kaksi varsin kiis-

[1] Esitän lämpimät kiitokset tutkimusta tukeneille tahoille, erityisesti Liikenne- ja viestintäministeriölle, Turvallisuuskomitean sihteeristölle ja Viestintävirastolle.
[2] Jarno Limnéll, Klaus Majewski, Mirva Salminen, *Kyberturvallisuus*, Docendo, Saarijärven Offset Oy, 2014, s. 29.
[3] Kybernetiikalla tarkoitetaan oppia konemaisista ja inhimillisistä tietoa käsittelevistä itseohjautuvista automaattisista järjestelmistä tai yleisesti itseohjautuvia automaattisesti säätyviä systeemejä. Norbert Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine*, Cambridge, The MIT Press 1948.
[4] Kyborgilla viitataan kyberneettiseen eliöön, eli esimerkiksi ihmiseen, johon on yhdistetty tekniikkaa. Ks. mm. Kevin Warwick, *I, Cyborg*, University of Illinois Press, 2004.
[5] http://www.oxforddictionaries.com/definition/english/cyber 2.10.2014.

teltyä ja monimerkityksellistä käsitettä (kyber ja turvallisuus, kyber ja terrorismi), joiden merkityssisällöistä esiintyy hyvinkin erilaisia tulkintoja. Käytännön näkökulmasta kyberpuhe ja -kieli on merkittävällä tavalla yleistynyt muun muassa liike-elämän ja turvallisuuspolitiikan yhteydessä. Kyberpuhetta ja -kieltä on myös kritisoitu,[6] sitä on pidetty ”hypetyksenä” ja kansallista kyberstrategiaa kapulakielisenä.

Oman haasteensa kyber-sanan määrittelyyn tuovat muut käsitteet, joita käytetään joko kyber-sanan alakäsitteinä, toisensa leikkaavina käsitteinä, samanvertaisina käsitteinä tai yläkäsitteinä, ilmaisijan näkemyksestä riippuen. Esimerkiksi kyberturvallisuuden, tietoturvallisuuden, verkkoturvallisuuden ja tietokoneturvallisuuden yhteneväisyyksistä ja eroavaisuuksista käydään parhaillaan Suomessa suhteellisen aktiivista keskustelua. Yleisesti kyberturvallisuutta voi todeta pidettävän tietoturvallisuutta, verkkoturvallisuutta ja tietokoneturvallisuutta laajempana kokonaisuutena ja ulottuvuutena, jota arvioidaan Suomessakin lisääntyvissä määrin tasavertaisena muihin toimintaympäristöihin (maa, meri, ilma, avaruus).[7] Tätä voi pitää varsin yleisenä kansainvälisenä kyberturvallisuuden ajattelutapana.

Tämän tutkimuksen tarkoituksena on selvittää miten ja erityisesti milloin kyber-puhe ja -kieli ovat ilmestyneet suomalaiseen hallinnolliseen turvallisuusajatteluun. Milloin valtionhallinnon ja tämän tutkimuksen kannalta sen keskeisimpien virastojen asiakirjoissa alettiin käyttää kyber-käsitteitä ja minkälaisia merkityssisältöjä käsitteille on annettu? Kyber-käsite ei ole ilmestynyt Suomeen tyhjästä ja siksi on merkityksellistä tutkia, että milloin ja millaisten annettujen merkityssisältöjen kautta kyber-käsite[8] on hallinnolliseen turvallisuusajatteluun rantautunut. Selvyyden vuoksi todetaan, että tutkimuksen tavoitteena ei ole määritellä kyber-sanaa tai siihen yhdistettäviä lisämääreitä.

1.1 Tutkimuskysymykset

Tutkimuksessa vastataan neljään tutkimuskysymykseen:

- Missä, milloin ensi kertaa ja minkälaisessa kontekstissa ”kyberturvallisuus” käsitteenä mainitaan valtionhallinnon turvallisuusasiakirjoissa?

[6] Ks. mm. Jari Rantapelkonen, ”Kansallinen turvallisuus kohtaa kybertrendit”, *Futura*, No. 2 / 2014, s. 53.

[7] Mm. pääministeri Alexander Stubb on todennut, että ”Monissa maissa on maa-, meri- ja ilmavoimat, ja niiden rinnalla oma puolustushaara kybertoiminnoille. Mielestäni Suomessa olisi harkittava samaa.” *Verkkouutiset*, ”Alexander Stubb: Suomen haettava Nato-jäsenyyttä seuraavalla hallituskaudella”, 22.5.2014.

[8] Käsitteiden avulla kuvataan todellisuutta (luoden merkityssisältöjä miten todellisuus tulisi kyseisen käsitteen kautta ymmärtää), kommunikoidaan sekä pyritään jäsentämään ja luokittelemaan maailmaa.

- Miten paljon kyberturvallisuuden käsitettä käytetään eri hallinnonalojen asiakirjoissa ja millaisissa konteksteissa?

- Mitä muita käsitteitä kyberturvallisuuteen yhdistetään ja mikä on käsitteiden välinen merkityssuhde toisiinsa?

- Minkälaisia merkityssisältöjä kyberturvallisuudelle annetaan?

1.2 Tutkimusaineisto ja rajaukset

Valtionhallinnossa korostetaan turvallisuuden osalta kokonaisturvallisuuden käsitettä, mikä kuvataan tavoitetilaksi, jossa valtion itsenäisyyteen, väestön elinmahdollisuuksiin ja muihin yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat ovat hallittavissa.[9] Kokonaisturvallisuuden käsitteellä halutaan korostaa kokonaisvaltaisen sekä eri toimijoiden poikkihallinnollisen yhteistoiminnan välttämättömyyttä turvallisuuden tuottamisessa. Ajattelumallin perusteella jokaista hallinnonalaa ja viranomaista voi pitää tämän päivän Suomessa turvallisuusviranomaisena.

Kokonaisturvallisuuden korostamisesta huolimatta tähän tutkimukseen on tutkimusaineiston osalta tehty rajauksia, ja osa hallinnonaloista ja viranomaistahoista on jätetty tutkimuksen ulkopuolelle. Tutkimuksen aineistossa on keskitytty keskeisimpien suomalaista kokonaisturvallisuutta määrittävien ja ohjaavien ministeriöiden sekä toimivaltaisten viranomaisten[10] asiakirjoihin sekä valtionhallinnon keskeisimpiin turvallisuusasiakirjoihin. Tutkimusaineistossa on pyritty keskittymään erityisesti sellaisiin valtionhallinnon turvallisuusasiakirjoihin, joilla on ajallinen jatkumo, mikä on perusteltua ajallista käsitemuutosta ja kyber-käsitteen ilmaantumista tutkittaessa. Toisaalta lähdemateriaaliin on otettu mukaan keskeisimmät ICT[11]-alaa koskevat valtionhallinnon strategia-asiakirjat, joilla voi arvioida olleen keskeinen asema ICT-alan käsitemäärittelyissä.

Tutkimuksen lähdeaineistona on käytetty seuraavia asiakirjoja:

- Hallitusohjelmat 2003–2014
- Huoltovarmuuskeskuksen vuosikertomukset vuosilta 2004–2013
- ICT 2015 -työryhmän raportti, 2013
- Julkisen hallinnon ICT:n hyödyntämisen strategia 2012–2020, 2013
- Parlamentaarisen selvitysryhmän raportti 2014
- Sisäisen turvallisuuden ohjelma 2004, 2008, 2012

[9] *Valtioneuvoston periaatepäätös kokonaisturvallisuudesta*, 5.12.2012, s 7.
[10] Ks. mm. ibid. s. 9-11.
[11] ICT tarkoittaa tieto- ja viestintätekniikkaa.

- Suomen kyberturvallisuusstrategia ja taustamuistio 2013, sekä Kyberturvallisuusstrategian toimeenpano-ohjelma 2014
- Kansallinen tietoturvastrategia 2003 (yhdistettynä neuvottelukunnan kertomukseen 2004) ja Kansallinen tietoyhteiskuntastrategia 2007–2015
- Tulevaisuuskatsaukset 2006, 2010 ja 2014
  - Liikenne- ja viestintäministeriö
  - Puolustusministeriö
  - Sisäasiainministeriö
  - Ulkoasianministeriö
  - Valtiovarainministeriö[12]
- Turvallisuus- ja puolustuspoliittinen selonteko 2004, 2009 ja 2012[13]
- Varautuminen ja kokonaisturvallisuus, komiteamietintö 2010 (ns. Hallbergin komitean mietintö)
- Viestintäviraston vuosikertomukset vuosilta 2005–2013
- Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2003, 2006
- Yhteiskunnan turvallisuusstrategia 2010

Tutkimusaineiston keskittyessä valtionhallinnon ja viranomaisten asiakirjoihin, on tutkimuksesta rajattu pois muun muassa kyber-käsitteen ilmeneminen suomalaisessa lehdistössä, puheissa, akateemisissa julkaisuissa sekä kyber-käsitteen käyttö ja merkityssisällön arviointi kansainvälisessä kontekstissa. Tutkimuksen ulottamista nyt tehtyjen rajausten ulkopuolelle, esimerkiksi suomalaiseen lehdistöön ja akateemisiin julkaisuihin, voi pitää suositeltavana jatkotutkimusaiheena. Ajallisesti tutkimus keskittyy 2000-luvun alkuun. Viimeisimpänä tutkimuksessa huomioituna lähdemateriaalina on Parlamentaarisen selvitystyöryhmän raportti, mikä julkistettiin lokakuussa 2014.

