HELSINGIN YLIOPISTO

Kyberturvallisuuden keskeiset käsitteet

Terminologinen käsiteanalyysi suomi–venäjä

Heidi Pekander
Pro gradu -tutkielma
Venäjän kääntäminen
Nykykielten laitos
Helsingin yliopisto
Huhtikuu 2016

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta – Fakultet – Faculty	Laitos – Institution – Department
Humanistinen tiedekunta	Nykykielten laitos

Tekijä – Författare – Author

Heidi Pekander

Työn nimi – Arbetets titel – Title

Kyberturvallisuuden keskeiset käsitteet. Terminologinen käsiteanalyysi suomi–venäjä

Oppiaine – Läroämne – Subject

Venäjän kääntäminen

Työn ohjaaja(t) – Arbetets handledare – Supervisor	Vuosi – År – Year
Päivi Pasanen	2016

Tiivistelmä – Abstrakt – Abstract

Tarkastelen tutkielmassani kyberturvallisuusalan käsitteitä terminologisen käsiteanalyysin avulla. Tutkielman tavoite on laatia käsitteellinen katsaus kyberturvallisuuden keskeisimmistä käsitteistä ja kuvata olemassa olevaa kyberturvallisuusalan käsitteistöä. Tutkielman lähtökielenä on suomi ja tutkimuksen lähtökohdaksi on valittu Suomen kyberturvallisuusstrategiassa 2013 määritellyt käsitteet.

Kyberturvallisuus on uusi tietoturvallisuutta sivuava erikoisala, jonka käsitteistö ei ole vielä vakiintunutta. Aiheen ajankohtaisuudesta huolimatta toistaiseksi ei ole julkaistu yhtään suomenkielistä kyberturvallisuussanastoa. Myöskään kyberturvallisuusalan suomi–venäjä-sanastoa ei ole julkaistu.

Tutkielma on käsitelähtöinen ja siinä noudatetaan terminologisen sanastotyön yleisiä periaatteita ja menetelmiä. Käsiteanalyysin avulla selvitetään käsitteiden sisältö, käsitteiden väliset suhteet ja etsitään suomenkielisille käsitteille venäjänkieliset vastineet. Työssä noudatetaan systemaattisen ja deskriptiivisen sanastotyön periaatteita.

Tämän tutkimuksen aineisto on rajattu koskemaan Suomen ja Venäjän viranomaisten laatimia, julkisesti saatavilla olevia, vuoteen 2015 mennessä ilmestyneitä asiakirjoja. Lisäksi aineistoon kuuluu standardeja, lakeja ja terminologisia sanastoja. Tutkimuksessa on myös laajasti hyödynnetty suomalaisten ja kansainvälisten kyberturvallisuusalan asiantuntijoiden julkaisemia teoksia ja kirjoituksia.

Kyberturvallisuusalan käsitteet ovat abstrakteja ja viittaavat usein laajoihin ilmiöihin. Kyberturvallisuus on tieteenalana suhteellisen nuori, käytössä olevat käsitteet ovat suurelta osin määrittelemättä ja niiden käytössä esiintyy horjuvuutta.

Uusia käsitteitä muodostetaan englanninkielistä lähteistä suomen ja venäjän kielille. Käsitteitä määritellään kohdekielen käyttötarkoitukseen, jolloin niiden merkitys voi muuttua alkuperäisestä.

Käsiteanalyysi paljasti venäläisen käsitteistön heijastavan venäläistä turvallisuusajattelua, joka poikkeaa länsimaisesta. Käsitteet informaatioturvallisuus ja kyberturvallisuus voidaan määritellä eri tavoin näkökulmasta ja käyttötarkoituksesta riippuen.

Avainsanat – Nyckelord – Keywords

terminologinen käsiteanalyysi, deskriptiivinen sanastotyö, kyberturvallisuus, informaatioturvallisuus

Säilytyspaikka – Förvaringsställe – Where deposited

Helsingin yliopiston kirjasto – Helda / E-thesis (opinnäytteet)*ethesis.helsinki.fi*

Sisällysluettelo

KUVALUETTELO

Oh, East is East and West is West, and never the twain shall meet-
Rudyard Kipling

О, Запад есть Запад, Восток есть Восток, и вместе им никогда не сойтись - Редьярд Киплинг

1 Johdanto

Tämä tutkielmatyö tarkastelee kyberturvallisuusalan käsitteistöä. Tutkielman tavoitteena on käytettävän käsitteistön kuvaaminen, mikä tehdään deskriptiivisen sanastotyön periaatteita ja menetelmiä soveltaen. Lähtökielenä on suomi ja kohdekielenä venäjä.

Kyberturvallisuus on uusi tietoturvallisuutta sivuava erikoisala, jonka käsitteistö ei ole vielä vakiintunut. Kyberturvallisuus on aiheena ajankohtainen, ja siitä kirjoitetaan runsaasti. Uusia käsitteitä tarvitaan kuvaamaan uusia käsitteitä ja asioita. *Kyber-* etuliite on muodissa ja sen avulla muodostetaan sanaliittoja. Monet kyberturvallisuuteen liittyvät käsitteet ovat peräisin englannin kielestä. Vastine voi olla myös suora käännös vieraskielisestä ilmauksesta, mutta sen nimeämän käsitteen sisältö ja merkitys eivät välttämättä ole sama kuin lähtökielessä. Käsitteiden ja termien käyttö on kirjavaa, mikä kertoo terminologisen ohjauksen puutteesta ja tarpeesta.

Kyberturvallisuus ymmärretään yleensä tietoturvallisuutta laajemmaksi käsitteeksi, ja usein se liitetään koko yhteiskuntaa koskevaan kokonaisturvallisuuteen. Valtioneuvosto julkaisi vuonna 2013 *Suomen kyberturvallisuusstrategian* (Kyberstrategia 2013), jossa on määritelmä 11 kyberturvallisuuteen liittyvälle käsitteelle. Strategian mukaan *kyberturvallisuus* on: ”Tavoitetila, jossa sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettuun toimintaympäristöön voidaan luottaa ja sen toiminta turvataan” (Kyberstrategia 2013). Tämän tutkimuksen lähtökohtana on Suomen kyberturvallisuusstrategia ja siinä määritellyt käsitteet.

Tässä tutkimuksessa kyberturvallisuusalaa tarkastellaan Suomen ja Venäjän viranomaisten laatimien asiakirjojen pohjalta. Valtioneuvosto on määritellyt tietyt toiminnot sellaisiksi, jotka yhteiskunnan on pyrittävä turvaamaan kaikissa mahdollisissa olosuhteissa. *Yhteiskunnan elintärkeät toiminnot* -käsite muodostaa yhden keskeisimmistä kyberturvallisuuteen liittyvistä käsitteistä.

Ulkoministeriöön on perustettu kybersuurlähettilään tehtävä vuonna 2014 (UM 2014). Suomi on asettanut tavoitteekseen olla maailmanlaajuisesti edelläkävijä kyberuhkiin varautumisessa vuonna 2016 (Kyberstrategia 2013, 3). Kyberturvallisuuden ajankohtaisuudesta huolimatta, toistaiseksi ei ole julkaistu yhtään suomenkielistä kyberturvallisuuteen keskittyvää suomenkielistä sanastoa. Myöskään kyberturvallisuusalan suomi–venäjä-sanastoa ei ole julkaistu. Sanastokeskuksen julkaisemaan *Kokonaisturvallisuussanastoon* (TSK 47) on otettu muutamia keskeisiä kyberturvallisuuden käsitteitä.

Tutkimusaiheen valintaan vaikutti erityisesti se, että kyberturvallisuusala on suhteellisen uusi, ja siitä ei ole tehty terminologista tutkimusta suomen kielellä. Kyberturvallisuusalan termistö ei ole vielä vakiintunut, mikä luo haasteita myös tähän tutkimustyöhön. Myöskään Euroopan maissa (ENISA 2015b.) ja Venäjällä (SF 2014a.) *kyberturvallisuus*-käsitteistö ei ole vakiintunut. Tutkimuksen kohderyhmäksi valikoituivat erikoisalaa (kyberturvallisuusalaa) tuntevat ja siitä kiinnostuneet.

Tutkimuksen aiheeksi valittiin *kyberturvallisuus*, josta oletettiin löytyvän runsaasti lähdeaineistoa. Aineistoa rajatessa päätettiin keskittyä tutkimaan viranomaisten asiakirjoissa käytettävää kieltä. Näin ollen aineisto koostuu pääosin suomalaisten ja venäläisten viranomaisten laatimista asiakirjoista. Sen lisäksi aineistoon on valittu standardeja ja viranomaiskäyttöön laadittuja sanastoja molemmilla kielillä.

Tutkielmassa sovelletaan käsitekeskeisen sanastonteon yleisiä periaatteita ja menetelmiä, joiden avulla selvitetään käsitteiden sisältö ja eri käsitteiden väliset suhteet. Suomenkielisille käsitteille etsitään venäjänkieliset vastineet, joten vastinehaun tuloksia voidaan hyödyntää myös kaksikielisen sanaston laatimisessa (suomi–venäjä). Tutkimuksen menetelmä on deskriptiivinen eli se kuvaa erikoisalalla käytettävää termistöä ja käsitteistöä ja antaa tietoa käsitteiden käyttöympäristöstä. Sanastotyön lähtökohtana pidetään käsitteistä lähtevää systemaattista

työskentelytapaa. Ensin selvitetään erikoisalan käsitteistö ja sen muodostamat käsitejärjestelmät, jonka pohjalle rakennetaan käsitteiden määritelmät (Nuopponen 1999, 92).

Tutkimuksen aiheen valintaan vaikutti tekijän pääaine Venäjän kielen kääntäminen sekä Venäjän ja Itä-Euroopan tutkimuksen sivuaineopinnot, teknisen alan koulutus sekä aiemmin hankitut perustiedot tietotekniikasta ja ohjelmoinnista. Nämä ovat antaneet hyvän pohjan erikoisalan omaksumiselle. Aiheen valintaa tuki myös työkokemus teknisenä kirjoittajana tietotekniikan alan dokumentoinnissa, jossa edellytetään tekniikan ymmärtämisen lisäksi erityisesti kykyä hankkia ja muokata asiantuntijoilta saatua tietoa.

Koulutus- ja työkokemustaustaa voi hyödyntää terminologisessa sanastotyössä. Termityötä suositellaan erityisesti sellaiselle, jolla on jo entuudestaan jonkin ammattialan tuntemusta. Tällöin käsitteistö on tuttu ja tätä tuntemusta voidaan hyödyntää sanastotyössä. (Vehmas-Lehto 1999.)

Tämä pro gradu -tutkielma alkaa johdannolla. Sen jälkeen toisessa luvussa esitellään kyberturvallisuusala. Kolmannessa luvussa esitellään tutkimuksessa käytetty suomenkielinen ja venäjänkielinen tutkimusaineisto. Neljännessä luvussa on teoria, terminologinen käsiteanalyysi ja siihen liittyvät käsitteet. Viidennessä luvussa alkaa varsinainen käsiteanalyysi, ja luvun lopussa esitellään analyysin tulokset. Kuudennessa luvussa on pohdinta. Tästä työstä on tehty myös venäjänkielinen lyhennelmä, joka on tutkimuksen liitteenä. Liitteisiin on sijoitettu myös käsitekaaviot, joissa käsitteiden väliset suhteet on kuvattu graafisessa muodossa.

2 Johdanto kyberturvallisuusalaan

Suomessa on 1990-luvulta alkaen laadittu kansallisia linjauksia Suomen kehittämisestä tietoyhteiskunnaksi. *Suomi tietoyhteiskunnaksi* -suunnitelma on vuodelta 1995. (HTYS 2015.) Sittemmin on hallituksen toimesta laadittu *Kansallinen tietoyhteiskuntastrategia vuosille 2007–201*5, jossa määriteltiin kansalliset visiot sekä asetettiin tavoitteeksi luoda Suomesta ihmisläheinen ja kilpailukykyinen osaamis- ja palveluyhteiskunta (KTO 2007). *Kyberturvallisuusstrategian* mukaan Suomi on asettanut tavoitteekseen olla maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa vuonna 2016 (Kyberstrategia 2013, 3).

Tietoyhteiskunnan kehittyessä yhä enemmän toimintoja ja palveluja käytetään tietoverkkojen tai internetin kautta eli sähköisessä toimintaympäristössä. Kansalaisen näkökulmasta asiointi helpottuu, mutta samalla yhteiskunnasta tulee haavoittuva, sillä edellä mainittuihin sähköisen ympäristön palveluihin voidaan pyrkiä vaikuttamaan jollakin niille haitallisella ohjelmalla. Haittaohjelman avulla voidaan estää pääsy yksittäiselle palvelimelle tai lamauttaa jokin tietojärjestelmä, kuten vaikkapa sähkölaitoksen ohjausjärjestelmä.

Tietojärjestelmää kohtaan tehdyt hyökkäykset, tietoverkkoihin tunkeutuminen ja palvelunestohyökkäykset ovat esimerkkejä toimenpiteistä, joiden avulla voidaan vaikuttaa koko yhteiskunnan toimintaan. Esimerkiksi sähkön- ja vedenjakelu, pankkien maksuliikenne ja ennen kaikkea yhteiskunnan johtaminen muodostavat osan yhteiskunnan toimintakyvyn kannalta tärkeistä toiminnoista. Niiden suojaaminen ja toimintakyvyn turvaaminen ovat kyberturvallisuuden keskeisiä tavoitteita. (Kyberstrategia 2013.)

Turvallisuuskomitea (entinen Turvallisuus- ja puolustusasiain komitea, TPAK) on ohjannut *Suomen kyberturvallisuusstrategian* ja *Suomen kyberturvallisuusstrategian toimeenpano-ohjelman* laatimista (PLM 2013). Turvallisuuskomitea on kokonaisturvallisuuteen keskittyvä laajapohjainen yhteistoimintaelin, joka perustettiin asetuksella vuonna 2013. Komitean jäseninä on asiantuntijoita eri hallinnonaloilta. (TK 2014.) Tässä yhteydessä on syytä mainita Kyberturvallisuuskeskus**,** joka on toiminut vuoden 2014 alusta alkaen Viestintävirastossa (VIVI 2015). Kyberturvallisuuskeskus on

tietoturvallisuusviranomainen ja Suomen virallinen CERT-toimija (eng. Computer Emergency Response Team). Sen tehtäviin kuuluu tietoturvaloukkausten ja tietoturvauhkien ennaltaehkäisy, tiedottaminen sekä avustaminen tietoturva-asioissa. (VIVI 2014b.) Liikenne- ja viestintäministeriön (LVM) toimialaan kuuluu sähköinen viestintä ja viestintäpalvelujen tietoturvallisuus (VN 2015b, VNOS 262/2003).

Valtioneuvoston ohjesäännön mukaisesti huoltovarmuuden kehittäminen kuuluu työ- ja elinkeinoministeriölle. Huoltovarmuuskeskus toimii työ- ja elinkeinoministeriön ohjauksessa tukien yhteiskunnalle tärkeiden yritysten ja elinkeinoelämän toimialojen varautumista poikkeusoloihin kyberuhka mukaan luettuna. (VNK 21/2010.)

Kansallisten toimenpiteiden lisäksi Suomi on aktiivisesti mukana myös Euroopan unionin, Pohjoismaiden sekä Naton rauhankumppanuusmaiden yhteistyössä kyberturvallisuusalalla (MPKK 2013).

Maailman ensimmäinen laajamittaisesti yhteiskuntaan ja sen toimintoihin kohdistunut palvelunestohyökkäys tehtiin Virossa 2007. Palvelunestohyökkäyksessä hakkerit ottavat suuren määrän suojaamattomia tietokoneita käyttöönsä, lähettävät niiden kautta valtavan määrän esimerkiksi sähköpostia jollekin kohteelle ja siten tukkivat palvelun toimintakyvyttömäksi. Hakkeri pystyy sen lisäksi kaappaamallaan tietokoneella ohjaamaan suurta määrää muita koneita, jotka myös lähettävät sähköpostia haluttuun kohteeseen. (Ottis2008.) Viroon kohdistunut palvelunestohyökkäys oli tapahtuma, joka nosti kyberturvallisuuden sekä julkiseen turvallisuuspoliittiseen keskusteluun että valtioiden turvallisuuspoliittiseen tarkasteluun.

Tämä palvelunestohyökkäys sai alkunsa samoihin aikoihin kun Virossa alkoi keskustelu Pronssisoturi-patsaan (neuvostosotilaiden hautamuistomerkki) siirtämisestä Tallinnan keskustasta Tallinnan sotilashautausmaalle. Patsaan siirto suututti Viron venäläiset, ja internetissä eri sivustoille alkoi ilmaantua siirtoa vastustavia mielenilmauksia. Hyökkäyksiä kohdistettiin Viron valtionhallintoon, tiedotusvälineisiin ja pankkien verkkopalveluihin. Hyökkäyksiä tuli 178 maasta. (Ottis 2008.) Käytännössä palvelunestohyökkäysten alkuperäistä lähdettä on vaikea todentaa.

Vuonna 2008 alkanut Georgian sota on ensimmäinen sota, jossa kybertoimia käytettiin osana sotatoimia. Internetin kautta tehdyt kyberiskut Georgiaa vastaan aloitettiin noin kolme viikkoa ennen Venäjän varsinaisia sotilaallisia toimia perinteisin asevoimin. Georgian valtion, presidentin ja monien muiden toimijoiden internet-sivut lakkasivat toimimasta niihin kohdistettujen palvelunestohyökkäysten takia. Georgian ulkoasiainministeriö joutui siirtämään valtionhallinnon viralliset sivut yhdysvaltalaisille palvelimille, jonka kautta Georgia suojasi virallista tiedotustaan verkkohyökkäyksiltä. (Georgiamfa 2008a.) Vastaavasti myös venäläisille uutissivuille tehtiin hyökkäyksiä Georgiasta käsin ja useita sivuja saatiin kaatumaan (Georgiamfa 2008b). Georgiaan kohdistuva verkkohyökkäys oli tyypillinen palvelunestohyökkäys ja muistutti tekotavaltaan Viroon vuonna 2007 kohdistunutta kyberhyökkäystä. Yhteiskunnan sisäisen turvallisuuden kannalta tiedotuspimentoon joutuminen on vaarallista.

Edellä kuvatut palvelunestohyökkäykset ovat toteutustavaltaan aika yksinkertaisia. Uusimmat haittaohjelmat voivat olla erittäin monimutkaisia, sillä toiminta voidaan suunnitella yksityiskohtaisesti ja vaikutus kohdistaa täsmäaseen tavoin ennalta valittuun kohteeseen. Haittaohjelma voidaan ohjelmoida aktivoitumaan esimerkiksi tiettynä ajankohtana tai tiettyjen olosuhteiden toteutuessa. Esimerkki tällaisesta monimutkaisesta haittaohjelmasta on Stuxnet, jota pidetään maailman ensimmäisenä fyysistä tuhoa aiheuttavana haittaohjelmana. Symantec, yksi maailman johtavista tietoturvayhtiöistä, julkaisi vuonna 2010 Stuxnet-haittaohjelmaa koskevan tutkimusraportin *W32.Stuxnet Dossier*. (Symantec 2011.) Samalla Symantec toi julkisuuteen siihen saakka salassa pidetyn haittaohjelman, jota pidetään vuosikymmenen merkittävimpänä haittaohjelmana. Stuxnet on huolellisesti suunniteltu ja raportin mukaan sen verran monimutkainen, ettei kukaan yksittäinen hakkeri voisi sitä toteuttaa, vaan sen toteutus vaatii vähintään valtiollisen tason voimavarat. (Symantec 2011.)

Stuxnetia käytettiin vuonna 2009 hyökkäyksessä Iranin ydinlaitosten tietojärjestelmiä vastaan. Stuxnetia ei voinut huomata, sillä se pystyi nauhoittamaan tavallista tehdastoimintaa ja esittämään nauhoitettua, normaalilta näyttävää toimintaa valvojille. Valvojat luulivat kaiken olevan kunnossa, mutta samaan aikaan Stuxnet teki taustalla tuhojaan. Stuxnet ohjelmoitiin kohdistetusti tietynlaisille laitteille ja olemaan

toimimattomana, kunnes se havaitsee olevansa oikeassa paikassa, jolloin se aktivoituu.

Stuxnet leviää muistitikkujen ja tietokoneverkon kautta, joten kuka tahansa ydinvoimalan työntekijä voi saada Stuxnet-haittaohjelman esimerkiksi työpaikkansa ulkopuolelta joltain tietokoneelta tai sähköpostin kautta. Näin Stuxnetin pääsee siirtymään muistitikulta työpaikan tietokoneelle ja sitä kautta koko ohjausjärjestelmään. (Symantec 2011.)

Stuxnetin saavutus lienee se, että sen avulla saatiin viivästettyä Iranin ydinaseohjelman toteutuminen ja ydinaseen valmistuminen. Se tekeytyi uraaninjalostuslaitoksella ohjausohjelmaksi, joka taajuusmuuttajia säätämällä sekoitti sentrifugit, ja tuloksena oli ydinaseisiin käyttökelvotonta uraania. Stuxnetin ansioksi voidaan katsoa myös se, että kansainvälinen yhteisö havahtui teollisuusautomaatiojärjestelmiin kohdistuviin kyberuhkiin. (Collins & McCombie 2012.)

Suomen valtiota ja viranomaisjärjestelmiä vastaan kohdistettu haittaohjelmakampanja paljastui vuonna 2013. Tuolloin Suojelupoliisi käynnisti esitutkinnan virallisen syytteen alaisesta vakoilurikoksesta. Vakoiluoperaation kohteena oli ulkoasianministeriö, jonka verkkoon tunkeuduttiin ja saatiin haltuun merkittävä määrä ulko- ja turvallisuuspolitiikkaa käsitteleviä asiakirjoja. Vakoilusta epäillään valtiollisia tahoja. (SUPO 2015, 6.) Tässä yhteydessä käytettiin Suomessa ensimmäistä kertaa käsitettä *kybervakoilu.* Vakoilu toteutettiin tietoverkon kautta siten, että ulkoasianministeriön työasemiin saatiin kohdistettua haittaohjelma, jonka kautta kyettiin sekä antamaan komentoja että vastaanottamaan tietolähetyksiä. (SUPO 2015, 7.) Suojelupoliisin laatimassa *Suojelupoliisin toimintaympäristö vuosina 2015–2016* -raportissa (SUPO 2015) esiintyy muitakin uusia käsitteitä, kuten *valtiolliset kyberaseet, kybervakoiluohjelmat, kybervakoiluoperaatiot, kyberhyökkäykset ja kybertiedustelu*. (SUPO 2015.)

Suomi on tehnyt selkeän ulkopoliittisen linjauksen osallistua aktiivisesti globaaliin, eurooppalaiseen ja lähialueidensa kansainväliseen yhteistyöhön turvallisuusalalla. Suomi on osa Euroopan unionia ja noudattaa yhtenäistä poliittista linjaa muiden jäsenmaiden kanssa. Samaan aikaan Suomi pyrkii ylläpitämään kahdenvälisiä

yhteistyösuhteita strategisiin kumppaneihinsa, kuten Kiinaan, Yhdysvaltoihin ja Venäjään. (VNK 5/2012, 9.)

Suomi liittyi Euroopan Unionin jäseneksi vuonna 1995 ja samalla hyväksyi Maastrichtin sopimuksen, joka määrittää Euroopan unionin yhteisen ulko- ja turvallisuuspolitiikan. *Euroopan unionin turvallisuusstrategia* (EU Council 2009) määrittelee EU:n turvallisuuspoliittiset linjaukset ja sen tavoitteena on mm. turvallisuuden ja vakauden edistäminen. Turvallisuusstrategia päivitettiin vuonna 2008, jolloin huomiota kiinnitettiin ilmastonmuutoksen ja energiaturvallisuuden lisäksi erityisesti myös kyberturvallisuuteen. (MPKK 2013, 34.) Tässä on huomautettava, että EU:n turvallisuusstrategiassa käytettiin tosiasiassa *tietoverkkoturvallisuus*-käsitettä (EU Council 2009, 13), johon myöhemmin julkaistussa asiakirjassa on viitattu *kyberturvallisuus*-käsitteellä (MPKK 2013, 34).

Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta (L66/2009) laajensi yhteisen politiikan toimialaa. Tarkoituksena oli vahvistaa jäsenmaiden keskinäistä sitoutumista yhteiseen turvallisuus- ja puolustuspolitiikkaan. Lissabonin sopimuksen yhteisvastuulausekkeen SEUT 222 artiklan mukaisesti Suomi varautuu toimimaan ja kehittämään valmiuksia terrorismin, luonnonmullistusten tai kyberhyökkäysten tapahtuessa. (PuVL 4/2013.)

Euroopan unionin kyberturvallisuusstrategia on laadittu vuonna 2013 (EU CSS 2013) ja se pyrkii edistämään siviili- ja sotilasyhteistyötä kyberturvallisuusuhkien ennaltaehkäisyssä (EK 2013). Suomi osallistuu Euroopan puolustusviraston (EDA, European Defence Agency) toimintaan. EDA on Euroopan unionin neuvoston alainen virasto, jonka tavoite on edistää ja tukea jäsenmaiden sotilaallisten suorituskykyjen kehittämistä mukaan luettuna kyberpuolustus. (EDA 2015.)

Euroopan unionin verkko- ja tietoturvallisuusvirasto (ENISA, European Network and Information Security Agency) on verkko- ja tietoturvallisuusalan laitos, joka on perustettu kyberturvallisuuden asiantuntijaorganisaatioksi. ENISA on koonnut internetsivustolleen EU-maiden kyberstrategiat. Suomen ja EU-maiden kyberstrategioiden lisäksi myös Euroopan ulkopuolisten maiden strategioita on julkaistu ENISA:n internetsivulla. Suurin osa strategioista on laadittu vuoden 2011

jälkeen. (ENISA 2015a.) ENISA:lla on myös omaa sanastotyötä, ja sen laatimaa sanastoa on hyödynnetty tässä tutkimuksessa (ENISA 2015b). ENISA järjestää vuosittaisen Euroopan laajuisen tietoturvaharjoituksen, Cyber Europen. Suomesta Cyber Europe -harjoitukseen on osallistunut Kyberturvallisuuskeskus, liikenne- ja viestintäministeriö sekä suomalaisia yksityisen sektorin organisaatioita. (VIVI 2014a.) Suomi noudattaa Euroopan unionin antamia kyberturvallisuusdirektiivejä (EEAS 2013).

Suomi ei ole Naton jäsenmaa, mutta Naton rauhankumppanimaana se voi osallistua erikseen hyväksyttyyn yhteistyöhön esimerkiksi kyberturvallisuusalalla. Nato on käsitellyt kyberturvallisuutta jo vuoden 2002 Prahan huippukokouksesta alkaen. Viron tapahtumat vuonna 2007 saivat liittouman aktivoitumaan, ja sen jälkeen on perustettu kyberturvallisuusalan toimielimiä niin poliittiselle, operatiiviselle kuin asiantuntijatasollekin. (Nato 2002.) Naton keskeiset turvallisuusympäristön painopisteet ovat terrorismi, kriisinhallinta ja kyberturvallisuus (VNK 5/2012, 60).

Viron kyberhyökkäysten jälkeen, vuonna 2008, Virossa avattiin Cooperative Cyber Defence Centre of Excellence, josta yleisimmin näkee käytettävän suomenkielistä käännöstä Naton kyberpuolustuskeskus. Osuvampi käännös olisi Naton kyberosaamiskeskus, koska sillä ei ole operatiivisia tehtäviä. Se ei myöskään suoranaisesti ole Pohjois-Atlantin liiton osa, vaikkakin se on Naton hyväksymä kansainvälinen tutkimusorganisaatio ja toimii Natoa tukevana asiantuntijaelimenä kyberturvallisuutta koskevissa asioissa. (CCDCOE 2015a.)

Naton kyberpuolustuskeskus, NATO CCDCOE tekee aktiivisesti tutkimusta kyberturvallisuusalalla. Se järjestää vuosittain Tallinnassa International Conference on Cyber Conflict -konferenssin, jossa on muun ohjelman lisäksi myös kyberturvallisuusalan termistöä käsitteleviä työryhmiä. Työryhmien tulokset julkaistaan Naton kyberosaamiskeskuksen internetsivuilla. (CYCON 2015.)

Euroopan Unionin Nato-jäsenmaat harjoittelevat Naton viitekehyksessä ja järjestävät Cyber Coalition -harjoituksen, joka on puolustus- ja siviiliviranomaisten kansainvälinen kyberyhteistoimintaharjoitus. Suomesta harjoitukseen osallistuu viranomaisia puolustusvoimista, poliisista, ulkoministeriöstä ja

valtiovarainministeriöstä. (TK 2015.) Suomi on hyväksytty syksyllä 2015 Naton kyberosaamiskeskukseen osallistuvaksi kumppanimaaksi (CCDCOE 2015c).

Naton kyberosaamiskeskuksen tunnetuin julkaisu on sen tuottama tutkimusraportti *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt 2013). Raportti on julkaistu vuonna 2012, ja se tunnetaan yleisesti nimellä *Tallinnan manuaali.* Se on lakitieteellinen tutkimus siitä, miten kansainvälistä oikeutta sovelletaan kybertoimintaympäristössä ja kuinka kansainvälinen laki sodankäynnistä pätee verkossa. Toisin sanoen kysymys on siitä, miten verkkosodankäynti on huomioitava uutena ja yhtenä sodankäynnin muotona Naton kyberosaamiskeskuksen mukaan tutkimus ei perustu Naton doktriiniin, eikä se ole mitään tiettyä valtiota edustava virallinen asiakirja. (CCDCOE 2015b.)

Tallinnan manuaalin (Schmitt 2013) lopussa on sanasto, jossa on termeille annettu määritelmät. Sanastoa on ollut laatimassa terminologien lisäksi kansainväliseen oikeuteen erikoistuneita juristeja (CCDCOE 2015b). Sanastotyönprojektin yhtenä tavoitteena on ollut termistön yhdenmukaistaminen. Sanastoprojektin aikana osallistujat kommentoivat ja esittävät omia näkemyksiään määritelmien sisällöstä. Lopuksi sanastoon kootaan määritelmät. Joillakin käsitteillä on vain yksi, kaikkien maiden hyväksymä määritelmä. Joillakin käsitteillä määritelmiä on useita, eri maiden mukautettuja määritelmiä. (CCDCOE 2015d.)

Vaikka Suomi onkin asettanut tavoitteekseen olla maailmanlaajuisesti edelläkävijä kyberuhkiin varautumisessa vuonna 2016 (Kyberstrategia 2013, 3), niin USA lienee kuitenkin kiistatta edelläkävijä kyberturvallisuusalalla – ainakin kyberuhkien visioinnissa. Vuoden 2001 terrori-iskujen jälkeen Yhdysvalloissa perustettiin United States Department of Homeland Security (DHS), Yhdysvaltain ministeriön tasoinen virasto, jolla on merkittävä rooli Yhdysvaltain kyberturvallisuuden kehittämisessä. (DHS 2014.)

Vuonna 2006 DHS organisoi ensimmäisen kerran Yhdysvalloissa kansallisen Cyber Storm -kyberharjoituksen (CSI). Maailmanlaajuisesti tuolloin ei vielä kovinkaan monessa valtiossa ollut edes määritelty käsitettä *kyberturvallisuus*, saati visioitu mitä se voisi tarkoittaa. Cyber Storm -harjoituksissa visioidut uhkat ovat suurilta osin toteutuneet ja siten muuttuneet visioista reaalimaailman ilmiöiksi. On selvää, että

kansainvälisessä yhteistyössä englanninkielistä käsitteistöä siirtyy yhdysvaltalaisilta tutkijoilta Eurooppaan. Käsitteiden sisältö voi kuitenkin olla hyvin erilainen eurooppalaisessa kontekstissa verrattuna lähtökielen kontekstiin.

Venäjän valtionhallinnon ulkopolitiikka on selkeä osa valtion turvallisuuspolitiikkaa. Kansalliset intressit on määritelty kansallisen kokonaisturvallisuuden lähtökohdista, joissa korostuvat sotilaallinen turvallisuus ja perinteiset sotilaalliset uhkakuvat. Venäjällä kansallinen turvallisuus on lainsäädännöllisesti rakennettu kokonaisuus, joka sitoo tiiviisti yhteen sekä valtion että yhteiskunnan turvallisuuden. (PLM 2012.)

Venäjän kansallisen kyberstrategian valmistelu on vielä kesken. Vuoden 2013 loppupuolella Venäjän Parlamentin ylähuoneessa eli liittoneuvostossa (ven. Совет Федерации) oli käsittelyssä *Venäjän kyberturvallisuusstrategian luonnos*. (SF 2014a.) Liittoneuvosto julkaisi *kyberturvallisuusstrategian luonnoksen* internetsivustollaan pyytäen sekä viranomaisten että siviilien kommentteja ja ehdotuksia sisällöstä. Seuraavan vuoden alussa liittoneuvoston sivulla on maininta, että luonnosta edelleen käsitellään ja kerätään kommentteja, mutta sen etenemisestä ei löydy uudempaa tietoa vielä vuoden 2015 loppuun mennessä. (SF 2014b.)

Venäjä tekee yhteistyötä eurooppalaisella tasolla ja on muun muassa Euroopan neuvoston jäsen. Venäjä ei kuitenkaan ole ratifioinut *Euroopan neuvoston tietoverkkorikollisuutta koskevaa yleissopimusta vuodelta 2001* (L60/2007), joka tunnetaan *Budapestin sopimuksena*. Kun yhteistä linjaa ei ole saatu muodostettua länsimaiden kanssa, on Venäjä tiivistänyt yhteistyötä tietoturvallisuusalalla erityisesti Kiinan kanssa. (IISI MSU 2015.)

Venäjä mainitsee *valtiollisen suvereniteetin* yhdeksi tärkeimmistä syistä, miksi Venäjä ei voi hyväksyä Budapestin sopimusta:

> Конвенция Совета Европы о киберпреступности 2001 года (Будапештская конвенция), содержит неприемлемые для России, а также ряда других государств, положения, идущие в разрез с принципом уважения государственного суверенитета (MID 2013).

Venäjän lisäksi muutama muukin maa on jättäytynyt *Budapestin sopimuksen* ulkopuolelle (COE 2015). Venäjän on laatinut oman ehdotuksensa *Budapestin*

sopimuksen tilalle, *Venäjän konvention* (ven. *Конвенция об обеспечении международной информационной безопасности (концепция)* (SBRF 2011).

Information Security Institute (ven. Институт проблем информационной безопасности) on Moskovan M. V. Lomonosovin mukaan nimetyn valtion yliopiston yhteyteen perustettu tutkimuslaitos, jolla on keskeinen asema kyberturvallisuuden tutkimuksessa Venäjällä. Se on ollut mukana laatimassa edellä mainittua *Venäjän konventiota* (SBRF 2011), *Venäjän kyberturvallisuusstrategian luonnosta* (SF 2014a) sekä tässä tutkimuksessa hyödynnettyjä kaksikielisiä venäjä–englanti *Bilateraalisia kyberturvallisuussanastoja* (Bilat 2011en; Bilat 2011ru; Bilat 2014). Tutkimuslaitos tekee läheistä yhteistyötä Venäjän valtion turvallisuus-viranomaisten kanssa. Laitos tekee laaja-alaista tutkimustyötä valtionhallintoon kuuluville organisaatioille ja sen asiakkaita ovat mm. Venäjän presidentin hallinto, turvallisuusneuvosto, FSB, ulkoministeriö, Venäjän asevoimien esikunta, tulli sekä Gazprom. (IISI MSU 2014a.) Sen tutkijoiden kyberturvallisuutta käsitteleviä kirjoituksia on hyödynnetty tässä tutkimuksessa.

Tutkimuslaitos on aktiivisessa yhteistyössä myös kansainvälisten toimijoiden kanssa. Tutkimuslaitoksen edustaja kuuluu myös Nato–Venäjä-neuvoston (eng. NATO-Russia Council, lyhennettynä NRC) alaiseen tiede- ja rauhaohjelman asiantuntijaryhmään. (IISI MSU 2014b). Yhteistyö valtiollisella tasolla alkoi NRC:n muodossa vuonna 2002 (NRC 2002). NRC on tuottanut myös englanti–venäjä sanastoja ja tehnyt yhteistyötä lingvistiikan ja terminologian alalla (NRC 2013). Huhtikuussa 2014 NRC ilmoitti internetsivuillaan, että kaikki siviili- ja sotilasyhteistyö on päätetty toistaiseksi keskeyttää ja syyksi kerrotaan Venäjän toiminta Ukrainassa. Tämä päätös keskeyttää siis myös sanastotyöhankkeet toistaiseksi. (NRC 2014.)