1.3 Metodologia

Tutkimuksen metodina on kvalitatiivinen sisällönanalyysi[14], jonka tavoitteena on kuvata aineiston jakautumista luokkiin ja kategorioihin ja sillä tavoin kuvata tutkimusaineiston sisältöä sanallisesti. Sisällönanalyysi on tässä tutkimuksessa ymmärrettävä menettelytavaksi, jonka avulla tutkimusaineistoa analysoidaan systemaattisesti ja induktiivisesti. Tavoitteena on luoda selkeyttä varsin laajaan tutkimusaineistoon, jotta voidaan tehdä selkeitä ja luotettavia johtopäätöksiä. Tutkimukseen on tehty aineistolähtöiset luokittelutaulukot asiakirjoittain, jotka ovat saatavissa tutkijalta.

[12] Valtiovarainministeriö vastaa julkisen hallinnon tieto- ja viestintäteknisten toimintojen ohjaamisesta ja kehittämisestä.
[13] Tutkimuksessa on myös huomioitu Turvallisuus- ja puolustuspoliittisista selonteoista eduskunnassa annetut Ulkoasianvaliokunnan sekä puolustusvaliokunnan lausunnot ja mietinnöt.
[14] Sisällönanalyysistä tarkemmin mm. Jouni Tuomi & Anneli Sarajärvi, *Laadullinen tutkimus ja sisällönanalyysi*, Tammi, Helsinki 2013.

Tutkimuksen kannalta on metodisesti oleellista kiinnittää huomio ”kyber-ilmiöön”, jolle tutkimusaineistossa annetaan merkityssisältöjä. Tutkimuksen tavoitteena ei ole tutkia ovatko kyber-käsitteen ja sen yhdyssanojen määritelmät ja käsitteet sekä niihin yhdistettävät kontekstit oikeita tai vääriä, vaan millaista kontekstuaalista merkityssisältöä kyber-käsitteelle tutkimusaineistossa rakennetaan ja mikä on näiden käsitteiden ja merkityssisältöjen ajallinen ilmentymä.[15]

Tutkimuksen sisällönanalyysin metodologiassa aineistoa ryhmitellään[16] ja tulkitaan sisällöllisten luokittelujen avulla. Ryhmittelyn pohjalta kyetään esittämään empiiriselle aineistolla konkreettisia kysymyksiä sekä todentamaan eroavaisuuksia eri käsitemäärittelyiden ja niihin yhdistettävien kontekstien välille. Ryhmittelyä ei tule nähdä mekaanisena tai kvantitatiivisena vaan luovana ja kontekstisidonnaisena metodisena apuvälineenä. Turvallisuus[17] toimii ryhmittelyä ohjaavana teemana. Empiirisen aineiston ryhmittely on tutkimuksessa tehty seuraavasti:

a) Kyber-käsitteeseen tai kyber-etuliitteeseen yhdistettyjen lisämääreiden esiintyminen:
    a. Eri asiakirjoissa
    b. Ajallinen esiintyminen
    c. Esiintymistiheys
    d. Esitetty merkityssisältö ja konteksti
b) Kyberturvallisuutta lähellä olevien käsitteiden esiintyminen:
    a. Eri asiakirjoissa
    b. Ajallinen esiintyminen
    c. Esiintymistiheys
    d. Esitetty merkityssisältö ja konteksti

[15] Tutkimuksessa ei myöskään arvioida käsitteiden taustalla olevia toiminnallisia tai muita motiiveja, eikä tutkimuksessa huomioida tutkimusaineistossa mahdollisesti piilossa olevia viestejä.
[16] Tutkimusaineistosta etsitään samankaltaisuuksia ja eroavaisuuksia kuvaavia kyber-käsitteitä. Ryhmittelyä on tutkimuksessa pidetty joustavana, sillä erillisiä hypoteeseja ei tutkimuksessa asetettu. Ks. Tuomi, Sarajärvi s. 93, 105–116.
[17] Tutkimusaineistosta etsitään samankaltaisuuksia ja eroavaisuuksia kuvaavia kyber-käsitteitä. Ryhmittelyä on tutkimuksessa pidetty joustavana, sillä erillisiä hypoteeseja ei tutkimuksessa asetettu. Ks. Tuomi, Sarajärvi s. 93, 105–116.

2. Aika ennen kyberiä

Suomessa ilmestyi vuonna 1980 Teknologiakomitean mietintö, jossa kuvataan siirtymistä informaatioyhteiskuntaan, teknologian mahdollisuuksia ja kehityksen sosiaalisia vaikutuksia sekä teknologian arvioinnin merkitystä. Mielenkiintoisena yksityiskohtana on pidettävä sitä, ettei pääasiana mietinnössä pidetty teknologian ennustamista vaan ensisijaisesti erilaisten uhkakuvien tunnistamista. Käsite tietotekniikka levisi Suomessa yleiseen tietoisuuteen 1980-luvun alussa.[18]

Suomalaisen tietoyhteiskunnan mahdollisuuksien tarkastelua ja sitä koskevia linjauksia tehtiin 1990-luvulla useilla hallinnonaloilla. Samalla tietoyhteiskunnan käsite vakiintui valtionhallinnossa. 1990-luvulla kirjoitettiin kaksi tietoyhteiskuntastrategiaa[19], joissa luotiin visio Suomesta verkostomaisena tietoyhteiskuntana, joka kilpailisi maailman kärkimaiden kanssa. Strategioissa turvallisuus oli teemana esillä ja käsitteinä puhuttiin tietoturvallisuudesta ja tietosuojasta. Vuonna 1999 Lipposen II hallituksen ohjelmassa todettiin, että julkisten palveluiden saumattomuutta ja kustannustehokkuutta tuli parantaa tieto- ja viestintätekniikan avulla huolehtien samalla tietoturvallisuudesta. Ohjelman mukaan hallitus aikoi selvittää miten tietoliikenteen ja tietoverkkojen turvallisuus- ja suojaustekniset kysymykset tulisi hallinnollisesti järjestää. Selvitystyön tuloksena Viestintävirasto vakiinnutti asemansa Suomessa niin kansalaisten, yritysten kuin julkisyhteisöjenkin toimijoiden tietoturvaa edistävänä ja tukevana viranomaisena.

Anneli Jäätteenmäen sekä Matti Vanhasen I ja II hallitusohjelmissa olivat esillä käsitteet tietoyhteiskunta, tietotekniikka, tietoteknologia, tietoturva, tietoturvauhka ja tietotekniikkarikollisuus. Jäätteenmäen hallitusohjelmassa tietoturva yhdistetään tietoyhteiskunnan luottamuksen ylläpitämiseen ja vahvistamisen. Matti Vanhasen ensimmäisessä hallitusohjelmassa käsiteltiin var-

[18] Ks. Laajemmin varhaisemmasta kehityksestä: Risto Nevalainen, *Suomi tietoyhteiskunnaksi – eespäin tiedon poluilla ja valtateillä, Tietoyhteiskuntatoiminnan lyhyt historia*, SITRA 1999. Vuonna 1983 Kalevi Sorsan IV hallituksen ohjelman mukaan tutkimus- ja kehitystyötä tuli edistää valtioneuvoston teknologiapoliittisen periaatepäätöksen pohjalta ja hallituksen tuli antaa esitykset telelaiksi, kaapelitelevisiolaiksi ja tietosuojalaiksi. Harri Holkerin ja Esko Ahon hallitusohjelmat vuosina 1987 ja 1991 edellyttivät, että tietoliikenneverkkoja parannetaan ja kehitetään Suomessa alueellisesti kattavalla tavalla ja muun muassa teollisuuden kilpailuedellytysten turvaamiseksi.

[19] Ks. *Suomi tietoyhteiskunnaksi – kansallisten linjausten arviointi*, koonnut Reijo Lilius, Sitra, Helsinki 1997 ja *Elämänlaatu, osaaminen ja kilpailukyky, Tietoyhteiskunnan strategisen kehittämisen lähtökohdat ja päämäärät*, Sitra, Helsinki 1998.

sin kattavasti tietoturvakysymyksiä osana tietoyhteiskunta- ja viestintäpolitiikkaa. Ohjelman mukaan kansalaisten ja yritysten luottamusta tietoyhteiskunnan palveluihin tuli edistää tietoturvaa ja viestinnän yksityisyyden suojaa parantamalla. Tietoturvauhkiin ja tietotekniikkarikollisuuteen tuli ohjelman mukaan varautua lainsäädäntöä uudistamalla ja kansallisen turvallisuuden varmistamiseksi tuli ottaa käyttöön uutta tekniikkaa sekä saattaa loppuun viranomaisverkon rakentaminen.

Matti Vanhasen I hallituksen yhtenä neljästä politiikkaohjelmasta oli Tietoyhteiskuntaohjelma, jonka tarkoituksena oli lisätä tieto- ja viestintäteknologiaa hyödyntämällä kilpailukykyä ja tuottavuutta, sosiaalista ja alueellista tasaarvoa sekä kansalaisten hyvinvointia ja elämänlaatua. Ohjelmalla pyrittiin säilyttämään Suomen asema tieto- ja viestintäteknologian johtavana tuottajana ja hyödyntäjänä. Ohjelman myötä pyrittiin myös varmistamaan se, että Suomi pysyy tietoturvallisena yhteiskuntana, tietoturvallisuusalan kilpailukyky on kunnossa ja että tietoturvallisuuden osaaminen ja tietoisuus ovat korkeaa tasoa.

Ensimmäinen poikkiyhteiskunnallinen kansallinen tietoturvastrategia hyväksyttiin syksyllä 2003, ja jo itsessään strategian nimi ”Tietoturvalliseen tietoyhteiskuntaan” loi vahvan turvallisuus-kontekstin.[20] Strategiassa puhuttiin laajasti tietoturvasta, tietoyhteiskunnasta ja tietoturvatietoisuudesta sekä muun muassa internet-kansalaisesta, palomuureista, verkkoterrorismista ja tietokoneviruksista. Tieto- ja viestintäteknologiaan perustavan yhteiskunnan lisääntyvä haavoittuvuus ja tietojärjestelmäriippuvuus kuvattiin vahvistuvina kehityssuuntina. Strategia oli Euroopassa ensimmäinen laatuaan. Strategialla pyrittiin torjumaan tietoturvallisuuden uhkia sekä toisaalta hyödyntämään korkeatasoisen tietoturvallisuuden tarjoamia mahdollisuuksia.

Tietoyhteiskuntaohjelman osana valmisteltiin ja julkaistiin vuonna 2006 tietoyhteiskuntastrategia vuosille 2007–2015. Strategiassa tietoyhteiskunnan yhdeksi uhkaksi nostettiin tietoyhteiskuntainfrastruktuurin haavoittuvuus. Tietoturva-asiat olivat varsin vahvasti strategiassa esillä ja uhkia kuvattiin seuraavasti: ”Keskeisiä uhkia ovat yksityisyyden loukkaukset, tietojärjestelmiin tunkeutuminen, tietokonevirukset, haittaohjelmat, erilaiset huijausyritykset (esimerkkinä verkkotunnusten kalastelu), teollisuusvakoilu, piratismi sekä ääritilanteissa verkkoterrorismi ja elektroninen sodankäynti.[21]

Tietoyhteiskuntaohjelma sai jatkoa Matti Vanhasen II hallituksen käynnistämässä Arjen tietoyhteiskunta -ohjelmassa, jonka tavoitteena on muun muassa varmistaa suomalaisen tietoyhteiskunnan voimakas, ripeä ja tasapainoinen kehittyminen, turvata palveluntarjonta ja sen kehittyminen sekä lisätä suoma-

[20] Tietoturvan vahvaa käsitteellistä asemaa valtionhallinnossa kuvaa hyvin myös Valtiovarainministeriön vuonna 2004 julkaisema tietoturvaselvitys. Valtiovarainministeriö, *Tietoturvallisuus ja tulosohjaus*, Edita Prima Oy, Helsinki 2004.

[21] *Kansallinen tietoyhteiskuntastrategia 2007–2015, Uudistuva, ihmisläheinen ja kilpailukykyinen Suomi*, Edita Prima Oy, Helsinki 2006, s. 19.

laisen yhteiskunnan kilpailukykyä ja tuottavuutta. Käsitteitä tietoturva tai tietoturvallisuus ei mainita Vanhasen II hallitusohjelmassa.

Tietoyhteiskuntaohjelman osana joulukuussa 2008 hyväksyttiin uusi kansallinen tietoturvastrategia[22] vuosille 2009–2015. Strategiassa määritettiin kolme painopistealuetta; tietoturvallisuuden perustaidot arjen tietoyhteiskunnassa, tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä kilpailukyky ja kansainvälinen verkostoyhteistyö. Tietoturvatietoisuus ja -osaaminen olivat käsitteinä tietoturvaratkaisujen, tietoturvavaatimusten ja tietoturvallisuuden ohella strategissa esillä.

Turvallisuus- ja puolustuspoliittinen selontekokäytäntö on vakiintunut Suomessa menettelytavaksi, jossa valtioneuvosto antaa selonteon muodossa turvallisuus- ja puolustuspoliittiset linjauksensa kerran vaalikaudessa eduskunnalle (ja suomalaiselle yhteiskunnalle) arvioitaviksi. Selontekomenettelystä on tullut keskeinen suomalaisen turvallisuus- ja puolustuspolitiikan linjauksen väline. Järjestyksessään neljännessä (vuonna 2004) ja viidennessä (vuonna 2009) turvallisuus- ja puolustuspoliittisissa selonteoissa ei esiinny kyberkäsitettä. Molemmissa selonteoissa teknologisten riskien ja tietojärjestelmiin kohdistuvien uhkien todetaan lisääntyneen nopeasti. Nämä uhkat ja riskit nostetaan esille laajan turvallisuuskäsitteen ja uusien uhkien kontekstissa. Konteksti yhdistyy verkkorikollisuuteen, informaatiosodankäyntiin, riippuvuuteen sähköstä ja tietojärjestelmistä sekä yhteiskunnan ja maailman kasvavaan verkottumiseen. Vuoden 2009 selonteossa kieli on aiempaan selontekoon verrattuna astetta vakavampaa ja uuden teknologian todetaan muuttavan sodankäyntiä. Selonteoissa esiintyvät käsitteet yhdistyvät tietoturvallisuuteen, tietojärjestelmäsodankäyntiin, tietoverkkorikollisuuteen ja informaatiohyökkäyksiin. Vuoden 2004 selonteossa esiintynyt tietoturvallisuushyökkäys -käsite muuttui vuoden 2009 selonteossa tietoverkkohyökkäys-käsitteeksi. Molemmissa selonteoissa tietoverkko- ja informaatiohyökkäykset olivat esillä sotilaallisen voimankäytön uhkakuvan sekä harmaan alueen toiminnan yhteydessä. Tietoyhteiskuntakehityksen ja verkottumisen todetaan laajentavan puolustusvoimien yhteistoimintakenttää.

Sisäasianministeriön johdolla on laadittu vuodesta 2004 alkaen sisäisen turvallisuuden ohjelmia, joissa on tarkoitus nimensä mukaisesti laaja-alaisesti kehittää Suomen sisäistä turvallisuutta. Vuoden 2004 ohjelmassa yhtenä seitsemästä keskeisimmästä sisäisen turvallisuuden haasteista todettiin olevan tietoyhteiskunnan haavoittuvuus. Tietojärjestelmärikokset otettiin ohjelmassa esille omana alalukunaan ja tietojärjestelmiin kohdistuvat uhkat kuvattiin kasvavina. Tietoyhteiskunnan uhkakuvat esitettiin vakavimmassa kontekstissa yhteiskunnan toimintoja lamauttavina, mutta pääasiassa vuoden 2004 Sisäisen turvallisuuden ohjelmassa puhuttiin verkko- ja tietojärjestelmärikoksista, joita todettiin olevan muun muassa hakkerointi ja tietoverkkojen tahallinen

[22] Liikenne- ja viestintäministeriö, *Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta "Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –",* 1.12.2008.

häirintä. Vuoden 2008 Sisäisen turvallisuuden ohjelmassa nostetaan esille systeemisten riskien käsite, joilla tarkoitetaan laajalle levinneitä teknisten järjestelmien riskejä. Tietoverkkorikollisuus saa ohjelmassa vahvan painotuksen, ja ohjelmassa puhutaan bottiverkoista, tietoturvaloukkauksista, huijaussivustoista ja palvelunestohyökkäyksistä. Kyber-käsitettä ei vuosien 2004 ja 2008 Sisäisen turvallisuuden ohjelmissa esiinny.

Vuonna 2003 valtioneuvoston antamassa periaatepäätöksessä Yhteiskunnan elintärkeiden toimintojen turvaamisesta sekä vuonna 2006 julkaistussa Yhteiskunnan elintärkeiden toimintojen turvaamisen strategiassa tuodaan esille suomalaisen yhteiskunnan elintärkeät toiminnot, niitä vaarantavat uhkat sekä uhkiin varautumisen strategiset tehtävät ministeriöille. Strategioilla ohjataan kokonaisvaltaisesti suomalaisen yhteiskunnan varautumista erityis- ja poikkeustilanteisiin. Molemmissa strategioissa on kuvattu yhdeksän yhteiskunnan elintärkeitä toimintoja uhkaavaa mallia, joista tietoturvallisuutta ja tietoverkkoalaa koskevat asiat esiintyvät pääsääntöisesti ”Sähköisen infrastruktuurin häiriintymisen” -uhkamallin yhteydessä. Suomalainen yhteiskunta kuvataan kiihtyvällä nopeudella muuttuvaksi ympäristöksi, jossa lähes kaikki perinteiset palvelut ovat tietoteknisesti ohjattuja. Tietoturva-asiat nousevat strategioissa esille voimallisimmin juuri sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistamisen yhteydessä, ja uhkat kuvataan voimistuvina. Tietoverkkoalan uhkina kuvataan kriittisten tietoteknisten järjestelmien häiriöt, ilkivalta sekä kansainvälisen rikollisuuden ja terrorismin vaikutukset tietoverkoissa. Strategioissa tietoturvallisuuden käsite määritellään varsin laajaksi kokonaisuudeksi: ”Tietoturvallisuudella tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi kaikissa turvallisuustilanteissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuus on myös asiantila, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä.” [23] Strategioissa esiintyvät useimmin käsitteet tietoturvallisuus, tietoliikenne, tietotekniikka, tietoverkkoala ja tietoverkkorikollisuus. Kyber-käsitettä ei strategioissa esiinny.