3 Tutkimusaineisto

Tässä luvussa esitellään tutkimusaineisto. *Sanastotyön käsikirja* (STK 1988) ja *Sanastotyön opas* (Suonuuti 2006) suosittelevat valitsemaan mahdollisimman monipuolista lähdeaineistoa. Tärkeiksi lähteiksi luokitellaan erilaiset asiakirjat, kuten lait, direktiivit ja säädökset sekä standardit. Lisäksi suositellaan hyödyntämään aikaisemmin laadittuja sanastoja ja sanakirjoja. (STK 1988, 142–144, Suonuuti 2006, 35.) Lähteiksi valittavan aineiston luotettavuus, ajankohtaisuus ja tarkoituksenmukaisuus tulee arvioida (Suonuuti 2006, 35). *Sanastotyön käsikirjassa* määritellään neljä erityyppistä aineistolajia: (1) auktorisoitu aineisto, (2) tiedeyhteisön hyväksymä aineisto, (3) ajankohtainen, mutta ei välttämättä yleisesti vakiintunut aineisto ja (4) suulliset lähteet (STK 1988, 142–143).

Tämän tutkimuksen aineisto on rajattu koskemaan viranomaisten julkisesti saatavilla olevia asiakirjoja, joita voidaan pitää luotettavina lähteinä (STK 1988, 142–144, Suonuuti 2006, 35). Tutkimuksen aiheen perusteella aineisto rajataan käsittelemään kyberturvallisuutta käsitteleviä asiakirjoja. Aineistolähteinä käytetään vuoteen 2015 mennessä ilmestyneitä viranomaisten asiakirjoja. Asiakirjojen ohella tarkastellaan myös jonkin verran asiakirjan laatineita viranomaisia. Suosituksen mukaan aineistoon on valittu myös muutama sanasto (Suonuuti 2006, 35). Sanastoja voidaan pitää luotettavina, sillä laatijat ovat terminologeja, läheisesti yhteistyössä viranomaisten kanssa tai laatineet sanastoa viranomaisten tarpeisiin. Aineiston ohella tutkimuksessa on hyödynnetty suomalaisten ja kansainvälisten kyberturvallisuusalan asiantuntijoiden julkaisemia teoksia ja kirjoituksia sekä asiantuntijalausuntoja. Ensin esitellään suomenkielinen ja luvun loppupuolella venäjänkielinen aineisto.

3.1 Suomenkielinen tutkimusaineisto

Suomenkieliseen aineistoon kuuluvat Valtioneuvoston periaatepäätökset ovat sekä ohjeita valtion hallinnolle että poliittisia kannanottoja, joilla linjataan kunkin hallituskauden aikana valmisteltavia päätöksiä. Periaatepäätöksellä ei ole välitöntä juridista vaikutusta, mutta ne sitovat sitä hallitusta, joka on ne hyväksynyt. Hallituksen vaihtuessa uusi hallitus päättää erikseen mitkä periaatepäätökset ovat voimassa sen hallituskaudella. Valtioneuvosto johtaa ja ohjaa kyberturvallisuuden poliittisia ja strategisia linjauksia. Kukin ministeriö vastaa omalla toimialallaan

kyberturvallisuudesta ja siihen liittyvistä mahdollisista häiriötilanteista ja niiden hallinnasta. (VN 2015a.) Nykyisistä kahdestatoista (12) ministeriöistä on tähän tutkimukseen rajattu kyberturvallisuuden toimenpanoon osallistuvat: valtioneuvoston kanslia (VNK), ulkoasiainministeriö (UM), sisäasiainministeriö (SM), puolustusministeriö (PLM), liikenne- ja viestintäministeriö (LVM) ja työ- ja elinkeinoministeriö (TEM). (L 28.2.2003/175.)

Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (YETT 2003) on valtioneuvoston periaatepäätös vuodelta 2003. Siinä on määritelty sekä yhteiskunnan elintärkeiden toimintojen turvaaminen että eri hallinnonaloille niiden oman toimialan turvallisuutta koskevat vastuualueet. Periaatepäätöksessä luetellaan seitsemän yhteiskunnan elintärkeää toimintoa, joita ovat: valtion johtaminen, ulkoinen toimintakyky, Suomen sotilaallinen puolustus, sisäinen turvallisuus, talouden ja yhteiskunnan toimivuus, väestön toimeentuloturva ja toimintakyky ja henkinen kriisinkestokyky. Asiakirjassa on kuvattu erityyppisiä tietojärjestelmiin kohdistuvia uhkia, mutta siinä ei vielä käytetä *kyberturvallisuus*-käsitettä, vaikka asiasisältö siihen viittaisikin. Sen sijaan käytetään käsitettä *tietojärjestelmäsodankäynti* uutena sodankäynnin keinona. (YETT 2003.)

Yhteiskunnan elintärkeiden toimintojen turvaamisstrategia (YETT 2003) päivitettiin viimeksi vuonna 2010. Samalla nimi muutettiin muotoon Y*hteiskunnan turvallisuusstrategia*, lyhennettynä YTS (YTS 2010). *YTS* määrittelee kokonaisturvallisuuden ja siihen liittyvän varautumisen sekä tarkentaa eri ministeriöille jaetut vastuualueet. Sen tavoite on yhtenäistää valtion, kuntien, järjestöjen ja elinkeinoelämän varautumista kriisitilanteisiin. (YTS 2010.) YTS:ssa on myös selitetty ja määritelty käsitteitä kuten *yhteiskunnan elintärkeät toiminnot* (YTS 2010, 17–52). Lisäksi *YTS* kuvaa elintärkeitä toimintoja vaarantavat *uhkamallit*, joista yksi on: ”*tietoliikenteen ja tietojärjestelmien vakavat häiriöt eli kyberuhkat”* (YTS 2010, 15). Tämä on ensimmäinen kerta kun *kyber*-etuliitteellä muodostettu yhdyssana esiintyy suomalaisen viranomaisen julkaisemassa asiakirjassa.

Tämän tutkimuksen tärkeimpiä aineistolähteitä on *Kyberturvallisuusstrategiana* tunnettu periaatepäätös. *Kyberturvallisuusstrategian* käsitteet luovat aineiston pohjan ja toistaiseksi se on ainoa viranomaisten laatima asiakirja, jossa on määritelty

kyberturvallisuuteen liittyviä käsitteitä. *Kyberturvallisuusstrategia* (Kyberstrategia 2013) on osa yhteiskunnan kokonaisturvallisuutta. Siinä pyritään ennakoimaan mahdolliset uhkat koko yhteiskuntaa koskevilla tietoturvallisuuden järjestelyillä. Valtioneuvoston kyberturvallisuutta ohjaava periaatepäätös määrittelee ja ohjaa kyberturvallisuuden toimeenpanoa valtion hallinnossa. (Kyberstrategia 2013.) *Suomen kyberturvallisuusstrategian taustamuistio* (Kyberstrategia 2013) on *Kyberturvallisuusstrategian* (Kyberstrategia 2013) ohessa julkaistu sitä tarkentava asiakirja. Koska ne on painettu yhdessä, niin tässä tutkielmassa viitataan näihin molempiin asiakirjoihin samalla viittauksella (Kyberstrategia 2013).

Kokonaisturvallisuuden asioita käsitellään muun muassa valtioneuvoston ministerivaliokunnissa ja ulko- ja turvallisuuspoliittisen valiokunnan yhteiskokouksissa (VN 2015c). *Valtioneuvoston periaatepäätös kokonaisturvallisuudesta 2012* -asiakirjassa (VNpp 2012) määritellään *kokonaisturvallisuus*-käsite ja muita siihen liittyviä keskeisiä käsitteitä. Asiakirjassa esiintyy *kyber*-etuliite vain kerran, silloin kun viitataan laadittavaan *Kyberturvallisuusstrategiaan* (VNpp 2012, 12). Johdantokappaleessa käytetään ilmaisua *verkottunut yhteiskunta on aiempaa haavoittuvampi,* millä viitataan tietoverkkoihin (VNpp 2012, 5).

Valtioneuvosto laatii eri toimialojen selontekoja Eduskunnalle. Valtioneuvoston turvallisuus- ja puolustuspoliittinen selonteko on Eduskunnan puolustusvaliokunnan käsittelemä ja sen jälkeen Eduskunnan hyväksymä asiakirja. Selonteko laaditaan puolustus- ja ulkoasianministeriössä kunkin hallituksen hallitusohjelman mukaisesti ja se ohjaa Suomen turvallisuuspolitiikan toimeenpanoa ministeriöissä.

Valtioneuvoston turvallisuus- ja puolustuspoliittinen selonteko on asiakirja, joka arvioi Suomen ulko- ja turvallisuuspolitiikan kokonaisvaltaisesti ja määrittelee sen periaatteet ja tavoitteet lähitulevaisuudelle. Vuoden 2009 *Turvallisuus- ja puolustuspoliittisessa selonteossa* (VNS 9/2009) todetaan sen luovan perustan valtioneuvoston turvallisuutta käsitteleville selonteoille ja strategioille. (VNS 9/2009, 3). Vuoden 2009 selonteossa ei vielä esiinny *kyberturvallisuus*-käsitettä, mutta siinä käsitellään tietoturvallisuuden ja tietoverkkojen keskeistä merkitystä yhteiskunnan toimintojen kannalta. Tietoverkkorikollisuuden torjuntaa pidetään erityisen tärkeänä,

mutta sitä ei käsitellä koko valtakunnan kokonaisturvallisuutta uhkaavana tai ainakaan valtiolliselta taholta tulevana uhkatekijänä. (VNS 9/2009, 85.)

Valtioneuvoston turvallisuus- ja puolustuspoliittinen selonteko vuodelta 2012 (VNK 5/2012) on viimeisin Eduskunnalle annettu turvallisuus- ja puolustuspoliittinen selonteko ja se korvaa aikaisemmat selonteot. Sen tarkastelu ulottuu 2020-luvulle muodostaen perustan Suomen politiikan ohjaamiselle lähitulevaisuudessa. Selonteko visioi kansainvälistä turvallisuusympäristön kehitystä ja samalla linjaa Suomen turvallisuuspolitiikkaa. Yhteiskunnan toimivuuden takaaminen on selonteossa keskeisessä asemassa ja siinä on ensimmäistä kertaa otettu käsiteltäväksi *kansallinen kyberturvallisuus*, joka on selonteossa saanut oman alalukunsa (VNK 5/2012, 94). Perinteisen sotilaallisen uhkakuvan lisäksi mainitaan tietoyhteiskunnan uusiksi haasteiksi kybertoimintaympäristön turvaaminen ja tietoturvahyökkäykset (VNK 5/2012, 14).

Aineistoon on näiden edellä esiteltyjen asiakirjojen lisäksi valittu sanastoja, jotka on laadittu terminologien, asiantuntijoiden ja viranomaisten yhteistyön tuloksena. *Valtionhallinnon tietoturvasanasto* (VAHTI 8/2008) on osa Sanastokeskus TSK:n Tietotekniikan termitalkoiden tuottamaa materiaalia. Se on laadittu sekä valtionhallinnon että tietoturvallisuusalalla työskentelevien tarpeisiin. Myös *Tiivis tietoturvasanasto* (TSK 31) on Sanastokeskus TSK:n sanastohanke ja osa hallituksen kansallista tietoturvastrategiaa. Sanastossa on termitietueet, käsitekaaviot ja noin 80 tietoturvallisuuteen liittyvää käsitettä. (TSK 31.)

Sanastokeskus TSK on ollut myös laatimassa *Kokonaisturvallisuuden sanastoa* (TSK 47). Sanastohankkeen työryhmään kuului muuan muassa opetus- ja kulttuuriministeriö, puolustusministeriö, sisäministeriö, sosiaali- ja terveysministeriö ja ympäristöministeriö sekä Huoltovarmuuskeskus ja Turvallisuuskomitean sihteeristö. (TSK 47.) Sanaston johdannossa todetaan alkuperäisen tavoitteen olleen *Varautumisen ja väestönsuojelusanaston* (2009) päivittäminen. Termistö, käsitteet ja niitä määrittelevät ohjausasiakirjat olivat viidessä vuodessa muuttuneet siinä määrin, että päädyttiin laatimaan kokonaan uusi sanasto, joka vastaisi paremmin kaikille hallinnonaloille yhteisiä kokonaisturvallisuuden käsitteitä (TSK 47, 6).

Sanastokeskus TSK:n internetsivustolla on *TEPA*-termipankki (TEPA 2015), josta voi hakea erikoisalojen termejä ja määritelmiä. Termipankissa on sekä Sanastokeskus TSK:n omia että muiden asiantuntijoiden laatimia alakohtaisia sanastoja. Haun voi kohdistaa kaikkiin TEPA:n sanastoihin, jolloin tuloksena saa käsitteen määritelmän lisäksi myös lähdesanaston tiedot ja julkaisuvuoden. Termipankin kautta haettuihin käsitteisiin viitataan lähdeluettelossa termipankin nimellä: *TEPA* ja sanaston julkaisuvuodella, esimerkiksi TEPA, 2002. (TEPA 2015.)

3.2 Venäjänkielinen tutkimusaineisto

Venäjällä kansallisen kyberstrategian valmistelu on vielä kesken. Toistaiseksi on julkaistu luonnos, *Концепция стратегии кибербезопасности РФ* (SF 2014a), josta tässä tutkimuksessa käytetään nimitystä *Venäjän kyberturvallisuusstrategian luonnos*. *Venäjän Kyberturvallisuusstrategian luonnoksen* edistymisestä ei löydy uudempaa tietoa vielä vuoden 2016 maaliskuuhun mennessä. Tässä pro gradu -tutkielmassa käsitellään vuonna 2013 julkaistua *Venäjän kyberturvallisuusstrategian luonnosta* (SF 2014a). Luonnoksessa todetaan, että kyberstrategian tulee perustua hyvin määriteltyihin käsitteisiin. Luonnoksessa on vain neljä käsitettä määritelmineen. Näitä käsitteitä tarkastellaan tarkemmin käsiteanalyysin yhteydessä. *Kyberturvallisuusstrategian luonnos* (SF 2014a) pohjautuu Venäjän kansallista turvallisuutta määritteleviin asiakirjoihin, joita ovat *Venäjän perustuslaki* (KRF 1993), *Venäjän federaatiolaki turvallisuudesta* (FZ 149) ja *Kansallinen turvallisuusstrategia vuoteen 2020* (UKAZ 537).

Venäjänkieliseen aineistoon kuuluu Venäjän turvallisuusneuvoston (Совет безопасности) internetsivustolla julkaistuja asiakirjoja (SB 2015), joista neljä on valittu tähän tutkimukseen lähdeasiakirjoiksi. Asiakirjat on koottu venäjänkielisen *информационная безопасность*-käsitteen alle. Yksi tärkeimmistä venäjänkielisistä aineistolähteistä on *Доктрина информационной безопасности Российской Федерации* (DIBRF 2000), josta tässä tutkimuksessa käytetään nimitystä *Venäjän informaatioturvallisuusdoktriini.* Siinä on käsitteiden lisäksi kuvattu laajemmin mitä *kansallinen turvallisuus* -käsite tarkoittaa. Venäläinen *информационная безопасность* -käsite on yksi keskeisimpiä kyberturvallisuutta määrittelevistä venäjänkielisistä käsitteistä, jonka suomenkielinen vastine selvitetään käsiteanalyysin yhteydessä.

Venäjän tavoite on muuttua nykyaikaiseksi tietoyhteiskunnaksi, mitä varten on laadittu muun muassa *Стратегия развития информационного общества в Российской Федерации* (SRIORF 2008), jota tässä tutkimuksessa nimitetään *Venäjän tietoyhteiskunnan kehitysstrategiaksi.* Asiakirja käsittelee nykyaikaisen tietoyhteiskunnan tietoturvallisuuteen liittyviä aiheita. Strategia asettaa tavoitteet ja määrittelee päälinjat, joita tulee soveltaa kaikissa asiakirjoissa, ja jotka koskevat kaikkia valtion organisaatioita. Valtion tehtäviksi on määritelty muuan muassa yhteiskunnan kehittäminen sekä valtion kilpailukyvyn ja kansalaisten hyvinvoinnin edistäminen. Yksi tärkeä tavoite on luoda turvallinen tietoyhteiskunta.

Kansalaisten perustuslailliset oikeudet voidaan parhaiten turvata kehittämällä tietoyhteiskunnan valvontaa. (SRIORF 2008.) Tietoturvallisuusalan tieteellisen tutkimuksen linjaukset on määritelty asiakirjassa *Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации.* (NIIBRF 2008) Asiakirjan sisällöstä ei selviä kovin paljoa, sillä asiakirjasta on julkaistu ainoastaan numeroidut alaotsikot, joissa on lueteltu muun muassa tieteellisen tutkimuksen linjauksia ja keinoja, joiden avulla valtion sekä yhteiskunnan turvallisuutta ylläpidetään ja kehitetään. (NIIBRF 2008.)

Asiakirjan yksi alaotsikoista viittaa Venäjän kansan kulttuurillisten ja moraalisten arvojen säilyttämiseen: ”1.1.77 Проблемы сохранения культурно-нравственных ценностей российского народа.” (NIIBRF 2008.) Viittaus arvojen säilyttämiseen poikkeaa länsimaisesta ajattelusta, jossa arvomaailmaan liittyviä kysymyksiä ei yleensä liitetä valtion tietoturva-asioihin tai tieteelliseen tutkimustyöhön. Länsimaisen ajattelun mukaan yhteiskunnan arvojärjestelmät eivät ole yhtenäisiä eikä niitä pyritä ohjaamaan valtiovallan toimesta (Levomäki 2008, 22).

Julkisen hallinnon rooli yhteiskunnassa on Venäjällä suurempi kuin esimerkiksi Suomessa. Taustalla on sosialistisen järjestelmän romahduksen aikaan saama uusi tilanne, jossa oli uudelleen määriteltävä valtion tehtävien sisältö sekä kansalaisen ja valtion välinen suhde (Levomäki 2008, 19). Länsimaisissa yhteiskunnissa yhteistä arvopohjaa ei helposti tunnista. Neutraalin liberalismin mukaan valtion tulisi antaa ihmisille vapaus toteuttaa omia intressejään ja pyrkimyksiään. (Levomäki 2008, 22.)

Tässä suhteessa Venäjällä määritellään määrätietoisemmin ja selvemmin mitkä arvot yhteiskuntaa ja kansalaisia ohjaavat.

Tämä selittänee syitä siihen, miksi Venäjä ei ole ratifioinut *Budapestin sopimusta, Euroopan neuvoston tietoverkkorikollisuutta koskevaa yleissopimusta vuodelta 2001* (L60/2007), vaan laatinut sen sijaan oman ehdotuksensa. *Конвенция об обеспечении международной информационной безопасности (концепция)* (SBRF 2011), josta tässä tutkimuksessa käytetään nimitystä *Venäjän konventio*. Lähdeaineistoon valitussa *Venäjän Konventiossa* (SBRF 2011) on määritelmä 20 käsitteelle, jotka ovat osa Venäjän virallisissa asiakirjoissa käytettyä turvallisuuskäsitteistöä. Koska länsimaat eivät ole hyväksyneet *Venäjän Konvention* (SBRF 2011) sisältöä, niin voidaan olettaa, etteivät termit ja niiden määritelmät ole yhdenmukaisia tai vastaavia länsimaissa käytetyn käsitteistön kanssa.

Länsimaiden ja Venäjän välistä näkökulmaeroa kyberturvallisuuskäsitteistössä on pyritty ratkaisemaan laatimalla sanasto, joka on syntynyt venäläisten ja amerikkalaisten kyberturvallisuusasiantuntijoiden yhteistyön tuloksena. Lähdeaineistoksi valittuun sanastoon on koottu kyberturvallisuuden keskeisiä käsitteitä määritelmineen. Sanasto on kaksikielinen (englanti–venäjä) kyberturvallisuussanasto, jonka ensimmäinen osa ilmestyi sekä englannin että venäjän kielellä vuonna 2011. Ensimmäisen osan venäjänkielinen nimi on *Двусторонний проект: Основы критически важной терминологии, Издание 1* (Bilat 2011ru). Englanninkielinen nimi on *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 1* (Bilat 2011en). Sanaston toinen osa on julkaistu pelkästään englanninkielisenä huhtikuussa 2014: *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2*. (Bilat 2014). Tässä tutkielmassa sanastosta käytetään nimitystä *Bilateraalinen sanasto* ja kuhunkin niistä viitataan omalla viitemerkinnällä.

Sanastotyön venäläisenä osapuolena on ollut tutkimuslaitos Институт проблем информационной безопасности, josta laitos käyttää englanninkielistä nimeä Information Security Institute, lyhennettynä *IISI* (IISI MSU 2014a). Toisena osapuolena on ollut riippumattomaksi itsensä luokitteleva ajatushautomo EastWest Institute, lyhennettynä EWI (EWI 2015). Sanastossa on käsitteiden lisäksi arvokasta taustatietoa sekä näkökulmaeroista että turvallisuusajatteluun liittyvistä asioista.

Tämän asiakirjan painoarvo on suuri poliittisten jännitteiden takia. Venäjä ja USA edustavat internetin hallinnon ääripäitä, joten on merkittävää, että ne ovat saavuttaneet yhteisymmärryksen - konsensuksen - kyberturvallisuuskäsitteistä. Asiakirja edustaa Venäjän virallista kantaa, tosin se on sovitettu länsimaiseen ajatteluun istuvammaksi.

Bilateraalisen sanaston (Bilat 2014) englanninkieliset termit ovat käyttökelpoisia myös suomalaisessa kyberturvallisuuskontekstissa (Tuukkanen 2015). Myös vertailun perusteella Kyberturvallisuusstrategian (Kyberstartegia 2013) käsitteistö näyttää olevan hyvin samansisältöistä kuin Bilateraalisen sanaston käsitteistö.

Tutkimusaineistoon on myös valittu Venäjän asevoimien sivulla julkaistu asiakirja *Концептуальные взгляды на деятельность Вооруженных Сил РФ в информационном пространстве* (KVDVSRF 2011), josta käytetään tässä tutkimuksessa nimitystä *Käsitteellinen katsaus Venäjän asevoimien toimintaan informaatioavaruudessa*. Katsauksessa käsitellään Venäjän asevoimien roolia ja tavoitteita uudessa ulottuvuudessa, johon kuuluvat tietoverkot ja tietojärjestelmät. Asiakirjassa esitellään ja määritellään kymmenen keskeistä käsitettä, jotka perustuvat Venäjän sotilasdoktriiniin ja ne on määritelty asevoimien toiminnan näkökulmasta.

Turvallisuusneuvoston sivulla on julkaistu myös muitakin asiakirjoja, jotka sivuavat tutkimusaihetta, mutta niitä ei tässä tutkimuksessa ole luokiteltu ensisijaisiksi aineistolähteiksi (SB 2014a, SB 2014b, SB 2014c, FSB 2015). Aineistoon kuuluu myös tietoturvallisuutta määritteleviä standardeja ja suosituksia sekä luotettaviksi katsottujen kyberturvallisuusalan asiantuntijoiden kirjoituksia.

Aineiston valinnassa on pyritty noudattamaan terminologien suosituksia (Nuopponen, Pasanen 2009, Suonuuti 2006, STK 1988). Grinev-Grinevich suosittelee tutkimaan millaisia termejä löytyy standardeista ja suosituksista, joita pidetään erityisen vahvoina ja luotettavina lähteinä. Grinev-Grinevich huomauttaa, etteivät standardit aina ole terminologisesti hyvin muotoiltuja. Lisäksi termien joukossa on sellaisiakin, joita erikoisalan asiantuntija eivät lainkaan käytä (Grinev-Grinevich 2008, 20).

4 Terminologinen käsiteanalyysi

Sanastokeskus TSK (vuoteen 2004 Tekniikan Sanastokeskus) perustettiin 1974. Koska perustajajäsenet olivat lähinnä tekniikan alan järjestöjä, niin sen toiminta-alue rajattiin tekniikkaan. Tavoite oli ennen kaikkea yhtenäistää termien käyttöä eri erikoisaloilla. Sanastokeskuksen laatimat sanastot ovat *normatiivisia,* eli ne pyrkivät ohjaamaan kielenkäyttöä. (TSK 2015.) Sanastotyö voi olla myös *deskriptiivistä*, jolloin tarkoituksena on olemassa olevan käsitteistön kuvaaminen (Nuopponen 1999, 92).

Terminologian teoria on siis alun perin syntynyt teknisten alojen tarpeesta yhtenäistää termistöä eli laatia standardeja. Terminologian tutkimus- ja työmenetelmiä voidaan kuitenkin hyödyntää minkä tahansa erikoisalan käsitteistöön tutustumisessa (Nuopponen 1999, 91). Nuopponen tiivistää terminologian teorian koostuvan termistöjen ja käsitteistöjen tarkastelusta ja muodostamisessa tarvittavista perusteista. Alan perustutkimukseen kuuluu muun muassa käsitteen ja termin muodostus, käsitteiden määritteleminen, käsitejärjestelmien muodostaminen ja kuvaaminen. (Nuopponen 1999, 91.)

Terminologiaa voidaan hyödyntää myös erikoisalan tekstien laatimisessa tai erikoisalan käsitteistön kartoittamisessa Käsitejärjestelmien analysointi ja jäsentely auttaa uuden erikoisalan käsitteistön ymmärtämisessä. (Nuopponen 1999,93.) Terminologia on monitieteinen ala, jonka tarkoituksena on tiedon järjestäminen ja välittäminen. Sen keskeinen elementti on *käsite*. Kaiken sanastoyön tulee perustua käsitteiden analysointiin ja käsitteiden välisten suhteiden selvittämiseen. (Suonuuti 2006, 11.) Terminologian lähtökohtana ovat siis *käsitteet* ja niiden väliset suhteet (TSK 36, 6).

Terminologisen tutkimuksen lähtökohtana on erottaa toisistaan käsitteet *termi*, *käsite* ja *tarkoite* (Nuopponen 1999, 91). Tähän on koottu terminologisen sanastotyön kannalta keskeiset käsitteet ja niiden määritelmät kahdesta eri lähteestä: *Terminologisesta sanastosta* (TSK 36), joka on laadittu terminologian asiantuntijoille (TSK 36, 2), ja *Sanastotyön oppaasta* (Suonuuti 2006), joka on tarkoitettu laajemmalle kohderyhmälle. Määritelmät ovat hieman erilaisia, mikä on esimerkki

siitä, miten määritelmien laatimisessa voidaan huomioida eri kohderyhmät (Isotalo 2004.)

Tarkoite on todellisuuden ilmiö (Suonuuti 2006, 11). *Terminologian sanaston* (TSK 36) mukaan *tarkoite* on: ”olio, joka voidaan osoittaa, käsittää tai kuvitella ja joka vastaa tiettyä käsitettä”. *Tarkoite* voi olla konkreettinen, abstrakti tai keksitty. (TSK 36, 10.)

Käsite on ajattelun tuote, abstrakti mielikuva jostain konkreettisesti tai abstraktista asiasta (Suonuuti 2006,11). *Käsite* on tiedon yksikkö, joka muodostuu käsitepiirteiden ainutkertaisesta yhdistelmästä (TSK 36, 10).*Termi* on erikoisalalla käytettävä nimitys (TSK 36, 22). *Termit* viittaavat tiettyihin käsitteisiin ja yleensä ne viittaavat nimenomaan erikoisalan käsitteisiin. Erikoisala vaatii erikoisosaamista, samoin kuin erikoisalan termistön hallinta. (TSK 36, 30.) *Termi* on käsitteeseen viittaava nimitys ja vakiintunut ilmaisu (Suonuuti 2006,11).

Käsitepiirteitä käytetään käsitteiden kuvaamisessa. *Käsitepiirre* on *tarkoitteen* tai tarkoitejoukon ominaisuuden abstraktio. Käsitteen kuvauksessa käytetään sille tunnusomaisia piirteitä eli *olennaisia käsitepiirteitä*. Se mikä katsotaan olennaiseksi tai epäolennaiseksi riippuu siitä mille kohderyhmälle käsitejärjestelmää laaditaan. Jotta käsite voidaan erottaa toisista, niin kuvauksessa käytetään *erottavia käsitepiirteitä.* Esimerkiksi vieruskäsitteiden *nojatuoli* ja *jakkara* välillä *erottava käsitepiirre* on selkänoja. (TSK 36, 11.)

Suonuuti konkretisoi *käsitepiirteen* antamalla esimerkin kuinka katsoessamme tarkoitetta, ajattelussamme syntyy tiettyjä sitä kuvaavia ominaisuuksia (Suonuuti 2006, 11). Käsitteen käsitepiirteiden muodostamaa joukkoa kutsutaan *käsitteen sisällöksi*. *Käsitteen sisältö* (intensio) yksilöi *käsitteen alan* eli sen mikä on käsitteen kattaman tarkoitteiden joukko. (TSK 36, 10.) Suonuutin mukaan *käsitteen sisältö* on käsitteen kaikkien käsitepiirteiden joukko (Suonuuti 2006, 11). *Käsitteen ala* (ekstensio) on tiettyä käsitettä vastaavien tarkoitteiden muodostama joukko (TSK 36, 10) tai sen kattamien tarkoitteiden joukko (Suonuuti 2006, 13).

Määritelmä on käsitteen sanallinen kuvaus (Suonuuti 2006, 11). *Terminologian sanaston* (TSK 36) mukaan *määritelmä* on käsitteen kuvaus, jonka tulee erottaa

käsite sen lähikäsitteistä (TSK 36, 19). *Sisältömääritelmä* kuvaa käsitteen yksilöimällä sen hierarkkisen yläkäsitteen ja erottavat piirteet (TSK 36, 19).

Määritelmää laativalla on mahdollisuus erottavien käsitepiirteiden avulla valita mitä käsitesuhteita haluaa tuoda esiin määritelmässä. Toisin sanoen määritelmän voi kohdentaa tietyn kohderyhmän tarpeisiin. Käsitteen määrittelemiseen voidaan käyttää sekä *käsitteen sisältöä* (intensio) että *alaa* (ekstensio) (Suonuuti 2006, 13).

Käsitteiden välille muodostuu erityyppisiä suhteita. Tavallisesti käsitesuhteet jaetaan kolmeen suhdetyyppiin: *hierarkiasuhde, koostumussuhde* ja *funktiosuhde*. (TSK 36, 16–17.) *Hierarkkinen suhde* syntyy esimerkiksi kahden käsitteen välille kun toisella käsitteistä (*alakäsite*) on yhteisten piirteiden lisäksi vähintään yksi erottava piirre. *Yläkäsitteen* ala on suurempi kuin alakäsitteen eli yläkäsite jakautuu alakäsitteisiin. Graafisesti hierarkkista suhdetta kuvataan puudiagrammeina. (Suonuuti 2006, 13.)

Sanastotyön opas sekä Suonuuti käyttävät nimitystä hierarkkinen suhde, joka on käsiteanalyysissa osoittautunut ongelmalliseksi. Päivi Pasanen suosittelee käyttämään nimitystä *geneerinen suhde*, jolla voidaan tehdä ero koostumussuhteesta, joka on myös hierarkkinen (Pasanen 2009, 142).

Koostumussuhteita on erilaisia, mutta yhteistä niille on se, että tietty kokonaisuus muodostuu osista eli yläkäsite muodostuu alakäsitteistä. Koostumussuhdetta kuvataan graafisesti kampadiagrammilla. (Suonuuti 2006, 16.)

Funktiosuhde on epähierarkkinen suhdetyyppi, joka kuvaa käsitteiden assosiatiivisia suhteita. Suhde voi olla esimerkiksi syy-seuraus-suhde tai vaikkapa esine-toiminta-suhde. Funktionaalisia käsitesuhteita kuvataan nuolidiagrammilla. (Suonuuti 2006, 17.) Hyvin usein käsitteiden välillä on samanaikaisesti useamman tyyppisiä käsitesuhteita, joita voidaan kuvata moniulotteisesti luokittelemalla käsite eri perusteiden mukaan (Suonuuti 2006, 18). Käsitteistä ja niiden välisistä suhteista muodostuu *käsitejärjestelmä*, jota voidaan kuvata graafisesti *käsitekaaviossa* (TSK 36, 16).

Käsiteanalyysia tarvitaan käsitteiden välisten suhteiden selvittämiseksi. *Käsiteanalyysi* on: ”sanastotyön osa, jonka avulla selvitetään ja kuvaillaan erikoisalan käsitteiden sisältöjä ja käsitteiden välisiä suhteita” (TSK 36, 31).

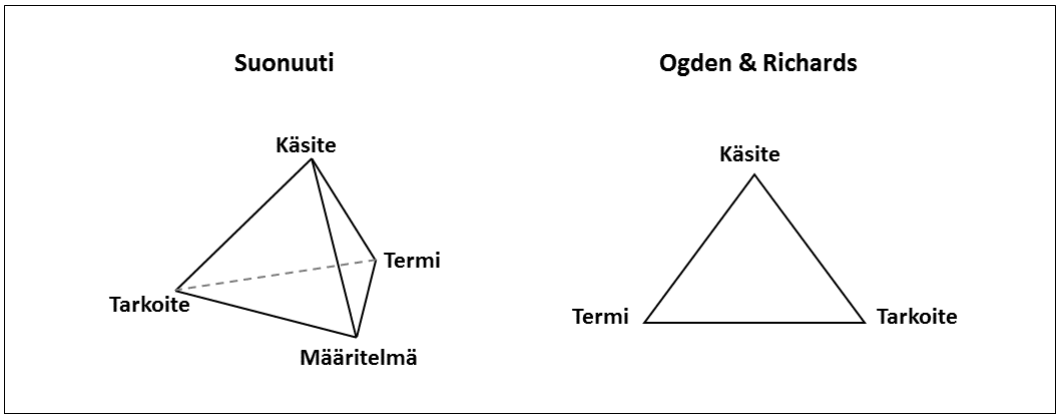
Käsiteanalyysi rakentuu terminologisen teorian pohjalle ja sen avulla selvitetään käsitteen sisältö, sen suhteet toisiin käsitteisiin sekä sen paikka käsitejärjestelmässä. Käsiteanalyysia tarvitaan, jotta voidaan määritellä käsite, verrata toiseen käsitteen sisältöön ja sen avulla voidaan myös selvittää vieraskielisten käsitteiden vastaavuudet. (Nuopponen 2003, 1.)

Terminologista käsiteanalyysia hyödynnetään systemaattisessa sanastotyössä, jonka tulosten perusteella voidaan laatia sekä kielellinen kuvaus (*määritelmä*) että graafinen kuvaus (*käsitekaavio*) käsitteistä ja niiden välisistä suhteista. Samaan käsitejärjestelmään kootaan käsitteet, jotka ovat olennaisia toistensa määrittelyn kannalta. Käsitteet pyritään määrittelemään yleispäteviksi eikä niitä yleensä rajata mihinkään tiettyyn käyttökontekstiin. (Kalliokuusi & Seppälä 2014.)

Terminologinen määritelmä pyritään laatimaan siten, että se sisältää vain välttämättömät, mutta riittävät käsitepiirteet käsitteen erottamiseksi lähikäsitteistä. Määritelmän laatimisessa tavoite on tehdä määritelmistä selkeitä ja sellaisia, että ne sisältävät aina lähimmän yläkäsitteen nimityksen. (Vehmas-Lehto 2007, 341.)

Loogisessa määritelmässä nimetään yläkäsite. Noudattamalla loogisuuden periaatetta käsitteet voivat toimia määritelmissä ja kaavioissa yläkäsitteenä. (Vehmas-Lehto 2007, 341.) Termi tulee voida korvata tekstissä määritelmällä. Näin voidaan kokeilla syntyykö järkeviä lauseita ja onko määritelmä korvausperiaatteen mukainen. (Vehmas-Lehto 2007, 343.)

Käsiteanalyysia voidaan tarkastella eri näkökulmista. Kielitieteessä C.K. Ogdenin ja I.A. Richardsin (1923) esittämää klassista semanttista kolmiota käytetään havainnollistamassa *symbolin*, *käsitteen* ja *tarkoitteen* välistä suhdetta (TTP 2015). Suonuuti (2006) on lisännyt kolmioon *määritelmän* (käsitteen kielellinen kuvaus) ja kuvannut tetraedilla *tarkoitteen*, *käsitteen*, *määritelmän* ja *termin* välistä suhdetta. (Suonuuti 2006, 12) Kuvassa 1 on kuvattu sekä perinteinen *semanttinen kolmio* että *Suonuutin tetraedi*.