Hallinnonalojen tukevaisuuskatsauksien tavoitteena on tuottaa yhteiskunnalliseen keskusteluun ja hallitusneuvottelujen pohjaksi tilanne- ja kehitysarvioita yhteiskunnan tilasta ja poliittista päätöksentekoa edellyttävistä kysymyksistä. Liikenne- ja viestintäministeriön, puolustusministeriön, sisäasiainministeriön ja valtionvarainministeriön vuosien 2006 ja 2010 tulevaisuuskatsauksissa nousevat esille teknologian kehityksen lisääntyvät vaikutukset, yhteiskunnan haavoittuvuuden lisääntyminen, teknologian mahdollisuuksien hyödyntäminen ja tietoyhteiskunnan arkipäiväistyminen. Tietojärjestelmiin kohdistuvat häiriöt ja hyökkäykset todetaan kasvava trendinä ja etenkin sisäiasiainministeriön katsauksissa tietoturvallisuuden merkityksen kasvua ko-

[23] *Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2003*, liite 4, ja *Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös 23.11.2006*, s.72.

rostetaan tietoverkkorikollisuuden yhteydessä. Tietoturvallisuus, tietoturvauhkat, tietoverkkorikollisuus ja verkkouhkat ovat käsitteellisesti esillä tietoyhteiskunnan sekä laajan turvallisuuden kontekstissa. Kyber-käsitettä ei tulevaisuuskatsauksissa esiinny.

3. Kyber-käsitteen ilmestyminen

Ensimmäisen kerran kyber-käsite esiintyy valtionhallinnon turvallisuusasiakirjoissa joulukuussa 2010 ilmestyneessä Yhteiskunnan turvallisuusstrategiassa. Strategiassa on kuvattu 13 uhkamallia, joista yksi on ”tietoliikenteen ja tietojärjestelmien vakavat häiriöt – kyberuhkat.” Kyberuhkan käsitteen todetaan olevan kansallisissa käytännöissä vakiintumaton, mutta strategiassa sitä käytetään ”kuvaamaan uhkaa, joka liittyy toisistaan riippuvaisiin verkostoihin, sisältäen erilaiset tieto- ja tiedonsiirtoverkot, internetin, puhelinverkot, tietokonejärjestelmät sekä kriittisen tuotannon sulautetut prosessorit ja kontrollointilaitteet.” [24] Kyberuhka kuvataan voimistuvaksi ja sen yhteiskunnallista merkitystä kasvavaksi. Kyberuhka kuvataan kaikkia koskettavavana.[25] Kyberuhkan lähde yhdistetään rikollisuuteen ja terrorismiin, mutta myös valtiollisiin toimijoihin. Strategiassa todetaankin, että useimpien valtioiden sotilaalliseen varautumiseen liittyy valmius tietojärjestelmien häirintään, hyväksikäyttöön ja tuhoamiseen. "Kyberuhka" on ainoa strategiassa esiintyvä kyber-etuliitteinen sana.[26]

Pääministeri Jyrki Kataisen kesäkuussa 2011 julkistetusssa hallitusohjelmassa käsitteet ”kyberstrategia” ja ”kyberturvallisuus” nousevat esille, mutta tietoturvallisuudesta, tietoyhteiskunnasta, tietoverkkoturvallisuudesta ja tietoverkkorikollisuudesta puhutaan huomattaavasti kyber-käsitteitä enemmän. Hallitusohjelmassa todetaan, että ”*hallitus laatii kansallista tietoverkkoturvallisuutta koskevan kyberstrategian* ja osallistuu aktiivisesti alan kansainväliseen yhteistyöhön.” [27] Kyberstrategia siis yhdistetään tietoverkkoturvallisuuteen. Hallitusohjelmassa asetetaan tavoite, että ”Suomi on yksi johtavista maista kyberturvallisuuden kehittämisessä.”[28]

---

[24] *Yhteiskunnan turvallisuusstrategia,* Valtioneuvoston periaatepäätös 16.12.2010, liite 5.

[25] ”Nykyisin voidaan siis sanoa, että uhka voi kohdistua kaikkiin, joilla on käytössään sähköisiä palveluita.” Ibid. s. 66.

[26] Joulukuussa 2010 ilmestyneessä kokonaisvaltaisessa selvityksessä yhteiskunnan varautumisesta (niin sanottu Hallbergin komitean mietintö) ei kyber-käsitteitä esiinny. Valtioneuvoston kanslia, *Varautuminen ja kokonaisturvallisuus*, komiteamietintö, Valtioneuvoston kanslian julkaisusarja 21/2010.

[27] *Pääministeri Jyrki Kataisen hallituksen ohjelma 22.6.2011*, s.22.

[28] Ibid. s.23.

"Kybertoimintaympäristössä on siirrytty uuteen aikakauteen, jossa haitta-ohjelmien avulla teollisuusautomaation ja ohjelmoitavan logiikan kautta kyetään vaikuttamaan kaikkiin yhteiskunnan elintärkeisiin toimintoihin."[29]

Turvallisuus- ja puolustuspoliittisiin selontekoihin kyber-käsite ilmaantui voimallisesti vuonna 2012. Selonteossa esiintyvät käsitteet kybertoimintaympäristö, kyberhyökkäys, kybertila, kyberuhka, kyberturvallisuus kyberhyökkääjä, kyberkysymys, kyberoperaatio, kybersodankäynti, kyberulottuvuus, kyberpuolustus, kybertoiminta, kyberkoordinaatiokeskus, kyberturvallisuusstrategia ja kyberkyky. Kyberuhkat ja -hyökkäykset yhdistetään selonteon toimintaympäristökuvauksessa laaja-alaisiin turvallisuuskysymyksiin, ja teknologian kehittymisen myötä myös muiden kuin valtiollisten toimijoiden vahingollisten vaikuttamiskeinojen todetaan kasvavan. Lähivuosien painopisteen todetaan olevan ”tietoyhteiskunnalle välttämättömän kybertoimintaympäristön turvaamisessa."[30] Huomionarvioista on, että kybertila rinnastetaan selonteossa muihin globaaleihin toimintaympäristöihin (valtameret, ilma, avaruus).[31] Kybertilan häiriöitä pidetään selonteossa kriittisenä uhkatekijänä ja Suomen todetaan joutuneen sekä sisäisten että ulkoisten kyberoperaatioiden kohteeksi. Kybersodankäynti on puolestaan esillä epäsymmetristen keinojen yhteydessä. Kyberturvallisuuden painoarvoa kuvaa se, että ”Kansallinen kyberturvallisuus” on selonteossa omana alalukunaan. Puolustusvoimien todetaan rakentavan kyberkykyjä osana puolustusvoimien johtamisjärjestelmää ja yhteiskunnan kokonaisturvallisuutta. Kyberuhkat yhdistetään rikollisuuteen, poliittiseen ja taloudelliseen painostuksen välineeseen sekä "vakavassa kriisissä yhtenä vaikuttamiskeinona."[32]

Turvallisuus- ja puolustuspoliittisesta selonteosta eduskunnassa annetussa Ulkoasiainvaliokunnan mietinnössä kyberturvallisuudelle annetaan merkittävä painoarvo. Eri käsitteiden välisiä suhteita kuvataan muun muassa todeten, että ”kyberturvallisuuden perustana on hyvä tietoturvallisuus.”[33] Kyberturvallisuudelle on valiokunnan mietinnössä oma lukunsa, jossa kyberympäristön ja kyberturvallisuuden todetaan koskettavan yhä konkreettisemmin kansalaisten jokapäiväistä elämää ja kyberuhkien merkitsevän uudenlaisen sodankäynnin mahdollisuutta ja toimintaympäristöä. Ulkoasiainvaliokunnan mietinnössä määritellään kybertoimintaympäristön käsite seuraavasti: ”Kybertoimintaympäristöllä tarkoitetaan sähköisessä muodossa olevan informaation käsittelyyn tarkoitettua, yhdestä tai useammasta tietojärjestelmästä muodostuvaa ympäristöä. Kybertoimintaympäristö ja sen turvallisuus on Suomessa kokonaisvaltainen käsite, joka kattaa mm. tietoturvallisuuden, tietoverkkoturvallisuuden ja tietojärjestelmien turvallisuuden.”[34] Kyberturvallisuus tulee Ulkoasiainvali-

[29] *Suomen turvallisuus- ja puolustuspolitiikka 2012*, Valtioneuvoston selonteko, Valtioneuvoston julkaisusarja 5/2012, s. 24.
[30] Ibid. s. 14.
[31] Ibid. s. 23.
[32] Ibid s. 96.
[33] *Ulkoasiainvaliokunnan mietintö 1/2013 vp*, s. 24.
[34] Ibid. s. 23.

kunnan mukaan siten ymmärtää tietoturvallisuutta ja tietoverkkoturvallisuutta laajempana ja kokonaisvaltaisempana käsitteenä. [35]

”Ulkoasiainvaliokunta katsoo, että kyberturvallisuuden tulee olla lähivuosien yksi keskeisistä turvallisuuspoliittisista painopisteistä uhkan vakavuus huomioon ottaen.”[36]

Hieman yllättävänä voi pitää, että Turvallisuus- ja puolustuspoliittisen selonteon kanssa samana vuonna (2012) ilmestyneessä Sisäisen turvallisuuden ohjelmassa ei esiinny kyber-käsitettä. Tietoturvaan ja esimerkiksi tietoverkkojen turvallisuuteen kiinnitetään ohjelmassa muutenkin varsin vähän huomiota.