Kuva 1: *Terminologian peruskäsitteet Suonuutin (2006) ja Ogdenin & Richardsin (TTP 2015.) mukaan.*

Nuopponen on käyttänyt semanttista kolmiota tarkastellessaan käsiteanalyysia eri näkökulmista (Nuopponen 2003, 3). Käsitekolmion *tarkoitetaso* vastaa todellisuuden tasoa, joka on useimmiten erikoisalojen asiantuntijoiden lähtökohta. He tutkivat ja tarkastelevat omaa erikoisalaansa ja etsivät ratkaisuja tutkimuskohteeseensa. He tarvitsevat käsitteitä kuvaamaan havaintojaan eli tarve syntyy tarpeesta kuvata todellisuutta. (Nuopponen 2003, 5.)

Käsitekolmion *käsitteiden tasoa* tarkastellaan kun aletaan perehtyä valmiiseen käsitemaailmaan tutkimalla tietyn alan käsitteistöä. Tällä tasolla lähtökohtana on perehtyä alan käsitteistöön ja sen edustaman käsitteistön todellisuuteen. (Nuopponen 2003, 5.)

Kolmantena on *ilmaisun taso* (termit ja tekstit), jonka lähtökohtana on selvittää lähtötekstiä, selvittää vaikeita sanoja ja termejä sekä etsiä sanoille vastineita. Tässä näkökulmassa tekstiä voidaan tarkastella esimerkiksi etsimällä millaisia piilomerkityksiä rivien taakse piiloutuu eli mitä sivumerkityksiä tekstiin on koodattu. Ilmaisun tasolla voidaan myös kartoittaa jonkin alan termistöä pohjaksi terminologiselle projektille. (Nuopponen 2003, 5.)

Nuopposen mukaan voidaan erottaa erilaisia asiantuntijatyyppejä sen perusteella mistä käsiteanalyysin semanttisen kolmion näkökulmasta tai miltä tasolta he lähestyvät käsiteanalyysia (*tarkoitteen, käsitteen* vai *ilmaisun taso*). *Kieliasiantuntija* voi olla esimerkiksi kielenhuoltaja, kääntäjä, kielten opettaja, kielentutkija, joka lähestyy käsiteanalyysia useimmiten tekstien eli ilmaisun tasolta. Sen sijaan

erikoisalan asiantuntijan (*substanssiasiantuntija*) lähtökohtana on usein tarkoite- tai käsitetaso. (Nuopponen 2003, 5–6.)

Kokeneilla asiantuntijoilla on kehittynyt omasta erikoisalastaan monipuolinen ja jäsentynyt käsitejärjestelmä. Asiantuntijoiden tietorakenteet ovat järjestäytyneet monitasoisiin hierarkioihin ja he pystyvät soveltamaan sitä nopeasti havainnoimalla ja valikoimalla olennaiset seikat laajoistakin kokonaisuuksista. (Nuopponen 2003, 6.)

Nuopponen sijoittaa terminologit kahden edellä mainitun asiantuntijatyypin väliin. Terminologit eivät usein ole pelkästään kieliasiantuntijoita, mutta terminologisen työn asiantuntijoina pystyvät selviytymään minkä tahansa erikoisalan käsitteistön kartoittamisesta. Terminologi ei kuitenkaan ole substanssiasiantuntijan asemassa, joten hän ei pääse vaikuttamaan erikoisalan tarkoitetasoon, vaikka voikin vaikuttaa käsitteistön yhtenäistämiseen ja terminmuodostamiseen. Yhdistelmäasiantuntija on saavuttanut asiantuntijuuden sekä terminologiassa että erikoisalalla. (Nuopponen 2003, 7.)

Termillä viitataan siis erikoisalan käsitteeseen. Usein termi on helppo tunnistaa, varsinkin kun sen yleiskielinen merkitys tuottaisi lauseessa kollokoinnin kannalta (toisten sanojen kanssa) oudon merkityksen. Osa termeistä on läpinäkyviä, eli ne kertovat jotain käsitteestä heijastamalla sen olennaispiirteitä. Kaikkien termien muodosta ei kuitenkaan voi päätellä niiden merkitystä. Termin muoto voi antaa väärän kuvan käsitteestä, eli termin sisäinen muoto ei heijasta käsitteen olennaispiirteitä. (Vehmas-Lehto 2010, 363.)

Erikoisalojen sanastotyössä hyvälle termille on asetettu muutamia ehtoja, jotka harvoin toteutuvat yhdellä kertaa. Uusia termejä muodostettaessa nämä ehdot on hyvä pitää mielessä. Termin tulee olla läpikuultava, jolloin se antaa oikean mielikuvan kuvattavasta käsitteestä. Koska termit liittyvät suurempaan kokonaisuuteen, niin termin tulisi olla johdonmukaisesti muodostettu ja sopia muiden aiheeseen liittyvien termien kanssa luontevasti yhteen. Termin tulisi olla lyhyt, tarkoituksenmukainen ja neutraali, mutta samalla erottua muista termeistä. Kun termi on omakielinen niin se soveltuu johdoston muodostamiseen ja on helppokäyttöinen. (Seppälä 1999.)

Normatiivisen terminologian tavoite on, että kutakin termiä vastaa yksi käsite. Siitä huolimatta synonymia ja polysemia ovat yleisiä terminologisia ongelmia. (Vehmas-Lehto 2010, 363.) Terminologian sanakirjan mukaan *synonymia* on samaan käsitteeseen viittaavien nimitysten välinen suhde (TSK 36, 27). *Polysemia* puolestaan viittaa siihen, että yksi nimitys viittaa kahteen tai useampaan käsitteeseen, joilla on tiettyjä yhteisiä käsitepiirteitä (TSK 36, 28). Terminologisessa analyysissa selviää käsitteiden ja käsitejärjestelmien yhteneväisyys tai eroavaisuus. Tuloksen perusteella voidaan päätellä onko kyse synonymiasta tai polysemiasta. (Nissilä & Nuopponen 2013, 246.)

Nuopponen on erikoiskieltä tutkiessaan havainnut, miten esimerkiksi tutkijat saavat erilaisia vaikutteita, jotka heijastuvat tutkijan oman termistön muodostamiseen. Toisistaan tietämättä tutkija tai kääntäjä voi kääntää kansainvälisessä tutkimuksessa käytettävää termistöä, minkä tuloksena suomen kieleen syntyy synonymiaa. (Nissilä & Nuopponen 2013, 252.) Uusilla tieteenaloilla syntyy paljon synonyymejä, ennen kuin käytettävää käsitteistöä on aloitettu yhtenäistämään (Nissilä & Nuopponen 2013; Nuopponen 1999.).

Grinev-Grinevich katsoo, että termien monimerkityksellisyys ja epätarkkuus vaikeuttavat viestintää erikoisaloilla. Termit tulisi määritellä ja rajata selkeästi, jotta esimerkiksi polysemiaa ei syntyisi. Polysemiaa syntyy esimerkiksi kun samaa termiä käytetään eri tieteenaloilla hieman eri merkityksessä tai kun termin sisällön ala laajenee tai supistuu. (Grinev-Grinevich 2008, 96– 99.)

Terminologian sanaston (TSK 36) mukaan *täydestä vastaavuudesta* on kyse silloin, kun nimitykset viittaavat täsmälleen samaan käsitteeseen. *Osittainen vastaavuus* on kyseessä silloin kun käsitteet vastaavat toisiaan vain tietyiltä osin. Sanasto antaa esimerkin suomenkielisestä käsitteestä *täti*, jolle ruotsinkielinen *moster*-käsite on vain osittain vastine. (TSK 36, 27.)

Osittaisen vastaavuuden syy voi selittyä myös lähtö- ja kohdekulttuurin erilaisella käsityksellä todellisuudesta (Vehmas-Lehto 2010, 365). Vehmas-Lehto mainitsee esimerkin suomalaisen ja venäläisen oikeusjärjestelmän erilaisuudesta, jolloin käsitteillä on merkittäviä sisällöllisiä eroja, mutta oleellisissa suhteissa niitä voidaan

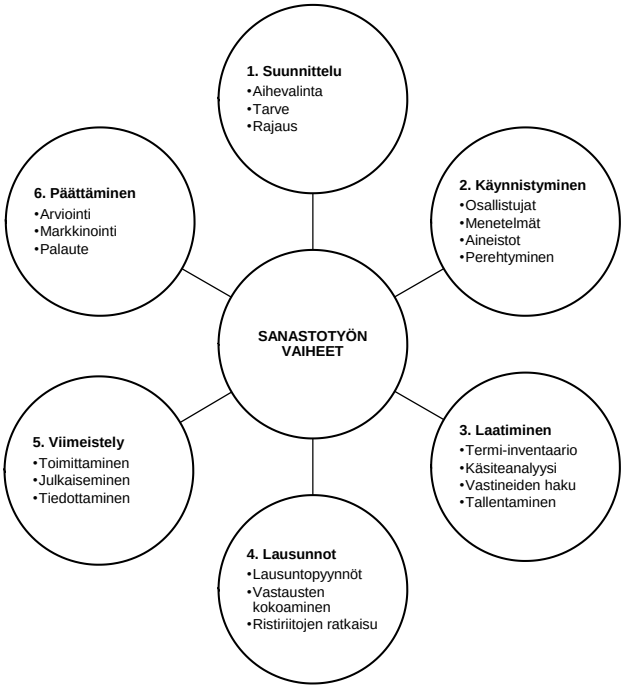
kuitenkin pitää vastineina (Vehmas-Lehto 2010). Voidaan siis olettaa suomalaisen ja venäläisen hallinnon ja hallintokulttuurien erojen heijastuvan myös käsitteistöön.

Vehmas-Lehto on myös käyttänyt semanttista tetraedia (ks. Kuva 1*: Terminologian peruskäsitteet)* tarkastellessaan erikoiskieliin liittyviä terminologisia ongelmia. Hän toteaa kääntäjien joutuvan liikkumaan kahden tason välillä: käsitetason ja terminologisen (kielellisen tason) välillä. Lähtötekstin termin ymmärtämiseksi on osattava mieltää sitä vastaava käsite. Vastinetyössä on käsitteelle löydettävä (tai luotava) nimitys toisella kielellä. Erikielisten termien muodossa ei välttämättä ole yhteistä. (Vehmas-Lehto 2010, 361–362.)

Sanastotyössä terminologi voi hyväksyä sen, ettei vastinetta joskus ole. Kääntäjä ei yleensä voi päätyä samaan ratkaisuun, vaan kääntäjän on ratkaistava jollakin tavalla vastineen puuttumisen esimerkiksi selittämällä tai antamalla termiehdotuksen. (Kosunen 2015.)

Terminologisessa sanastotyössä käsiteanalyysi on keskeinen osa sanastotyötä ja yksi työvaihe varsinaisen sanaston laadintavaiheen sisällä (Nuopponen 2009, 311). Sanastotyön oppaassa (Suonuuti 2006) on esitelty terminologisen sanastotyön periaatteet ja menetelmät. Ne perustuvat kansainvälisiin terminologiaa määritteleviin standardeihin (ISO/TC 37). Suonuuti luettelee seuraavia sanastotyön työvaiheita: sanastotyöryhmän kokoaminen, aiheen rajaus, aikataulutus, käsitteiden määrän rajaus, lähteiden ja käsitteiden valinta, käsitteiden määrittely, käsitejärjestelmien laatiminen ja sopivan termitietueen valinta ja tallennusohjelma (Suonuuti 2006, 34–36).

Nuopponen on hyödyntänyt *satelliittimallia* sanastotyön alkuvaiheessa tehdessään termi-inventaariota. Satelliittimalli helpottaa hahmottamaan käsitejärjestelmien muodostamia kokonaisuuksia. Vaikka malli ei kuvaa käsitteiden välisiä suhteita, niin se on hyvä apuväline käsitteiden jäsentämisessä. Kuvassa 2 on esitetty sanastotyön vaiheet yksinkertaistetun satelliittimallin avulla. (Nuopponen 2004.)



Kuva 2: Sanastotyön vaiheet (Nuopponen 2004)

Sanastotyön tulokset esitetään tiivistetysti *termitietueessa*. Sanastotyön oppaassa on esitelty perinteinen termitietuemalli. Kukin termitietue sisältää yhden käsitteen tiedot: termitietueen numero, suositettava termi, käsitettä vastaavat erikieliset termivastineet, käsitteen määritelmä ja huomautuksia. (Suonuuti 2006, 39.)

Esimerkki termitietueesta:

1 termitietueen numero

2 suomenkielinen termi
3 mahdolliset synonyymit
4 venäjänkielinen vastine
5 englanninkielinen termi
6 määritelmä suomeksi
7 määritelmää täydentävä selite

8 huomautukset alkavat isolla kirjaimella, niiden lopussa on piste, erotettu määritelmistä sisennyksellä.

huomautus täydentää tietoa käsitteestä tai sen venäjänkielisestä vastineesta, esim. viittaus lakiin

Esimerkin termitietueen kentät ovat (1) termitietueen numero; (2) suomenkielinen termi; (3) mahdolliset synonyymit; (4) venäjänkielinen vastine; (5) englanninkielinen termi; (6) määritelmä suomeksi; (7) määritelmää täydentävä selite ja huomautukset (8).

Kansainvälisten määritelmänkirjoitusperiaatteiden mukaisesti määritelmät alkavat pienellä kirjaimella eikä niiden lopussa ole pistettä. Termitietueessa osittaista vastaavuutta merkitään symbolilla ~. Erikieliset termit merkitään seuraavasti: suomenkielinen fi; englanninkielinen en ja venäjänkielinen ru. Lopulliseen termitietueeseen kootaan ja kirjataan pelkät käsitteet ja määritelmä. (Suonuuti 2006.)

Tässä tutkimuksessa tutkimusaihetta lähestytään perehtymällä käytössä oleviin käsitteisiin eli aiemmin luotuun käsitteistöön. Tutkimus ei normatiivisen sanastotyön tavoin pyri käsitteistön yhtenäistämiseen tai esimerkiksi määritelmien laatimiseen. Lähtökohtana on tarkastella Suomen kyberturvallisuusstrategian (Kyberstrategia 2013) käsitteitä määritelmineen, sen jälkeen tarkastella vastaavasti venäläisiä kyberturvallisuusalan asiakirjoja. Käsiteanalyysin avulla käsitepiirteitä vertailemalla voidaan etsiä suomenkielisille käsitteille venäjänkielisiä vastineita.

Tässä tutkimuksessa päädyttiin käyttämään tiivistettyä termitietuetta, joka on muokattu sekä laatijan että lukijan tarpeisiin. Termitietue on sijoitettu kunkin käsitteen käsiteanalyysin päätteeksi. Termitietueeseen tallennetaan suomenkielinen termi, mahdollinen termiehdotus, venäjänkielinen vastine, mahdollinen englanninkielinen vastine, määritelmä, mahdollinen määritelmäehdotus ja sitä täydentävät huomautukset. Tässä tutkimuksessa terLähteitä ei merkitä termitietueessa, sillä ne esitetään käsiteanalyysissa ennen termitietuetta. Esimerkki tässä tutkimuksessa käytettävästä tiivistetystä termitietueesta:

suomenkielinen termi
ru venäjänkielinen termi
en venäjänkielinen termi
määritelmä:
huomautus:

5 Käsiteanalyysi

Käsiteanalyysissä selvitetään käsitteen käsitepiirteet ja käsitesuhteet. Tässä tutkimuksessa käsiteanalyysiin valittiin lähtökäsitteiksi valikoima Suomen kyberturvallisuusstrategian (Kyberstrategia 2013) suomenkielisiä käsitteitä, joille asiakirja antaa valmiit määritelmät. Käsiteanalyysi aloitetaan tarkastelemalla määritelmissä olevia käsitepiirteitä. Käsite kerrallaan etsitään käsitteiden olennaiset ja erottavat käsitepiirteet. Koska määritelmässä ei luetella kaikkia käsitepiirteitä, lisätietoa on tarpeen etsiä eri asiakirjateksteistä. Käsiteanalyysin avulla hahmotellaan käsitteiden väliset suhteet ja käsitteet sijoitetaan käsitekaavioon, joka kuvaa graafisesti käsitteiden välisiä suhteita. (Suonuuti 2006, 13–17.)

Sitä mukaa kun käsitekokonaisuudet alkavat tarkentua, käsitekaaviota päivitetään ja muokataan. Erikoisalan asiantuntija tarkastelee käsitteitä erikoisalan näkökulmasta, joten käsitteet järjestyvät asiantuntijan mielessä eri tavalla kuin terminologin. Käsitekaavio auttaa erikoisalan asiantuntijaa hahmottamaan käsitteiden sijoittumisen toisiinsa. Terminologin laatima käsitekaavio voi erota erikoisalan asiantuntijoiden laatimasta käsitekaaviosta. Terminologi vastaa siitä, että asiantuntijoiden vahvistama tietosisältö esitetään oikein ja käsitekaavioiden merkintätavat perustuvat kansainvälisiin standardeihin kuten ISO 704 (Seppälä 2016).

Käsitekaavion graafista esittämistapaa voi soveltaa kohdealan asiantuntijalle soveltuvaksi, mikäli kuitenkin noudatetaan standardinmukaista esittämistapaa (Seppälä 2016). Käsitekaaviossa puukuvaimen oksan tai kampakuvaimen piikin voi jättää tyhjäksi. Tässä tutkimuksessa sovellettiin käsitekaavion merkintöjä siten, että käsitekaaviossa päädyttiin käyttämään *muu*-sanaa tyhjän merkinnän sijaan (Seppälä 2015). Tämä ratkaisu auttoi erikoisalan asiantuntijoita hahmottamaan kokonaisuuden ja hyväksymään tehdyn rajauksen. Käsitekaaviot on sijoitettu tämän tutkimuksen liitteisiin.

Monikielisen sanaston laadinnassa kokeneet terminologit neuvovat tekemään eri kielten käsiteanalyysit erikseen (Kosunen 2015). Tässä tutkimuksessa noudatetaan tätä työtapaa ja tehdään ensin käsitteiden analyysi suomen kielellä ja sen jälkeen venäjän kielellä. Käytännössä suomenkielinen analyysi painottuu enemmän ja vaatii myös enemmän aikaa. Suonuutin mukaan kun lähdekielinen osuus sanastotyöstä on

tehty, vastineiden hakuun käytettävä aika on huomattavasti lyhyempi, sillä sanastotyö perustuu lähdekielen käyttöön ja muille kielille haetaan vain termivastineet (Suonuuti 2013). Samaa periaatetta noudattaen tässä tutkimuksessa venäjänkielisiä vastineita haetaan lähtökielen näkökulmasta tarkasteltuna. Vastinetyössä on myös perehdyttävä myös muihin tietolähteisiin ja rinnakkaisteksteihin, jotta tarvittava tieto käsitteestä löytyy (Vehmas-Lehto, 2010).

Kunkin jakson päätteeksi käsiteanalyysin tulokset tiivistetään termitietueeseen. Koska käsiteanalyysin yhteydessä on annettu lähteet, niin termitietueessa niitä ei toisteta. Termitietue toimii tässä tutkimuksessa kunkin käsitteen tietojen kokoamista varten. Tarvittaessa se on helposti muutettavissa perinteiseen termitietuemalliin ja käytettäväksi, esimerkiksi sanaston laatimiseen.

5.1 *Tietoturvallisuus*-käsite

Kokonaisturvallisuuden sanastossa (TSK 47) käsitteet *tietoturva, tietoturvallisuus* esitetään rinnakkain, sillä ne ovat synonyymeja. Tässä käsitteiden määritelmä:

> tietoturva, tietoturvallisuus
> en information security; > data security (tietoaineistoturvallisuudesta)
> järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus
> huomautus: Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa.

Määritelmän yläkäsite on *järjestelyt*. Määritelmässä on kolme käsitepiirrettä: *tiedon saatavuus, eheys* ja *luottamuksellisuus*, joista tietotekniikan alalla käytetään yleisesti nimitystä CIA-malli (CIA-lyhenne muodostuu englannin kielen sanoista confidentiality, integrity ja availability). Venäjän kielessä on vakiintunut vastaavien venäjänkielisten käsitteiden käyttö: *конфиденциальность, целостность* ja *доступность*, lyhennettynä КЦД (ITU 2014, 74). Näiden kolmen venäjänkielisen käsitteen avulla määritellään Venäjällä tietoturvallisuuden käsitteet kansainvälisten standardien mukaisesti (RUSREG 2015; ISO/IEC 17799:2005). Myös GOST 17799 -standardissa ja muissa tietotekniikan alan julkaisuissa nämä kolme käsitettä (конфиденциальност, доступность, целостность) ovat vakiintuneita tietotekniikan peruskäsitteitä (GOST 17799:4).

Analysoimalla nämä kolme venäjänkielistä käsitettä selviää, voidaanko niitä pitää suomenkielisten *tiedon saatavuus, eheys* ja *luottamuksellisuus* käsitteiden vastineina. Ensimmäisenä *конфиденциальность информации* -käsitteen määritelmä:

> конфиденциальность информации
> обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (FZ 149:2:7).

Tässä määritelmässä yläkäsite on *обязательное требование* (ehdoton vaatimus). Venäjänkielisessä määritelmässä luottamuksellisuus on ehdoton vaatimus, jonka mukaan tietoa ei saa antaa kolmannelle osapuolelle ilman tiedon omistajan suostumusta (FZ 149:2:7). Suomenkielisen *tiedon luottamuksellisuus* -käsitteen määritelmän mukaan luottamuksellisuus toteutuu, mikäli tieto ei joudu sivulliselle. Vertailemalla venäjänkielisen *конфиденциальность информации* -käsitteen ja suomenkielisen *tiedon luottamuksellisuus*- käsitteen käsitepiirteitä, voidaan todeta käsitepiirteiden olevan riittävän samansisältöisiä, joten niitä voidaan pitää toistensa käsitevastineina.

Toisena venäjänkielisenä käsitteenä on *доступность; доступ к информации*. GOST-standardi rinnastaa käsitteet antaen niille yhteisen määritelmän: ”доступность; доступ к информации и связанным с ней активами авторизованных пользователей по мере необходимости” (GOST 17799:4**).** Federaatiolaissa (FZ 149) on käytetty *доступ*-käsitettä: ”доступ к информации - возможность получения информации и ее использования*”* (FZ:149: 2.6).

Venäjänkielisissä määritelmissä tiedon saatavuus on keskiössä kun taas suomenkielinen määritelmä tarkentaa tiedon olevan hyödynnettävissä haluttuna aikana. *Saatavuus* on *tietoturva*-käsitteen yhteydessä vakiintunut viittaamaan tiedon hyödynnettävyyteen (TSK 31, 11). Käsitepiirteissä on eroja, mutta kyseessä on vakiintuneet käsitteet tietotekniikan alalla. Näin ollen voidaan *доступ* ja *доступность* käsitteitä pitää suomenkielisen *saatavuus*-käsitteen vastineina. Tätä vahvistaa myös asiantuntijan lausunto, jonka mukaan käyttökontekstista riippuen saatavuudella voidaan tarkoittaa sekä tiedon ominaisuutta että tietojärjestelmän käyttäjän pääsyä saatavilla oleviin palveluihin ja palvelun toimivuuden edellyttämiin tietoihin (Tuukkanen 2015). (vrt. käsite *tietoverkko,* TEPA, TSK 37)

Kolmannen venäjänkielisen käsitteen, *целостность информации* -käsitteen määritelmä on: ”достоверность и полнота информации и методов ее обработки*”* (GOST 17799:4). Määritelmässä on käytetty käsitteitä *достоверность и полнота* (*luotettavuus ja täydellisyys*), jotka viittaavat samaan kuin suomenkielisen *eheys*-käsitteen määritelmä: ”tiedon yhtäpitävyys alkuperäisen kanssa*”* (TSK 47, 57). Tämän vertailun tuloksena voidaan päätellä, että *tiedon eheys* saa vastineen *целостность информации.*

Näiden kolmen analysoidun käsitepiirteen (конфиденциальность, доступность ja целостность) avulla etsitään venäjänkielistä vastinetta käsitteelle *tietoturvallisuus.* GOSTR 50.1.053 -standardissa venäjänkielinen *безопасность информации [данных]* määritellään samoilla kolmella käsitepiirteellä:

> **безопасность информации [данных]**
> состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность (GOSTR 50.1.053 :3.1.4).

Tässä määritelmässä yläkäsite on *состояние* (tila). Suomenkielisen *tietoturvallisuus*-käsitteen yläkäsite on *järjestelyt* (TSK 47, 57). Molempien käsitteiden määritelmissä on käytetty kolmea käsitepiirrettä, joiden (järjestelyt) avulla saavutetaan haluttu tiedon tila (tavoitetila). Käsitteiden määritelmiä ja käsitepiirteitä vertailemalla, voidaan päätellä, että *tietoturvallisuus* on käsitteen *безопасность информации [данных]* vastine.

Vastinehaun yhteydessä havaittiin, että GOSTR 50.1.053 -standardi on osittain kaksikielinen (venäjä–englanti). Siinä on venäjänkielisille käsitteille annettu myös englanninkielinen vastine. Standardissa on annettu kaksi määritelmää *безопасность информации* -käsitteelle. Näistä ensimmäinen on edellä käsitelty *безопасность информации (данных),* jossa б*езопасность информации* -käsitteen perään on lisätty tarkennukseksi suluissa *данные,* suomeksi *data. Безопасность информации (данных)* -käsite saa englanninkielisen vastineen *information (data) security* (GOSTR 50.1.053: 3.1.4).

Venäjänkielisissä asiakirjoissa käytetään yleisesti *informaatio*-sanan jälkeen lisätarkennuksena suluissa *data,* kun tarkoitetaan *konekielistä tietoa* eli *dataa*. Samanlainen *data*-sanan lisäys suluissa löytyy myös Suomen kyberturvallisuus-strategian englanninkielisestä versiosta, jossa *tietoturvallisuus*-käsite on käännetty

englanniksi: *information (data) security* (Cyber strategy 2013, 13). Vaikka sanastotyössä ei yleensä kelpuuteta käännöksiä lähteiksi, niin tätä havaintoa ei kuitenkaan voida kokonaan sivuuttaa. Ei liene aivan sattumaa, että venäjän- ja englanninkielisissä lähteissä käytetään samanlaista suluissa olevaa *data*-tarkennusta.

Informaatio-sana on monimerkityksinen, minkä takia tarkentava lisäys on katsottu tarpeelliseksi. Valtion hallinnon tietoturvasanastossa (Vahti 8/2008) on *tietoturvallisuudelle* annettu englanninkielinen vastine *information security* (Vahti 8/2008, 162). Kokonaisturvallisuuden sanasto (TSK 47) antaa *tietoturvallisuus*-käsitteelle englanninkielisen vastineen seuraavasti: ” tietoturvallisuus - *information security; > data security (tietoaineistoturvallisuudesta)”* (TSK 47, 15). Tämän mukaan *tietoaineistoturvallisuus* (*data security*) on suppeampi käsite kuin *tietoturvallisuus (information security).*

GOSTR 50.1.053 -standardin toinen *безопасность информации* -käsite on saanut suluissa lisäyksen *при применении информационных технологий*. Sen määritelmä on:

> безопасность информации (при применении информационных технологий)
> состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована (GOSTR 50.1.053:3.1.5).

Tässä määritelmässä lisäys suluissa viittaa tietotekniikan käyttöön ja saa sen perusteella englanninkielisen vastineen IT-*security* (GOSTR 50.1.053: 3.1.5). *IT-security*-käsite on Vahti-sanastossa suomenkielisten *tietotekniikan turvallisuus* ja *tietoturvallisuus* käsitteiden vastine (VAHTI 8/2008, 164).

Suomen kielessä ei ole tarpeen lisätä data-sanaa kuten englannin ja venäjän kielissä. Suomenkielisen *tietoturvallisuus*-käsitteen sisältö kattaa molempien venäjänkielisten käsitteiden (*безопасность информации [данных]* ja *безопасность информации (при применении информационных технологий*) käsitepiirteet. Yhteenvetona todetaan, että määritelmistä löydettyjen käsitepiirteiden avulla voidaan päätellä, että suomen kielen *tietoturvallisuus* saa vastineet venäjän kielellä *безопасность информации (данных)* ja englannin kielellä *information security.*

tietoturva, tietoturvallisuus
ru безопасность информации [данных]
безопасность информации (при применении информационных технологий)
en information (data) security
määritelmä: järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus
huomautus 1: Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa.

5.1.1 *Haavoittuvuus*-käsite

Käsitteellä *haavoittuvuus* on keskeinen merkitys *tietoturvallisuus*-käsitteen määrittelyssä. Tietotekniikan alalla *haavoittuvuus* on vakiintunut peruskäsite. Tiivis tietoturvasanasto määrittelee *haavoittuvuuden* lyhyesti: ”alttius tietoturvauhkille” (TSK 31, 14). *Haavoittuvuus*-käsitteen määritelmässä vahingon aiheuttajaa tai tekijää ei yksilöidä, eikä myöskään tarkenneta minkä haavoittuvuudesta on kyse. Asiantuntijan mukaan haavoittuvuus voi kohdistua tietojärjestelmään, tietoliikenneverkkoon, tietojenkäsittelypalveluun tai niiden osiin (Tuukkanen 2015). Yleinen näkökulma tietotekniikan alalla on, että esimerkiksi ohjelmistoon kohdistuva häiriö voi syntyä tahallisen tai tahattoman tapahtuman seurauksena (TSK 31, 14). Tietoturvasanasto antaa lisäksi huomautuksen:
”haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa” (TSK 31, 14).
Haavoittuvuus-käsitteen synonyymina käytetään yleisesti *tietoturva-aukko*-käsitettä (TSK 31, 14). *Tietoturva-aukko* kuvaa havainnollisemmin sitä, miten ohjelmassa, ohjelmistoissa, tietojärjestelmissä tai lähdekoodissa voi olla sellaisia puutteita (tietoturva-aukkoja), joiden kautta jokin tekijä pääsee tietojärjestelmään vaikuttamaan ja muuttamaan alkutilannetta. *Heikkous*-käsitteellä viitataan sellaiseen ohjelmiston ominaisuuteen, joka mahdollistaa vahingon syntymisen (TSK 31, 14).

Haavoittuvuus-sana on esimerkki siitä, miten yleiskielen sana on eriytynyt erikoiskieleen ja siitä on tullut tietotekniikan alalla käytettävä termi. Asiantuntija ymmärtää käsitteen sisällön ja sen taustalla olevan erikoiskielisen merkityksen, eikä yhdistä käsitettä sen yleiskieliseen merkitykseen tai toisen tieteenalan käsitteeseen. (Suomalainen 2002; Vehmas-Lehto 2010)

Bilateraalisessa sanastossa on *kyber*-etuliitteen kanssa muodostettu käsite *киберуязвимость*, jolle on annettu englanninkielinen vastine *cyber vulnerability* (Bilat 2014, 57). Muista venäjänkielisistä lähteistä ei löytynyt tätä käsitettä. *Vulnerability* on vastine suomenkieliselle *haavoittuvuus*-käsitteelle (TSK 31, 14). Suomalaisen asiantuntijan mukaan *haavoittuvuus*-käsitettä käytetään yleisesti, mutta suomen kielellä ei käytetä muotoa *kyberhaavoittuvuus* (Tuukkanen 2015).

Kyseessä ovat vakiintunut käsite tietotekniikan alalla, joten venäjänkielinen vastine löytyy GOSTR 50.1.053-standardista:

> уязвимость (информационной системы)
> свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.
> (GOSTR 50.1.053: 2.6.4)

Määritelmän yläkäsite on *свойство*(ominaisuus) eli kyseessä on tietojärjestelmän ominaisuus. Myös suomenkielisessä määritelmässä viitattiin tietojärjestelmän tai ohjelmiston *ominaisuuteen,* joka mahdollistaa vahingon syntymisen (TSK 31, 14).

Myös venäjänkielisen *уязвимость*-käsitteen yleiskielinen merkitys viittaa haavoittumiseen ja heikkouteen. Käsitteelle on annettu huomautus, jonka mukaan kyseessä voi olla tietojärjestelmän puute tai heikko kohta (недостаток или слабое место в информационной системе) (GOSTR 50.1.053: 2.6.4). Näin ollen voidaan todeta, että *уязвимость*-käsitteen piirteet vastaavat suomenkielisen *haavoittuvuus*-käsitteen käsitepiirteitä (TSK 31, 14) ja käsitteitä voidaan pitää vastineina.

> **haavoittuvuus**
> ru уязвимость
> en vulnerability
> määritelmä: alttius tietoturvauhkille
> huomautus 1: haavoittuvuus-käsitteen synonyymina käytetään yleisesti tietoturva-aukko-käsitettä.
> huomautus 2: haavoittuvuus on tietoturva-aukko, jonka heikkous mahdollistaa vahingon syntymisen

5.2 *Kyberturvallisuus*-käsite

Tässä tutkimuksessa ei käsitellä *kyber*-sanan etymologiaa. Suomenkyberturvallisuus-strategia (Kyberstrategia 2013) toteaa, että *kybe*r-sana yksinään ei saa sisältöä, vaan ainoastaan yhdyssanassa sen määriteosana (Kyberstrategia 2013, 12). *Kyber*-sanan merkityssisällöstä todetaan seuraavaa:

> Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation (tietojen) käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tieto- ja tietokonejärjestelmiin (Kyberstrategia 2013, 12).

Edellä olevassa tekstiotteessa on suomenkielisen *informaatio*-sanan jälkeen lisätty *tieto*-sana: ”informaation (tietojen) käsittelyyn” (Kyberstrategia 2013, 12). Suomenkielessä *tietojenkäsittely*-käsitettä käytetään yleensä ilman lisätarkennuksia (TEPA 2010).

Suomen kyberturvallisuusstrategia (2013) määrittelee *kyberturvallisuuden* näin:

> Tavoitetila, jossa sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettuun toimintaympäristöön voidaan luottaa ja sen toiminta turvataan (Kyberstrategia 2013, 13).

Määritelmän yläkäsite on *tavoitetila*. Määritelmän mukaan kyseessä on kybertoimintaympäristön tavoitetila, jossa ”toimintaympäristöön voidaan luottaa ja sen toiminta turvataan” (Kyberstrategia 2013, 13). *Tavoitetila*-käsitettä käytetään valtionhallinnossa tietoturvallisuuden arvioinnissa (VAHTI 2/2014). (ks. 5.6. kybertoimintaympäristö) Käsitteet *tavoitetila* ja *turvallisuus* ovat moniselitteisiä, joiden selvittäminen vaatisi jatkotutkimuksia.

Venäjän kansallinen kyberturvallisuusstrategian luonnos (SF 2014a) julkaistiin kommentoitavaksi tammikuussa 2014. Sen sisällöstä ei ole päästy kaikilta osin sopuun, sillä se on edelleen luonnosasteella. Viranomaisten sivuilta ei löydy aiheesta muuta tietoa kuin, että asia on edelleen käsittelyssä (SF 2014b). Tästä seuraa, että luonnosta voidaan pitää luotettavana lähteenä, mutta on huomioitava, ettei se ole lopullinen versio. Venäjän kyberstrategian luonnoksessa (SF 2014a) *кибербезопасность*-käsitteen määritelmä on:

> **кибербезопасность**
> совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями (SF 2014a, 2).

Tässä määritelmässä yläkäsite on *совокупность условий* (ehtojen joukko, tietyistä ehdoista muodostuva kokonaisuus). Määritelmän mukaan *кибербезопасность*-käsitteellä tarkoitetaan tiettyjen ehtojen toteutumista, joiden avulla kybertoimintaympäristö suojataan uhkilta ja epätoivotuilta vaikutuksilta (SF

2014a,2). Määritelmää voidaan perusajatukseltaan pitää samansisältöisenä kuin suomenkielisen *kyberturvallisuus*-käsitteen (Kyberstrategia 2013, 13). Kumpikaan määritelmistä ei anna *kyberturvallisuus*-käsitteen tarkkaa kuvausta, vaan molemmat jättävät varaa tulkinnalle

Määritelmien laatu vaikuttaa sekä sanaston laatuun että käsitekaavion laatimiseen Määritelmien tulisi tuoda esiin käsitteen olennaiset piirteet ja erot sitä lähellä oleviin käsitteisiin. Varsinkin uudella alalla on yleistä, että tutkimuskohteena olevan alan käsitteistöt eivät ole selvästi määriteltyjä eivätkä käsitteiden rajat tarkkoja. (Nuopponen 1999.) Terminologisessa käsiteanalyysissa joudutaan pohtimaan myös määritelmän laatijan tarkoitusperiä ja vertailemaan erilaisia määritelmiä toisiinsa (Nuopponen 2009, 313).

Venäjän Kyberstrategian luonnoksessa (SF 2014a) todetaan, että käsitettä *киберпространство* tulisi tarkastella selkeärajaisena informaatioavaruuden osana: ”киберпространство должно рассматриваться как определенный, имеющий четкие границы элемент информационного пространства” (SF 2014a, 2). Kuvassa 3 on kuvattu venäläinen näkemys *кибербезопасность* ja *информационная безопасность* -käsitteiden suhteesta. Luonnoksen mukaan sen edustama näkökulma on kansainvälisten standardien mukainen, mutta länsimaisen käsityksen mukaan käsitteet kuten *kybertoimintaympäristö* ja *kyberturvallisuus* eivät ole tarkkarajaisia. *Tallinnan manuaali* (Schmitt 2013) herätti keskustelua kybertoimintaympäristöstä ja nosti esille erilaisten käsitysten ja näkökulmien kirjon. Johdannossa todetaan, että käsitteiden sisältö vaihtelee eri valtioissa (Schmitt 2013). Suomen kybersuurlähettiläs, Marja Rislakki vahvistaa kyberturvallisuuden jakavan mielipiteitä:

> Jotkut maat korostavat internetin verkkojen vapautta. Toiset taas painottavat valtioiden suvereniteettia ja ehkä turvallisuuden vuoksi haluaisivat rajoittaa pääsyä internetiin. Tätä keskustelua käydään nyt eri foorumeilla (Tietosuoja 2/2015).

Venäjän Kyberstrategian luonnoksessa (SF 2014a) todetaan myös, ettei Venäjällä tehdä eroa käsitteiden *кибербезопасность* ja *информационная безопасность* välillä. Venäläisissä asiakirjoissa ei juurikaan esiinny *кибер*-sanaa, vaan sen sijaan yleisimmin on käytössä *информационная безопасность.* Luonnoksen mukaan

кибербезопасность-käsite on päädytty määrittelemään käytettäväksi kansainvälisessä yhteistyössä. (SF 2014a.)

Asiakirja tarkentaa, että *кибербезопасность*-käsite on suppeampi merkitykseltään kuin *информационная безопасность* -käsite: ”Кибербезопасность - более узкое по смыслу понятие, чем информационная безопасность” (SF 2014a, 2). Kuvassa 3 on havainnollistettu venäläistä näkemystä käsitteiden *кибербезопасность* ja *информационная безопасность* välisestä suhteesta:

Kuva 3: Venäläinen näkemys *кибербезопасность* ja *информационная безопасность* -käsitteiden suhteesta

Venäjällä Kyberstrategian luonnos (SF 2014a) on herättänyt laajaa keskustelua internetsivustoilla sekä myös asiantuntijoiden keskuudessa. Maksim Kornev, joka on tutkinut muuan muassa internetissä, sosiaalisessa mediassa ja joukkoviestimissä käytettäviä vaikutuskeinoja (TRIT 2015.), toteaa venäjänkielisten *информационная безопасность* ja *кибербезопасность* -käsitteiden olevan vaikeasti sovitettavissa länsimaiseen ajatteluun. Ajatus internetin rajattomuudesta ei istu Venäjän käsitykseen kansallisesta itsemääräämisoikeudesta. (Kornev 2015.; PLM 2012, 15–16.) Bilateraalisen sanaston mukaan *кибербезопасность*-käsite on:

> **кибербезопасность**
> свойство киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз (Bilat 2014, 33).

> cybersecurity
> is a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover (Bilat 2014, 33).

Tässä määritelmässä yläkäsite on *свойство киберпространства (киберсистемы)* (kybertoimintaympäristön ominaisuus). Määritelmässä on suluissa *киберсистема*-sana, jota käytetään joskus *киберпространства*-käsitteen synonyymina. Bilateraalisen sanaston määritelmä on sisällöltään hyvin samanlainen kuin suomenkielisen *kyberturvallisuus*-käsitteen määritelmä. Tämä samankaltaisuus on odotettavissa, sillä Bilateraalisessa sanastossa on pyritty huomioimaan molemmat näkökulmat, amerikkalainen ja venäläinen. Asiantuntija vahvistaa, että Bilateraalisen sanaston *cyber security* (Bilat 2011en, 31) ja suomalainen *kyberturvallisuus*-käsite (Kyberstrategia 2013, 13) ovat lähellä toisiaan (Tuukkanen 2015). Tämän voi todeta vertaamalla Suomen kyberturvallisuusstrategian (Kyberstrategia 2013) ja Bilateraalisen sanaston (Bilat 2014) määritelmiä.

Tässä yhteydessä on todettava, ettei yhtenäistä länsimaista käsitteistöä vielä ole muodostunut, kuten CCDCOE:n internetsivustolla julkaistusta kyberturvallisuussanastosta voi todeta:" There are no common definitions for Cyber terms - they are understood to mean different things by different nations/organisations" (CCDCOE 2015d).

Bilateraalisen sanaston ensimmäisen osan johdannossa on kuvattu näkökulmaeroja amerikkalaisen ja venäläisen ajattelun välillä (Bilat 2011ru, 8). Johdannossa selitetään tarkemmin venäläistä näkökulmaa, jonka mukaan kaikki informaatio on ihmisen tietoisen toiminnan tulosta ja *kybertoimintaympäristö* on erottamaton osa *informaatiokokonaisuutta* (Bilat 2011ru, 8–9). Näkökulma lähestyy filosofista ajattelutapaa, johon ei tässä tutkimuksessa tarkemmin perehdytä, mutta todetaan taustatietona niille asiantuntijoille, joita aihe kiinnostaa enemmän ja jotka tunnistavat *informaatio*-käsitteeseen liittyvän filosofisen näkökulman vaikutuksen.

Tämän analyysin perusteella käsitteitä *kyberturvallisuus* ja *кибербезопасность* voidaan pitää osittain toistensa vastineina, kuitenkin vain silloin kun huomioidaan näkökulmaero länsimaiden ja Venäjän välillä. Venäjä ei katso internetin olevan rajaton, vaan korostaa valtion oikeutta puolustaa kansallista suvereniteettia ja puuttua tiedon sisältöön, mikäli se luokitellaan haitalliseksi (SF 2014a, 2; MID 2013).

Näkökulmaeroa ei aina voi nähdä määritelmästä eikä terminologinen käsiteanalyysikaan välttämättä paljasta mitä piilomerkityksiä käsite sisältää.

> **kyberturvallisuus**
> ru ~ кибербезопасность
> en cybersecurity
> määritelmä: tavoitetila, jossa sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettuun toimintaympäristöön voidaan luottaa ja sen toiminta turvataan
> huomautus 1: kybertoimintaympäristön tavoitetila, jolloin sen toimintaan voidaan luottaa ja sen toiminta on turvattu.
> huomautus 2: kybertoimintaympäristön kyky suojautua uhkia ja epätoivottuja vaikutuksia seurauksia vastaan sekä kyky vastustaa, reagoida ja palautua niistä
> huomautus 3: Venäjä ei katso internetin olevan rajaton, vaan korostaa valtion oikeutta sekä puolustaa kansallista suvereniteettia että puuttua tiedon sisältöön, mikäli se luokitellaan haitalliseksi.

5.3 *Информационная безопасность* -käsite

Venäjänkielinen *информационная безопасность* -käsite esiintyy usein venäläisissä lähdeasiakirjoissa. Käsitteenä se on tärkeä ja keskeinen Venäjän kansallisen turvallisuuden kuvaamisessa, joten sitä on mahdotonta sivuuttaa. Lähemmässä tarkastelussa *информационная безопасность* -käsite osoittautui varsin laajaksi käsitteeksi. Havaittiin, että terminologisen käsiteanalyysin tueksi ja taustatiedoksi oli tarpeen saada lisätietoa koskien käsitteen sisältöä ja sen käyttökontekstia. Vastinehaussa pohdittiin *информационная безопасность* -käsitteelle suomenkielisiä vaihtoehtoja *tietoturvallisuus* ja *informaatioturvallisuus*. Näistä *tietoturvallisuus* on vakiintunut käsite tietotekniikan alalla. Hyvin nopeasti havaittiin, että venäjänkielinen *информационная безопасность* -käsite viittaa huomattavasti laajempaan kokonaisuuteen kuin mihin suomenkielinen *tietoturvallisuu*s-käsite. Toisena vastinevaihtoehtona oli *informaatioturvallisuus*-käsite, jota käytetään hyvin rajoitetusti suomen kielellä, ei lainkaan viranomaisten asiakirjoissa eikä myöskään tietotekniikan alalla. Tässä on mainittava, että Jyväskylän yliopistossa alkoi vuonna 2014 *Informaatio-turvallisuuden maisteriohjelma*, joka perustuu tietojenkäsittelytieteeseen (JYU 2015a, 9). Sittemmin koulutusohjelman nimi on muutettu *Kyberturvallisuuden maisteriohjelmaksi* (JYU 2015b). Maisteriohjelmien kuvauksissa käytetty *informaatioturvallisuus*-käsite ei ole sisällöltään venäjänkielistä *информационная безопасность* -käsitettä vastaava.

Sen sijaan *informaatioturvallisuus*-käsite liitetään usein *informaatiosodankäynti*- ja *informaatio-operaatio*-käsitteisiin, jotka on rajattu tämän tutkimuksen ulkopuolelle. Todettakoon, että Bilateraalisessa sanastossa (Bilat 2014) on *информационная безопасность* -käsitteen lisäksi määritelty useita informaatiosodankäyntiin kuuluvia käsitteitä, kuten *информационная операция* (information operation); *информационная война* (information war) ja *информационный конфликт* (information conflict) (Bilat 2014, 34–36).

Tässä tutkimuksessa keskitytään tarkastelemaan venäjänkielistä *информационная безопасность* -käsitettä sen verran kuin tämän tutkimuksen kannalta on olennaista. Koska vielä ei ole selvitetty tarkemmin *информационная безопасность* -käsitteen sisältöä, eikä ole tiedossa, mikä on sen suomenkielinen vastine, niin käytetään siitä tässä kontekstissa työnimenä *venäläinen informaatioturvallisuus*.

Kyberturvallisuus-käsitteen yhteydessä todettiin, että Venäjän kyberstrategian luonnoksen mukaan *кибербезопасность*-käsite ei poikkea sisällöllisesti *информационная безопасность* -käsitteestä (SF 2014a, 2). Luonnoksessa on annettu määritelmä molemmille käsitteille. *Информационная безопасность* -käsitteen määritelmä Venäjän kyberstrategian luonnoksen mukaan:

> информационная безопасность - состояние защищенности личности, организации и государства и их интересов от угроз деструктивных и иных негативных воздействии в информационном пространстве (SF 2014a, 2).

Tässä määritelmässä yläkäsite on *состояние защищенности* (suojauksen tila). Määritelmässä käytetään ilmaisua *угроз деструктивных и иных негативных воздействии*, jonka voi suomeksi kääntää ”destruktiivisten ja muiden negatiivisten vaikutusten uhkat ” (SF 2014a, 2). On vaikea päätellä onko tässä kyse pelkästään konekielisestä tiedosta vai myös tiedon sisällöllisestä merkityksestä. Hämmennystä aiheuttaa aiemmin tehty havainto, jonka mukaan näyttäisi, että samaa ilmaisua voidaan käyttää molemmissa tapauksissa sekä konekieliseen tietoon kohdistuvista haitallisista vaikutuksista että sisällöllisestä tiedosta. Bilateraalisen sanaston määritelmä on:

> **информационная безопасность**
> свойство информационного пространства противостоять угрозам, реагировать на них и восстанавливаться (после нанесения ущерба) (Bilat 2014,55).

> information security
> is a property of information space that is an ability to resist threats and respond and recover (Bilat 2014,55).

Määritelmän yläkäsite on *свойство информационного пространства* (informaatioavaruuden ominaisuus). Ominaisuus vastustaa uhkia, reagoida uhkiin sekä palautua niistä. Suomeksi käytetään myös ilmaisua kyky vastustaa ja reagoida (vrt. kyky havaita ja torjua kyberuhkat , Kyberstrategia 2013, 8)

Kyberstrategian luonnoksessa todetaan, että luonnoksen tulee perustua Venäjän lainsäädäntöön. Yksi luetelluista laeista on informaatiota, informaatioteknologiaa ja niiden suojausta määrittelevä laki: *Об информации, информационных технологиях и о защите информации* (FZ 149). Tämä laki antaa *информация*-käsitteelle tällaisen määritelmän: ”информация - сведения (сообщения, данные) независимо от формы их представления*”* (FZ 149: 2). Määritelmän mukaan informaatio voi olla missä tahansa muodossa. Määritelmässä on käytetty kolmea venäjänkielistä tietoa tarkoittavaa käsitettä: *сведение, сообщение* ja *данные*.

Tarkastellaan lyhyesti yleiskielen tasolla, millaisia suomenkielisiä vastineita nämä käsitteet saavat. Näistä *сведение*-käsite saa suomen kielessä usein vastineen *tieto*, kuten kerätään tietoja, jokin tulee tietoon tai lehtitiedot. Yleisessä kielenkäytössä se liittyy ihmisen kielelliseen tietoon erotuksena konekieleen viittaavasta datasta *(данные*). *Данные*-käsitteellä viitataan siis usein tietoaineistoon, jolla ei sellaisenaan ole sisällöllistä merkitystä (ks. jaksossa 5.1 *безопасность информации (данных),* GOSTR 50.1.053). *Сообщение*-käsite saa suomen kielellä usein vastineen *tiedotus, tiedonanto,* kuten virallinen tiedonanto tai vaikkapa uutistoimiston tiedote. Toisin sanoen kahdella käsitteistä, *сведение* ja *сообщение*, on selkeästi sisällöllinen merkitys.

Tieto on informaatiotutkimuksen keskeisiä käsitteitä. Informaatiotutkimuksen alalla *tiedon arvoketjussa* tieto jaetaan eri tasoihin. Sen mukaan tieto rakentuu alhaalta yksinkertaisemmasta konekielisestä tiedosta eli datasta monimutkaisemmaksi, ihmisen käytössä olevaksi *tietämykseksi* (data - informaatio - tieto - tietämys/viisaus) (Haasio & Vakkari 2015, 1).

Aihetta on käsitelty eri tieteenaloilla ja sen lähestymistapa lähenee monilta osin filosofisia näkemyksiä tiedosta. Tämä *tieto*-käsitteen jaottelu auttaa ymmärtämään, että käsitteet *tieto* ja *informaatio* voivat viitata sekä konekieliseen että sisällölliseen tietoon, joista jälkimmäisellä on erityinen merkitys venäläisessä ajattelussa. *Tiedon arvoketju* (tai *tiedon hierarkia*) kuvaa *datan* ja *informaation* välistä suhdetta. Alimmalla tasolla oleva *data* (данные) saa sisällöllisen merkityksen siirryttäessä ylemmälle tasolle *informaatio* (Haasio & Vakkari 2015, 1). Kuvassa 4 on esitetty *tiedon pyramidi*. DIKW-malli (englannin kielen sanoista: data, information, knowledge, wisdom) on myös Venäjällä yleisesti tunnettu *tiedon* kuvaamistapa, DIKW-модель (Sedyakin 2009).

***Kuva 4**: Tiedon pyramidi*

Venäjän turvallisuusneuvoston internetsivustolla venäjänkielistä *информационная безопасность* -käsitettä määrittelee seitsemän ohjausasiakirjaa (SBRF 2011). *Информационная безопасность* -käsitteen kannalta tärkein noista asiakirjoista on informaatioturvallisuusdoktriini, *Доктрина информационной безопасности* (DIBRF 2000). Sekä doktriini että muut ohjausasiakirjat käsittelevät laajasti yhteiskunnan kokonaisturvallisuutta, mikä olisi sisällöllisesti lähellä Suomen kyberturvallisuusstrategian (Kyberstrategia 2013) sisältöä.

Asiakirjoissa *информационная безопасност* ja *национальные интересы* -käsite (kansalliset intressit) ovat keskeisessä asemassa. Tämä johti etsimään olisiko *информационная безопасност* -käsitettä tutkittu Suomessa, Venäjällä tai muualla länsimaissa. Forrest Haren artikkeli sivuaa tätä aihetta (Hare 2010). Artikkeli tarkastelee syitä miksi eri valtioiden on vaikea päästä yhteisymmärrykseen

kansallisen turvallisuuden uhkista, erityisesti koskien kyberturvallisuutta. Haren mukaan on selvää, että ellei kansallisia eroavaisuuksia oteta huomioon, niin yhteistyö on vaikeaa, ellei mahdotonta. (Hare 2010, 211.) Hare viittaa Anatoly Streltsovin artikkeliin *International information security: description and legal aspects* (Streltsov 2007) ja arvioi sen perusteella Venäjän informaatioturvallisuusuhkien olevan luonteeltaan poliittisia (Hare 2010, 220).

Anatoly Streltsov on ollut mukana usean tämän tutkimuksen lähdeasiakirjan laatimisessa, samoin kuin Bilateraalisen sanaston laatimisessa. Streltsov toimii Venäjällä viranomaistasolla turvallisuusalan asiantuntijana (Bilat 2011ru; Bilat 2014). Streltsovin artikkelin (Streltsov 2007) mukaan *information security* tutkimusalana ja tutkimuskohteena tarkastelee vihamielisen valtion toiseen valtioon kohdistamia ICT:n (tietotekniikan) haittavaikutuksia ja hyökkäyksiä. Streltsov jatkaa tietoteknistä turvallisuutta kuvaavien uhkien luetteloa käyttämällä käsitteitä: *psykologinen vaikuttaminen, disinformaatio* ja *harhautus* (Streltsov 2007, 7), joita ei länsimaisessa ajattelussa yhdistetä lainkaan samaan asiayhteyteen.

Venäläiset katsovat hallinnolla olevan oikeus suojella kansalaisiaan haitalliselta informaatiolta (защита населения от вредной информации) ja sen toteuttamisessa on hyväksyttyä käyttää sensuuria tai muulla tavalla valvoa informaation välittämistä kansalaisille (Bilat 2011ru, 8). Bilateraalinen sanasto tiivistää osapuolten välisen näkökulmaeron näin:

> Американцы не рассматривают защиту информации, как нечто, что должно включать цензуру, или любую попытку контроля информированности населения" (Bilat 2011ru, 8).
>
> Americans do not see information protection as something that should include censorship, or any attempt to control the population's awareness (Bilat 2011en, 18).

Saksalainen oikeusoppinut Wolff Heintschel von Heinegg tarkastelee Venäjän edustamaa informaatio- ja kyberturvallisuutta kansainvälisen lain näkökulmasta, ja osoittaa selkeästi Venäjän pyrkimyksen määrätietoisesti valvoa internetissä ja kybertoimintaympäristössä ja kulkevan informaation sisältöä (Heinegg 2015, 3).

Konfliktitutkimuksen tutkija ja erityisesti Venäjään erikoistunut Keir Giles on perehtynyt *kyberturvallisuus*-käsitteistöön ja siihen liittyviin vastineongelmiin (Giles

& Hagestad 2013). Hän tarkastelee artikkelissaan kolmea hyvin erilaista yhteiskuntaa, niiden käyttämää termistöä ja sitä millaisia vaikeuksia niiden kääntämiseen liittyy. Artikkeli ei varsinaisesti ole kielitieteellinen, mutta siitä löytyy arvokasta tietoa tähän tutkimukseen. Englannin- ja venäjänkieliset termit voivat muodoltaan näyttää samalta, mutta ovat sisällöltään aivan eri käsitteitä. (Giles & Hagestad 2013, 1.) (ks. myös Vehmas-Lehto 2010, 363) Näin ollen termien suora kääntäminen voi aiheuttaa väärinymmärryksiä. Artikkelissa todetaan seuraavaa:

> There is the additional complication of direct translations of specific terms from Russian and Chinese which resemble English-language terms, and therefore give the misleading impression of mutual understanding, while in fact referring to completely different concepts (Giles & Hagestad 2013, 1).

Käsitteiden välisiä eroja on pohtinut myös Nikolai Kunjaev, joka työskentelee Venäjän valtionhallinnossa ja on saanut työstään valtiollisia tunnustuksia (Kunjaev 2015). Häntä voidaan pitää luotettavana lähteenä, vaikka hän ei ole yhtä tunnettu kuin Streltsov. Kunjaev tarkastelee *информационная безопасность* -käsitettä dokumentoinnin ja oikeustieteen näkökulmasta. Hän käyttää esimerkkinä venäjänkielistä käsitettä *национальные интересы* (kansalliset intressit) siitä, miten lainsäädäntöön syntyy uusia käsitteitä. Syntyneet uudet käsitteet kuvaavat ja heijastavat sen hetkistä yhteiskunnallista ja poliittista tilannetta. (Kunjaev 2010a.) Kuten aiemmin todettiin, н*ациональные интересы* -käsite liittyy läheisesti *информационная безопасность* -käsitteeseen.

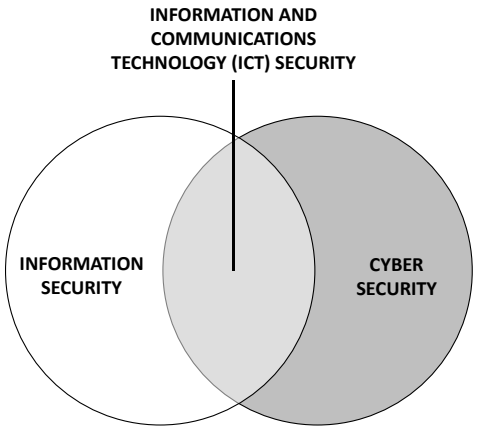
Kunjaev ehdottaa selkeää rajausta käsitteiden *информационная безопасность Российской Федерации* (Venäjän federaation informaatioturvallisuus) ja *информационная безопасность* (informaatioturvallisuus) välille (Kunjaev 2010b, 257). Käsitteen rajaaminen maantieteellisesti olisi perusteltua, sillä se selkeyttäisi viestintää sekä vähentäisi väärinkäsityksiä. Vastaavaa käsitteen rajaamista esiintyy muissakin venäläisissä asiakirjoissa.

Kansallista turvallisuutta määrittelevissä asiakirjoissa, kuten *Venäjän federaation informaatioturvallisuusdoktriinissa* (DIBRF 2000), käytetään kolmijaottelua *личность – общество – государство.* Sama kolmijaottelu on käytössä myös kun määritellään *информационная безопасность* -käsite. Käsite määritellään suhteessa jokaiseen näistä kolmesta: *yksilö – yhteisö – valtio*. Lisäksi tehdään selvä ero

valtiollisten toimijoiden ja *ei-valtiollisten toimijoiden* välillä. Vaatisi jatkotutkimusta selvittää mistä oikeustieteellistä tai yhteiskuntafilosofisesta suuntauksesta kyseinen kolmijaottelu saa alkunsa. Tieto auttaisi valitsemaan oikean suomenkielisen vastineen venäjänkieliselle *общество*-käsitteelle, joka voi saada suomen kielessä vastineet *yhteisö* tai *yhteiskunta*.

Länsimaisessa ajattelussa käsitteet *information security* ja *cyber security* eivät ole toistensa synonyymeja, vaikka merkitys on osittain sama tietyllä kapealla alalla. Kansainvälisesti arvostettu kyberturvallisuuden tutkija, professori Rossouw von Solms vahvistaa tekemänsä analyysin perusteella, että *information security* ja *cyber security* -käsitteillä on yhteisten käsitepiirteiden lisäksi myös piirteitä, jotka puuttuvat kokonaan toisesta. (Solms & Niekerk 2013.)

Kuva 5 on piirretty mukaillen artikkelissa (Solms & Niekerk 2013) esitettyä kuvaa, joka havainnollistaa miten englanninkieliset käsitteet *information security* ja *cyber security* ja *information and communication technology security (ICT)* ovat suhteessa toisiinsa (Solms & Niekerk 2013, 101).



K*uva 5:* *Englanninkieliset käsitteet information security, cyber security ja ICT (Solms & Niekerk 2013, 101)*

Tässä kuvassa 5 *cyber security* ja *information and communication technology security (ICT)* kuvaavat tietoja, jotka ovat sähköisessä muodossa. Sen sijaan kuvan *information security* -lohkon vasemman puoleinen osio voi sisältää myös sellaisia tietoja, jotka eivät ole sähköisessä muodossa, kuten paperimuodossa säilytettävät salaiset asiakirjat. (Solms & Niekerk 2013.)

Edellä on selvitetty venäjän *информационная безопасность*-käsitettä ja pyritty selvittämään voitaisiinko venäjän *информационная безопасность* merkitä suomen *informaatioturvallisuus*-käsitteen vastineeksi. Jos ne olisivat vastineet, niin mitkä ovat näiden käsitteiden väliset yhtäläisyydet ja erot.

Erikoisalaan perehtymätön voisi pitää käsitteitä *tietoturvallisuus* ja *informaatioturvallisuus* lähisynonyymeina. Käsitteet *informaatio* ja *tieto* näyttävät olevan keskenään varsin samalla tavalla määriteltäviä käsitteitä. Ne mielletään kuuluviksi tiedon-arvoketjuun (data, informaatio, tieto). Kaikki tieto on informaatiota, mutta kaikki informaatio ei ole välttämättä tietoa (jos informaatiota ei ole vastaanotettu tai tulkittu). (ks. tiedon-arvoketju)

Kokonaisturvallisuuden sanasto (TSK 47) määrittelee *tietoturvallisuuden* järjestelyiksi, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus (TSK 47, 2014). Oletetaan, että tarkasteltava käsite olisikin *tietoturvallisuuden* sijaan *informaatioturvallisuus* ja muokataan määritelmä uudelleen: informaatioturvallisuus - järjestelyt, joilla pyritään varmistamaan *informaation* saatavuus, eheys ja luottamuksellisuus.

Huomataan, että ehdotus ei tuota käsitteen sisällön ja merkityksen kannalta järkevää kuvausta *informaatioturvallisuus*-käsitteestä. Tässä yhteydessä on syytä muistuttaa, että käytännössä suomen kielessä ei juurikaan käytetä *informaatioturvallisuus*-käsitettä.

Lähteiden perusteella vaikuttaa siltä, että venäjän *информационная безопасность* -käsite olisi määriteltävä aivan eri tavalla kuin suomen *informaatioturvallisuus*-käsite. Tällöin kyseessä voisi olla polysemia. Edellä olevan perusteella todetaan, ettei käsitteitä *tietoturvallisuus* ja *informaatioturvallisuus* voida suomen kielessä pitää lähikäsitteinä. Analyysin perusteella ja johtopäätöksenä esitetään termiehdotus:

> **Venäjän informaatioturvallisuus; venäläinen informaatioturvallisuus**
> ru информационная безопасность
> määritelmä: järjestelyt, joilla pyritään varmistamaan se, että informaatio ei uhkaa Venäjän kansallista suvereniteettia, on Venäjän henkisten arvojen mukaista eikä ole haitallista kansalaisille
> huomautus 1: Venäjällä информационная безопасность -käsitettä määritellään valtion kokonaisturvallisuuteen ja yhteiskunnan turvallisuuteen liittyvissä asiakirjoissa, joiden sisältö viittaa eri ilmiöihin kuin mitä tietoturvallisuudella länsimaissa tarkoitetaan. Asiakirjoissa viitataan esimerkiksi Venäjän kansalliseen suvereniteettiin, henkisiin arvoihin sekä siihen, että kansalaisia tulee suojata haitalliselta informaatiolta.

5.4 *Kyberuhka*-käsite

Yhteiskunnan turvallisuusstrategia (YTS 2010) määrittelee *kyberuhka*-käsitteen rajoittaen sen vain kyseisessä asiakirjassa käytettäväksi. Käsitettä ei vielä tuolloin oltu määritelty, mikä selittää miksi *kyberuhka*-käsite on asiakirjassa mainittu vain otsikossa ja seuraavassa selitteessä:

> Termi on vielä kansallisissa käytännöissä vakiintumaton. Tässä 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 (YTS 2010, 86).

YTS kuvaa elintärkeitä toimintoja vaarantavat uhkamallit, joista yksi uhkamalli on otsikoitu: Tietoliikenteen ja tietojärjestelmien vakavat häiriöt eli *kyberuhkat* (YTS 2010, 67 ja 81). Kyberuhka siis rinnastetaan tietoliikenteen ja tietojärjestelmien vakavaksi häiriöksi. Tätä voisi pitää kyberuhkan määritelmänä, mutta asiantuntijan mielestä se on kuitenkin liian suppea (Tuukkanen 2015).

YTS määrittelee *kyberuhka*-käsitteen hyvin samansisältöisesti kuin myöhemmin julkaistu Kyberturvallisuusstrategia (Kyberstrategia 2013), joka antaa *kyberuhka*-käsitteelle tällaisen määritelmän:

> **kyberuhka**
> tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon (Kyberstrategia 2013, 13).

Määritelmän yläkäsite on *mahdollisuus*. Mahdollisuus kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka vaarantaa kybertoimintaympäristöstä riippuvaisen toiminnon. Määritelmän huomautuksessa todetaan, että kyse on *tietoturvauhkista*, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan (Kyberstrategia 2013, 13).

Kyberturvallisuusstrategian mukaan elintärkeät toiminnot on suojattava kyberuhkaa vastaan (Kyberstrategia 2013, 2). Kyberturvallisuusstrategian taustamuistiossa tarkennetaan, että uhkat kohdistuvat yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin ja/tai kansalaisia vastaan (Kyberstrategia 2013, 18). Kyberturvallisuusstrategia velvoittaa kaikki hallinnonalat varautumaan

kyberuhkiin, joten niillä on kyberuhkan suhteen varautumisvelvoite. Normaalioloissa kyberturvallisuus on hallinnassa, mutta kyberuhkan toteutuessa häiriötilanne muuttuu poikkeustilaksi. (Kyberstrategia 2013, 20.)

Kyberuhkat muodostavat laaja-alaisen ja merkittävän haasteen yhteiskunnan kokonaisturvallisuudelle (VNK 5/2012, 94). Kyberturvallisuusstrategiassa todetaan, että on tärkeää ylläpitää ”kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja kyberhäiriötilanteet” (Kyberstrategia 2013, 8). Suomessa Kyberturvallisuuskeskus seuraa ja varoittaa, mikäli se havaitsee yhteiskunnan elintärkeiden toimintoja uhkaavia kyberuhkia (Kyberstrategia 2013, 24).

Kyberuhka voi siis olla tietoturvauhka, mutta aina se ei ole. Tätä on havainnollistettu kuvassa 5 (ks. Kuva 5, jakso 5.3) oikeanpuoleisella harmaalla alueella, joka kuvaa tieto-/informaatioriippumattomia kybertoimintoja.

Kokonaisturvallisuuden sanastosta (TSK 47) löytyy samanlainen *kyberuhka*-käsitteen määritelmä kuin Kyberturvallisuusstrategiassa (Kyberstrategia 2013).

Lisäksi sanastossa on annettu esimerkki *kyberuhka*-käsitteen käytöstä:

> Kyberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös sähköisessä viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista (TSK 47, 72).

Tässä huomautuksessa on tuotu esille *tietoturvauhkien* lisäksi myös *teot*, joilla viitataan ulkoisiin toimijoihin. Myös Valtioneuvoston selonteossa, *Suomen turvallisuus- ja puolustuspolitiikka 2012* -asiakirjassa (VNK 5/2012) on todettu, että kybertilaan kohdistuu sekä tahattomia että tahallisia häiriöitä:

> Erityisesti kybertilan häiriöt ovat kriittinen uhkatekijä. Kyberuhkaa aiheuttavat tietoverkkojen sisäiset heikkoudet sekä vahinkoa aiheuttavat tai laittomasti tietoa hankkivat ulkoiset toimijat. Laajat tietoverkot ovat alttiita tahattomillekin toimintahäiriöille, vahinkoa aiheuttavien valtiollisten ja ei-valtiollisten toimijoiden erottaminen ja uhkien alkuperän selvittäminen vaikeutuvat (VNK 5/2012, 2).

Kyberstrategian taustamuistiossa (Kyberstrategia 2013) on pohdittu kyberuhkamallin avulla miten kyberuhkia voi aiheutua:

> Kyberuhkamalli tarkoittaa kuvausta kyberuhkien aiheuttamista häiriöistä, uhkan vaikutusmekanismista, lähteestä, kohteesta ja vaikutuksesta kohteeseen (Kyberstrategia 2013,18).

Kyberstrategian taustamuistiossa (Kyberstrategia 2013) on havainnollistettu kyberuhkamallia kuvalla (ks. Kuvio 1 Suomen kyberuhkamalli, Kyberstrategia 2013,19). Kuva ei kuitenkaan vastaa selostusta kyberuhkamallista (vrt. edellinen tekstiote, Kyberstrategia 2013,18).

Kyberuhkamallia on mallinnettu myös kansainvälisellä tasolla. Tietotekniikka-alan järjestö Institute of Electrical and Electronics Engineers, IEEE on julkaissut poikkitieteellisen tutkimusryhmän artikkelin *Dimensions of Cyber-Attacks. Social, Political, Economic and Cultural* (Gandhi & Sharma & Mahoney & Sousan & Zhu & Laplante 2011), jossa tarkastellaan ja analysoidaan toteutuneita kyberhyökkäyksiä viimeisten kymmenen vuoden ajalta. Analysointiin on koottu tietoja kyberhyökkäyksistä eri näkökulmista ja niiden perusteella on laadittu kyberuhkamalli. Kyberuhkaa on tarkasteltu neljästä eri näkökulmasta: sosiaalisesta, poliittisesta, taloudellisesta ja kulttuurisesta.

Kyberstrategian (Kyberstrategia 2013) ja artikkelin esittämän luokittelun perusteella on tässä tutkimuksessa laadittu suomalaiseen kyberturvallisuuskäsitteistöön soveltuva kyberuhkamalli (ks. Liite 2). Kyberuhkamalli kuvaa kyberuhkien synty- ja vaikutusmekanismin, kohteen, toteutustavan, eri tekijän ja tekijän motiivien mukaan. Sen avulla voidaan havaita, että *kyberuhka* voi olla hyvin moniulotteinen. (Kyberstrategia 2013, 18). Kyberuhka voi samanaikaisesti kuulua useampaan käsitekaavion muodostamaan haaraan ja eri kriteerit eivät ole toisiaan poissulkevia. *Kyberuhkaa* voi olla vaikea rajata toiminnallisesti ja käsitteellisestikin sen tarkka rajaus on haasteellista.

Kyberstrategian (Kyberstrategia 2013) mukaan kyberuhkamallissa kyberuhkia ovat:

> kyberaktivismi, (kybervandalismi, haktivismi); kyberrikollisuus; kybervakoilu; kyberterrorismi, kyberoperaatiot (Kyberstrategia 2013:18).

Edellä luetellut ovat Kyberstrategian (Kyberstrategia 2013) mukaan *kyberuhka*-käsitteen alakäsitteitä. Tässä havaitaan puutteita käsitejärjestelmässä, joka ei näytä täyttävän terminologisia vaatimuksia systemaattisuudesta. Ensinnäkin, *kyberuhka*-käsitteen yläkäsite on *mahdollisuus* (Kyberstrategia 2013, 13), joten edellä mainitut

eivät voi olla sen alakäsitteitä. Toiseksi, Kyberstrategian (Kyberstrategia 2013) mukaan *kyberuhka* voi olla *tietoturvauhka*, mutta edellä mainittuja käsitteitä ei voi luokitella tietoturvauhkiksi, eikä kaikkia myöskään vieruskäsitteiksi. Luettelossa on rinnastettu rikoslain alaisia rikoksia, kuten *kyberrikollisuus, kybervakoilu, kyberterrorismi*, ja toisaalta kansalaisyhteiskunnassa positiivisena pidettäviä ilmiöitä kuten *aktivismi*.

Tässä havaitaan, että Kyberturvallisuusstrategian (Kyberstrategia 2013) määritelmät eivät ole sanastotyön edellyttämässä muodossa. Koska tämän tutkimuksen näkökulma on lähtökohtaisesti deskriptiivinen, niin tässä tyydytään osoittamaan mahdolliset puutteet käsitejärjestelmässä sekä toteamaan, että käsitteiden terminologiseen määrittelyyn tulisi kiinnittää nykyistä enemmän huomiota. Vastinehaussa löytyi Bilateraalisesta sanastosta *киберугроза*-käsitteelle määritelmä:

> **киберугроза**
> обнаруженная или установленная угроза использования киберуязвимости (Bilat 2014, 38).
>
> cyber threat
> a danger, whether communicated or sensed, that can exercise a cyber vulnerability (Bilat 2014, 38).