Tietoyhteiskunnan, tietoturvallisuuden, tietoturvaloukkausten ja tietoturvapolitiikan kaltaiset käsitteet ovat sekä Huoltovarmuuskeskuksen että Viestintäviraston vuosikertomuksissa vahvasti esillä tarkastelujakson alusta alkaen, mutta vuonna 2011 kyber-käsite ilmenee ensimmäisen kerran. Huoltovarmuuskeskuksen kyseisen vuoden vuosikertomuksessa kyberturvallisuus nostetaan esille jo alussa, osana johdon katsausta. Viestintäviraston vuoden 2011 vuosikertomuksessa mainitaan kyberturvallisuusstrategia vain kerran, ja muuten pysyttäydytään aiempien vuosikertomusten mukaisissa määritelmissä. Myös Viestintäviraston vuosien 2012 ja 2013 vuosikertomuksissa kyber-käsitteen käyttö on varsin vähäistä. Huoltovarmuuskeskuksen vuosikertomuksissa siirrytiin ”kyber-aikaan” vuoden 2013 vuosikertomuksessa, jossa kyberturvallisuus ja eri kyber-käsitteet[37] ovat vahvasti esillä. Kyberturvallisuus esiintyy vuosikertomuksessa omana lukunaan johdon katsauksen yhteydessä.

[35] Puolustusvaliokunnan lausunnossa kyberturvallisuus niin asiana kuin käsitteinä on esillä, mutta vähäisemmässä määrin kuin Ulkoasianvaliokunnan mietinnössä. Ks. *Puolustusvaliokunnan lausunto 4/2013 vp*.

[36] *Ulkoasiainvaliokunnan mietintö 1/2013 vp*, s. 22.

[37] Kyberturvallisuus, kyberhyökkäys, kyberturvallisuusstrategia, kyberuhka, kyberturvallisuuskeskus, kyber-asiat, kyberturvallisuuskoulutus. *Huoltovarmuuskeskus, Vuosikertomus 2013*.

4. Läpimurto ja nykytilanne

Kyber-käsitteen läpimurron ja hallinnollisen institutionalisoitumisen[38] *voi katsoa tapahtuneen vuoden 2013 alussa ilmestyneen Suomen Kyberturvallisuusstrategian myötä.* Valtioneuvoston periaatepäätöksenä strategia ja sen taustamuistio toivat kyber-käsitteen konkreettisesti hallinnolliseen turvallisuusajatteluun ja kyber-käsitteet myös käytännön toimenpiteisiin. Kyberturvallisuusstrategian visiona on, että 1) Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan; 2) kansalaisilla viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti ja että 3) vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallitsemisessa. Strategian toimeenpanemiseksi laadittiin virkamiestasolla toimeenpano-ohjelma[39].

Erilaisia kyber-käsitteitä strategiassa ja sen taustamuistiossa esiintyy kymmeniä, joista yleisimpiä ovat kybertomintaympäristö, kyberturvallisuus ja kyberuhka. Kyberkäsitteet myös määritellään strategiassa, joskin samanaikaisesti annetaan ymmärtää, että käsitteiden määrittely on vielä kehitysvaiheessa.[40] Strategiassa annetaan määritelmät käsitteille: ”Kyber-”, kyberriski, kybertoimintaympäristö, kyberturvallisuus ja kyberuhka. Kyberturvallisuudella tarkoitetaan strategiassa tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.[41] Kybertoimintaympäristö puolestaan määritellään sähköisessä muodossa olevan informaation käsittelyyn tarkoitetuksi, yhdestä tai useammasta tietojärjestelmästä muodostuvaksi toimintaympäristöksi.[42] Strategiassa tehdään eroa kyberturvallisuuden ja tietoturvallisuuden välille, jälkimmäisen määrittyessä tiedon käytettävyyden, eheyden ja luottamuksellisuuden varmistamisen järjestelyiksi.

---

[38] Institutionalisoitumisella tarkoitetaan tässä käsitteiden sekä niihin liittyvien käytäntöjen vakiintumista. Vrt. Markus Laine & Pekka Jokinen, ”Politiikan ulottuvuudet”, Teoksessa *Ympäristöpolitiikka. Mikä ympäristö, kenen politiikka.* Toim. Yrjö Haila & Pekka Jokinen, Osuuskunta Vastapaino, Tampere 2001, s. 61–62.

[39] Turvallisuuskomitea, *Kansallisen Kyberturvallisuusstrategian toimeenpano-ohjelma*, 11.3.2014.

[40] Tämä ilmenee myös eri käsitteiden käytössä strategian toimeenpano-ohjelmassa, mm. ” Tieto- ja kyberturvallisuus sekä tietosuoja on huomioitava kaikessa perustietovarantoihin liittyvässä toiminnassa olemassa olevien linjausten mukaisesti.” Ibid. s. 5.

[41] *Suomen Kyberturvallisuusstrategia*, Valtioneuvoston periaatepäätös 24.1.2013, s.13.

[42] Ibid. s.12.

Kyber-käsitteen institutionalisoitumista ja vakiinnuttamista hallinnolliseen turvallisuusajatteluun ilmentää hyvin Kyberstrategian varsin laaja toimeenpano-ohjelma, jossa laajalle joukolle ministeriöitä, virastoja ja laitoksia määritetään kyberturvallisuustehtäviä (sic!). Näissä tehtävissä huomioidaan kansallinen ja kansainvälinen yhteistyö, hallinnon eri tasot sekä elinkeinoelämän ja järjestöjen rooli. *Kyberturvallisuusstartegian ja erityisesti sen toimeenpano-ohjelman voi nähdä sekä levittäneen kyber-käsitettä laaja-alaisesti suomalaiseen yhteiskuntaan että luoneen tarkoituksellisesti yhteistyörakenteita ja käytännön toimenpiteitä kyber-käsitteen ympärille*. Yhtenä keskeisenä kyber-käsitteen institutionalisoitumisena on pidettävä kyberturvallisuusstrategian myötä vuoden 2014 alusta perustetua Kyberturvallisuuskeskusta. Se on uudelleen nimetty ja vahvistettu Viestintäviraston turvallisuus-toimiala. Kyberturvallisuuskeskuksen myötä kyberturvallisuus-käsite esiintyy siten myös hallinnollisena yksikkönä. Kyberturvallisuuskeskuksen toimintasuunnitelmassa puhutaan muun muassa kyberturvallisuuden tilannekuvasta ja kybertapahtumista,[43] mikä kuvaa kyber-käsitteiden arkipäiväistämistä käytännön toiminnan tasolle. Myös Maanpuolustuskurssien vuonna 2013 ilmestyneeseen ”Turvallinen Suomi, Tietoja Suomen kokonaismaanpuolustuksesta” opetuskirjassa[44] kyber-käsitteet nousivat voimallisesti esille. Kirjassa on oma ”Tietoyhteiskunta ja kyberturvallisuus” lukunsa ja kyberturvallisuus määritellään kokonaisvaltaiseksi käsitteeksi: ”Kybertoimintaympäristö ja sen turvallisuus tulee jatkossa käsittää Suomessa kokonaisvaltaisena käsitteenä, joka kattaa osa-alueinaan muun muassa tietoturvallisuuden, tietoverkkoturvallisuuden ja tietojärjestelmien turvallisuuden.”[45]

Kyber-käsitteen ilmenemistä valtionhallinnon turvallisuusjattelussa todentaa Kansallista kyberturvallisuusstrategiaa seuraavana vuonna ilmestyneet hallinnonalojen tulevaisuuskatsaukset. Kyber-käsite on näissä katsauksissa esillä, joskin on huomioitava kösitteen käytön erot eri hallinnonalojen välillä. Eniten kyber-käsitettä käytetään sisäasiainministeriön ja puolustusministeriön katsauksissa. Sisäasianministeriön katsauksessa kybertoimintaympäristö kuvataan painopistealueeksi ja kyber-tulevaisuudelle yhdessä digitalisaation kanssa on katsauksessa oma alalukunsa. Vahvimmin esillä ovat kyberrikollisuuden asiat. Puolustusministeriön tulevaisuuskatsauksessa esiintyy kyberpuolustuksen, kyberympäristön ja kyberoperaation kaltaisia käsitteitä.