Tämä määritelmä on muodostettu *угроза*-käsitteestä, joka on määritelmän yläkäsite. Määritelmä on aika vaikeaselkoinen, mutta sen mukaan *киберугроза* (kyberuhka) voi aiheutua hyödyntämällä киберуязвимость (kyberhaavoittuvuus) (ks. jakso 5.1.1 haavoittuvuus). Käsitteet on muodostettu lisäämällä *кибер*-etuliite vakiintuneisiin ja tuttuihin käsitteisiin *угроза* (uhka) ja *уязвимость* (haavoittuvuus), mikä osaltaan helpottaa käsitteiden ymmärtämistä ja sijoittamista käsitejärjestelmässä.

Venäjän konventiossa (SBRF 2011) ei esiinny *киберугроза*-käsitettä, vaan siinä käytetään ilmaisua *угроза в информационном пространстве* tai *угроза информационной безопасности*. Kuten aiemmin on todettu, venäläisissä asiakirjalähteissä ei esiinny *кибер*-etuliitteellä muodostettuja sanoja. Sen sijaan käytetään yleisesti *информационная безопасность* -käsitettä ja sen avulla muodostetaan sanaliittoja. Silloinkin kun viitataan selkeästi samaan mihin suomenkielisellä *kyber*-käsitteellä, ei venäjäksi käytetä vastaavaa *кибер*-sanaa . Tämä selittyy sillä, että Venäjällä kyberkäsitteistö on uutta ja käsitteistö on vasta

muodostumassa. Venäjän konventiossa (SBRF 2011) on annettu *угроза в киберпространстве* -käsitteen määritelmä:

> **угроза в киберпространстве**
> факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве (SBRF 2011).

Määritelmän yläkäsite on *факторы* (tekijät). Tekijät, jotka aiheuttavat vaaraa. Määritelmässä on käytetty jälleen kolmiluokittelua yksilö, yhteisö ja valtio, joita kohtaan uhka kybertoimintaympäristössä kohdistuu. Mutta määritelmä ei tarkenna millaisesta uhkasta on kyse. Rinnakkaisteksteistä löytyi myös *угроза в киберпространстве -käsite* (Kazarin & Salnikov & Sharipov & Yashenko 2010, 71). Vaatisi lisätutkimusta selvittää onko se *кибератака*-käsitteen synonyymi.

Kyberuhka-käsitteelle ei tässä tutkimuksessa löydetä venäjänkielistä vastinetta. Analyysin perusteella ei ole saatu riittävästi vahvistusta, jotta vastaavuus voitaisiin todeta. Löydettyjä venäjänkielisiä käsitteitä voidaan kuitenkin hyödyntää jatkotutkimuksessa. Suomenkielisen *kyberuhka*-käsitteen tiedot on koottu termitietueeseen.

> **kyberuhka**
> määritelmä**:** kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoiminta-ympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon
> huomautus **1:** kohdistuu elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria, ja /tai kansalaista vastaan
> huomautus **2:** vaarantaa elintärkeät toiminnot tai muun kybertoimintaympäristöstä riippuvaisen toiminnon
> huomautus **3:** tietoturvauhka, on tietoliikenteen ja tietojärjestelmien vakava häiriö, tahaton toimintahäiriö tai tahallisesti toteutettu

5.5 Kyberriski-käsite

Suomen kyberturvallisuusstrategiassa esiintyy vain pari kertaa *kyberriski*-käsite. Kyberstrategian määritelmä *kyberriski*-käsitteelle on seuraava:

> **kyberriski**
> määritelmä**:** Kybertoimintaympäristöön kohdistuva vahinkomahdollisuus tai haavoittuvuus, joka toteutuessaan tai jota hyväksi käyttäen kybertoiminta-ympäristön toiminnasta riippuvalle toiminnolle voi aiheutua vahinkoa, haittaa tai häiriötä (Kyberstrategia 2013, 12).

Määritelmän yläkäsite on *vahinkomahdollisuus* tai *haavoittuvuus*. Kohteena on kybertoimintaympäristön toiminnasta riippuva toiminto. Kyberturvallisuusstrategian (Kyberstrategia 2013) määritelmä *kyberriski*-käsitteelle kuvaa tosiasiassa paremmin *kyberuhka*-käsitettä. Tätä olettamusta vahvisti se, että Kokonaisturvallisuuden sanaston määritelmä *kyberuhka*-käsitteelle on hyvin samansisältöinen (vrt. kyberriski, Kyberstrategia 2013, 12):

> **kyberuhka**
> määritelmä**:** uhka, joka toteutuessaan vaarantaa yhteiskunnan elintärkeän toiminnon tai muun kybertoimintaympäristöstä riippuvaisen toiminnon (TSK 47, 72).

Määritelmän yläkäsite on *uhka*, joka kohdistuu kybertoimintaympäristöstä riippuvaiseen toimintoon. Suomenkielisissä asiakirjoissa *kyberriski*-käsitettä ei esiinny kovinkaan usein. Kyberstrategiasta löytyy *kyberriskianalyysi*-käsite, jonka avulla voidaan kartoittaa haavoittuvuutta (Kyberstrategia 2013, 36).

Venäjänkielistä lähteistä ei löytynyt suomenkieliselle *kyberriski*-käsitteelle vastinetta. Eikä myöskään Bilateraalisesta sanastosta, josta usein löytyy länsimaissa käytetyt käsitteet ja niiden vastineet. *Кибер-риск*-käsitettä yhdyssanana näkee venäläisten tietotekniikka-alan asiantuntijoiden kirjoituksissa, mutta sitä käytetään selkeästi muotisanana ja silloin yleensä *tietoturvariskin* synonyymina. Näin ollen tälle käsitteelle ei tässä tutkimuksessa löydetä venäjänkielistä vastinetta.

Sekä *kyberuhkan* että *kyberriskin* käsiteanalyysin perusteella on ilmeistä, että Kyberturvallisuusstrategian (Kyberstrategia 2013) kuvaamassa käsitejärjestelmässä on puutteita.

5.6 *Kybertoimintaympäristö*-käsite

Suomen kyberturvallisuusstrategian (Kyberstrategia 2013) määritelmä *kybertoimintaympäristölle* on seuraava:

> **Kybertoimintaympäristö**
> on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö (Kyberstrategia 2013, 12).

Määritelmä olisi selkeämpi, jos se alkaisi yläkäsitteellä, joka tässä määritelmässä on *toimintaympäristö*. Määritelmä on tiivis ja muodostettu useammasta käsitteestä, joiden merkitys ei helposti avaudu ilman erikoisalan tuntemusta, joten on perusteltua tarkastella määritelmässä käytettyjä käsitteittä tarkemmin. Määritelmässä käytetty *tietojärjestelmä*-käsite on keskeinen *kybertoimintaympäristön* määrittelyssä:

> Tietojärjestelmällä tarkoitetaan ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuvaa järjestelmää, jonka tarkoituksena on informaatiota käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi (Kyberstrategia 2013, 13).

Kokonaisturvallisuuden sanasto (SKT 47) antaa kybertoimintaympäristön tietojärjestelmistä esimerkkinä erilaiset tietojärjestelmiin perustuvat ohjausjärjestelmät (SKT 47, 56). Tämän tutkielman toisessa luvussa kuvattiin Stuxnet-haittaohjelman toimintaa teollisuuden ohjausjärjestelmässä. (ks. Luku 2: Johdanto kyberturvallisuuteen)

Tietojärjestelmiä hyödynnetään kaikilla ihmistoiminnan ja yhteiskunnan aloilla. Suomessa *tietojärjestelmä* on myös lainsäädännöllisesti määritelty (L1406/2011) ja sillä tarkoitetaan tietojenkäsittelylaitteista, ohjelmista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä. Tietoliikennejärjestelyillä tarkoitetaan tiedonsiirtoverkosta, tiedonsiirtolaitteista, ohjelmistoista ja muista tietojenkäsittelystä koostuvista järjestelyistä muodostuvaa järjestelmää (L 1406/2011 §2 momentit 1–2).

Kybertoimintaympäristön määritelmä ei oteta huomioon tietoliikenne järjestelyjä tai tietoverkkoa. TEPAN mukaan *tietoverkko*-käsitteen määritelmä on:

> **tietoverkko**
> tietokoneiden ja niiden välisten tiedonsiirtoyhteyksien sekä niiden molempien avulal tarjottavien palvelujen yhdistelmä (TEPA, Tietotekniikan termitalkoot, 1999).

Kyberstrategia (2013) antaa kaksi tarkennusta *kybertoimintaympäristö*-käsitteelle. Niistä ensimmäinen antaa lisätietoa sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitetusta toimintaympäristöstä:

> Tarkennus 1: Ympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet. (Kyberstrategia 2013, 12.)

Tarkennuksessa 1 viitataan *dataan* ja *informaatioon*, jotka sijoittuva tiedon arvoketjussa alemmalle tasolle kuin *kybertoimintaympäristön*-määritelmässä käytetty *informaatio (tieto)* (Kyberstrategia 2013, 12). Käsitteitä *data, informaatio ja tieto* on käytetty horjuvasti. Jossain *informaatio*-käsite esiintyy yksin, toisaalla se on saanut suluissa lisäyksen *informaatio (tieto)* tai toisen sanan kanssa rinnasteisena kuten *data* ja *informaatio*. (ks. Jakso 5.3 tiedon arvoketju) Ilmeinen ristiriita voidaan ratkaista myöhemmin annettavassa määritelmäehdotuksessa.

Tarkennuksessa käytetty *elektroniikan käyttö* voi viitata laajasti tietokoneisiin ja muihin sähköisessä tiedonsiirrossa käytettäviin laitteisiin, välineisiin jopa ohjelmiin. Sähkömagneettisen spektrin käyttö viestintäverkkojen avulla viittaa esimerkiksi langattomaan viestintään, jossa radioaaltoja käytetään esimerkiksi matkapuhelinverkoissa ja langattomissa tietokoneverkoissa. Sähkömagneettinen säteily jaetaan sähkömagneettisten aallonpituuden mukaan eri osa-alueisiin (radioaallot, valo, röntgensäteily), joista muodostuu kokonaisuus eli sähkömagneettinen spektri. (TTL 2006.)

Määritelmän toisessa tarkennuksessa on luettelo tietojenkäsittelyyn kuuluvista toimenpiteistä:

> Informaation (tietojen) käsittely tarkoittaa informaation (tietojen) keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita informaatioon (tietoihin) kohdistuvia toimenpiteitä (Kyberstrategia 2013, 12).

Sekä Kyberturvallisuusstrategian (2013) johdannossa että Yhteiskunnan turvallisuusstrategian (2010) johdantokappaleessa on molemmissa kuvattu kybertoimintaympäristöä näin:

> Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja tietojärjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Tästä keskinäisriippuvaisesta ja moninaisesta sähköisessä muodossa olevan tiedon käsittelyyn tarkoitetusta ympäristöstä on kansainvälisesti ryhdytty käyttämään termiä kybertoimintaympäristö. (YTS 2010, 1; Kyberstrategia 2013, 1)

Suomen turvallisuus- ja puolustuspolitiikka 2012 -asiakirjassa (VNK 5/2012) todetaan kybertoimintaympäristöön kohdistuvien haittaohjelmien uhkaavaan erityisesti teollisuusautomaation ja ohjelmoitavan logiikan kautta yhteiskunnalle elintärkeitä toimintoja (VNK 5/2012, 24). Kybertoimintaympäristöön kohdistuvat

uhkat ovat koko yhteiskunnalle vaarallisia tietoturvaloukkauksia ja rikoksia, joita voidaan käyttää myös poliittisena ja taloudellisena vaikuttamis- ja painostuskeinoina perinteisten sotilaallisten voimakeinojen tapaan (VNK 5/2012, 96).

Kyberturvallisuusstrategian (2013) taustamuistio kuvataan *kybertoimintaympäristö*-käsitettä seuraavasti:

> Globaali kybertoimintaympäristö muodostuu monimutkaisesta ja monikerroksisesta maailmanlaajuisesta informaatioverkostosta, johon kuuluu kansallisia turvallisuusviranomaisten, muun julkishallinnon ja yritysmaailman kommunikaatioverkkoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta- ja ohjausjärjestelmiä (Kyberstrategia 2013, 17).

Kybertoimintaympäristö on yhtä aikaa kansallinen sekä globaali toimintaympäristö, joka yhdistää valtioita, yrityksiä ja kansalaisia reaaliajassa. Jos tietotekniset laitteet ja järjestelmät eivät toimi, voi informaatioinfrastruktuuri luhistua, mikä vaikuttaa julkisiin palveluihin, liike-elämän, hallinnon ja koko yhteiskunnan toimintaan. (Kyberstrategia 2013, 17.)

Edellä käsitellystä voidaan päätellä *kybertoimintaympäristön* olevan laaja käsite, joka on tarkoitettu sähköisessä muodossa olevan informaation (tiedon) käsittelyyn. Se on siis *järjestelmien järjestelmä*, joka muodostuu muun muassa ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista. *Järjestelmien järjestelmä* -käsite kuuluu kompleksisuusteoriaan (Hyötyniemi 2009).
Kybertoimintaympäristössä ihminen on tietojen tuottaja ja käyttäjä, ja kohteena on *data* ja *informaatio*. Siihen kuuluu myös sähköiseen tiedonkäsittelyyn liittyvät ohjelmat, ohjelmistot sekä fyysiset rakenteet (varastointi, muokkaus, siirto).

Käsiteanalyysin perusteella etsitään venäjänkielisistä lähteistä vastinetta. Venäjän kyberstrategian luonnoksen mukaan (SF 2014a) *киберпространство*-käsite on:

> **киберпространство**
> сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государств) (SF 2014a, 2.)

Määritelmän yläkäsite on *сфера деятельности* (toimintaympäristö), joka sijoittuu laajempaan kokonaisuuteen *сфера деятельности в информационном пространстве* (informaatioympäristöön tai informaatioavaruuteen).

Määritelmän mukaan *киберпространство* (kybertoimintaympäristö) on *сфера деятельности* (toimintaympäristö), johon kuuluu *коммуникационные каналы Интернета* (internetin viestintäkanavat) , *телекоммуникационные сети* (telekommunikaatioverkot) ja *технологическая инфраструктура* (tekninen infrastruktuuri) Nämä ovat samoja käsitepiirteitä, joita lueteltiin suomenkielisen *kybertoimintaympäristö*-käsitteen yhteydessä.

Bilateraalisesta sanastosta löytyy käsitteen *киберпространство* määritelmä:

> **киберпространство**
> электронная (включая фотоэлектронные и пр.) среда, (посредством) которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается. (Bilat 2014, 17)
>
> cyberspace
> is an electronic medium through which information is created, transmitted, received, stored, processed and deleted. (Bilat 2014, 17)

Määritelmässä on käytetty käsitettä *электронная* (*включая фотоэлектронные*) *среда*, joka viittaa sähköiseen toimintaympäristöön (GOST 52292). Vertailemalla suomenkielisen *kybertoimintaympäristö*-käsitteen ja venäjänkielisen *киберпространство* käsipiirteitä voidaan todeta niiden olevan vastineita. Bilateraalisen sanaston englanninkielinen vastine on *cyberspace* (Bilat 2014, 17).

Edellisen analyysin perusteella annetaan *kybertoimintaympäristölle*-määritelmäehdotus:

> **kybertoimintaympäristö**
> ru киберпространство
> en cyberspace
> määritelmäehdotus: toimintaympäristö, joka muodostuu yhdestä tai useammasta, sähköisessä muodossa olevan datan, informaation tai tiedon käsittelyyn tarkoitetusta, tietoverkosta ja tietojärjestelmästä

Määritelmäehdotuksen yläkäsite on *toimintaympäristö*. Määritelmäehdotus ottaa huomioon sekä tiedon arvoketjun että kybertoimintaympäristön kokonaisarkkitehtuurin, jossa tietoverkot ovat vähintään yhtä tärkeässä asemassa kuin tietojärjestelmät. Asiantuntijalta pyydettiin arviota määritelmäehdotuksesta.

Palautteen mukaan määritelmäehdotus on loogisempi ja kuvaa paremmin kybertoimintaympäristöä (Tuukkanen 2015).

5.6.1 *Kriittinen kybertoimintaympäristö* -käsite

Käsiteanalyysia ja käsitekaaviota laadittaessa huomattiin, ettei lähdeasiakirjoista löydy termiä, jolla voitaisiin erottaa kybertoimintaympäristöstä se osa, joka on yhteiskunnan elintärkeille toiminnoille välttämätön kybertoimintaympäristö. Useimmat muut käsitteet on luokiteltu kriittisiksi ja ei-kriittisiksi, joten olisi perusteltua toimia samoin myös tämän keskeisen käsitteen kohdalla. Huomautuksena, että tässä tutkielmassa ei tehdä eroa *elintärkeä, kriittinen* ja *välttämätön* välillä.

Yhteiskunnalle elintärkeä toiminto, lyhennettynä YET, voi olla riippuvainen kybertoimintaympäristöstä (ne toiminnot jotka ovat sähköisessä muodossa). Toisaalta YET voi olla myös riippumaton kybertoimintaympäristöstä. YET ei aina ole kybertoimintaympäristöstä riippuvainen, mutta mikäli se on riippuvainen kybertoimintaympäristöstä niin silloin siitä osasta, joka on *kriittinen kybertoimintaympäristö*.

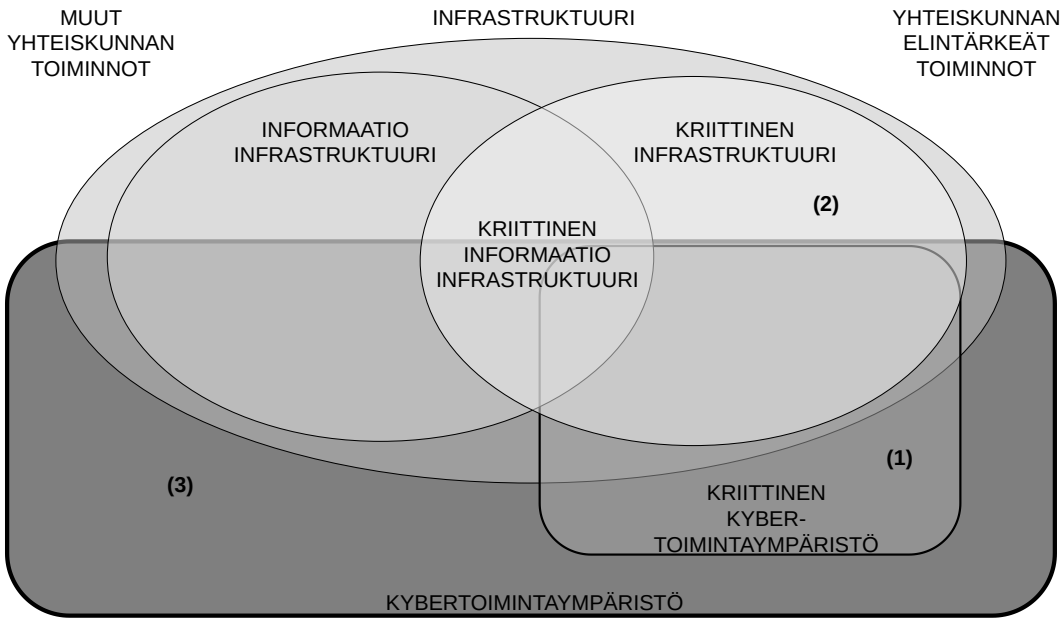
Tietojenkäsittely mielletään usein pelkästään sähköiseksi, mutta on muistettava, että sen lisäksi on huomattava määrä paperimuodossa olevaa tietoa (ks.Solms & Niekerk 2013). Olisi siis perusteltua erottaa kybertoimintaympäristöstä se osa, joka on yhteiskunnan toiminnalle välttämätön kybertoimintaympäristö. Annetaan tässä tutkimuksessa termiehdotuksena: *kriittinen kybertoimintaympäristö.* Tätä termiehdotusta tukee asiakirjalähteestä löydetty *välttämätön kybertoimintaympäristö*: ”Lähivuosien painopiste on tietoyhteiskunnalle *välttämättömän kybertoimintaympäristön* turvaamisessa ” (VNK 5/2012, 11–12).

Tästä edellä esitetystä voidaan laatia *kriittinen kybertoimintaympäristö* -käsitteen määritelmäehdotus:

> **kriittinen kybertoimintaympäristö**
> määritelmä: kybertoimintaympäristön osa, joka on välttämätön yhteiskunnan elintärkeille toiminnoille
> huomautus: kriittiseen kybertoimintaympäristöön kohdistuvat uhkat ovat aina vaarallisia koko yhteiskunnalle.

Asiantuntijalta pyydettiin arviota tästä termiehdotuksesta. Hänen mukaansa ehdotettua käsitettä *kriittinen kybertoimintaympäristö* ei suomen kielessä juurikaan käytetä. Käsite olisi erittäin käyttökelpoinen, koska se rajaa tarkastelun siihen kybertoimintaympäristön osaan, josta yhteiskunnan elintärkeät toiminnot ovat riippuvaisia. Asiantuntijan mukaan olisi tarpeen verrata myös käsitteiden *kriittinen kybertoimintaympäristö* ja *kriittinen* i*nformaatioinfrastruktuuri* sisältöjä sekä selvittää käsitteiden yhteneväisyydet ja eroavuudet. (Tuukkanen 2015)

Havainnollistetaan kuvalla miten käsitteet sijoittuvat toisiinsa nähden (ks. Kuva 6: Kriittinen kybertoimintaympäristö -käsite suhteessa lähikäsitteisiin). Käsitteiden tarkastelu paljastaa useita päällekkäisyyksiä käsitteiden sisällöissä. Osa päällekkäisyyksistä on kuitenkin puhtaasti teoreettisia ja tämän tutkimuksen aiheen kannalta epärelevantteja.



Kuva 6: *Kriittinen kybertoimintaympäristö -käsite suhteessa lähikäsitteisiin*

Kuvassa on käytetty seuraavia käsitteitä:

(1) yhteiskunnan elintärkeä toiminto, joka on riippuvainen kriittisestä kybertoimintaympäristöstä (1)
(2) yhteiskunnan elintärkeä toiminto, joka EI ole riippuvainen lainkaan kybertoimintaympäristöstä (2)
(3) muu kybertoimintaympäristöstä riippuvainen toiminto, (joka ei ole yhteiskunnalle elintärkeä toiminto) (3)

Edellä käsitellyn perusteella on *kybertoimintaympäristö*-käsitettä kuvattu liitteessä 3. (ks. Liite 3). Kuvauksessa on hyödynnetty käsitekaavion laatimisessa käytettävää kuvaustapaa sekä kuvan 6 apukäsitteitä. Liitteessä on kuvattu käsitteiden välisiä suhteita ja niiden sijoittumista toisiinsa nähden. Kuva ei sellaisenaan ole terminologinen käsitekaavio, mutta sen avulla on laadittu käsitteen *kybertoimintaympäristö* ja *kriittinen kybertoimintaympäristö* määritelmäehdotukset. Kuva auttaa myös lukijaa hahmottamaan nämä käsitteet. Jatkotutkimuksessa, sanastotyötä varten kuvasta voidaan muokata käsitekaavio.

Bilateraalinen sanasto määrittelee *критически важное киберпространство*-käsitteen:

> **критически важное киберпространство**
> [часть (элементы)] киберинфраструктуры и киберуслуг, которые необходимы для осуществления жизненно важных функций поддержания общественной безопасности, экономической стабильности, национальной безопасности и международной стабильности (Bilat 2014, 20).
>
> critical cyberspace
> is cyber infrastructure and cyber services that are vital to preservation of public safety, economic stability, national security and international stability (Bilat 2014, 20).

Venäjänkieliset käsitteet *киберинфраструктура* (kyberinfrastruktuuri) ja *киберуслуга* (kyberpalvelu) muodostavat laajemman kokonaisuuden: *критически важное киберпространство*(kriittisen kybertoimintaympäristön). Asiantuntijan mukaan *киберинфраструктура* (kyberinfrastruktuuri) viittaa käytännössä *informaatioinfrastruktuuriin* ja käsite *киберуслуга* puolestaan johonkin kybertoimintoympäristön toimintaan. Asiantuntijan mukaan käsitteitä *критически важное киберпространство* ja *critical cyberspace* voidaan pitää suomenkielisen *kriittinen kybertoimintaympäristö* -käsitteen vastineena. (Tuukkanen 2015.)

Pelkästään käsitepiirteitä vertaamalla on vaikea päätyä samaan johtopäätökseen, mutta taustaselvityksen perusteella ja erikoisalan asiantuntijan perustelut hyväksyen voidaan vahvistaa *kriittisen kybertoimintaympäristön* vastineeksi *критически важное киберпространство.*

Määritelmäehdotus viedään termitietueeseen:

> **kriittinen kybertoimintaympäristö**
> ru критически важное киберпространство
> määritelmä: kybertoimintaympäristön osa, joka on välttämätön yhteiskunnan elintärkeille toiminnoille
> huomautus: kriittiseen kybertoimintaympäristöön kohdistuvat uhkat ovat aina vaarallisia koko yhteiskunnalle.

5.7 *Yhteiskunnan elintärkeä toiminto* -käsite

Yhteiskunnan elintärkeä toiminto tai lyhyemmin e*lintärkeä toiminto* on keskeinen käsite kyberturvallisuudessa. Yhteiskunnan turvallisuusstrategia (YTS 2010) luonnehtii elintärkeitä toimintoja sellaisiksi, jotka on oltava turvattuna kaikissa tilanteissa (YTS 2010, 7) ja määrittelee *elintärkeät toiminnot* seuraavasti:

> Yhteiskunnan toiminnalle välttämätön toimintokokonaisuus: Elintärkeiden toimintojen turvaamisella ylläpidetään valtiollinen itsenäisyys, yhteiskunnan turvallisuus sekä väestön elinmahdollisuudet (YTS 2010, 85).

Suomessa tuetaan lainsäädännöllisesti poikkihallinnollista yhteistyötä eri viranomaisten kesken (YTS 2010, 29). Elintärkeitä toimintoja ovat seitsemän poikkihallinnollista ja yhteiskunnalle välttämätöntä toimintakokonaisuutta. Terminologian kannalta nämä käsitteet ovat hankalia, koska ne eivät ole keskenään rinnastettavissa. Osa niistä kuvaa ihmisen toimintaa ja osa puolestaan yhteiskunnan toimintoja. *Elintärkeät toiminnot* on määritelty luettelemalla nämä seitsemän toimintakokonaisuutta, joten yläkäsitteen näille kaikille pitäisi olla *toimintokokonaisuus*. Tässä on lueteltu elintärkeät toiminnot ja joihinkin on lisätty YTS:ssa annettu lisäselitys:

> *(1)valtion johtaminen* (YTS 2010, 19)
>
> (2) *kansainvälinen toiminta* (YTS 2010, 22): valtion toiminnan tasolla yhteydet muihin valtioihin, ulkomaankaupan ja elinkeinoelämän toiminnan turvaaminen
>
> (3) *Suomen puolustuskyky* (YTS 2010, 27)
>
> (4) *sisäinen turvallisuus* (YTS 2010, 29): tähän kuuluu Suomen ja sen väestöön kohdistuvien uhkien hallinta

> (5) *talouden ja infrastruktuurin toimivuus* (YTS 2010, 29): tarkoitetaan teknisiä rakenteita ja organisaatioita, jotka ovat välttämättömiä väestön elinmahdollisuuksille ja yhteiskunnan toimivuudelle
>
> (6) *väestön toimeentuloturva ja toimintakyky* (YTS 2010, 46)
>
> *(7) henkinen kriisinkestävyys* (YTS 2010, 51): kansakunnan kyky kestää turvallisuustilanteiden aiheuttamat henkiset paineet, selviytyä niiden vaikutuksilta ja nopeuttaa kriiseistä toipumista

Tässä ilmenee vaikeus, miten määritellä näiden seitsemän *yhteiskunnan elintärkeä toiminto* -käsitteen yläkäsite ja niiden käsitepiirteet. Nämä käsitteet on kirjattu tässä muodossa *Yhteiskunnan turvallisuusstrategiaan* (YTS 2010), joka on Valtioneuvoston periaatepäätös (VNpp 16.12.2010). Käytännössä sillä on sama vaikutus kielenkäyttöön kuin säädöskielellä, johon ei yleensä tehdä muutoksia vaan niissä käytetyt ilmaisut leviävät sellaisenaan kielenkäyttöön (KOTUS 2015). Tästä ilmiöstä voi olla esimerkkinä se, että Kokonaisturvallisuuden sanastossa (TSK 47) on samansisältöinen *elintärkeän toiminnon* määritelmä ja määritelmän jälkeen lisätty luettelona edellä mainitut seitsemän toimintoa (TSK 47, 21).

Vastinehaussa ilmeni, ettei Bilateraalisessa sanastossa ei ole määritelty vastaavaa käsitettä. Toinen havainto oli, että suomen kielellä käytetään ilmaisua *elintärkeä toiminto*. Vastaavasti Venäjällä keskiössä ovat *kriittisesti tärkeä kohde* (критически важный объект), jonka toiminnot on turvattava. Käsitteinä ne ovat erilaisia, toiminto on toimintakäsite ja kohde on oliokäsite. Tässä pohdittiin, voidaanko nämä katsoa kuuluviksi tapauksiin, joissa ”termit eivät vastaa toisiaan semanttisesti, mutta viittaavat kuitenkin samaan tilanteeseen eli laajempaan semanttiseen kokonaisuuteen, jolloin ne edustavat tilannevastaavuutta” (Vehmas-Lehto 2010, 368).

Venäläisissä asiakirjalähteissä esiintyy yleisemmin *жизненно важный* kuin *критически важный* -ilmaisu. Molempia voidaan pitää suomenkielisten käsitteiden *elintärkeä* tai *kriittisiä* vastineina.

Venäjällä kriittiset kohteet on lainsäädännöllisesti määritelty federaatiolaissa. (FZ 38). Sen mukaan *критически важный объект* -käsitteeseen kuuluvat ydinvoimalat, sähkölaitokset, tärkeät tuotantolaitokset ja muut joiden toiminnan keskeytyminen haittaa taloutta tai on muuten vaarallista (FZ 38).

Venäjän informaatiodoktriinista (DIBRF 2000) löytyi ilmaisu *жизненно важные функции общества и государства* (yhteiskunnalle ja valtiolle tärkeät toiminnot), mitä voitaisiin pitää elintärkeiden toimintojen vastineena varsinkin kun käsitteet sisällöllisesti viittaavat samaan ilmiöön. Asiakirjassa on myös käytetty ilmaisua *наиболее важные сферы жизни и деятельности общества и государства*, joka myös viittaa yhteiskunnan ja valtion tärkeimpiin toimintoihin (DIBRF 2000).

Yhteiskunnan elintärkeät toiminnot määritellään kansallisella tasolla. Eri valtioissa jaottelu- ja luokitteluperusteet voivat olla hyvin erilaisia, vaikka yleisellä tasolla kyse on saman ilmiön kuvaamisesta.

> **yhteiskunnalle elintärkeä toiminto**
> ru ~ жизненно важные функции общества и государства
> määritelmä: valtion johtaminen (2) kansainvälinen toiminta, (3) Suomen puolustuskyky, (4) sisäinen turvallisuus (5) talouden ja infrastruktuurin toimivuus, (6) väestön toimeentuloturva ja toimintakyky ,(7) henkinen kriisinkestävyys

5.8 Kriittinen infrastruktuuri, kriittinen tuotanto, kriittiset palvelut

Käsitteet *kriittinen infrastruktuuri, kriittinen tuotanto ja kriittiset palvelut ja* liittyvät läheisesti toisiinsa, joten ne analysoidaan tässä jaksossa rinnakkain. Kokonaisturvallisuuden sanaston määritelmä käsitteelle *kriittinen infrastruktuuri*:

> perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. Kriittiseen infrastruktuuriin kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja. Muun muassa energian tuotanto-, siirto- ja jakelujärjestelmät, liikenne ja logistiikka, tieto- ja viestintäjärjestelmät sekä vesi- ja jätehuolto ovat osa kriittistä infrastruktuuria (TSK47, 51).

Tässä huomataan, että käsitteet *kriittinen tuotanto, kriittiset palvelut* ja *kriittinen infrastruktuuri* ovat lähikäsitteitä toisilleen. Suomen kielessä käytetään vaihtelevasti ja toistensa synonyymeina käsitteitä *kriittinen, välttämätön ja elintärkeä.* On todennäköistä, että *kriittinen*-käsite on tullut käyttöön englannin kielestä, kuten *critical infrastructure* (TSK47, 51). Tässä tutkielmassa noudatetaan niitä muotoja, joissa ne asiakirjoissa esiintyvät.

Yhteiskunnan turvallisuusstrategiassa (YTS 2010) ei ole määritelmää *infrastruktuuri*-käsitteelle, mutta asiakirjassa todetaan, että ”infrastruktuurin ylläpitämisellä

tarkoitetaan niitä teknisiä rakenteita ja organisaatioita, jotka ovat välttämättömiä väestön elinmahdollisuuksille ja yhteiskunnan toimivuudelle” (YTS 2010, 36).

Suomen turvallisuus- ja puolustuspolitiikka 2012 (VNK 5/2012) toteaa *kriittisestä infrastruktuurista* seuraavaa: ”nykyaikainen yhteiskunta ja sen rakenteet ovat riippuvaisia kriittisestä infrastruktuurista, johon kuuluu muuan muassa liikenne, viestintä ja energiahuolto” (VNK 5/2012, 11). Myös seuraavasta tekstiotteesta ilmenee kuinka tärkeä merkitys *kriittisellä infrastruktuurilla* on nykyajan tietoyhteiskunnassa:

> Lähes kaikki yhteiskunnan kriittiset toiminnot ja palvelut perustuvat teknisten, erityisesti sähköenergian ja tietoliikenteen varassa toimivien järjestelmien käyttöön, ja yhteiskuntaan laajasti vaikuttavien häiriöiden riski kasvaa (VNK 5/2012, 11–12).

Suomen turvallisuus- ja puolustuspolitiikan selonteosta:

> Modernit verkostoihin perustuvat yhteiskuntarakenteet ovat yhä riippuvaisempia kriittisestä infrastruktuurista, johon kuuluvat muun muassa liikenne, viestintä ja energiahuolto. Samaan aikaan tämän infrastruktuurin haavoittuvuus lisääntyy. Käytännössä lähes kaikki yhteiskunnan kriittiset toiminnot ja palvelut perustuvat teknisten, erityisesti sähköenergian ja tietoliikenteen varassa toimivien järjestelmien käyttöön. Langattoman tiedonsiirron yleistyessä ja järjestelmien verkottuessa yhteiskuntaan laajasti vaikuttavien häiriöiden riski muodostuu yhä vakavammaksi. (VNK 5/2012, 21.)

Huoltovarmuustoiminnan tavoitteena on turvata yhteiskunnan toimivuuden kannalta välttämätön infrastruktuuri ja kriittinen tuotanto sekä normaaliolojen vakavissa häiriöissä että poikkeusoloissa (VNK 5/2012, 93). Huoltovarmuuskeskuksen internetsivustolla on käytetty seuraavia käsitteitä *kriittinen teollisuustuotanto* ja *kriittinen teollisuus*, joiden tehtävä on tuottaa hyödykkeitä ja palveluja yhteiskunnan elintärkeiden toimintojen turvaamiseksi (HVK 2015). Huoltovarmuuskeskuksen sanastosta löytyi käsite *kriittiset materiaalit*, joka on määritelty näin: tuotannon jatkamiselle välttämättömiä raaka-aineita ja tarvikkeita (HVK 2015). Tässä havaittiin, että nämä käsitteet kuuluvat huoltovarmuustoimijoiden käsitteistöön. Käsitteistö ei näin ollen ole tarkasti rajattavissa, vaan samat käsitteet voivat kuulua toiseen läheisen alan erikoisalan käsitteistöön.

Suomen kyberturvallisuusstrategiassa (2013) ei ole määritelty käsitettä *kriittinen tuotanto*. Huoltovarmuuskeskuksen käsiteanalyysiraportti (Hagelstam 2005)

tarkastelee muun muassa miten *kriittinen infrastruktuuri* on määritelty. Sen mukaan käsite on syntynyt yhteiskunnan muuttuessa tietoyhteiskunnaksi, jossa eri infrastruktuurisektorit ovat vahvasti toisiinsa sidoksissa. Kaikki *infrastruktuuri* ei ole kriittistä, mutta ne yhteiskunnalliset toiminnot, jotka ovat mahdollisia infrastruktuurin ansiosta ovat *kriittisiä* (Hagelstam 2005, 17). *Kriittinen infrastruktuuri*- käsitteeseen liitetään kaikki yhteiskunnalliset toiminnot mukaan lukien *tietotekniset infrastruktuurit* (Hagelstam 2005, 14). Tuolloin ei vielä oltu tehty käsitteellistä eroa *kriittisen infrastruktuurin* ja *kriittisen informaatioinfrastruktuurin* käsitteiden välillä.

Seuraava tekstiote vahvistaa käsitystä, että *kriittinen infrastruktuuri* -käsite saa hyvin erilaisia määritelmiä kansallisella tasolla. Seuraavassa tekstiotteessa arvioidaan englanninkielistä c*ritical infrastructure* -käsitettä:

> Se mitä aloja ja toimintoja käsite sisältää, vaihtelee eri maissa. Useimmilla mailla on kriittisestä infrastruktuurista tarkka määritelmä, jossa ilmenee sen tärkeys yhteiskunnalle, siihen kohdistuvat uhkat, sen eri osat ja sektorit sekä usein myös tapa, jolla sitä turvataan. Määritelmä on yleensä syntynyt uuden, sisäistä turvallisuutta koskevan lainsäädännön yhteydessä. (MPKK 2013, 175.)

Seuraavaksi tarkastellaan käsitettä *kriittinen tuotanto*. Kyberturvallisuusstrategian mukaan yhteiskunnan elintärkeisiin toimintoihin voidaan toteuttaa kyberiskuja teollisuustuotanto- ja ohjausjärjestelmissä. Teollisuustuotannossa käytettävä ohjelmoitava logiikka on haavoittuvaa, ja siksi ovat mahdollisia hyökkäyskohteita juuri kybertoimintaympäristössä (Kyberstrategia 2013, 8). Yhteiskunnan toiminnalle elintärkeä tuotanto eli *yhteiskunnan kriittiset tuotantoprosessit* ovat entistä riippuvaisempia automaatiojärjestelmistä (Kyberstrategia 2013, 25*)*.

Kokonaisturvallisuussanaston (TSK 47) *huoltovarmuus*-käsitteen määritelmässä käytetään käsitteitä *välttämätön tuotanto, palvelut* ja *infrastruktuuri*:

> huoltovarmuustoiminta, jonka tarkoituksena on turvata väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämätön tuotanto, palvelut ja infrastruktuuri vakavien häiriötilanteiden ja poikkeusolojen varalta (TSK 47, 49).

Tässä määritelmässä ei käytetä *yhteiskunnalle elintärkeä toiminto* -käsitettä, mutta sanaston käyttämä *välttämätön tuotanto*-käsite (TSK 47, 49) viittaa samaan käsitteeseen kuin Kyberstrategiassa käytetty *yhteiskunnan kriittiset tuotantoprosessit*

(Kyberstrategia 2013, 25). *Väestön toimeentulo* (YTS 2010, 43) on yksi elintärkeistä toiminnoista. Myös viittaukset talouselämään ja infrastruktuuriin (YTS 2010,34) tukevat olettamusta, että kyse on nimenomaan yhteiskunnalle elintärkeistä toiminnoista.

Kokonaisturvallisuuden sanaston (TSK 47) määritelmät käsitteille *kriittinen tuotanto ja kriittiset palvelut:*

> **kriittinen tuotanto (**critical production) - tuotanto, joka on välttämätön yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi (TSK 47, 50).
>
> **kriittiset palvelut (**critical services) - palvelut, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi (TSK 47, 51).

Molemmille on annettu samanlaisen määritelmän lisäksi samanlainen lisäselvennys:

> Kriittiseen tuotantoon kuuluvat elintarvikehuoltoa, terveydenhuoltoa, peruspalveluita, teollisuutta ja sotilaallista maanpuolustusta tukeva tuotanto (TSK 47, 50).
>
> Kriittisiin palveluihin kuuluvat elintarvikehuoltoa, terveydenhuoltoa, peruspalveluita, teollisuutta ja sotilaallista maanpuolustusta tukevat palvelut (TSK 47, 51).

Analysoidut kolme käsitettä kuuluvat läheisesti *yhteiskunnan elintärkeisiin toimintoihin.* Niiden avulla voidaan kuvata *kybertoimintaympäristöä* ja ne auttavat hahmottamaan käsitteiden välisiä suhteita käsitekaaviossa, vaikkakaan eivät kybertoimintaympäristön kannalta ole keskeisimpiä käsitteitä. Ongelmallista kuitenkin, ettei käsitteillä ole erottavia piirteitä, joten niiden sijoittaminen toistensa suhteen on vaikeaa.

Venäjänkielisen vastineen haussa etsittiin tietoa vastaavista venäjänkielisistä käsitteistä. Löytyi suomenkielisiä tutkimuksia, joista toisessa tarkastellaan venäläiseen kriittiseen infrastruktuuriin liittyviä käsitteitä (Pynnöniemi 2013) ja toisessa on tarkasteltu kriittiseen infrastruktuuriin läheisesti kuuluvaa *kokonaisturvallisuuden* käsitettä (Heusala 2011). Tutkimustulokset ovat hyvin samankaltaisia sen kanssa, mitä tässä tutkimuksessa on selvinnyt käsiteanalyysin avulla. Käsitteet ovat merkitykseltään epämääräisiä ja sen verran laajoja, että tässä

tutkimuksessa niitä voidaan käsitellään vain päällisin puolin. Niiden tarkempi tutkimus on jätettävä jatkotutkimukseen.

Venäjänkielistä vastinetta etsittiin Bilateraalisesta sanastosta (Bilat 2014), jossa määritelty *критически важная киберинфраструктура* (kriittinen kyberinfrastruktuuri) seuraavasti:

> **критически важная киберинфраструктура**
> киберинфраструктура, которая необходима для, осуществления жизненно важных функций, поддержания общественной безопасности, экономической стабильности, национальной безопасности, международной стабильности, а также для поддержания работоспособности и функций эффективного восстановления [критически важного киберпространства] (Bilat 2014, 21)

Määritelmän mukaan *критически важная киберинфраструктура* (kriittinen kyberinfrastruktuuri) on välttämätön elintärkeiden toimintojen ylläpitämiselle, yhteiskunnan turvallisuudelle, talouden vakaudelle, kansalliselle turvallisuudelle, kansainvälisen vakauden toteuttamiselle sekä myös toimintojen ylläpitämiselle ja (kriittisen kybertoimintaympäristön) toimintojen palauttamiselle. Kyberinfrastruktuuri on siis se osa kybertoimintaympäristöä, jonka toiminnot halutaan ylläpitää kaikissa mahdollisissa olosuhteissa. Johtopäätöksenä voidaan todeta, että käsitteiden *kriittinen kyberinfrastruktuuri* ja *kriittinen infrastruktuuri* ja *kriittinen kybertoimintaympäristö* merkitysalat ovat osittain päällekkäisiä.

Bilateraalisessa sanastossa on määritelmät venäjän- ja englanninkielisille käsitteille:

> **киберсервисы** – (услуги, службы), различные виды обмена данными в киберпространстве для прямой или косвенной пользы людям (Bilat 2014, 19).
>
> **cyber services** – are a range of data exchanges in cyberspace for the direct or indirect benefit of humans (Bilat 2014, 19).

Näissä määritelmissä palveluita ei liitetä elintärkeisiin toimintoihin. Määritelmä toteaa palvelujen olevan suoraan tai välillisesti ihmisen käyttöön tarkoitettuja, ja ne toteutetaan kybertoimintaympäristössä. Määritelmä ei yksilöi eikä anna tietoa palvelujen merkityksestä yhteiskunnalle.

Venäjän informaatiodoktriinissa (DIBRF 2000) käytetään useamman kerran ilmaisua *экономически важное производство* (taloudellisesti tärkeä tuotanto), joten siitä

voidaan johtaa suomenkielisen *kriittisen tuotannon* vastineeksi *критически важное производство*. Jatkotutkimukseen jää *экономически важное производство* -käsitteen syvällisempi tarkastelu, silloin selviäisi onko se *kriittinen tuotanto* -käsitteen alakäsite.

5.9 Informaatioinfrastruktuuri ja kriittinen informaatioinfrastruktuuri

Suomen kyberturvallisuusstrategiassa (Kyberstrategia 2013) on annettu tämä määritelmä käsitteelle *informaatioinfrastruktuuri:*

> Informaatioinfrastruktuurilla tarkoitetaan tietojärjestelmien perustana olevia rakenteita ja toimintoja, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely (Kyberstrategia 2013, 12).

Kriittisen informaatioinfrastruktuuri -käsitteen määritelmä on:

> Kriittisellä informaatioinfrastruktuurilla tarkoitetaan yhteiskunnan elintärkeiden toimintojen tietojärjestelmien perustana olevia rakenteita ja toimintoja, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely (Kyberstrategia 2013, 12).

Kriittisen informaatioinfrastruktuuri-käsitteen perustana olevat tietojärjestelmät liittyvät elintärkeisiin toimintoihin. Sen sijaan *informaatioinfrastruktuuri* on yläkäsite, joka ei rajaudu pelkästään *kriittiseen kybertoimintaympäristöön*. Määritelmät *informaatioinfrastruktuurille* ja *kriittiselle informaatioinfrastruktuurille* eroavat vain jälkimmäiseen tehdyllä lisäyksellä elintärkeät toiminnot, joka on käsitteiden toisistaan erottava käsitepiirre.

Kyberstrategian taustamuistiossa todetaan, että tietojärjestelmiin kohdistuvat hyökkäykset aiheuttavat tietoteknisten laitteiden ja järjestelmien toimimattomuuden ja pahimmillaan seurauksena voi olla informaatioinfrastruktuurin luhistuminen (Kyberstrategia 2013, 17).

Kyberstrategia mainitsee käsitteen *kriittinen informaatioinfrastruktuuri* samassa yhteydessä kun toteaa EU:n valmistelevan ohjeita ja direktiivejä *kriittisen informaatioinfrastruktuurin* suojelemiseksi (Kyberstrategia 2013, 28).

Pekka Neittaanmäki, Jyväskylän yliopiston informaatioteknologian tiedekunnan professori, määrittelee *informaatioinfrastruktuuri*-käsitteen näin:

> Yhteiskunnan kriittinen infrastruktuuri muodostuu niistä välineistä ja laitteista, palveluista ja tietojärjestelmistä, jotka ovat maalle elintärkeitä. Kiinteän tietoliikenneverkoston avulla kriittinen infrastruktuuri muodostaa verkottuneen kokonaisuuden (Neittaanmäki 2014).

Nykyajan tietojärjestelmiin perustava yhteiskunta ei toimi ilman tietojärjestelmiä, joista on muodostunut osa kriittistä infrastruktuuria, jotka verkottavat rakenteet ja palvelut kokonaisuudeksi (Neittaanmäki 2014).

Käsiteanalyysissa ilmeni ongelma käsitteiden laajuudessa ja määritelmissä. Käsitteiden *kriittinen kybertoimintaympäristö* ja *kriittinen informaationinfrastruktuuri* merkityksen alat leikkaavat toisensa, joten niiden merkitys on osittain päällekkäinen. *Kriittinen kybertoimintaympäristö* muodostuu tietojärjestelmistä ja *kriittinen informaatioinfrastruktuuri* on tietojärjestelmien perustana olevat perusrakenteet.

Kriittinen kybertoimintaympäristö näyttäisi tässä suhteessa määritelmänsä puolesta olevan suppeampi käsite kuin *kriittinen informaatioinfrastruktuuri*, vaikka on ilmeistä että asia on juuri päinvastoin. Tämän analyysin perusteella näyttäisi, että määritelmät tarvitsevat tarkentamista.

Tarkastellaan seuraavaksi venäjänkielistä vastineita. Bilateraalisessa sanastossa ei ole kumpaakaan käsitettä. Venäjän konventiossa (SBRF 2011) on määritelty käsite *информационная инфраструктура* (informaatio infrastruktuuri):

> **информационная инфраструктура** - совокупность технических средств и систем формирования, преобразования, передачи, использования и хранения информации (SBRF 2011).

Määritelmä GOST 7.0-99 -standardin mukaan:

> **информационная инфраструктура** - совокупность информационных центров, банков данных и знаний, систем связи, обеспечивающая доступ потребителей к информационным ресурсам (GOST 7.0-99)

Myös toisessa GOST-standardissa määritelmä on hyvin samansisältöinen, joten termi näyttää olevan vakiintunut asiakirjoissa (GOST 53114). Kun venäjänkielisiä

määritelmiä verrataan suomenkielisiin, niin havaitaan niiden olevan hyvin samansisältöisiä. Näin ollen, *информационная инфраструктура*-käsitettä voidaan pitää suomenkielisen *informaatioinfrastruktuuri*-käsitteen vastineena.

Asiakirjalähteissä on *критическая информационная инфраструктура* -käsite(SB 2014b ja SB 2014a.), mutta ilman määritelmää.

Federaatiolaissa koskien kriittisen informaatioinfrastruktuurin turvallisuutta (FZ 2013) käsite *критическая информационная инфраструктура (КИИ) РФ* on määritelty Venäjän valtion kontekstissa. Seuraavassa tekstiotteessa määritelmä:

> **критическая информационная инфраструктура (КИИ) РФ**
> совокупность автоматизированных систем управления КВО (КВО критически важный объект) и обеспечивающих их взаимодействие информационно- телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий; (FZ 2013.)

Tämän määritelmän mukaan Venäjän federaation *kriittinen informaatioinfrasstruktuuri* on kriittisesti tärkeiden kohteiden ja automatisoitujen ohjausjärjestelmien muodostama kokonaisuus, jonka avulla turvataan valtion tietojärjestelmien ja telekommunikaatioverkkojen toiminta. Sen lisäksi luetellaan suomalaisiin elintärkeisiin toimintoihin rinnastettavia toimintoja, kuten puolustuskyky, oikeusjärjestyksen ja turvallisuuden ylläpito, joiden toiminta on turvattava.

Venäjän federaatiolakiin (FZ 2013) on tehty vuoden 2015 alussa voimaan tulevia lisäyksiä, joissa mm. rikkomukset katsotaan kuuluvat rikoslain alaisuuteen ja rikkomuksista voi saada enimmillään 10 vuoden vankeustuomion. Erot suomalaisen ja venäläisen määritelmän välillä on se, että suomalainen määritelmä rajaa yleisellä tasolla elintärkeät toiminnot kriittisen infrastruktuurin piiriin, kun taas venäläisen määritelmä ottaa mukaan valtion sotilaallisen puolustuskyvyn turvaamisen sekä asettaa rikkomukset rikosoikeuden alaisiksi. (FZ 2013.)

> **informaatioinfrastruktuuri**
> ru информационная инфраструктура

määritelmä: tietojärjestelmien perustana olevat rakenteet ja toiminnot, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely

kriittinen informaatioinfrastruktuuri
ru критическая информационная инфраструктура
määritelmä: elintärkeiden toimintojen tietojärjestelmien perustana olevia rakenteita ja toimintoja, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely

5.10 *Kyberhyökkäys*-käsite

Kyberhyökkäykset voivat muodostaa nopeasti koko yhteiskuntaa koskevia laaja-alaisia vakavia kriisejä, joita voidaan luoda ilman suoranaista aseellista voimaa. Ja kybertilan häiriöt muodostavat kriittisen uhkatekijän, sillä laajat tietoverkot ovat herkkiä ja voivat vahingoittua tahattomistakin toimintahäiriöistä kaiken lisäksi niiden alkuperän selvittäminen on vaikeaa (VNK 5/2012, 24).

> Kyberkysymykset ovat keskeisessä asemassa sotilaallisen turvallisuuden ja yhteiskunnan elintärkeiden toimintojen kannalta. Kybertoimintaympäristössä on siirrytty uuteen aikakauteen, jossa haittaohjelmien avulla teollisuusautomaation ja ohjelmoitavan logiikan kautta kyetään vaikuttamaan kaikkiin yhteiskunnan elintärkeisiin toimintoihin. Maailmalla tapahtuva kehitys kybertoimintaympäristössä lisää uusien uhkien mahdollisuutta. Myös Suomi on jo joutunut sekä sisäisten että ulkoisten kyberoperaatioiden kohteeksi (VNK 5/2012, 24)

Sodankäynti on saanut uusia muotoja perinteisten rinnalle kuten informaatio- ja kybersodankäynti. Varsinkin länsimaissa tietojärjestelmien käytöllä on huomattava osuus yhteiskunnan toiminnoista, joten siksi ne myös ovat erittäin haavoittuvia. (VNK 5/2012, 39.)

Bilateraalissa sanastosta (Bilat 2014) löytyy venäjänkielinen käsite *кибератака* ja sen englanninkielinen vastine *cyber attack,* joiden määritelmä on seuraava:

> **кибератака** – наступательное использование кибероружия с целью нанесения вреда определенной цели (Bilat 2014, 44).

> **cyber attack** – is an offensive use of cyber weapon intended to harm a designated target (Bilat 2014, 44).

Huomionarvoista on, että *kyberhyökkäys*-käsitteen käyttö määrittyy käytettävien vaikutuskeinojen, ei kohteen eikä tekijän mukaan: ”A cyber attack is defined by the weapon type and not the nature of the target” (Bilat 2014,44).

Asiantuntijan mukaan usein käytetään *kyberhyökkäys*-käsitettä vaikka oikeampi olisi *kyberhäiriötilanne* (Tuukkanen 2015) Lehdistössä *kyberhyökkäys*-käsite on yleisesti käytetty. Viranomaisdiskurssissa sen sijaan käytetään kyberhäiriötä (Tuukkanen 2015). Tämä selittynee sillä, että *hyökkäys*-sanalla on selkeästi kansainvälisoikeudellinen merkitys. Kyberhyökkäyksiä on tarkasteltu kansainvälisen oikeuden ja politiikan näkökulmista sekä esitetty toimenpiteitä Euroopan Unionin kyberturvallisuuden kehittämiseksi. (Klimburg & Tirmaa-Klaar 2011.) *Kyberhyökkäys*-käsitteen analysointi jätetään jatkotutkimukseen sen moniulotteisuuden takia (vrt. Gandhi ym.).

5.11 Käsiteanalyysin tulokset

Tietoturvallisuus-käsite on vakiintunut suomenkielellä ja samoin kuin sen vastineet venäjän ja englannin kielillä. Käsitteet myös määritellään samoilla tietotekniikan alalla käytetyillä tiedon käsitepiirteillä (saatavuus, luottamuksellisuus, eheys). Analyysissa kävi ilmi, ettei suomenkielinen *tietoturvallisuus*-käsite tarvitse lisätarkennusta, sillä se sisältää sisäänrakennettuna ajatuksen teknisen palvelujärjestelmän toimintavarmuudesta. (vrt. information (data) security; безопасность информации [данных]) Tämän havainnon vahvisti myös asiantuntija. (Tuukkanen 2015)

Tietotekniikan alalla *haavoittuvuus*-käsite on vakiintunut peruskäsite, jolla on keskeinen merkitys *tietoturvallisuus*-käsitteen määrittelyssä. Sitä pidetään yleisesti *tietoturva-aukko*-käsitteen synonyymina (TSK 31, 14). *Haavoittuvuus* on alttius tai heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa” (TSK 31, 14). *Haavoittuvuus*-sana on esimerkki siitä, miten yleiskielen sana on eriytynyt erikoiskieleen ja siitä on tullut tietotekniikan alalla käytettävä termi. Myös *haavoittuvuuden* venäjänkielinen vastine *уязвимость*-käsite on vakiintunut tietotekniikan alalla. Bilateraalisesta sanastosta löytynyt *киберуязвимость*-käsite (Bilat 2014, 57) ei ole käytössä venäjänkielisissä lähteissä,

eikä myöskään suomen kielellä käytetä muotoa *kyberhaavoittuvuus* (Tuukkanen 2015).

Suomenkielisen *kyberturvallisuus*-käsitteen (Kyberstrategia 2013, 13) määritelmä ei anna käsitteen tarkkaa kuvausta, vaan jättää varaa tulkinnalle. Havaittiin, että *kyberturvallisuus*-käsitteen määritelmät eri kielissä eivät ole yhteneväisiä ja määritelmät ovat epämääräisiä (CCDCOE 2015d). *Kyberturvallisuus*-käsite on vaikea määritellä tarkkarajaisesti, sillä se kuvaa laaja-alaisia yhteiskunnallisia ilmiötä. Laaja-alaisuus ja tarkka-rajaisuus eivät sinänsä ole ristiriidassa tai toisiaan poissulkevia. *Kyberturvallisuus*-käsitteen tarkka rajaus on haasteellista, sillä käsitteistö uutta eivätkä käsitteiden merkitykset vielä ole tarkentuneet. Epämääräisyys antaa mahdollisuuden lisätä uusia käsitepiirteitä käsitteeseen.

Kyberturvallisuus-käsitteen määrittelyyn vaikuttaa myös kunkin valtion näkemys internetin vapaudesta, valtiollisesta suvereniteetista ja kansallisesta turvallisuudesta (Tietosuoja 2/2015; Kornev 2015; SF 2014a, 2; MID 2013; DIBRF 2000; Tuukkanen 2013.). Venäjällä *кибербезопасность*-käsitettä ei vielä ole virallisesti vahvistettu, sillä Venäjän kyberturvallisuusstrategia on vielä luonnoksen asteella. Venäläisissä asiakirjoissa ei juurikaan esiinny *кибер*-etuliitteellä muodostettuja sanoja, vaan yleisimmin on edelleen käytössä *информационная безопасность.* Luonnoksen mukaan Venäjällä ei tehdä eroa käsitteiden *кибербезопасность* ja *информационная безопасность* välillä (SF 2014a). *Информационная безопасность* -käsite on keskeinen Venäjän turvallisuusdiskurssissa. Käsitteen merkityksen selvittäminen vaatisi laajemman analyysin Venäjän turvallisuusneuvoston internetsivustolla julkaistuista seitsemästä ohjausasiakirjasta (SBRF 2011). Vastinehaussa olisi huomioitava suomen- ja venäjänkielisten turvallisuuskäsitteistön näkökulmaerot. Erityistä huomiota tulisi kiinnittää käsitteiden *tietoturvallisuus* ja *informaatioturvallisuus* merkityksiin.

Kyberuhka rinnastetaan tietoliikenteen ja tietojärjestelmien vakavaksi häiriöksi. *Kyberuhka* voi olla tietoturvauhka, mutta aina se ei ole (ks. Kuva 5, jakso 5.3). Kyse voi olla tahallisesta teosta tai tahattomasti aiheutuneesta ((YTS 2010, 67; Kyberstrategia 2013, 13; VNK 5/2012, 2).

Kyberuhka-käsite eroaa *tietoturvauhka*-käsitteestä siten, että jälkimmäinen on merkitykseltään suppeampi ja se kohdistuu tietoon. Suomenkielisissä asiakirjoissa kuvattu *kyberuhka* kohdistuu yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin tai kansalaisiin. *Kyberuhka* vaarantaa kybertoimintaympäristöstä riippuvaisen toiminnon (Kyberstrategia 2013, 13).

Suomen kyberstrategiassa on lueteltu kyberuhkia kuten *kyberaktivismi* (aktivismi on kansalaistoimintaa ja se katsotaan kansalaisyhteiskunnassa positiiviseksi toiminnaksi, eikä sitä ole kriminalisoitu); kybervandalismi (vandalismi ei kuulu viranomaisdiskurssin lainkaan vaan se esiintyy pikemminkin lehdistön kirjoituksissa); *kyberrikollisuus; kybervakoilu*; *kyberterrorismi* (rikollisuus, vakoilu ja terrorismi ovat rikoslain alaisia); kyberoperaatiot (kuuluu sotilaalliseen diskurssiin). Näin ollen näyttäisi, että *kyber*-etuliitteen kanssa on muodostettu yhdyssanoja kovin heppoisin perustein.

Kyberuhka-käsitettä käytetään yleisemmin kuin käsitettä *kyberriski. Kyberriski*-käsitteen määritelmä Suomen kyberturvallisuusstrategiassa muistuttaa pikemminkin *kyberuhka*-käsitettä. Käsitteiden *kyberuhka* ja *kyberriski* suomenkieliset määritelmät tulisi tarkistaa ja päivittää sekaannusten välttämiseksi. Sekä *kyberuhkan* että *kyberriskin* käsiteanalyysin perusteella on ilmeistä, että Kyberturvallisuusstrategian (Kyberstrategia 2013) kuvaamassa käsitejärjestelmässä on puutteita.

Kybertoimintaympäristö-käsite viittaa hyvin laajaan kokonaisuuteen, johon kuuluvat tietojärjestelmät, ihmiset ja ohjelmat. Kybertoimintaympäristö on yhtä aikaa kansallinen sekä globaali toimintaympäristö, joka yhdistää valtioita, yrityksiä ja kansalaisia reaaliajassa (Kyberstrategia 2013, 17). Näyttää olevan riidatonta, että kybertoimintaympäristöön kohdistuvat uhkat ovat koko yhteiskunnalle vaarallisia. Sitä vastoin näkemyseroja on katsotaanko kybertoimintaympäristön olevan globaali, kansallisvaltioiden rajat ylittävä toimintaympäristö. On ymmärrettävää, että valtiot haluavat säilyttää kansallisen päätäntävallan lainsäädännön ja toimeenpanovallan suhteen myös kybertoimintaympäristössä. Tämä selittää myös miksi käsite on kiinteästi sidoksissa kokonaisturvallisuuteen. Venäläisistä lähteissä *киберпространство*-käsite määritellään ainoastaan Venäjän kyberstrategian luonnoksessa ja silloinkin kiinteästi *информационная безопасност* -käsitteeseen kuuluvaksi. (SF 2014a.)

Kybertoimintaympäristö-käsitteen määrittelyä selkeyttäisi, jos määrittelyssä käytettäisiin *informaatioinfrastruktuuri*-käsitettä, joka on olennainen osa *kybertoimintaympäristöä.* Tämän tutkimuksen termiehdotus on *kriittinen kybertoimintaympäristö* -käsite, jonka avulla voidaan erottaa kybertoimintaympäristöstä se osa, joka on yhteiskunnan elintärkeille toiminnoille *välttämätön kybertoimintaympäristö.* Asiantuntijan arvio termiehdotuksesta oli myönteinen.

Yhteiskunnan elintärkeä toiminto -käsite on keskeinen käsite kyberturvallisuuden määrittelyssä. Käsite määritellään sisällöllisesti eri tavalla eri valtioissa, sillä käsitteen sisältö heijastelee kansallista turvallisuuspolitiikkaa. Kyseessä on yhteiskunnallisesti sama ilmiö. Yhteiskunnassa on tiettyjä toimintoja, jotka on turvattava kaikissa olosuhteissa. Venäjällä kriittiset kohteet luokitellaan tärkeyden mukaan ja niiden toiminta on turvattava. (vrt. elintärkeät toiminnot).

Suomalaisen näkemyksen mukaan yhteiskunnan elintärkeisiin toimintoihin kuuluvat esimerkiksi sisäinen turvallisuus, Suomen puolustuskyky ja henkinen kriisinkestävyys. Venäjän *информационная безопасность* -käsitteen alle kuuluvat seitsemän asiakirjaa käsittelevät laajasti kokonaisturvallisuutta. Asiakirjoissa kuvatut ilmiöt vastaavat osittain Suomen kyberturvallisuusstrategiassa (2013) kuvattuja elintärkeitä toimintoja.

Kriittinen infrastruktuuri -käsite käsittää kaikki yhteiskunnalle elintärkeät perusrakenteet ja toiminnot, mukaan lukien tietotekniset informaatioinfrastruktuurit. Se mitä aloja ja toimintoja käsite kussakin valtiossa sisältää, vaihtelee eri maissa. Kriittiseen infrastruktuuriin kuuluu kriittinen tuotanto ja kriittiset palvelut. Käsiteanalyysissä ilmeni myös, että käsitteiden *kriittinen kyberinfrastruktuuri, kriittinen infrastruktuuri, kriittinen kybertoimintaympäristö* merkitykset leikkaavat toisensa. Suomalaisten käsitteiden venäjänkielisiksi vastineiksi voidaan hyvin valita *критически важная инфраструктура, критически важные услиги* ja *критически важное производство*.

Informaatioinfrastruktuuri ja *kriittisen informaatiostruktuuri* käsitteiden erottava käsitepiirre on niiden suhde elintärkeisiin toimintoihin. Venäläisen vastineen

информационная инфраструктура -käsitteen määritelmä on hyvin samansisältöinen.

Tutkimuksessa havaittiin, että asiakirjalähteissä esiintyy suuri määrä käsitteitä, joille ei löydy määritelmiä eikä niiden merkitys selviä asiakirjan tekstissä. Epäselväksi jää oletetaanko kohderyhmän tietävän asiakirjoissa käytettyjen termien merkitys. Myöskään ei ole tiedossa ovatko ne määritelty jossain toisessa esimerkiksi julkaisemattomassa asiakirjassa. Suomen kyberturvallisuusstrategiassa (Kyberstrategia 2013) ja sen taustamuistiossa on runsaasti *kyber*-etuliitteen kanssa muodostettuja sanaliittoja. Vain muutamalle niistä on annettu määritelmä ja muutamaa käsitellään tekstissä siten, että niiden merkitys selviää. Strategiassa todetaan, että *kyber*-etuliitteen muodostama yhdyssanan sisältö ”liittyy yleensä sähköisessä muodossa olevan informaation (tietojen) käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tieto- ja tietokonejärjestelmiin ” (Kyberstrategia 2013, 4). Tämä väittämä ei aina kuitenkaan toteudu *kyber*-etuliitteellä muodostetuissa käsitteissä.

Tähän on koottu Suomen kyberturvallisuusstrategiassa (2013) esiintyviä käsitteitä, joita ei asiakirjassa ole selitetty. Käsitteen jälkeen on suluissa Kyberstrategian sivunumero (Kyberstrategia 2013). Käsite on siinä muodossa kuin se on lähdetekstissä:

> kyber /tietoturvakurssi (18); kyberosaamisklusteri (31); kyberharjoitustoiminta (32); kyberriskianalyysi (36) ja kyberkyky (97).

Osa termeistä on selvästi muodostettu sotilasalan tai turvallisuusviranomaisten termeistä *kyber*-etuliitteen avulla, kuten:

> kyberhyökkäysmuoto (4); kyberpuolustuskyky (8); kyberoperaatio (17); kybervakoilu (17); kyberisku (18); kyberloukkaus (24); kybervaikuttaminen (28); kybertiedustelu (28), kyberpuolustus (29); kyberkonflikti (30); kyberselkkaus (33); kyberhyökkäys (33) ja kybervaikutuskeino (35).

Näiden lisäksi on useita yhdyssanoja, jotka voivat olla *kybertoimintaympäristö*-käsitteen variaatioita, kuten *kyberympäristö* (25) ja *kybermaailma* (17). Lisäksi on joukko eri toimialojen käsitteitä, joihin on lisätty *kyber*-etuliite:

> kyberturvallisuusklusteri (26); kyberturvallisuustoiminta (29); kyberturvallisuusyhteistyö (30); kyberturvallisuuskeskustelu (30); kyberturvallisuusliiketoiminta (31); kyberturvallisuusprosessi (39) ja kyberturvallisuustoimenpiteet (36).

Kyberhäiriötilanne-käsite esiintyy 11 kertaa Kyberturvallisuusstrategian taustamuistiossa, jossa sille ei kuitenkaan anneta määritelmää tai tarkennusta. (Kyberstrategia 2013.) *Suomen turvallisuus- ja puolustuspolitiikka 2012*-asiakirjasta löytyi käsitteet *kybertila* (VNK 5/2012, 21 ja *kyberulottuvuus* (VNK 5/2012, 37). *Kyberavaruus*-käsitettä ei esiinny viranomaisten asiakirjoissa. (ks. kybertoimintaympäristö)

Havaitaan, että käsitteitä käytetään asiakirjoissa, mutta niitä ei määritellä missään. Käsitteet tulisi määritellä, jotta ei synny väärinkäsityksiä ja kaikki tietävät mistä puhutaan. Asiakirjoja on laatimassa eri toimialoja edustavia virkamiehiä ja asiantuntijoita. Asiakirjojen tekstit joudutaan laatimaan tietyn ajan puitteissa eikä käsitteen määrittelylle ole aikaa tai resursseja. (Tuukkanen 2015)

6 Pohdinta

Tutkimuksen tavoitteena oli kuvata Suomessa ja Venäjällä käytettävää *kyberturvallisuus*-käsitteistöä. Kyberturvallisuus on suhteellisen uusi tieteenala, jonka käsitteistö on vasta muodostumassa. Kyberturvallisuusala on myös varsin poikkitieteellinen, koko yhteiskuntaa koskeva ala. Käsitteistöä muodostuu useamman toimialan käsitteistä. Näin ollen myös käsitteiden määritelmät kuvastavat sitä toimialaa (erikoisalaa), jolle ne on laadittu. Toisaalta määritelmät voivat myös edustaa eri toimialojen kesken saavutettua konsensusta.

Tämän tutkimuksen tarkastelun kohteeksi valittiin viranomaisten asiakirjat, sillä niiden voidaan olettaa edustavan jonkinlaista pysyvyyttä ja harkintaa verrattuna joukkoviestimien horjuvaan käsitteiden käyttöön.

Ennen työhön ryhtymistä tavoitteeksi oli asetettu deskriptiivisen suomi–venäjä-sanaston laatiminen. Tämä tavoite toteutui vain osittain, sillä lukumäärällisesti tutkimus ei tuottanut niin paljon käsitteitä kuin alussa oli kaavailtu. Ennen tutkimukseen ryhtymistä oli tiedossa, että abstraktit käsitteet vievät huomattavasti enemmän aikaa kuin konkreettiset käsitteet. Kuitenkin oli yllättävää, miten laajaksi kokonaisuudeksi venäjänkielinen *информационная безопасность* -käsite osoittautui.

Vaikka tuloksena ei syntynyt sanastoa, niin asetettu tavoite kuvata kyberturvallisuusalan käsitteistöä on kuitenkin onnistunut. Keskeiset käsitteet on analysoitu ja sanastotyölle tehty perusteellinen pohjatyö, mikä luo hyvän perustan jatkotutkimukselle. Tutkimustyön tuloksena on sanaston sijaan käsitteellinen katsaus kyberturvallisuudesta. Käsitteellisestä katsauksesta toivotaan olevan hyötyä jokaiselle kyberturvallisuudesta kiinnostuneelle ja erityisesti jokaiselle kyberturvallisuusalan ammattikielen käyttäjälle.

Tutkimusaineisto käsitti valikoiman viranomaisasiakirjoja, joten aineisto edustaa viranomaisten asiakirjoissa käyttämää erikoiskieltä. Valitun aineiston laajuus on tutkimukselle riittävä ja sitä voidaan pitää luotettavana. Tekstilajina viranomaiskieli ei ole kaikkein helpointa. Lisäksi käytettävä termistö voi kätkeä piilomerkityksiä poliittisten linjausten, kansallisen turvallisuuden tai muiden seikkojen takia. Myös

kahden erilaisen hallintokulttuurin välisten erojen havaitseminen ja niiden ymmärtäminen toi omia haasteita tutkimustyöhön.

Viranomaislähteiden lisäksi käsitteisiin liittyvää taustatietoa etsittiin myös kyberturvallisuusalan asiantuntijoiden tekemistä raporteista, arvioista ja tutkimuksista. Pyrkimys oli etsiä tasapuolisesti tietoa kyberturvallisuudesta sekä länsimaisilta että venäläisiltä asiantuntijoilta. Tämäkin tavoite saavutettiin. Valittua aineistoa voidaan pitää tämän tutkimuksen tarpeisiin validina ja soveltuvana. Taustakirjallisuutta ja muuta aineistoa kerääntyi tutkimuksen aikana runsaasti. Sitä mukaa kun tutkimuksen aihe täsmentyi, niin aineistoa jouduttiin jättämään tutkimuksen ulkopuolelle.

Käsiteanalyysi aloitettiin tarkastelemalla valmiita määritelmiä, joten määritelmien laatiminen ja arviointi rajattiin tutkimuksesta pois. Analyysin edetessä huomattiin määritelmissä puutteita. Määritelmiä ei aina ole laadittu terminologisten periaatteiden mukaan. Määritelmän tulisi nimetä lähin yläkäsite, erottaa se lähikäsitteistä ja antaa riittävästi tietoa käsitteen olennaisista käsitepiirteistä, mutta tätä periaatetta ei aina noudatettu. Jatkotutkimuksessa tulisi tarkastella ja arvioida tarkemmin myös määritelmiä.