”Kyberpuolustuksesta on tullut kriittinen suorituskykyalue yhteistoimintaverkon laajentuessa ja asejärjestelmien teknistyessä.”[46]

Valtiovarainministeriön tulevaisuuskatsauksessa huomiota kiinnitetään digitalisaatioon, tietoturvaan ja yksityisyydensuojaan, eikä kyber-käsitettä katsa-

[43] Viestintävirasto, *Kyberturvallisuuskeskus, Toimintasuunnitelma*. mm. s.6.
[44] Maanpuolustuskorkeakoulu, *Turvallinen Suomi, Tietoja Suomen kokonaisturvallisuudesta*, Tampereen Yliopistopaino Oy, Helsinki 2013.
[45] Ibid, s. 110.
[46] Puolustusministeriö, *Suomen puolustus 2020-luvulla*, Puolustusministeriön hallinnonalan tulevaisuuskatsaus 2014, s. 10.

uksessa esiinny. Kyber-käsitteen käyttö on vähäistä myös Liikenne- ja viestintäministeriön sekä Ulkoasiainministeriön tulevaisuuskatsauksissa, sillä molemmissa kyber-alkuinen sana esiintyy vain kerran.[47] Huomioitavaa on, että molemmissa katsauksissa digitalisoituminen on vahvasti esillä niin yhteiskunnallisena kuin kansainvälisenä trendinä, jonka yhteydessä etenkin Liikenne- ja viestintäministeriön tulevaisuuskatsauksessa puhutaan tietoturvasta: "Tietoturvan varmistaminen ja luottamuksen vahvistaminen kuuluu kaikille palvelujen tarjoajille ja käyttäjille. Keskeistä on panostaa tietoturvatietoisuuteen ja -osaamiseen koko yhteiskunnassa."[48]

Vuonna 2013 ilmestyneissä Julkisen hallinnon ICT-strategiassa ja ICT 2015-työryhmän raportissa kyber-käsitteitä esiintyy, mutta varsin maltillisella tavalla. ICT-strategiassa turvallisuuden yhteydessä esiintyy tietosuoja, tietoturva ja tietoturvataso kaltaisia käsitteitä. Kyber-käsitteistä esiintyvät ainoastaan kyberturvallisuusstrategia ja kyberturvallisuuskeskus – molemmat yhden kerran. Julkisen hallinnon ICT-strategian lopussa määritellään keskeiset käsitteet ja termit, joista ei kyber-käsitteitä löydy, mutta sen sijaan muun muassa tietoturvantason käsite on ICT-strategiassa määritelty.[49] ICT 2015-ryhmän raportissa ”21 polkua kitkattomaan Suomeen” määritellään tiekartta 10 vuoden pitkäjänteiselle työlle Suomen nostamiseksi tietotekniikan soveltamisen kärkimaaksi. Tietoturva tuodaan raportissa yhtenä kärkihankkeen aiheena esille ja yhden alaluvun otsikkona on ”Tietoturva on elinehto.”[50] Erityisen vahvasti ICT 2015-ryhmän raportissa tuodaan esille tietoturvaosaaminen, jonka todetaan vahvistavan Suomen ja vientiteollisuuden vientikykyä. Tietoturvaosaajien puute sekä suomalaisten tietoturvayritysten pieni koko todetaan kehityksen pullonkaulaksi. Kuvaavaa on tietoturva-käsitteen vahva käyttö raportissa. Myös maanpuolustuksen yhteydessä puhutaan tietoturvan tärkeydestä. Raportissa mainitut kyber-käsitteet yhdistyvät pääosin viittauksiin kyberstrategiasta.

Kesäkuussa 2014 aloittaneen pääministeri Alexander Stubbin suhteellisen lyhyessä hallitusohjelmassa tietoturvan tai tietoturvallisuuden kaltaisia käsitteitä ei löydy. Kyberturvallisuudesta mainitaan hallitusohjelmassa tiiviisti: ”Hallitus jatkaa kyberstrategian määrätietoista toimeenpanoa. Tavoitteena on, että Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden häiriötilanteiden hallinnassa.”[51]

---

[47] ”Kyberuhka” / Liikenne- ja viestintäministeriö, *Liikenne ja viestintä digitaalisessa Suomessa*, Liikenne- ja viestintäministeriön tulevaisuuskatsaus 2014, s. 11. ”Kyberturvallisuus” / Ulkoasiainministeriö, *Suomen asema ja turvallisuus ja hyvinvointi monimutkaistuvassa maailmassa*, Ulkoasiainministeriön tulevaisuuskatsaus 2014, s. 10.

[48] *Liikenne ja viestintä digitaalisessa Suomessa*, s. 11.

[49] ”Tietoturvallisuustasojen avulla määritellään organisaatiolle ja tietojenkäsittely-ympäristöille tekniset ja hallinnolliset tietoturvavaatimukset. Tietoturvallisuustasot kuvaavat niitä tietoturvatoimintaan ja -prosesseihin liittyviä vaatimuksia, jotka jokaisessa organisaatiossa tulee toteuttaa.” *Julkisen hallinnon ICT:n hyödyntämisen strategia 2012–2020, Palvelut ja tiedot käytössä*, Julkisen hallinnon ICT-strategia, huhtikuu 2013, s. 18.

[50] *21 Polkua kitkattomaan Suomeen*, ICT 2015-työryhmän raportti, Työ- ja elinkeinoministeriön julkaisuja 4/2013, s. 43.

[51] *Pääministeri Alexander Stubbin hallituksen ohjelma 24.6.2014*, s. 5.

Maanpuolustuksen pitkän aikavälin haasteita selvittäneen parlamentaarisen selvitysryhmän lokakuussa 2014 julkaistussa raportissa kyber-käsitteet ovat vahvasti esillä. Raportissa puhutaan muun muassa kyberoperaatioista, kyberkyvyistä, kyberturvallisuudesta, kybervalmiudesta ja kyberympäristöstä. Vaikka raportissa esiintyvät kyber-käsitteet yhdistyvät läheisesti sotilaalliseen toimintaan, halutaan kyberturvallisuus ymmärtää laajempana yhteiskunnallisena kokonaisuutena; ”Kyberturvallisuuden kehittämisessä korostuvat koko yhteiskunnan osallistuminen, yhteiset toimintatavat ja osaaminen.”[52] Tietoturvallisuuden käsitteitä ei raportissa ilmene.

[52] *Puolustuksen pitkän aikavälin haasteet*, s. 20.

5. Johtopäätöksiä

Kyberturvallisuus ei ole uusi yhteiskunnallinen ilmiö, vaan jatkumoa tieto- ja viestintäteknologian hyödyntämisen ja siihen liittyvien uhkien hallinnan pitkästä perinteestä, jossa suomalaiset ovat olleet monessakin mielessä edelläkävijöitä jo vuosikymmenten ajan. Informaatioyhteiskunnasta, tietoyhteiskunnasta, digitalisaatiosta, johtamis- ja tietojärjestelmistä ja tietotekniikasta on valtionhallinnon turvallisuusasiakirjoissa ja vuosikertomuksissa puhuttu vuosikymmeniä. Vastaavalla tavalla teknologian kehitykseen, tietoverkkoihin ja -järjestelmiin sekä digitaalisen toimivuuden varmistamiseen ja luotettavuuteen yhdistyvä turvallisuus on valtionhallinnossa ollut esillä vuosikymmeniä. Turvallisuudesta on tässä kontekstissa puhuttu pääosin tietoturvallisuuden, tietoturvan ja tietosuojan käsittein. Yhtenä turvallisuuden trendinä valtionhallinnossa on viimeisen vuosikymmenen aikana ollut, että teknologia ulottaa lonkeronsa yhä laajemmalle ja kriittisempiin kohteisiin suomalaisessa yhteiskunnassa, joka on kasvavissa määrin haavoittuvaisempi erilaisia uhkatekijöitä ja häiriötilanteista kohtaan. Turvallisuuden teema tässä teknologisessa toimintaympäristössä on ajallisesti voimistunut 2000-luvun alusta alkaen, ja sekä turvallisuutta uhkaavat tekijät (kuten tietoturvahyökkäykset, tietoturvaloukkaukset, verkkohyökkäykset, tietoturvauhka) on ajallisesti kuvattu valtionhallinnossa 2000-luvun alussa voimakkaasti kasvavina sekä vaikutuksiltaan jatkuvasti yhä vakavammiksi muuttuvina.

Kyber-käsite ilmenee valtionhallinnon turvallisuusasiakirjoissa ensimmäisen kerran loppuvuonna 2010, Yhteiskunnan turvallisuusstrategiassa. Tällöinkin mainitaan vain ”kyberuhka”, mikä käsitteellisesti rinnastetaan strategiassa tietoliikenteen, tietojärjestelmien ja toisistaan riippuvaisten verkostojen vakaviin häiriöihin. *Kyber-alkuiset käsitteet ja termit ovat siten ajallisesti tarkasteltuna varsin nuoria valtionhallinnossa ja turvallisuusviranomaisten keskuudessa.*

Keskeisenä käännekohtana kyber-käsitteen vakiinnuttamisessa valtionhallintoon voi pitää pääministeri Jyrki Kataisen hallituksen ohjelmaa,[53] jossa hallituksen todetaan laativan kansallisen kyberstrategian ja Suomen tavoitteena on olla yksi kyberturvallisuuden kehittämisen johtavista maista. Hallitusohjelman kyber-käsitteet yhdistettynä kyberstrategian laatimiseen ja kyberturvallisuuden johtajuuden saavuttamiseen kansainvälisesti merkitsivät käy-

[53] Se miksi juuri kyber-käsite nostettiin hallitusohjelmassa esille, eikä laadittavaa kansallista strategiaa päätetty kutsua jollain toisella nimellä, ei tutkimuksen lähdeaineistosta selviä.

tännössä kyber-käsitteen levittämistä ja leviämistä valtionhallintoon. Sama tavoitteellisuus ja kyber-käsitteiden käyttäminen jatkuivat pääministeri Alexander Stubbin hallituksen ohjelmassa.