Muutamia käsitteitä oli määritelty siten, ettei niissä ollut lainkaan erottavia käsitepiirteitä (kriittinen tuotanto ja kriittiset palvelut). Joidenkin määritelmien yläkäsite aiheutti ongelmia käsitejärjestelmien loogisuudessa. *Yhteiskunnan elintärkeä toiminto* -käsitteen alakäsitteiden tulisi myös olla *toimintoja*. Alakäsitteet ovat kuitenkin laajoja kokonaisuuksia, kuten sisäinen turvallisuus tai henkinen kriisinkestävyys, joihin *toiminto*-käsite ei oikein sovi. Tämä vaikeutti käsitekaavion laatimista ja sen seurauksena myös käsitteiden välisten suhteiden selvittämistä.

Kyber-etuliitteen merkitys on laaja. Tämän työn perusteella näyttäisi, että *kyber*-määrite ei rajoitu pelkästään sähköiseen toimintaympäristöön, vaan se kuvaa parhaiten laajempaa verkottuneisuutta yli järjestelmärajojen. Se on samalla sekä kansallinen että globaali käsite.

Data, informaatio ja *tieto* käsitteiden käyttö ei näytä noudattavan logiikkaa tiedon arvoketjun mukaisesti. Suomen- ja venäjänkielissä niiden käyttö on horjuvaa. Usein niiden yhteydessä käytetään suluissa tarkennusta tai muita lisämääreitä.

Käsiteanalyysin yhteydessä todettiin näkökulmaeroja esimerkiksi siviilien ja sotilaiden käyttämissä käsitteissä ja niiden määritelmissä. Monet asiakirjalähteistähän on laadittu laaja-alaisena, eri viranomaisten, yhteistyönä, mikä heijastuu määritelmissä.

Erityinen haaste oli asiakirjoissa käytettyjen termien ja niiden määritelmien kirjo. Osassa lähdeasiakirjoja termejä oli runsaasti, mutta niiden määritelmät puuttuivat. Olisi syytä pohtia, miksi viranomaisten asiakirjoja on julkaistu runsaalla termistöllä ilman minkäänlaisia määritelmiä.

Osa määritelmistä vaikuttaa olevan peräisin virallisista lakimääritelmistä (säädöskieltä) ja osa selvästi poliittiseen ilmapiiriin mukautettuja. Eri alan asiantuntijat voivat kirjoittaa erilaiset määritelmät samalle käsitteelle. Tämä on ymmärrettävää, sillä esimerkiksi Valtioneuvoston selonteot laaditaan kunkin hallituksen toimesta senhetkisen poliittisten linjausten mukaisesti.

Tutkimuksen lähde - ja tausta-aineisto viittaavat siihen, että kybertermistöä luodaan suomen kieleen osin sodankäynnin englanninkielisen termistön pohjalta. Tietotekniikan alalla englannin kieli ohjaa käsitteistön muodostumista ja uusia käsitteitä käännetään suoraan englanninkielisistä termeistä. Lopputulos ei aina ole onnistunut, varsinkin jos merkitys on muuttunut lähtökielestä.

Venäläisessä turvallisuusdiskurssissa keskeinen *Информационная безопасность*-käsitteen (Venäjän informaatioturvallisuus) voisi virheellisesti olettaa olevan suomenkielisten *tietoturvallisuus* tai *informaatioturvallisuus* käsitteiden vastine. Analyysin perusteella suomen kielestä näytti puuttuvan vastine, joka kuvaisi laajassa merkityksessä samaa mitä venäjänkielinen *информационная безопасность* -käsite. Venäjänkielinen *информационная безопасность* -käsite kuvaa venäläistä turvallisuuskulttuuria, jossa valtion puuttuminen informaation sisältöön on lainsäädännöllisesti oikeutettu ja sallittu. Käsitteelle on annettu vastine-ehdotus *venäjän informaatioturvallisuus*, jota tulisi käyttää.

Venäjänkielisten vastineiden haussa olisi huomioitava, että venäjänkieliset vastineet edustavat laajempaa kokonaisuutta heijastaen Venäjän turvallisuusajattelua ja siihen liittyvää hallintokulttuuria.

Terminologiseen sanastotyöhön voisi yhdistää muiden tieteenalojen analyysimenetelmiä kuten diskurssianalyysin. Lisäksi olisi hyödyllistä tutkia *kyberturvallisuus*-aihetta terminologisen käsiteanalyysin ohella myös yhteiskuntatieteellisten tai tieteenfilosofian menetelmin. Tämän tutkimuksen tuloksia voidaan hyödyntää sekä kielitieteellisessä että yhteiskuntatieteellisessä tutkimuksessa.

Käsitteet heijastavat yhteiskuntarakenteita, lainsäädäntöä ja poliittisia linjauksia ja ne määritellään niihin soveltuviksi. Suomi ja Venäjä edustavat hyvin erilaisia hallintokulttuureja, joten joskus on vaikea kuvata ilmiöitä, joita toisessa ei ole tai ne ovat niin erilaisia, etteivät ilmiöt ole ilman tarkennuksia ymmärrettävissä oikein. Bilateraalinen sanasto on esimerkki kuinka kansainväliseen yhteistyöhön on laadittu käsitteet useamman osapuolen näkökulmat huomioiden.

Sanastotyön tekijän tai kääntäjän ei tarvitse ottaa kantaa miten hän arvottaa kahta keskenään erilaista hallintokulttuuria. Kääntäjä ei tulisi kuitenkaan sivuuttaa venäjänkielisten käsitteiden taustalla piileviä merkityksiä vastinehaussa toiselle kielelle.

Lähdeluettelo

Bilat 2011en = Rauscher, Karl Fredrick & Yashenko, Valery (toim.) 2011: *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 1*. The East West Institute. New York. Information Security Institute of Moscow State University. Moscow.

Bilat 2011ru = Rauscher, Karl Fredrick & Yashenko, Valery (toim.) 2011: Главные редакторы: Карл Фредерик Раушер & Валерий Ященко, 2011: *Двусторонний проект Россия-США по кибербезопасности. Основы критически важной терминологии. Издание 1*. Институт Восток-Запад. Институт проблем информационной безопасности МГУ имени М.В. Ломоносова.

Bilat 2014 = Rauscher, Karl Fredrick & Yashenko, Valery (toim.) 2014: *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2*. The EastWest Institute. New York. Information Security Institute of Moscow State University. Moscow.

CCDCOE 2015a = Nato Cooperative Cyber Defence Centre of Excellence 2015: *About us*. Saatavissa: https://ccdcoe.org/. Luettu 24.10.2014.

CCDCOE 2015b = Nato Cooperative Cyber Defence Centre of Excellence 2015: *Tallinn Manual Process*. Saatavissa: https://ccdcoe.org/tallinn-manual.html. Luettu 10.4.2015.

CCDCOE 2015c = Nato Cooperative Cyber Defence Centre of Excellence 2015: *Finnish, Greek and Turkish Flag Fly at the NATO Cooperative Cyber Defence Centre of Excellence*. Saatavissa: https://ccdcoe.org/finnish-greek-and-turkish-flag-fly-nato-cooperative-cyber-defence-centre-excellence.html. Luettu 15.11.2015

CCDCOE 2015d = Nato Cooperative Cyber Defence Centre of Excellence 2015: *Cyber Definitions*. Saatavissa: https://ccdcoe.org/cyber-definitions.html. Luettu 10.4.2015.

COE 2015 = Council of Europe 2015: *Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime*. Saatavissa: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Luettu 13.11.2015.

Collins, Sean & McCombie, Stephen 2012: *Stuxnet: the emergence of a new cyber weapon and its implications*. Journal of Policing, Intelligence and Counter Terrorism, Vol. 7(1), 80–91

Cyber strategy 2013 = *Finland´s Cyber security Strategy*. Government Resolution 24.1.2013. Secretariat of the Security Committee.

CYCON 2015 = International Conference on Cyber Conflict 2015: *About*. Saatavissa: https://ccdcoe.org/cycon/about.html. Luettu10.4.2015.

DHS 2014 = United States Department of Homeland Security 2014: *About DHS*. Saatavissa: http://www.dhs.gov/about-dhs. Luettu 24.10.2014.

DIBRF 2000 = *Доктрина информационной безопасности Российской Федерации, Утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895*. Saatavissa: http://www.scrf.gov.ru/documents/6/5.html. Luettu 24.10.2014.

EDA 2015 = European Defence Agency: *About us.* Saatavissa: http://www.eda.europa.eu/home. Luettu 25.4.2015.

EEAS 2013 = European External Action Service 2013: *Directive of the European parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union.* Saatavissa: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf. Luettu 25.10.2015

EK 2013 = Euroopan komissio 2013: EU:n ulkoasioiden ja turvallisuuspolitiikan korkea edustaja. Yhteinen tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. *Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö.* Saatavissa: http://ek.fi/wp-content/uploads/Euroopan-unionin-kyberturvallisuusstrategia.pdf. Luettu 2.5.2015.

ENISA 2015a = European Union Agency for Network and Information Security 2015: *About ENISA*. Saatavissa: https://www.enisa.europa.eu/about-enisa. Luettu 10.04.2015.

ENISA 2015b = European Union Agency for Network and Information Security 2015: *National Cyber Security Strategies, Practical Guide on Development and Execution, Annex 1, Glossary of Terms*. Saatavissa: http://www.enisa.europa.eu. Luettu 30.10.2014.

EU Council 2009 = Euroopan Unionin neuvosto 2009: *Euroopan Unionin turvallisuusstrategia. Turvallisempi Eurooppa oikeudenmukaisemmassa maailmassa.* Saatavissa: https://www.consilium.europa.eu/uedocs/cms_data/librairie/-PDF/QC7809568FIC.pdf. Luettu 25.5.2015.

EU CSS 2013 = *EU Cyber Security Strategy – open, safe and secure*. Saatavissa: http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm. Luettu 29.08.2015.

EWI 2015 = EastWest Institute 2015: *About.* Saatavissa: http://www.eastwest.ngo/about. Luettu 24.10.2015.

FSB 2015= Федеральная служба безопасности 2015: *Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.* Saatavissa: http://www.fsb.ru/fsb/npd/more.htm!id%3D10437521%40fsbNpa.html. Luettu 10.4.2015.

FZ 149 = Федеральный закон от 27.7.2006 N 149-ФЗ (ред. от 31.12.2014) *Об информации, информационных технологиях и о защите информации* (*с изм. и доп., вступ. в силу с 1.9.2015*). Saatavissa: http://regulation.gov.ru. Luettu 24.10.2014.

FZ 2013= Федеральный закон 00/04-5890/08-13/20–13-4: *О безопасности критической информационной инфраструктуры РФ*. Saatavissa: http://regulation.gov.ru. Luettu 24.10.2014.

FZ 38 = Федеральный закон от 8 марта 2015 г. N 38-ФЗ.*О внесении изменений в Федеральный закон "О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера"*. Saatavissa: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102033560. Luettu 25.11.2015.

Gandhi, Robin, Sharma, Anup, Mahoney William, Sousan, William, Zhu, Qiuming, Laplante, Phillipp 2011: *Dimensions of Cyber-Attacks. Social, Political, Economic and Cultural.* IEEE Technology and society magazine. Spring 2011, 28-38

Georgiamfa 2008a = Ministry of Foreign Affairs of Georgia 2008: *CyberAttacks Disable Georgian Websites*.11.8.2008. Saatavissa:http://georgiamfa.blog-spot.fi/2008/08/cyber-attacks-disable-georgian-websites.html. Luettu 24.1.2014.

Giles, Keir & Hagestad, William 2013: 5th International Conference on Cyber Conflict. Podins, K. & Stinissen, J. & Maybaum, M. (toim.), *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English.* Tallinn: NATO CCD COE Publications.

GOST 17799 = ГОСТ Р ИСО/МЭК 17799-2005: *Информационная технология. Практические правила управления информационной безопасностью.* Saatavissa: http://vsegost.com/Catalog/22/2262.shtml . Luettu 21.12.2015.

GOST 52292 = ГОСТ Р 52292-2004: *Информационная технология. Электронный обмен информацией термины и определения. Information technology. Electronic information exchange. Terms and definitions*. ИПК, Издательство стандартов. Москва 2005.

GOST 53114 = ГОСТ Р 53114-2008: Защита информации. Обеспечение информационной безопасности в организации. *Основные термины и определения.* Примечания. Saatavissa: http://www.pqm-online.com/-assets/files/standards/gost_r_53114-2008.pdf. Luettu 29.8.2015.

GOST 7.0-99 = ГОСТ 7.0-99: Система стандартов по информации, библиотечному и издательскому делу. Информационно-библиотечная деятельность, библиография. *Термины и определения*. Госстандарт РФ, 1999.

GOSTR 50.1.053 = ГОСТ Р 50.1.053-2005: Настоящие рекомендации по стандартизации должны применяться совместно с ГОСТ Р 50922. Рекомендации по стандартизации. Информационные технологии. *Основные термины и определения в области технической защиты информации.Information technologies. Basic terms and definitions in scope of technical protection of information.* Стадартинформ, 2005.

Grinev-Grinevich 2008 = Гринев-Гриневич С.В, 2008: *Терминоведение*. Издательский центр, Академия. Saatavissa: http://padaread.com/?book=76705&pg=16. Luettu 10.5.2015.

Haasio, Ari & Vakkari, Pertti 2015*: Informaatiotutkimuksen perusteet*. Saatavissa: https://viestintatieteet-wiki.wikispaces.com/Informaatiotutkimuksen+perusteet. Luettu 30.10.2015.

Hagelstam, Axel 2005: *CIP – Kriittisen infrastruktuurin turvaaminen. Käsiteanalyysi ja kansainvälinen vertailu*. Huoltovarmuuskeskus, julkaisuja 1/2005. Helsinki.

Hare, Forrest 2010: *The cyber threat to national security: Why can´t we agree?* Saatavissa: von Heinegg, Wolff Heintschel 2015: *International law and international information security: A respons to Krutskikh and Streltsov.* Nato Cooperative Cyber Defence Centre of Excellence 2015. The Tallinn papers No. 9. https://ccdcoe.org/multimedia/conference-cyber-conflict-proceedings 2010.html. Luettu 21.1.2015.

Heusala, Anna-Liisa 2011: *Kokonaisturvallisuus-käsite Venäjän turvallisuuspolitiikan tutkimuksessa.* Kosmopolis Vol. 41, nro 4. 2011, 23–38.

HVK 2015 = Huoltovarmuuskeskus. *Toiminnan perusteet*. Saatavissa: http://www.huoltovarmuus.fi/toimialat/kriittinen-teollisuustuotanto/toiminnan-perusteet/.Luettu 30.10.2015.

Hyötyniemi, Heikki 2009: *Luentoja kybernetiikan alkeista: Kompleksisten järjestelmien tutkimus.* Teknillinen korkeakoulu. Saatavissa: http://neocybernetics.com/luentoja/. Luettu 25.10.2015

IISI MSU 2014a = Институт проблем информационной безопасности. *О нас*. Saatavissa: http://www.iisi.msu.ru/about/. Luettu 9.4.2015.

IISI MSU 2014b = Институт проблем информационной безопасности. *Главная.* Saatavissa: http://www.iisi.msu.ru/main/. Luettu 9.4.2015.

IISI MSU 2015 = Институт проблем информационной безопасности. *Новости.* Saatavissa: http://www.iisi.msu.ru/news/news59/. Luettu: 2.8.2015.

ISO 704: = International Organization for Standardization, 2009: ISO 704:2009(E). Third edition. *Terminology work -- Principles and methods*. Geneva: ISO.

ISO/IEC 17799:2005 = ГОСТ Р ИСО/МЭК 17799-2005. *Информационная технология. Практические правила управления информационной безопасностью*. Saatavissa: http://www.gosthelp.ru/gost/gost2262.html. Luettu 25.1.2015.

ISO/TC 37 = ISO/TC 37 - Terminology and other language and content resources. Saatavissa: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_ browse.htm?commid=48104. Luettu 25.10.2015.

Isotalo, Pauliina 2004: *Sanastotyön juhlavuosi*. Kielikello 1/2004. Saatavissa. http://www.kielikello.fi/index.php?mid=2&pid=11&aid=1479. Luettu 15.1.2016.

ITU 2014 = International Telecommunication Union: *В поисках кибердоверия.* Saatavissa: http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.02-1-2014-PDF-R.pdf. Luettu 25.10.2015.

JYU 2015a = Jyväskylän yliopisto. Informaatioteknologian tiedekunta, 2014: *Informaatioturvallisuuden maisteriohjelma (INTU) 2014–2017*. Saatavissa: https://www.jyu.fi/it/maisterin-tutkinnot/dokumentit/intu. Luettu 25.2.2016.

JYU 2015b = Jyväskylän yliopisto. Informaatioteknologian tiedekunta, 2015, *Kyberturvallisuus - yliopiston strateginen painoala*. Saatavissa: https://www.jyu.fi/it/kyber. Luettu 16.3.2016.

Kalliokuusi, Virpi & Seppälä, Katri: *Terminologisen käsiteanalyysin rooli käsitemallinnuksessa*. Terminfo 4/2014. Saatavissa: http://www.terminfo.fi/sisalto/terminologisen-kasiteanalyysin-rooli-kasitemallinnuksessa-23.html. Luettu 14.1.2016.

Kazarin & Salnikov & Sharipov & Yashenko 2010 = Казарин, О., Сальников, А., Шаряпов, Р., and Ященко, В: *Новые акторы и безопасность в киберпространстве*. Вестник Московского университета. Серия 12. Политические науки, 2. 2010, 71–84.

Klimburg, Alexander & Tirmaa-Klaar, Heli 2011: *Study, Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU.* EXPO/B/FWC/2009-01/LOT6/09. European Parliament, 2011. Saatavissa: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf. Luettu 25.3.2015.

Kornev, Maksim 2015: Журналист» №02/2015. 4.12.2015. *Суверенная кибербезопасность*. Saatavissa: http://journalist-virt.ru/archive/2015/6686/2015/02/04/Suverennaya-kiberbezopasnost.phtml. Luettu 27.3.2015.

Kosunen, Riina 2015: TSK, *Sanastotyönperusteet koulutus*, Luentokalvot 28.10.2015.

KOTUS 2015 = Kotimaisten kielten keskus: Säädöstekstin vaikutus virkakieleen. Saatavissa: http://www.kotus.fi/kielitieto/virkakieli/yleista_virkakielesta/-virkakielikampanja/tekstitalkoot/saadostekstin_vaikutus_virkakieleen. Luettu 25.1.2016.

KRF 1993 = *Конституция Российской Федерации.* Принята всенародным голосованием 12 декабря 1993 г. Saatavissa: http://www.constitution.ru/. Luettu 25.4.2015

KTO 2007 = *Kansallinen tietoyhteiskuntaohjelma* 2007–2015. Saatavissa: http://www.tietoyhteiskuntaohjelma.fi/esittely/fi_FI/1142405427272/index.html. Luettu 24.4.2015

Kunjaev 2010a = Куняев, Николай 2010: *Механизмы обеспечения национальных интересов Российской Федерации в информационной сфере*. Кафедра документоведения и документационного обеспечения управления. Московская финансово-юридическая академия. Вестник РУДН, серия Юридические науки, 2010, № 3.

Kunjaev 2010b = Куняев, Николай 2010: *Правовое обеспечение национальных интересов Российской федерации в информационной сфере*. Логос. Москва, 2010.

Kunjaev 2015 = Куняев, Николай 2015: Saatavissa: http://193.232.218.56/web-ocal/fak/rj/index.php?id=23&p=144#2010__3. Luettu 20.11.2015.

KVDVSRF 2011 = *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве*. Министерство обороны Российской Федерации, 2011. Saatavissa: www.mil.ru. Luettu 24.1.2014.

Kyberstrategia 2013 = *Suomen kyberturvallisuusstrategia*.Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuuskomitean sihteeristö. 2013.

L 1406/2011: *Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista*.

L 28.2.2003/175: *Laki valtioneuvostosta. Valtioneuvoston organisaatio ja toimialajako.*

L60/2007: *Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus*.

L66/2009: *Laki Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta tehdyn Lissabonin sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.*

Levomäki, Irma 2008: *Arvojen moninaisuus tietoyhteiskunnassa*. SITRA Suomen itsenäisyyden juhlarahasto. Saatavissa: https://www.sitra.fi/julkaisut/tietoyhteiskunta/sitra178.pdf. Luettu 19.3.2016.

MID 2013 = МИД России: Информационные материалы Министерства иностранных дел. Пресс–служба МИД России. *Выступление спецпредставителя Президента РФ по вопросам международного сотрудничества в борьбе с терроризмом и транснациональной организованной преступностью А.В.Змеевского*. Владивосток, 4 июля 2013 года. Saatavissa: http://archive.mid.ru//BDOMP/Brp_4.nsf/arh/AA9A9DCC4B0EF45844257B9E002D46D6?OpenDocument. Luettu 25.10.2015.

MPKK 2013 = Maanpuolustuskorkeakoulu 2013: *Turvallinen Suomi, Tietoja Suomen kokonaisturvallisuudesta*. Helsinki, 2013.

Nato 2002 = NATO 2002: *Prague Summit Declaration 2002*. Saatavissa: http://www.nato.int/docu/pr/2002/p02-127e.htm. Luettu 24.10.2014.

Neittaanmäki, Pekka 2014: Jyväskylän yliopisto, Informaatioteknologian tiedekunta, Luentokalvo: *Informaatioteknologian vuosisadan strateginen investointi*, 23.2.2014. Saatavissa: www.jyu.fi. Luettu 24.10.2015.

NIIBRF 2008 = *Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации*. Saatavissa: http://www.scrf.gov.ru/documents/94.html. Luettu: 25.9.2015.

Nissilä, Niina & Nuopponen, Anita 2013: *Tieteen termit termipankkiin – haasteena synonymia*. Konferenssijulkaisussa: Haasteena näkökulma. Saatavissa: http://www.vakki.net/publications/2013/VAKKI2013_Nissila&Nuopponen.pdf. Luettu 18.12.2015.

NRC 2002 = NATO-Russia Council 2002: *About NRC*. Saatavissa: http://www.nato.int/nrc-website/en/about/index.html. Luettu 9.4.2015.

NRC 2013 = NATO-Russia Council 2013: *Linguistic Experts meet in Moscow*. Saatavissa: http://www.nato.int/nrc-website/en/articles/20130415-nrc-egt-moscow-meeting/index.html. Luettu 9.4.2015.

NRC 2014 = The NATO-Russia Council 2014: *Statement by NATO Foreign Ministers*. Saatavissa: http://www.nato.int/nrc-website/en/news/index.html. Luettu 9.4.2015.

Nuopponen, Anita 1999: *Mihin terminologian teoriaa ja menetelmää voidaan hyödyntää*. Toimikunnista termitalkoisiin, 91–98. Toim. Kuhmonen. Helsinki. Tekniikan Sanastokeskus.1999

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

Nuopponen, Anita 2004: *Teetä ja terminologiaa*. Julkaisussa: Koskela & Pilke (toim.), Erikoiskielet ja käännösteoria. VAKKI-symposiumi XXIV. http://lipas.uwasa.fi/~atn/papers/artikkelit/LinkedDocuments/Nuopponen_Teeta_Vakki04.pdf. Luettu 15.1.2016.

Nuopponen, Anita 2009: *Käsiteanalyysia käsiteanalyysista – kohti systemaattista käsiteanalyysia*, Viestintätieteiden laitos, Vaasan yliopisto: 308–319 Saatavissa: http://www.vakki.net/publications/2009/VAKKI2009_Nuopponen.pdf. 25.4.2015.

Ottis, Rain 2008: *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*. Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Academic Publishing Limited, 163–168.

Pasanen, Päivi 2009: *Merenkulun turvallisuuden koetinkiviä. Terminologisen tiedon poiminta teksteistä.* Helsingin yliopisto. Slavistiikan ja baltologian laitos. Venäjän kääntäminen ja tulkkaus. Saatavissa: https://helda.helsinki.fi/bitstream/handle/10138/19287/merenkul.pdf?sequence= Luettu 10.11.2015.

PLM 2012 = Puolustusministeriö. *Muutosten Venäjä*. Saatavissa: http://www.defmin.fi/files/2118/muutosten_venaja_nettiin.pdf. Luettu 20.4.2015.

PLM 2013 = Puolustusministeriö. Etusivu. Ajankohtaista. Tiedotteet 2013. *Suomi mukaan EDA:n kyberharjoituskonseptiin*. Saatavissa: http://www.defmin.fi/ajankohtaista/tiedotteet/2013/suomi_mukaan_eda_n_kyberharjoituskonseptiin.5524.news. Luettu 24.10.2014.

PuVL 4/2013 = Puolustusvaliokunnan lausunto 4/2013 – VNS 6/20212. *Valtioneuvoston selonteko: Suomen turvallisuus- ja puolustuspolitiikka* 2012.

Pynnöniemi, Katri 2013: *Kriittisen infrastruktuurin problematiikka Venäjän turvallisuuspolitiikassa.* Kosmopolis Vol. 43.3/2013. Saatavissa: http://www.fiia.fi/assets/news/Kosmopolis.pdf. Luettu 14.12.2015.

RUSREG = Русский регистер. *Стандарты ISO 27001. Системы менеджмента информационной безопасности.* Saatavissa: http://www.rusregister.ru/lt/services/ms-certification/standards/detail/index.php?ID=6093. Luettu 25.10.2015.

SB 2014a = Совет безопасности 2014*: Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ*. Saatavissa: http://www.scrf.gov.ru/documents/6/. Luettu 20.10.2014.

SB 2014b = Совет безопасности 2014: *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.* Saatavissa: http://www.scrf.gov.ru/documents/6/114.html. Luettu 20.10.2015.

SB 2014c = Совет безопасности 2014: *Национальная безопасность России. Информационная безопасность. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации*. Утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803. Saatavissa: http://www.scrf.gov.ru/documents/6/113.html. Luettu 28.8.2014.

SB 2015 = *Совет Безопасности Российской Федерации*. Saatavissa: http://www.scrf.gov.ru/. Luettu 10.8.2015.

SBRF 2011 = Совет Безопасности Российской Федерации, 2011: *Конвенция об обеспечении международной информационной безопасности (концепция).* Saatavissa:http://www.scrf.gov.ru/documents/6/112.html. Luettu 24.1.2014.

Schmitt, Michael 2013 = Schmitt, Michael (toim.) 2013: *Tallinn manual on the international law applicable to cyber warfare, prepared by the International Group of Experts at the invitation of the Nato Cooperative Cyber Defence Centre of Excellence*. Nato Cooperative Cyber Defence Centre of Excellence. Cambridge University. 2013.

Sedyakin 2009 = Седякин Владимир 2009: *Информация и знания*. Научные ведомости. 8 (63). 2009. Saatavissa: http://cyberleninka.ru/article/n/informatsiya-i-znaniya. Luettu 24.10.2015.

Seppälä, Katri 1999: *Tietotekniikan termitalkoot*. Kielikello 1/1999. Saatavissa: http://www.kielikello.fi/index.php?mid=2&pid=11&aid=553. Luettu 2.12.2015.

Seppälä, Katri 2015: *Kysymys käsitekaavion piirtämisestä*, TSK ry. Sähköpostiviesti tekijälle, 3.11.2015

Seppälä, Katri 2016: *Käsitekaaviosta*, TSK ry. Sähköpostiviesti tekijälle, 14.3.2016

SF 2014a = Совет Федерации 2014:*Концепция стратегии кибербезопасти РФ. Проект*. Saatavissa: http://council.gov.ru/press-center/discussions/38324/. Luettu 13.4.2015.

SF 2014b = Совет Федерации, 2014: Главная. Пресс-центр. *Обсуждения*: *Концепция стратегии кибербезопасности Российской Федерации.* Saatavissa: http://council.gov.ru/press-center/discussions/38324/.Luettu: 13.4.2015.

von Solms, Rossouw & van Niekerk, Johan. 2013: *From information security to cyber security*. Computers & Security vol. 38. 2013, 97–102

SRIORF 2008 = *Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212*. Saatavissa: www.scrf.gov.ru. Luettu 20.10.2014.

STK 1988 = Sanastotyön käsikirja 1988: Soveltavan terminologian periaatteet ja työmenetelmät (1989). Toim. Tekniikan Sanastokeskus ry. SFS-käsikirja 50. Helsinki: Suomen Standardisoimisliitto SFS, Tekniikan Sanastokeskus

Streltsov, Alexander 2007: *International information security: description and legal aspects*. Disarmament forum. UNIDIR, United Nations. Saatavissa: http://unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf. Luettu 22.11.2015.

Suomalainen, Johanna 2002: *Erikoiskielistä yleiskieleen - termeistä sanoiksi.* Kielikello 1/2002. Saatavissa: http://www.kielikello.fi/index.php?mid=2&pid=11&aid=1317. Luettu 15.1.2016.

Suonuuti, Heidi 2006: *Sanastotyön opas*. Sanastokeskus TSK ry. 2006

Suonuuti, Seija 2013: *Sanastotyön alkutaipale: perusteet hyvälle sanastotyön aloitukselle.* Terminfo 1/2013. Saatavissa: http://www.terminfo.fi/sisalto/sanastotyon-alkutaipale-perusteet-hyvalle-sanastotyon-aloitukselle-83.html. Luettu 2.12.2015.

SUPO 2015 = *Suojelupoliisin toimintaympäristö vuosina 2015–2016*. Saatavissa: www.poliisi.fi. Luettu 10.04.2015.

Symantec 2011 = Falliere, Nicolas & Murchu, Liam & Chien, Eric: *Symantec* Corporation 2011. *W32.Stuxnet Dossier, Version 1.4 (February 2011).* Saatavissa:https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Luettu 24.1.2015.

TEPA 2010 = *Sanastokeskus TSK:n TEPA-termipankki*. Tietotekniikan termitalkoot. Saatavissa: www.tsk.fi.

TEPA 2015 = *Sanastokeskus TSK:n TEPA-termipankki*. Saatavissa: www.tsk.fi.

TK 2014 = Turvallisuuskomitea 2014: *Turvallisuuskomitea on kokonaisturvallisuuteen liittyvä ennakoivan varautumisen pysyvä ja laajapohjainen yhteistoimintaelin.*Saatavissa: www.turvallisuuskomitea.fi. Luettu 24.10.2014.

TK 2015 = Turvallisuuskomitea 2015: *Suomi osallistui Naton Cyber Coalition 2004-harjoitukseen*.Saatavissa:http://www.turvallisuuskomitea.fi/index.php/fi/materiaalia/20-ajankohtaista/88-suomi-osallistui-naton-cyber-coalition-2014-harjoitukseen. Luettu 2.3.2015.

TRIT 2015 = ТРИТ: Кафедра телевизионных радио- и интернет-технологий. *Максим Корнев*. Saatavissa: http://www.rsuh.ru/media/people/detail.php?ID=111005. Luettu 20.11.2015.

TSK 2015 = Sanastokeskus TSK: Saatavissa: http://www.tsk.fi/tsk/fi. Luettu 25.10.2015.

TSK 31 = *Tiivistietoturvasanasto TSK 31*. Helsinki: Sanastokeskus TSK ry. 2004. Saatavissa: http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf. Luettu 24.1.2014.

TSK 36 = *Terminologian sanasto TSK 36*. Sanastokeskus TSK ry. 2006. Saatavissa: http://www.tsk.fi/tiedostot/pdf/TerminologianSanasto.pdf. Luettu 10.4.2015.

TSK 47 = *Kokonaisturvallisuuden sanasto, TSK 47* Helsinki: Sanastokeskus TSK ry. 2014. Saatavissa:http://www.spek.fi/loader.aspx?id=1c66e01d-a75e-4a9a-80ec-9816340ce752. Luettu 10.4.2015.

TTL 2006 = Työterveyslaitos 2006: *Turvallinen työskentely tukiasemien lähellä*. Saatavissa: www.ttl.fi. Luettu 30.10.2015.

TTP 2015 = Tieteen termipankki: Semioottinen kolmio. Saatavissa: http://tieteentermipankki.fi/wiki/Nimitys:semioottinen_kolmio. Luettu 25.4.2015

Tuukkanen, Topi 2013: *Sovereignty in the Cyber Domain*. Rantapelkonen, Jari & Salminen, Mirva (toim.), National Defence University, Department of Leadership and Military Pedagogy, Series 2: Article Collection nro 10. Tampere 2013, 41–50

Tuukkanen, Topi 2015: Tietoverkkosodankäynti-tutkimusalan johtaja, yleisesikuntakomentaja, Puolustusvoimien Tutkimuslaitos. Haastattelut Riihimäellä 10.4.2015, 25.4.2015, 24.10.2015,15.11.2015

TYK 2015: Tampereen yliopiston kirjasto: *Internet-aineiston arviointikriteerejä*. Saatavissa: http://www.uta.fi/kirjasto/oppaat/arviointikriteereja.htm. Luettu 19.11.2015.

UKAZ 537 = *Указ № 537 об утверждении Стратегии национальной безопасности Российской Федерации до 2020 года*, Утверждена Президентом Российской Федерации от 12 мая 2009 г. Saatavissa: http://www.scrf.gov.ru/documents/99.html.Luettu 24.10.2014.

UM 2014 = Ulkoasianministeriö, Lehdistötiedote 186/2014, 29.8.2014. *Ulkoministeriöön perustettu uusi kybersuurlähettiläänn tehtävä*. Saatavissa: http://formin.finland.fi/public/default.aspx?contentid=311621&contentlan=1&culture=fi-FI. Luettu 3.11.2014.

VAHTI 2/2014 = *Tietoturvallisuuden arviointiohje*. Valtionvarainministeriö. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ce1ccede-8669-4166-b084-9cafbe6e1e60&groupId=10128&groupId=10229. Luettu 26.2.2016

Vahti 8/2008 = *Valtionhallinnon tietoturvasanasto*. Valtiovarainministeriö.2008.

Vehmas-Lehto, Inkeri 1999: *Sanastoa kartoittamassa*. 1999. Saatavissa: http://nettiradiomikaeli.internetix.fi/mikaeli/arkisto/tutkimus/terminologia/index.htm. Luettu 22.11.2015.

Vehmas-Lehto, Inkeri 2007: *Puutavaralajeja ja kasvupaikkaluokkia. Ongelmia käsitejärjestelmien ja määritelmien muodostamisessa*. VAKKI- julkaisut N:o 34, Vaasa, 340–351. Saatavissa: http://www.vakki.net/publications/2007/VAKKI2007_Vehmas-Lehto.pdf. Luettu 25.2.2016.

Vehmas-Lehto, Inkeri 2010: *Termit kääntäjän näkökulmasta*. Vakki-julkaisut. 2010, numero 37. Saatavissa: http://www.vakki.net/publications/no37_fin.html. Luettu 20.11.2015.

VIVI 2014a = Viestintävirasto 2014: *Euroopan laajuinen Cyber Europe 2014 tietoturvaharjoitus käynnissä.* Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/10/ttn20141030 1538.html Luettu 30.10.2014.

VIVI 2014b = Viestintävirasto 2014: *Kyberturvallisuus, Kyberturvallisuuskeskuksen palvelut, CERT-toiminto*. Saatavissa: https://www.viestintavirasto.fi/tietoturva/viestintavirastontietoturvapalvelut/cert-fi.html.Luettu 4.11.2014.

VIVI 2015 = Viestintävirasto 2015: *Viraston esittely ja tehtävät*. Saatavissa: https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat.html. Luettu 24.06.2015.

VN 2015a = Valtioneuvosto 2015: *Periaatepäätökset*. Saatavissa: http://valtioneuvosto.fi/periaatepaatokset.Luettu 15.5.2015.

VN 2015b = Valtioneuvosto 20105: *Ministeriöt*. Saatavissa: http://valtioneuvosto.fi/ministeriot/lvm/fi.jsp. Luettu 26.6.2015.

VN 2015c = Valtioneuvosto 2015: Valtioneuvoston ministerivaliokunnat. Saatavissa: http://valtioneuvosto.fi/hallitus/ministerivaliokunnat/fi.jsp. Luettu 24.06.2015.

VNK 21/2010 = Valtioneuvoston kanslian julkaisusarja 21/2010, *Varautuminen ja kokonaisturvallisuus,* Komiteamietintö, Valtioneuvostonkanslia, Helsinki 2010.

VNOS 262/2003 = Valtioneuvoston ohjesääntö. 3.4.2003/262.

VNpp 2012 = Valtioneuvoston periaatepäätös kokonaisturvallisuudesta. 5.12.2012

VNS 9/2009 = *Valtioneuvoston turvallisuus – ja puolustuspoliittinen selonteko 2009.* Valtioneuvoston kanslian julkaisusarja 9/2009.Saatavissa: www.defmin.fi. Luettu 10.4.2015.