Kyber-käsitteen läpimurron ja hallinnollisen institutionalisoitumisen voi katsoa tapahtuneen vuoden 2013 alussa ilmestyneen Suomen Kyberturvallisuusstrategian myötä. Strategia taustamuistioineen sekä seuraavana vuonna ilmestynyt toimeenpano-ohjelma toivat kyber-käsitteen konkreettisesti hallinnolliseen turvallisuusajatteluun ja myös käytännön toimenpiteisiin.[54] Kyberstrategiassa myös määriteltiin keskeiset kyber-alkuiset käsitteet, joskin käsitteiden määrittely on edelleen käynnissä valtionhallinnossa ja suomalaisessa yhteiskunnassa. Strategiassa kyberturvallisuus määriteltiin tavoitetilaksi, kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyber-käsitteen vakiintumista on edistänyt kyberturvallisuusstrategian seurauksena Suomeen perustettu Kyberturvallisuuskeskus.

Huoltovarmuuskeskuksen ja Viestintäviraston vuosikertomuksiin kyber-käsite ilmestyi ensimmäisen kerran vuonna 2011, jonka jälkeen kyber-käsitteen käyttö on lisääntynyt vuosi vuodelta. Vuoden 2012 Turvallisuus- ja puolustuspoliittisessa selonteossa kyber-käsite esiintyy eri muodoissaan jo hyvinkin kattavalla tavalla, kun esimerkiksi samana vuonna ilmestyneessä Sisäasianministeriön johdolla valmistellussa Sisäisen turvallisuuden ohjelmassa kyber-käsitetteitä ei mainita kertaakaan. Tosin Sisäasiainministeriön tulevaisuuskatsauksessa kahta vuotta myöhemmin kyber-käsite esiintyy jo useamman kerran, erityisesti rikollisuuteen yhdistyen.

Liikenne- ja viestintäministeriön sekä ulkoasianministeriön asiakirjoissa kyber-käsitteitä esiintyy, mutta niiden käyttö on varsin vähäistä. Liikenne- ja viestintäministeriössä ”kyber” yhdistyy koko yhteiskunnan yhteiskunnan digitalisaatioon, mutta myös tietoturvallisuuden käsitteet ovat vahvasti esillä. Ulkoasianministeriössä kyberturvallisuus yhdistyy informaatiosodankäyntiin ja tietomurtoihin, jonka todetaan tuovan turvallisuuspolitiikkaa enemmän yksittäisen kansalaisen tasolle ja lisäävän tarvetta laajasti ymmärretylle yhteiskunnalliselle turvallisuudelle. Puolustusministeriön tulevaisuuskatsauksessa vuonna 2014 ja samana vuonna ilmestyneessä parlamentaarisen selvitysryhmän raportissa kyber-käsitteitä käytetään jo varsin vakiintuneella tavalla ja kyber-asioiden merkitystä kasvavasti korostaen. *Hallinnonaloista voi kyber-käsitteen todeta esiintyvän runsaimmin puolustushallinnossa sekä puolustuspolitiikkaan liittyvissä asiakirjoissa.*

Tutkimuksen johtopäätöksenä voi todeta, että *kyber-käsitteet ovat rantautuneet Suomessa valtionhallinnon turvallisuusasiakirjoihin.* Maailman ja suomalaisen yhteiskunnan tietointensiivisyyden kasvaessa, riippuvuuden tie-

[54] Kyberturvallisuusstrategian linjauksissa muun muassa edellytetään, että viranomaisille ja elinkeinoelämän toimijoille tulee määritellä kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.

toverkoista ja viestintäjärjestelmistä lisääntyessä sekä digitaalisen ulottuvuuden läpitunkeutuessa kaikille yhteiskunnan ja ihmiselämän alueille voi *kyberturvallisuuden sekä käsitteenä että etenkin ilmiönä todeta pysyvän jatkossa vahvasti esillä*. On toki huomioitava mahdollisuus, että kyber-käsitteet korvautuisivat muilla käsitteillä, mutta tätä kehitystä voi pitää epätodennäköisenä jo senkin takia, että kansainvälisesti ”cyber”-käsite on yleisessä kielenkäytössä jo varsin vakiintunut. Tätä kuvaa käsitteellisesti hyvin vuonna 2013 ilmestynyt Euroopan unionin Kyberturvallisuusstrategia[55], jossa eri kyber-alkuiset käsitteet ovat vahvasti esillä.

Lähtökohtaisesti kyberturvallisuus, ja kyber-käsitteet kaikkinensa, on ymmärrettävä monitahoisena ja voimistuvana ilmiönä. Ei ole yhdentekevää millä kielellä ja millä tavalla suomalaisessa yhteiskunnassa turvallisuudesta puhumme ja pyrimme sitä tuottamaan. Käsitteet ovat välttämättömiä, sillä ne ovat tapa, jonka kautta hahmotamme ja jäsennämme maailmaa – tai miten haluamme sitä hahmotettavan. Käsitteet muodostavat monitasoisia käsitehierarkioita suhteessa toisiinsa – toiset käsitteet hahmottuvat yläkäsitteiksi, toiset yläkäsitettä jäsentäviksi alakäsitteiksi. Käsitteillä on myös käytännön merkitystä, sillä painottaessa eri toimijoiden turvallisuusroolia, ”kyber” siirtää vastuuta niiden toiminnalle. Tällöin kyberturvallisuuden kaltainen kokonaisvaltainen käsite pakottaa toimijoita sovittamaan erilaisia turvallisuuskäsityksiä uudella tavalla yhteen myös käytännön toimissa.

Kyber-käsitteiden merkityssisältöjen eroavaisuuksien määrittely suhteessa esimerkiksi tietoturvallisuuden ja tietoturvauhkien käsitteisiin on toistaiseksi vakiintumatonta ja eri käsitteille annettavat sisällöt monimerkityksellisiä.

On hyvä, että suomalaisessa yhteiskunnassa puhutaan nyt uudesta ”kyber”-käsitteestä. Kyberturvallisuutta ei tule pitää synonyymina tietoturvallisuudelle, tietosuojalle tai millekään muulle turvallisuustermille. Kyber kuvastaa tietynlaista ilmiötä ja kokonaisuutta, johon vanhat käsitteet ja kieli ei kykene. *Kyberturvallisuus kuvastaa valtionhallinnon turvallisuusasiakirjoissa uudenlaista digitaalisen turvallisuusulottuvuuden holistisuutta.* Kun kyber-käsitteellä ei ole vanhoja merkityssisältöjä, on käsite mahdollista määritellä alusta alkaen ilmiön kokonaisuutta kuvaavalla tavalla. Toisaalta on hyvä pitää mielessä, että käsitteet ja niiden merkityssisällöt muuttuvat ajan myötä.

Tärkeää on kyetä määrittelemään selkeästi mitä kyber-alkuisilla käsitteillä tarkoitetaan, mitä käsitteiden tietynlaisella määrittelyllä halutaan saavuttaa ja mikä on eri käsitteiden välinen keskinäinen suhde. Tämä määrittely on Suomessa vasta käynnissä, ja Suomen Kyberturvallisuusstrategiassa esitettyjä määrittelyjä voi pitää eräänlaisena välitilinpäätöksenä. Määrittelytyö jatkuu, vaikka kyber-käsitteiden voi jo todeta rantautuneen suomalaiseen turvallisuusajatteluun.

[55] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, European Commission, 7.2.2013 Brussels.

Lähteet

21 Polkua kitkattomaan Suomeen, ICT 2015-työryhmän raportti, Työ- ja elinkeinoministeriön julkaisuja 4/2013.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Commission, 7.2.2013 Brussels.

Elämänlaatu, osaaminen ja kilpailukyky, Tietoyhteiskunnan strategisen kehittämisen lähtökohdat ja päämäärät, Sitra, Helsinki 1998.

Huoltovarmuuskeskus, *Vuosikertomus 2004*.

Huoltovarmuuskeskus, Vuosikertomus 2005.

Huoltovarmuuskeskus, *Vuosikertomus 2006*.

Huoltovarmuuskeskus, *Vuosikertomus 2007*.

Huoltovarmuuskeskus, *Vuosikertomus 2008*.

Huoltovarmuuskeskus, *Vuosikertomus 2009*.

Huoltovarmuuskeskus, *Vuosikertomus 2010*.

Huoltovarmuuskeskus, *Vuosikertomus 2011*.

Huoltovarmuuskeskus, *Vuosikertomus 2012*.

Huoltovarmuuskeskus, *Vuosikertomus 2013*.

Julkisen hallinnon ICT:n hyödyntämisen strategia 2012–2020, Palvelut ja tiedot käytössä, Julkisen hallinnon ICT-strategia, huhtikuu 2013.

Kansallinen tietoyhteiskuntastrategia 2007–2015, Uudistuva, ihmisläheinen ja kilpailukykyinen Suomi, Edita Prima Oy, Helsinki 2006.

Laine, Markus & Jokinen, Pekka, ”Politiikan ulottuvuudet”, Teoksessa *Ympäristöpolitiikka. Mikä ympäristö, kenen politiikka*. Toim. Yrjö Haila & Pekka Jokinen, Osuuskunta Vastapaino, Tampere 2001.

Liikenne- ja viestintäministeriö, *Digitaalinen Suomi, uusi liikennepolitiikka*, Liikenne- ja viestintäministeriön tulevaisuuskatsaus puolueille 10.9.2010.

Liikenne- ja viestintäministeriö, *Tietoturvalliseen tietoyhteiskuntaan*, Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 14.12.2004.

Liikenne- ja viestintäministeriö, *Liikenne ja viestintä digitaalisessa Suomessa*, Liikenne ja viestintäministeriön tulevaisuuskatsaus 2014.

Liikenne- ja viestintäministeriön tulevaisuuskatsaus – Katsauksia erityiskysymyksiin, Liikenne- ja viestintäministeriö 15.10.2010.

Liikenne- ja viestintäministeriö, *Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta "Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla –",* 1.12.2008.

Limnéll, Jarno, *Suomen uhkakuvapolitiikka 2000-luvun alussa*, väitöskirja, Maanpuolustuskorkeakoulun Strategian laitos, Edita Prima Oy, Helsinki 2009.

Limnéll, Jarno & Majewski, Klaus & Salminen, Mirva, *Kyberturvallisuus*, Docendo, Saarijärven Offset Oy, 2014.

Maanpuolustuskorkeakoulu, *Turvallinen Suomi, Tietoja Suomen kokonaisturvallisuudesta,* Tampereen Yliopistopaino Oy, Helsinki 2013.

Nevalainen, Risto, *Suomi tietoyhteiskunnaksi – eespäin tiedon poluilla ja valtateillä, Tietoyhteiskuntatoiminnan lyhyt historia*, SITRA 1999.

Oxford University Dictionary, http://www.oxforddictionaries.com/definition/english/cyber 2.10.2014.

Puolustuksen pitkän aikavälin haasteet, Parlamentaarinen selvitysryhmä, Eduskunnan kanslian julkaisu 3/2014.

Puolustushallinnon tulevaisuuskatsaus, *Suomen puolustus 2020-luvulla*, 9.9.2010.

Puolustusministeriö, *Puolustusministeriön tulevaisuuskatsaus*, 2006.

Puolustusministeriö, *Suomen puolustus 2020-luvulla*, Puolustusministeriön hallinnonalan tulevaisuuskatsaus 2014.

Puolustusvaliokunnan lausunto 4/2013 vp.

Pääministeri Alexander Stubbin hallituksen ohjelma 24.6.2014.

Pääministeri Anneli Jäätteenmäen hallituksen ohjelma 17.4.2003.

Pääministeri Esko Ahon hallituksen ohjelma 26.4.1991.

Pääministeri Harri Holkerin hallituksen ohjelma 30.4.1987.

Pääministeri Jyrki Kataisen hallituksen ohjelma 22.6.2011.

Pääministeri Kalevi Sorsan IV hallituksen ohjelma 11.5.1983.

Pääministeri Matti Vanhasen hallituksen ohjelma 24.6.2003.

Pääministeri Matti Vanhasen II hallituksen ohjelma 19.4.2007

Pääministeri Paavo Lipposen II hallituksen ohjelma 15.4.1999.

Rantapelkonen, Jari, ”Kansallinen turvallisuus kohtaa kybertrendit”, *Futura*, No. 2 / 2014.

Sisäasiainministeriö, *Arjen turvaa, Sisäisen turvallisuuden ohjelma*, Sisäasiainministeriön julkaisuja 44/2004.

Sisäasiainministeriö, *Turvallinen elämä jokaiselle, Sisäisen turvallisuuden ohjelma*, Sisäasiainministeriön julkaisuja 16/2008.

Sisäasiainministeriö, *Turvallisempi huominen, Sisäisen turvallisuuden ohjelma*, Helsinki 2012.

Sisäministeriö, *Sisäinen turvallisuus tulevaisuuden menestystekijänä ja hyvinvointimme varmistajana*, Sisäministeriön tulevaisuuskatsaus 2014.

Sisäasiainministeriö, *Turvallinen ja moniarvoinen Suomi – sisäinen turvallisuus ja maahanmuutto 2020*, Sisäasiainministeriön tulevaisuuskatsaus, Sisäasiainministeriön julkaisuja 25/2010, Helsinki 2010.

Suomen Kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013.

Suomen turvallisuus- ja puolustuspolitiikka 2004, Valtioneuvoston selonteko VNS 6/2004.

Suomen turvallisuus- ja puolustuspolitiikka 2009, Valtioneuvoston selonteko 23.1.2009.

Suomen turvallisuus- ja puolustuspolitiikka 2012, Valtioneuvoston selonteko, Valtioneuvoston julkaisusarja 5/2012.

Suomi tietoyhteiskunnaksi – kansallisten linjausten arviointi, koonnut Reijo Lilius, Sitra, Helsinki 1997.

Tuomi, Jouni & Sarajärvi, Anneli, *Laadullinen tutkimus ja sisällönanalyysi*, Tammi, Helsinki 2013.

Turvallinen, monikulttuurinen, hyvinvoiva ja kilpailukykyinen Suomi, Sisäasiainministeriön tulevaisuuskatsaus 2006, Sisäasiainministeriön julkaisuja 37/2006.

Turvallisuuskomitea, *Kansallisen Kyberturvallisuusstrategian toimeenpano-ohjelma*, 11.3.2014.

Ulkoasiainministeriö, *Suomen asema ja turvallisuus ja hyvinvointi monimutkaistuvassa maailmassa*, Ulkoasiainministeriön tulevaisuuskatsaus 2014.

Ulkoasiainministeriö, *Ulkoministeriön tulevaisuuskatsaus 2006, 30.6.2006*.

Ulkoasiainministeriön tulevaisuuskatsaus 2010, *Ulkopolitiikka 2020*, Ulkoasiainministeriö 9.10.2010.

Ulkoasiainvaliokunnan mietintö 1/2013 vp.

Uuteen käyttäjälähtöiseen ja innovatiiviseen liikennepolitiikkaan, Uuteen arjen tietoyhteiskuntaan, Liikenne- ja viestintäministeriön tulevaisuuskatsaukset eduskuntapuolueille 30.6.2006.

Valtioneuvoston kanslia, *Varautuminen ja kokonaisturvallisuus*, komiteamietintö, Valtioneuvoston kanslian julkaisusarja 21/2010.

Valtioneuvoston periaatepäätös kokonaisturvallisuudesta, 5.12.2012.

Valtioneuvoston tiedonanto Eduskunnalle 22.6.2010 nimitetyn pääministeri Mari Kiviniemen hallituksen ohjelmasta.

Valtiovarainministeriö, *Hallinto hyvinvoinnin ja talouden tasapainottajana*, Valtiovarainministeriön julkaisuja 40/2010.

Valtiovarainministeriö, *Talouspolitiikan strategia-raportti 2006*, Valtiovarainministeriön jukaisuja 2/2006.

Valtiovarainministeriö, *Tietoturvallisuus ja tulosohjaus*, Edita Prima Oy, Helsinki 2004.

Valtiovarainministeriö, *Vakaa ja tehokas Suomi yhdentyvässä Euroopassa*, Valtiovarainministeriön tulevaisuuskatsaus 2014.

Verkkouutiset, ”Alexander Stubb: Suomen haettava Nato-jäsenyyttä seuraavalla hallituskaudella”, 22.5.2014.

Viestintävirasto, *Kyberturvallisuuskeskus, Toimintasuunnitelma*.

Viestintäviraston verkkovuosikertomus 2005, Viestintävirasto.

Viestintäviraston verkkovuosikertomus 2006, Viestintävirasto.

Viestintäviraston verkkovuosikertomus 2007, Viestintävirasto.

Viestintäviraston verkkovuosikertomus 2008, Viestintävirasto.

Viestintäviraston verkkovuosikertomus 2009, Viestintävirasto.

Viestintäviraston verkkovuosikertomus 2010, Viestintävirasto.

Viestintäviraston verkkovuosikertomus 2011, Viestintävirasto.

Viestintäviraston vuosikertomus 2012, Viestintävirasto.

Viestintäviraston vuosikertomus 2013, Viestintävirasto.

Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2003. http://www.yetts.fi/content/common/yett_html/index.html 10.11.2014.

Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös 23.11.2006.

Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 16.12.2010.

Warwick, Kevin, *I, Cyborg*, University of Illinois Press, 2004.

Wiener, Norbert, *Cybernetics: or Control and Communication in the Animal and the Machine*, Cambridge, The MIT Press 1948.

Aalto-TT 12/2014

ISBN 978-952-60-6021-7 (painettu)
ISBN 978-952-60-6022-4 (pdf)
ISSN-L 1799-487X
ISSN 1799-487X (painettu)
ISSN 1799-4888 (pdf)

Aalto-yliopisto
Sähkötekniikan korkeakoulu
Sähkötekniikan korkeakoulu
www.aalto.fi

KAUPPA +
TALOUS

TAIDE +
MUOTOILU +
ARKKITEHTUURI

TIEDE +
TEKNOLOGIA

CROSSOVER

DOCTORAL
DISSERTATIONS