YETT 2003 = *Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös, 27.11.2003.*

YTS 2010 = Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010. Puolustusministeriö. 2011.

Liitteet

Liite 1: Venäjänkielinen lyhennelmä

Liite 2: Kyberuhkamalli

Liite 3: Kybertoimintaympäristö

Liite 1: Venäjänkielinen lyhennelmä

Хельсинкский университет

Кибербезопасность – анализ основных понятий предметной области «кибербезопасность» в финском и русском языках

Хейди Пекандер

Автореферат дипломной работы

Хельсинкский университет
Отделение современных языков
Кафедра перевода русского языка

Апрель 2016

Содержание

1 Введение

Данная дипломная работа посвящена изучению основных понятий специальной лексики по теме «кибербезопасность», употребляемой в официальных документах в Финляндии и России.

За последние два десятилетия в мире произошли существенные изменения, в число которых входят появление Интернета, стремительная глобализация и развитие современного информационного общества. Развитие информационных технологий и сети Интернет составляют технологический и организационный базис современного общества, пронизывающий все его структуры и оказывающий значительное влияние на жизнь каждого человека.

Глобальное Интернет-пространство носит комплексный характер, что порождает также и множество нежелательных последствий, так как необходимые обществу информационные системы могут стать предметом и средством деструктивных действий. В связи с этим во многих государствах мира, в том числе в Финляндии и России, кибербезопасность входит в сферу вопросов национальной безопасности. «Кибербезопасность» – весьма актуальная тема. Актуальность ее определяется тем, что современное общество живет в эпоху внедрения информационных технологий во все сферы общества, и кибербезопасность является глобальной тенденцией. При этом терминология по кибербезопасности, несомненно, еще находится в стадии становления.

Первые государственные стратегии кибербезопасности начали появляться в мире в последние два десятилетия. Насколько известно, Соединенные Штаты Америки были первой страной в мире, опубликовавшей «Национальную стратегию безопасности в киберпространстве» (US CYBER 2003). В 2010 году был обнаружен компьютерный червь «Стакснет» *(Stuxnet)* (Symantec 2011), атакующий автоматизированные системы управления технологическими процессами (АСУ ТП). После этого по всей Европе кибербезопасность начали воспринимать как вопрос государственной важности и разрабатывать национальные стратегии кибербезопасности (ENISA 2015).

В основе «Стратегии кибербезопасности Финляндии от 2013 года» (Kyberstrategia 2013) лежит подход к кибербезопасности как к проблеме

экономического характера, связанной с развитием финского информационного общества. Некоторые страны, в том числе Россия, в настоящий момент еще разрабатывают собственную стратегию.(SF 2014a.) Подходы к определению понятия «кибербезопасность» и других ключевых понятий значительно различаются в разных странах. В настоящий момент как на европейском, так и на международном уровне отсутствует согласованное определение понятия «кибербезопасность». «Кибербезопасность», «компьютерная безопасность», «безопасность информации» и «информационная безопасность» – эти понятия по-разному определяются в разных языках и зачастую смешиваются.

Терминология по кибербезопасности в финском и русском языках формируется чаще всего на основе англоязычных публикаций. Перевод новых английских терминов на финский на русский языки часто осуществляется специалистами по информационным технологиям. Относительная новизна темы кибербезопасности усложняет определение терминов, в результате чего нет единой терминологии, а есть множество синонимов.

Целью данной работы является изучение и описание терминов, употребляемых в области кибербезопасности. С помощью понятийного анализа уточняется содержание понятий и их соотношение с близкими понятиям, входящими в данную понятийную систему. В ходе анализа производится сравнение финских понятий с русскими, в результате чего становится возможным подобрать русские эквиваленты. Результаты исследования можно в дальнейшем использовать при составлении краткого двуязычного терминологического словаря сферы кибербезопасности.

Теоретико-методологической базой исследования послужили основные положения финского и международного терминоведения и терминографии, в том числе российского терминолога С.В. Гринёва. Практическим пособием по терминологической методике послужил справочник, составленный финским терминологом Хейди Суонуути (Suonuuti, 2006.) и основывающийся на международных стандартах по терминологической работе ISO/TC 37/SC. (ISO/TC 37/SC.)

Научная новизна исследования заключается в том, что оно, по-видимому, является первой попыткой комплексного анализа терминологии по кибербезопасности в русском и финском языках. Эта предметная область еще не подвергалась детальному систематическому описанию и настоятельно требует создания двуязычного терминологического словаря. Кроме того, отсутствуют как финский толковый, так и финско-русский словарь по кибербезопасности.

Тема работы была выбрана из-за собственного интереса к ней автора и его опыта работы в сфере информационных технологий. Материалами исследования послужили официальные документы двух стран, терминологические словари, стандарты, законы и другие тексты, касающиеся сферы кибербезопасности.

Результаты работы могут представлять интерес для переводчиков и специалистов, занимающихся вопросами защиты информации и работающих со специальной научно-технической литературой по этой проблеме на финском и русском языках.

Дипломная работа состоит из введения, четырех глав и заключения. Первая глава работы – введение. Во второй главе описывается развитие и особенности финского информационного общества в рамках международного сотрудничества и соглашений. Третья глава является исследовательской главой, в ней излагается материал исследования: сначала финские, а затем российские документы.

В четвертой главе излагается теоретическая основа данной работы, описывается метод исследования и практика составления терминологического словаря с помощью понятийного анализа. В разделах этой главы определяются основные понятия терминологии, а также описывается практическое выполнение работы. В пятой главе производится понятийный анализ и сравнение терминов, а также устанавливается степень их эквивалентности. Здесь же приводятся результаты анализа, также словарные статьи, отражающие результаты проведенного анализа. В шестой главе подводятся итоги работы. В

приложениях приводятся автореферат дипломной работы на русском языке и понятийные схемы.

2 Теория и метод исследования

Теоретико-методологической базой исследования послужили основные положения финского и международного терминоведения и терминографии, в том числе и русских терминологов С.В. Гринёва. «Практическое пособие по составлению терминологического словаря» (Sanastotyön opas) составлено финским терминологом Хейди Суонуути (Suonuuti, 2006.) на основе международных стандартов по терминологии, в том числе ISO/TC 37/SC. В данном пособии изложены основные принципы терминоведения, терминографии и практические методы составления словарей. В нем приводятся рекомендации, объясняются ключевые понятии терминологии, раскрываются принципы и методика проведения понятийного анализа, в том числе описывается порядок выполнения самого анализа. Данное пособие соответствует принципам, применяемым в финском Терминологическом центре TSK.

Прежде чем перейти к описанию терминологической методики данной работы, необходимо определить ключевые понятии. При этом необходимо отметить, что финская и российская лингвистическая терминология несколько различаются. В русском языке «терминология» как наименование отрасли знаний является устаревшим термином, вместо которого чаще используется «терминоведение». В данной работе будем придерживаться терминологии, принятой в вышеуказанном пособии. (Suonuuti, 2006.)

«Терминология – совокупность терминов определенной отрасли знания или производства, а также учение об образовании, составе и функционировании терминов.» (Гринёв 2008: 9)

Практическая терминологическая работа включает в себя описание терминосистемы и поиск эквивалентов, с помощью которых осуществляется понятийный анализ, относящийся к методам составления словарей. (Nuopponen, 1999.)

В терминологической работе принято выделять понятия «понятие» и «референт». В так называемом «семантическом треугольнике», или «треугольнике Огдена–Ричардса» изображаются взаимосвязи трех лингвистических категорий: «понятие», «референт» и «слово». «Символ» (слово, принятое в человеческом обществе наименование объекта), «референс» (мысль) и «референт» (предмет о котором мы мыслим или имеем в виду) (Grinev& Sorokina 2012:90–91)

Понятие – это отображенная в мышлении совокупность существенных признаков конкретных предметов или явлений, для определения которых используются словесные описания (TSK 36:10) Гринёв-Гриневич определяет понятие следующим образом: «Понятие – это форма мысли, отражающая материальные и нематериальные объекты, при которой сознанием выделяются и фиксируются только существенные признаки объекта.» (Гринёв-Гриневич 2008:81) Также, по Гриневу, понятие – это «возникающий в сознании людей мысленный образ данного объекта.» (Grinev& Sorokina 2012:90)

Признаки, с помощью которых предметы выделяются и обобщаются, называются **свойствами**. (TSK 36: 10–12, Гринёв 2008,30) Референт – данный в ощущениях объект реальной действительности или явление психического мира. (Grinev& Sorokina 2012:90)

Термин – это выражение определенной предметной области, например профессиональной. (Suonuuti 2006,11). Имеется в виду выражение специальной лексики, например определенной профессиональной сферы. (TSK 36, 22). Использование специальной лексики той или иной научной дисциплины предполагает необходимый профессионализм (компетентность), т.е. знание определенной специальной области. (TSK 36,30). Короче говоря, специальная лексики применяется для точного наименования специальных понятий и, следовательно, термины отличаются от общеупотребительных слов своей семантической организацией (Nuopponen 1999.) По Гриневу «термин является основной единицей специальной лексики». (Гринёв-Гриневич 2008,43) Классификация понятий в терминологической работе проводится с помощью систематизации. Согласно Гриневу, систематизация понятий есть их

расположение в соответствии со структурой данной области знания. (*Гринёв-Гриневич 2008*,82)

Между понятиями существуют три основных вида связей: родовидовые, партитивные и ассоциативные. **Родовидовые связи** изображаются в виде древообразного графа. Например, деревья можно разделить по породам на хвойные и лиственные. (Suonuuti, 2006,14). **Партитивные отношения** выражают отношения части и целого. Например, дерево состоит из нескольких частей – ствола, ветвей и корней. Партитивные связи обозначаются в логико-понятийных схемах гребневидными линиями. (Suonuuti, 2006,16–17).К **ассоциативным связам** относятся все остальные виды связей, которые не могут быть отнесены к двум вышеупомянутым категориям. С помощью ассоциативных связей можно описать такие функции и явления, как причина и следствие, материал и продукция, предмет и место, действие и результат. Ассоциативные связи изображаются в виде односторонних или двусторонних стрелок. Приведем пример причинно-следственной связи: наступила весна (причина) – распустились листья (следствие) (Suonuuti, 2006,17–18).

На первом этапе терминологической работы осуществляется проектирование словаря, в частности определяется его тип, целевая аудитория и ее потребности. Целевой аудиторией нашего словаря являются специалисты и переводчики, занимающиеся вопросами защиты информации и работающие со специальной научно-технической литературой, у которых возникает потребность выяснить содержание понятий, а также сходство и различие терминов по теме кибербезопасности.

В качестве материала мы выбрали нормативные документы и решили исключить Интернет-источники. В этом случае не возникает проблемы оценки достоверности материала, т.к. нормативные документы можно считать достоверными. (Гринев 2008,20; TYK 2015.) Исходным языком был выбран финский, т.е. понятия рассматривались на основе финского языка. Поиск эквивалентов в русском языке осуществлялся с помощью понятийного анализа. На основе него были отобраны источники на обоих языках. Окончательный объем работы определился после проведения понятийного анализа.

Терминологическую работу обычно рекомендуются проводить в групповой форме, тогда в проекте по составлению словаря участвуют терминологи, переводчики и специалисты-предметники. Объем дипломной работы значительно меньше и работа выполняется одним человеком, поэтому чрезвычайно важно иметь возможность проконсультироваться со специалистами, работающими в данной области.

В ходе понятийного анализа терминосистема изображается графически. Идеальным вариантом было бы моделирование терминосистем отдельно на разных языках с последующим их сравнением для подбора эквивалентов. Однако на практике часто приходится опускать этап моделирования терминосистемы на языке перевода. (Kosunen 2015.)

Результаты понятийного анализа, в том числе определения понятий и эквиваленты на русском языке, оформляются в виде словарных статей. Словарные статьи могут быть организованы тематически или в алфавитном порядке. (Suonuuti 2006, 34–40)

3 Материал исследования

В качестве материала исследования на финском языке использованы нормативные документы, касающиеся темы кибербезопасности, в том числе ряд резолюции парламента (VN 2015a). Главным из них является *Стратегия по кибербезопасности Финляндии* (Kyberstrategia 2013), опубликованная в 2013 году. (Kyberstrategia 2013.) В ней определено 11 основных понятий кибербезопасности. В материал исследования входят также такие резолюции парламента, как *Стратегия обеспечения критически важных функции общества* (YETT 2003) и *Стратегия национальной безопасности* (YTS 2010), *Доклады правительства по национальной безопасности и оборонной политике 2009 года* (VNS 9/2009, 3) и *Доклады правительства по национальной безопасности и оборонной политике 2012 года* (VNK 5/2012).

Кроме того, были изучены словари, опубликованные на сайте финского Терминологического центра TSK (TEPA 2015). (1) «Вахти» – терминологический словарь, составленный для работников сферы

компьютерной безопасности (VAHTI 8/2008); (2) «Словарь по компьютерной безопасности», в котором даны определения понятий и приведены логико-понятийные схемы (TSK 31) и (3) «Словарь по общественной безопасности» (TSK 47), который является новейшим из перечисленных словарей и в котором приведены обновлённые термины, определения и логико-понятийные схемы.

В материал исследования на русском языке входят документы, опубликованные на Интернет-сайте Совета Безопасности Российской Федерации (FSB 2015, SB 2015, SB 2014a, SB 2014b, SB 2014c,). К ним относятся, в частности, следующие документы: Концепция стратегии кибербезопасности РФ (SF 2014a), Доктрина информационной безопасности Российской Федерации (DIBRF 2000), Стратегия развития информационного общества в Российской Федерации (SRIORF 2008), Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации (NIIBRF 2008) и Конвенция об обеспечении международной информационной безопасности (концепция) (SBRF 2011).

Институт проблем информационной безопасности (IISI MSU 2014) и Институт Восток-Запад (*EastWest Institute*) составили словарь ключевых терминов в сфере кибербезопасности и информационной безопасности. Эти краткие словари называются «Двусторонний проект: Основы критически важной терминологии, Издание 1» (Bilat 2011) и «Двусторонний проект: Основы критически важной терминологии, Издание 2» (Bilat 2014).

Целью совместного проекта являлся поиск консенсуса по терминологии в области кибербезопасности. Россия и Америка считаются сверхдержавами в киберпространстве и являются странами с очень разной историей, идеологией и точками зрения. Несмотря на это, был достигнут консенсус в отношении 40 терминов, хотя перед участниками стоял ряд проблем, связанных с принципиальными разногласиями. Помимо этих документов, в материалы исследования были включены стандарты и законы обеих стран.

4 Анализ и результаты исследования

Приведем пример проведенного нами понятийного анализа. Понятийный анализ начинается с финского понятия «tietoturvallisuus», которое определяется тремя признаками (saatavuus, eheys, luottamuksellisuus) (TSK 47:10). Русское понятие «безопасность информации (данных)» определяется в рекомендации ГОСТа аналогичным образом (GOSTR 50.1.053: 3.1.4). Соответственно, мы можем выбрать русские эквиваленты «доступность» (FZ:149: 2.6), «целостность» (GOSTR 50.1.053: 3.1.4) и «конфиденциальность» (FZ 149: 2.7).

В ГОСТе приводятся два понятия: безопасность информации [данных] (GOSTR 50.1.053:3.1.4) и безопасность информации (при применении информационных технологий) (GOSTR 50.1.053 :3.1.5). Видимо, в русском языке для правильного понимания требуется дополнение в скобках, однако отметим, что содержание финского понятия «tietoturvallisuus» охватывает оба понятия.

Анализ финского понятия «kyberturvallisuus» (кибербезопасность) основывается на анализе определения, приведенного в Киберстратегии Финляндии (Kyberstrategia 2013). «Кибербезопасность» определяется как состояние киберпространства, при котором обеспечивается его функционирование, в частности способность противостоять угрозам и восстанавливаться после атак (Kyberstrategia 2013,13.). В принципе, определение русского понятия «кибербезопасность» в Концепции стратегии кибербезопасности РФ (SF 2014a) – «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» (SF 2014a, 2) – по содержанию схоже с финским определением. Проблема здесь возникает не при анализе отдельных понятий, а когда данное понятие рассматривается в контексте информационной безопасности. В Стратегии кибербезопасности РФ четко сказано, что «в официальных российских документах в области информационной безопасности термин ”кибербезопасность” не выделяется из объема понятия ”информационная безопасность” и не используется отдельно» (SF 2014a, 3). Также отмечено, что для осуществления сотрудничества между российской и иностранными сторонами в сфере кибербезопасности было необходимо создать термин «кибербезопасность» и в русском языке.

Необходимо учитывать, что определение и подходы к пониманию понятия «кибербезопасность» и других ключевых понятий, несмотря на трансграничность данного явления, в разных странах различаются. Проблема возникает в том случае, когда под сходными по форме терминами подразумеваются совершенно разные вещи. Как уже отмечалось выше, проблема заключается в отсутствии единой терминологии.

В финском языке, как и во многих языках, выделяются понятия tietoturvallisuus и kyberturvallisuus, не являющиеся по содержанию синонимичными. Содержание российского понятия информационной безопасности исследовано российскими и международными специалистами. На Интернет-сайте Совета Безопасности под рубрикой «Информационная безопасность» опубликованы семь документов, определяющих понятие «информационная безопасность». Изучив содержание документа «Конвенция об обеспечении международной информационной безопасности» (SF 2014a), мы пришли к выводу, что содержание понятия «информационная безопасность» и подход к информационной безопасности в России существенно отличаются от Финляндии. В связи с наличием серьезных противоречий между западной и российской точками зрения в настоящее время Россия не считает возможным присоединиться к Конвенции Совета Европы о киберпреступности от 2001 г. (Будапештской конвенции), а разработала вышеупомянутую Концепцию. (Streltsov 2007.)

Приведем отрывок из словаря «Двусторонний проект: Основы критически важной терминологии», касающийся этой несогласованности:

”… американцы не рассматривают защиту информации как нечто, что должно включать цензуру или любую попытку контроля информированности населения…” (Bilat 2011, 8 .)

На основе проведенного анализа можно сделать вывод, что понятия «kyberturvallisuus» и «кибербезопасность» по содержанию не эквиваленты, хотя соответствующие термины и сходны по форме. Помимо понятия «кибербезопасность», в анализе раскрывается значение и других ключевых понятий. Следует отметить, что при переводе терминов сферы

кибербезопасности требуется уделять особое внимание контексту. Необходим анализ узкого или широкого контекста, поскольку определение не всегда дает полное представление о значении понятия. В этом случае в дополнение к понятийному анализу рекомендуется использовать метод контекстуального анализа.

5 Заключение

Целью данной дипломной работы было изучение основных понятий и специальной лексики по теме кибербезопасности, употребляемых в официальных документах в России и Финляндии. Изначально было известно, что терминология в области кибербезопасности еще находится в стадии становления. Решение включить в материалы исследования нормативные документы оказалось правильным.

Также ставилась цель выяснить с помощью понятийного анализа содержание понятий и отношений между ними для поиска эквивалентов в русском языке с целью включения их в краткий двуязычный терминологический словарь сферы кибербезопасности. Задача по поиску русских эквивалентов была решена частично. Это объясняется тем, что при анализе таких понятий, как «информационная безопасность» и «кибербезопасность», возник ряд проблем при установлении переводческой эквивалентности, разрешение которых потребовало бы значительно больше времени, чем было запланировано.

Само понятие «кибербезопасность» еще не закрепилось в российских государственных документах. В финских документах понятие «кибербезопасность» определено, однако употребляется и ряд других понятий, не снабженных определением. Проблема заключается не только в отсутствии единой терминологии на национальном уровне. Следует отметить, что отсутствие общих понятий затрудняет или полностью исключает возможность международного сотрудничества.

Результаты проведенного исследования позволяют сформулировать круг вопросов для будущих исследований. Перспективным, по нашему мнению,

будут исследования особенностей терминов в различных терминологических системах с учетом различий во взглядах. В исследовании отмечено, что российская точка зрения на информационную безопасность отличается от финской, т.к. акцент делается на «всеобъемлющем характере информации», т.е. киберпространство включает в себя всю информацию, в том числе и информацию человеческого сознания, охватывая, таким образом, не только её техническую часть (данные). Такой подход, естественно, отражается и в используемых понятиях.

6 Библиография

Материал исследования

Bilat 2011 = Rauscher, Karl Fredrick& Yashenko, Valery (toim.) 2011. *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 1.* The EastWest Institute.New York.USA.Information Security Insitute of Moscow State University.Moscow.

Bilat 2014 = Rauscher, Karl Fredrick& Yashenko, Valery (toim.) 2014. *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2*. The EastWest Institute.New York.USA. Information Security Insitute of Moscow State University.Moscow.

DIBRF 2000 = *Доктрина информационной безопасности Российской Федерации,* Утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895.Saatavissa: http://www.scrf.gov.ru/documents/6/5.html. Luettu 24.10.2014

FSB 2015= Федеральная служба безопасности: *Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.* Saatavissa: http://www.fsb.ru/fsb/npd/more.htm!id%3D10437521%40fsbNpa.html. Luettu 10.4.2015

FZ 149 = Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.12.2014) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.09.2015)

GOSTR 50.1.053 = ГОСТ Р 50.1.053-2005: Информационные технологии. *Основные термины и определения в области технической защиты информации (en. Information technologies. Basic terms and definitions in scope of technical protection of information).* Издание официальное. Стадартинформ, 2005.

ISO/TC 37/SC= ISO/TC 37/SC 5 Translation, interpreting and related technology. Saatavissa: http://www.iso.org/iso/standards_development/technical_committees/other_bodies/iso_technical_committee.htm?commid=654486. Luettu: 5.10.2015

KVDVSRF 2011 = *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве*. Министерство обороны Российской Федерации, 2011. Saatavissa: www.mil.ru.Luettu 24.1.2014.

Kyberstrategia 2013 = *Suomen kyberturvallisuusstrategia*.Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuuskomitean sihteeristö.2013

NIIBRF 2008 = *Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации*. Saatavissa: http://www.scrf.gov.ru/documents/94.html. Luettu: 25.9.2015

SB 2014a = Совет безопасности 2014*: Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.*Saatavissa: http://www.scrf.gov.ru/documents/6/.Luettu 20.10.2014

SB 2014b = Совет безопасности 2014: *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.* Saatavissa: http://www.scrf.gov.ru/documents/6/114.html. Luettu 20.10.2015

SB 2014c = Совет безопасности 2014: *Национальная безопасность России. Информационная безопасность. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации*. Утверждены

Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803. Saatavissa: http://www.scrf.gov.ru/documents/6/113.html. Luettu 28.8.2014.

SB 2015 = СБ, Совет Безопасности Российской Федерации, Saatavissa: http://www.scrf.gov.ru/.Luettu 10.08.2015

SBRF 2011 = Совет Безопасности Российской Федерации, 2011. *Конвенция об обеспечении международной информационной безопасности (концепция).* Saatavissa:http://www.scrf.gov.ru/documents/6/112.html.Luettu 24.1.2014.

SF 2014a: Совет федерации 2014:.*Концепция стратегии кибербезопасти РФ.Проект*. Saatavissa: http://council.gov.ru/press-center/discussions/38324/.Luettu 13.4.2015.

SRIORF 2008 = *Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212*. Saatavissa: www.scrf.gov.ru. Luettu 20.10.2014

Suonuuti, Heidi: *Sanastotyön opas*. Sanastokeskus TSK ry. 2006

TSK 31 = *Tiivistietoturvasanasto TSK 31*. Helsinki: Sanastokeskus TSK ry.2004. Saatavissa: http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf. Luettu 24.1.2014

TSK 36 = *Terminologian sanasto TSK 36*. Sanastokeskus TSK ry.2006. Saatavissa: http://www.tsk.fi/tiedostot/pdf/TerminologianSanasto.pdf. Luettu 10.4.2015.

TSK 47 = *Kokonaisturvallisuuden sanasto, TSK 47* Helsinki: Sanastokeskus TSK ry,2014. Saatavissa:http://www.spek.fi/loader.aspx?id=1c66e01d-a75e-4a9a-80ec-9816340ce752.Luettu 10.4.2015.

Vahti 8/2008 = *Valtionhallinnon tietoturvasanasto*. Valtiovarainministeriö.2008.

VN 2015a = Valtioneuvosto 2015: *Periaatepäätökset*. Saatavissa: http://valtioneuvosto.fi/periaatepaatokset.Luettu 15.5.2015.

VNK 5/2012: Valtioneuvoston kanslian julkaisusarja 5/2012: *Suomen turvallisuus- ja puolustuspolitiikka 2012*, Valtioneuvoston selonteko. Saatavissa: www.vnk.fi. Luettu 25.10.2014.

Kyberstrategia 2013 = *VNpp Suomen kyberturvallisuusstrategiasta 24.1.2013.* Saatavissa: http://valtioneuvosto.fi/paatokset/periaatepaatokset. Luettu 10.4.2015

VNS 9/2009 = *Valtioneuvoston turvallisuus – ja puolustuspoliittinen selonteko 2009.* Valtioneuvoston kanslian julkaisusarja 9/2009.Saatavissa: www.defmin.fi. Luettu 10.4.2015

YETT 2003 = *Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös, 27.11.2003.*

YTS 2010 =Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010. Puolustusministeriö. 2011.

Научная литература

ENISA 2015 = European Union Agency for Network and Information Security 2015: *National Cyber Security Strategies, Practical Guide on Development and Execution, Annex 1, Glossary of Terms*. Saatavissa: http://www.enisa.europa.eu. Luettu 30.10.2014.

Grinev-Grinevich = Гринев-Гриневич С.В: *Терминоведение*. Издательский центр Академия, 2008

Grinev& Sorokin = Гринёв-Гриневич С.В., Сорокин Э.А: *Основы семиотики*, Издательство Наука,Москва. 2012

IISI MSU 2014a = ИПИБ МГУ 2014: Институт проблем информационной безопасности.*О нас*. Saatavissa: http://www.iisi.msu.ru/about/.Luettu 9.4.2015

Kosunen, Riina 2015: TSK, *Sanastotyönperusteet koulutus*, Luentokalvo 28.10.2015.

Nuopponen, Anita 1999: *Mihin terminologian teoriaa ja menetelmää voidaan hyödyntää*. Toimikunnista termitalkoisiin, 91–98.Toim. Kuhmonen. Helsinki. Tekniikan Sanastokeskus.1999

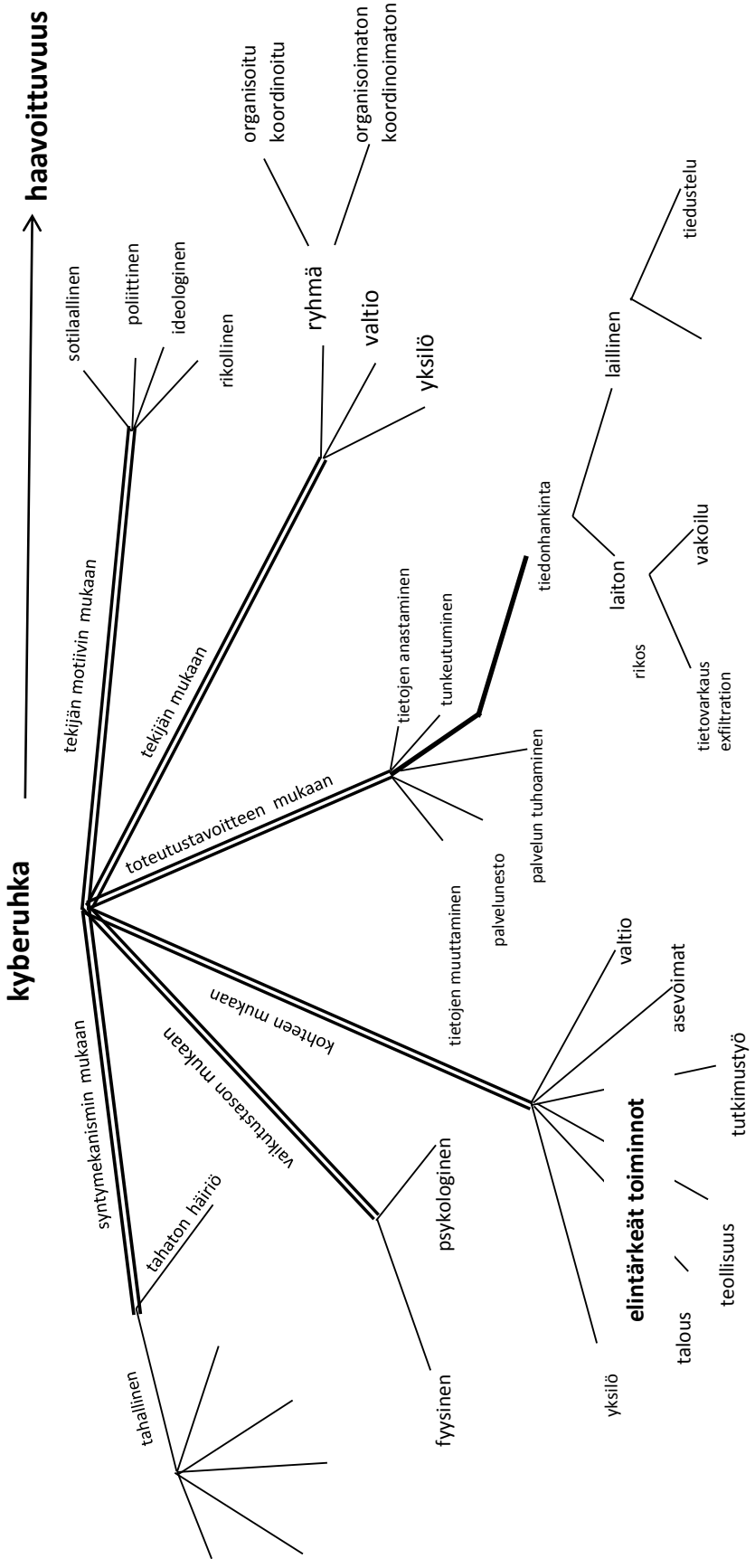
Symantec 2011 = Falliere, Nicolas; Murchu, Liam & Chien, Eric: Symantec Corporation 2011.*W32.Stuxnet Dossier, Version 1.4 (February 2011).* Saatavissa:https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Luettu 24.1.2014.

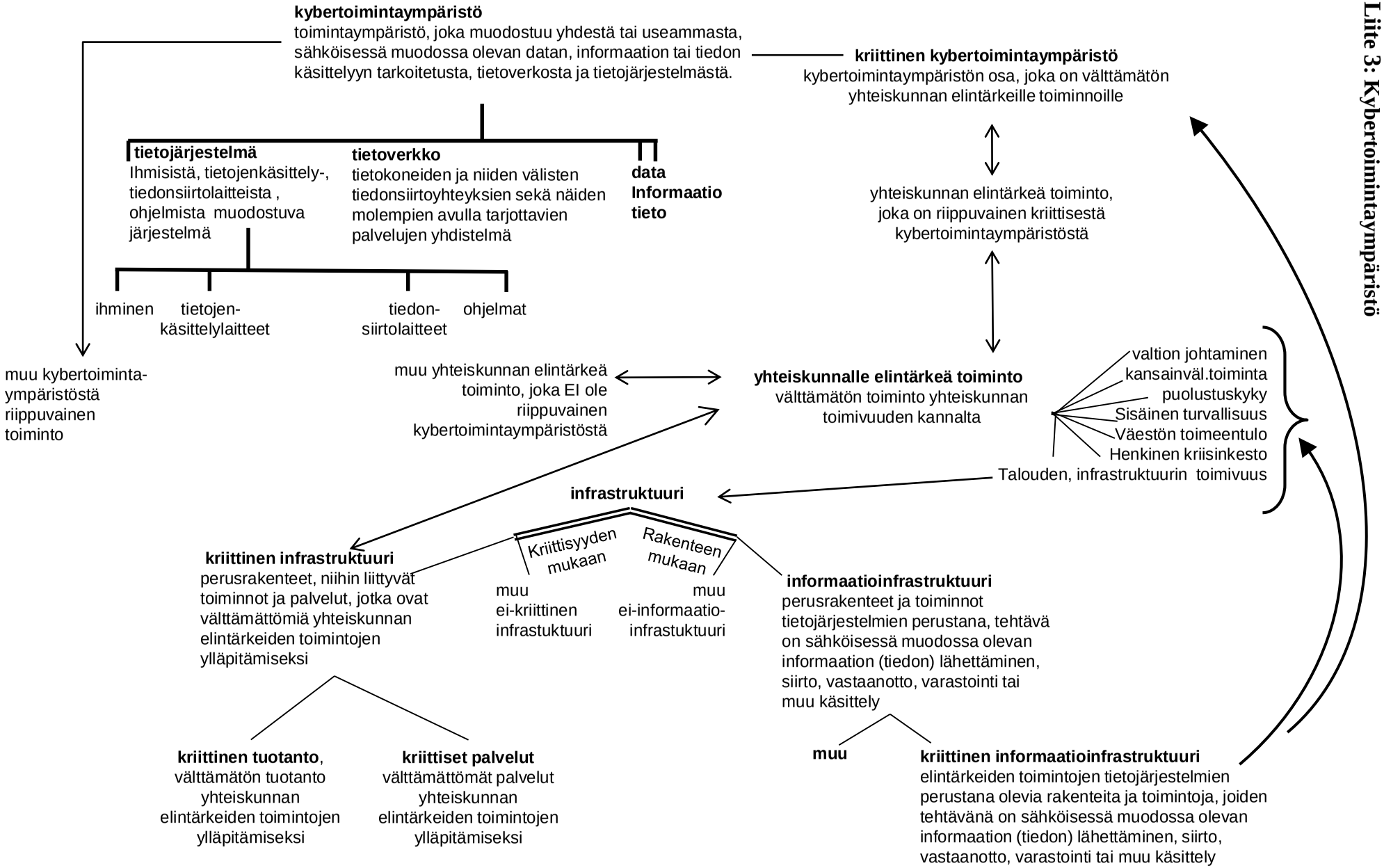
TEPA 2015 = TEPA. *Sanastokeskus TSK:n termipankki*. Saatavissa: www.tsk.fi. Luettu 31.10.2015

TYK 2015: Tampereen yliopiston kirjasto: *Internet-aineiston arviointikriteerejä*. Saatavissa: http://www.uta.fi/kirjasto/oppaat/arviointikriteereja.htm.Luettu 19.11.2015.

US CYBER = The national strategy to secure Cyberspace. February 2003.Saatavissa: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. Luettu 10.4.2015

Liite 2: Kyberuhkamalli




kybertoimintaympäristö
toimintaympäristö, joka muodostuu yhdestä tai useammasta, sähköisessä muodossa olevan datan, informaation tai tiedon käsittelyyn tarkoitetusta, tietoverkosta ja tietojärjestelmästä.
kriittinen kybertoimintaympäristö
kybertoimintaympäristön osa, joka on välttämätön yhteiskunnan elintärkeille toiminnoille
tietojärjestelmä
Ihmisistä, tietojenkäsittely-, tiedonsiirtolaitteista , ohjelmista muodostuva järjestelmä
tietoverkko
tietokoneiden ja niiden välisten tiedonsiirtoyhteyksien sekä näiden molempien avulla tarjottavien palvelujen yhdistelmä
data
Informaatio
tieto
yhteiskunnan elintärkeä toiminto, joka on riippuvainen kriittisestä kybertoimintaympäristöstä
ihminen
tietojen-käsittelylaitteet
tiedon-siirtolaitteet
ohjelmat
muu kybertoiminta-ympäristöstä riippuvainen toiminto
muu yhteiskunnan elintärkeä toiminto, joka EI ole riippuvainen kybertoimintaympäristöstä
yhteiskunnalle elintärkeä toiminto
välttämätön toiminto yhteiskunnan toimivuuden kannalta
valtion johtaminen
kansainväl.toiminta
puolustuskyky
Sisäinen turvallisuus
Väestön toimeentulo
Henkinen kriisinkesto
Talouden, infrastruktuurin toimivuus
infrastruktuuri
Kriittisyyden mukaan
Rakenteen mukaan
kriittinen infrastruktuuri
perusrakenteet, niihin liittyvät toiminnot ja palvelut, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi
muu ei-kriittinen infrastuktuuri
muu ei-informaatio-infrastuktuuri
informaatioinfrastruktuuri
perusrakenteet ja toiminnot tietojärjestelmien perustana, tehtävä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely
kriittinen tuotanto, välttämätön tuotanto yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi
kriittiset palvelut välttämättömät palvelut yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi
muu
kriittinen informaatioinfrastruktuuri
elintärkeiden toimintojen tietojärjestelmien perustana olevia rakenteita ja toimintoja, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely