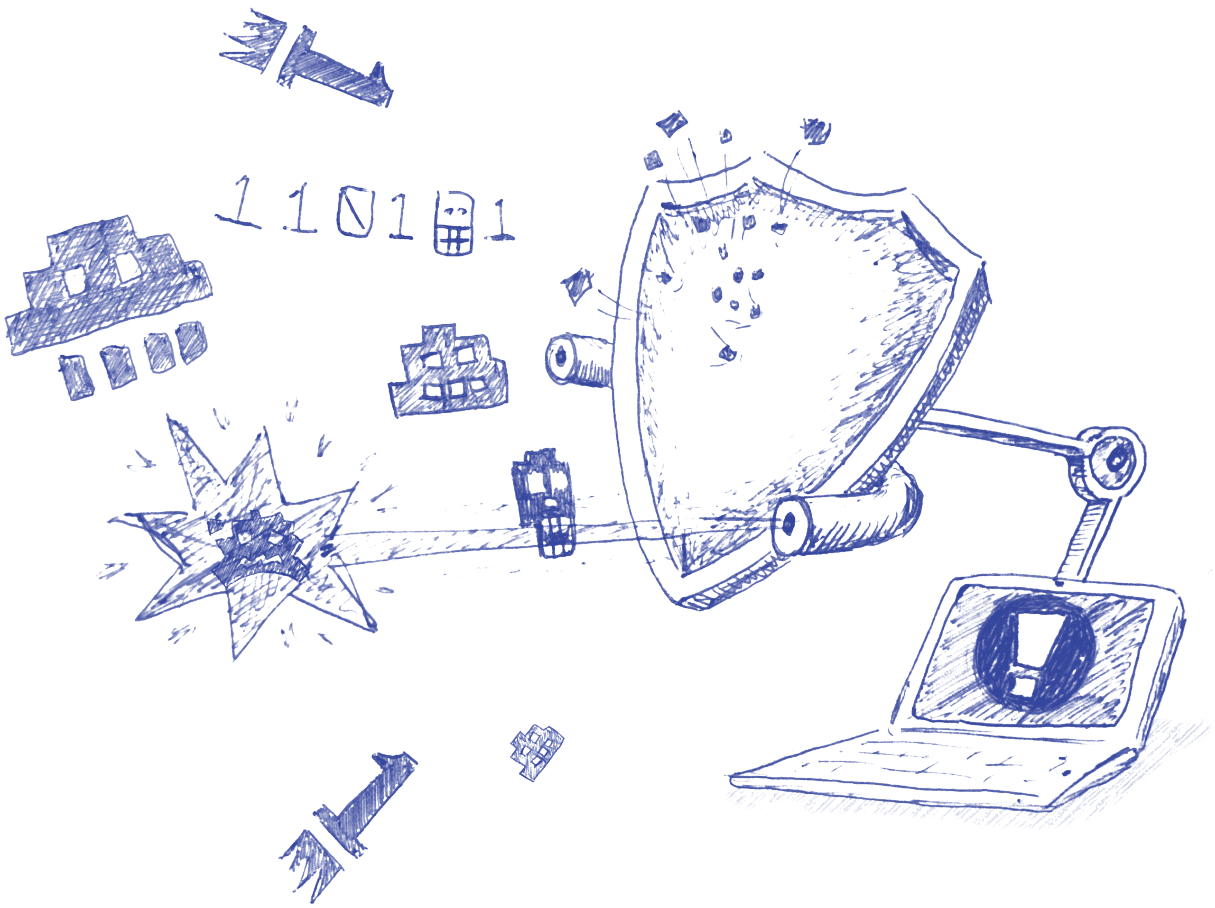
Informaatioteknologian tiedekunnan julkaisuja
No. 20/2015

Martti Lehto, Aili Kähkönen

Kyberturvallisuuden kansallinen osaaminen



JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 20/2015

Editor: Pekka Neittaanmäki
Covers: Kati Valpe
Cover picture: Seppo Tarvainen

ISBN 978-951-39-6105-3 (verkkoj.)
ISSN 2323-5004

Jyväskylän yliopistopaino, Jyväskylä 2015

Kyberturvallisuuden kansallinen osaaminen

Martti Lehto, Aili Kähkönen

Tiivistelmä

Tässä raportissa kuvataan yliopistoissa ja ammattikorkeakouluissa annettavaa kyberturvallisuuden/informaatioturvallisuuden/tietoturvallisuuden tutkimusta, koulutusta, infrastruktuureita ja kansainvälistä toimintaa.

Kyberturvallisuuden/informaatioturvallisuuden/tietoturvallisuuden tutkimus on laaja-alaista ja kattaa merkittävän osan alan tutkimuskentästä. Suomen Akatemian ja Tekesin vuosien 2014–2015 ohjelmassa Information Security sekä valmisteilla olevissa tutkimushankekokonaisuuksissa CyberTrust 2015–2019 ja INKA kyberturvallisuusteema 2014–2020 laajentuu alan tutkimus edelleen. Näissä hankkeissa on mukana yli 10 korkeakoulua ja tutkimuslaitosta sekä yli 50 alan yritystä.

Kyberturvallisuuden/informaatioturvallisuuden/tietoturvallisuuden koulutus on laajentumassa. Koulutuksen toteuttamisessa on kaksi mallia: kyberturvallisuuteen keskittyvä koulutusohjelma tai kyberturvallisuuden opetuksen integroiminen osaksi eri koulutusohjelmia. Ensiksi mainittu malli on käytössä Jyväskylän ja Turun yliopistoissa ja integroitu malli muissa korkeakouluissa. Molemmat mallit ovat välttämättömiä alan osaamisen parantamiseksi. Kyberturvallisuuden koulutusohjelma tuottaa kyberturvallisuuden kokonaisuutta hallitsevia alan ammattilaisia, jotka ovat profiloituneet jollekin eritysosaamisalueelle. Integroitu malli tuottaa osaajia, jotka ymmärtävät sekä tietyn teknologia-alan (tietotekniikka, tietoliikenne, automaatiotekniikka jne.) että siihen liittyvät kyberturvallisuuskysymykset.

Suomeen on rakentunut ja rakentumassa kyberturvallisuuden kehitysympäristöjä. Osassa korkeakouluja ja tutkimuslaitoksia kehitysympäristöt on rakennettu laajentamalla olemassa olevia laboratorioympäristöjä. Tämän lisäksi on rakennettu ja rakennetaan aivan uusia erityisesti kyberturvallisuuden tutkimukseen ja opetukseen keskittyviä ympäristöjä kuten Tampereen teknillisessä yliopistossa, Jyväskylän ja Kymenlaakson ammattikorkeakouluissa, VTT:llä, FISC:ssä ja puolustusvoimissa.

Kansainvälinen yhteistyö on myös laajaa ja laajentuu edelleen. Yliopistoilla ja ammattikorkeakouluilla on useita kansainvälisiä yhteistyökumppaneita, joiden kanssa toteutetaan professorivierailuja, jatko-opiskeluvierailuja, luennoitsijavaihtoa, kursseille osallistumista, konferenssiyhteistyötä ja tutkimushankeyhteistyötä.

Raportissa on esitetty kyberturvallisuuskoulutusta kolmessa ulkomaisessa yliopistossa: University of Gjøvik, Norja, Deakin University, Australia ja University of Washington Tacoma, USA.

SISÄLLYS

KUVIOT

TAULUKOT

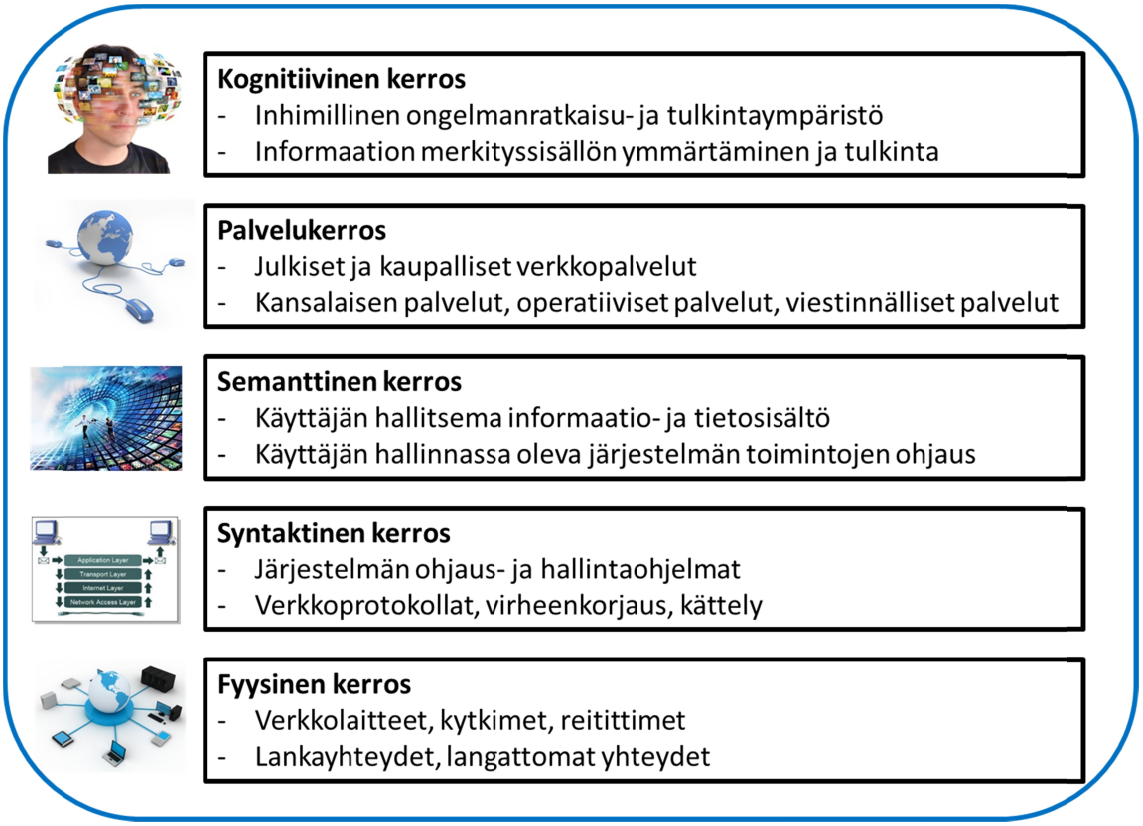
1 JOHDANTO

Tässä raportissa esitellään kyberturvallisuuden tutkimuksen ja koulutuksen nykytilaa Suomessa. Päätavoite on ollut selvittää yleisellä tasolla kyberturvallisuuden osaamisen jakautuminen Suomessa. Raportti on koostettu yhteistyössä korkeakoulujen ja tutkimuslaitosten kanssa. Tässä tutkimuksessa on keskitytty kyberosaamisen osa-alueisiin, joita ovat tutkimus, koulutus, infrastruktuuri, ja kansainväliset verkostot.

Raportissa on lisäksi esitetty muutamia ulkomaisten yliopistojen koulutusohjelmia benchmarking-näkökulmasta.

1.1 Kyberturvallisuuden määritelmä

Martin C. Libicki on luonut kybermaailmaan rakenteen, jonka idea perustuu OSI-malliin (Open Systems Interconnection Reference Model). Tätä Libickin kybermaailman mallia on laajennettu ja sovellettu viisikerroksiseksi, jossa kerroksina ovat fyysinen, syntaktinen, semanttinen, palveluntarjonta ja kognitiivinen (kuva 1). Fyysiseen kerrokseen kuuluvat tiedonsiirtoverkon fyysiset osat kuten verkkolaitteet, kytkimet, reitittimet sekä langalliset että langattomat yhteydet. Syntaktinen kerros muodostuu erilaisista järjestelmän ohjaus- ja hallintaohjelmista sekä toiminnoista, joilla verkkoon kytketyt laitteet ovat vuorovaikutuksessa keskenään kuten verkkoprotokollat, virheenkorjaus, kättely jne. Semanttinen kerros on koko kybermaailman ydin. Siihen kuuluu käyttäjän päätelaitteissa oleva informaatio ja tietosisällöt sekä erilaiset käyttäjän hallinnassa ovat toiminnot kuten printterin ohjaus. Palvelukerrokseen kuuluvat kaikki julkiset ja yksityiset digitaaliset verkkopalvelut. Kognitiivinen kerros kuvaa käyttäjän informaation ymmärrysmaailmaa, maailmaa, jossa informaatiota tulkitaan ja muodostetaan henkilökohtainen ymmärrys ja käsitys. (Libicki 2007)



KUVA 1 Kybermaailman tasomalli

Kyberturvallisuus voidaan lyhyesti määritellä toimenpiteiksi, joilla suojaudutaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteutetaan tarvittavia vastatoimenpiteitä. Kyberturvallisuus rakentuu organisaation tai instituution uhka-analyysille. Kyberturvallisuusstrategian ja -ohjelman rakenne ja elementit riippuvat organisaation arvioiduista uhkatekijöistä ja riskeistä. Useissa tapauksissa on välttämätöntä laatia organisaatiolle useita kohdennettuja kyberturvallisuusstrategioita/ohjeita.

Yhteiskunnan turvallisuusstrategia määrittelee tietoturvallisuuden seuraavasti: ”*Tietoturvallisuudella tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi kaikissa turvallisuustilanteissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuus on myös asiantila, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä.*”

Kansallisessa kyberturvallisuusstrategiassa kyberturvallisuus on määritelty seuraavasti: Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Strategiassa on 3 tarkennusta, joita ovat:

Tarkennus 1
Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle.

Tarkennus 2
Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä (”yhteisöllinen tietoturva”). Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia.

Tarkennus 3
Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.

1.2 Kyberturvallisuuden tutkimuksen ja opetuksen perusteet

1.2.1 Euroopan unionin kyberturvallisuusstrategia 2013

Euroopan unionin kyberturvallisuusstrategian mukaan EU:n olisi turvattava verkkoympäristö, joka tarjoaa mahdollisimman laajan vapauden ja tietoturvan kaikkien hyödyksi. Strategiassa esitelty EU:n visio rakentuu viidelle strategiselle painopisteelle, joita ovat:

- Verkon vakaus
- Verkkorikollisuuden huomattava vähentäminen
- Yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) liittyvän verkkopuolustuspolitiikan ja valmiuksien kehittäminen
- Kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittäminen
- Johdonmukaisen kansainvälisen verkkotoimintapolitiikan luominen Euroopan unionille
- EU keskeisten arvojen edistäminen

EU:n kyberturvallisuusstrategian tavoitteiden saavuttamiseksi komissio on pyytänyt jäsenvaltioita tehostamaan kansallisia toimia verkko- ja tietoturvaopetuksen ja -koulutuksen alalla aloittamalla kouluissa verkko- ja tietoturvaopetus vuoteen 2014 mennessä, antamalla tietotekniikan opiskelijoille opetusta verkko- ja tietoturvasta, tietoturvallisten ohjelmistojen kehittämisestä ja henkilötietojen suojasta sekä antamalla julkishallinnon työntekijöille peruskoulutusta verkko- ja tietoturvan alalla.

1.2.2 Suomen digitaalinen agenda 2011

Valtioneuvoston selonteon Tuottava ja uudistuva Suomi – Digitaalinen agenda vuosille 2011–2020 mukaan tieto- ja viestintäteknologinen kehitys vaikuttaa merkittävästi koulutuksen, tutkimuksen ja kulttuurin tuottamiseen, välittämiseen ja hyödyntämisen ta-

poihin. Sähköisen asioinnin yleistyminen sekä tieto- ja viestintätekniikan hyödyntäminen laajasti kaikessa työelämässä edellyttää koko väestöltä riittäviä tietoyhteiskunta- ja mediataitoja. Lähes kaikki yhteiskunnan elintärkeät toiminnot, mukaan lukien kansallinen ja kansainvälisiin yhteisöihin liittyvä päätöksenteko, ovat jo sidoksissa tieto- ja viestintäinfrastruktuurin sekä tietojärjestelmien toimintaan.

Kansalaisten tulee kokea päivittäinen sähköinen asiointi turvalliseksi ja verkon kaikilla toimijoilla tulee olla luottamus siihen, että tietoturva toimii. Toisaalta kansalaisten ja yritysten tietoisuutta verkon sisältämistä riskeistä ja turvallisista käyttötavoista on lisättävä.

Tieto- ja viestintäteknologinen kehitys vaikuttaa merkittävästi koulutuksen, tutkimuksen ja kulttuurin tuottamiseen, välittämiseen ja hyödyntämisen tapoihin. Sähköisen asioinnin yleistyminen sekä tieto- ja viestintätekniikan hyödyntäminen laajasti kaikessa työelämässä edellyttää koko väestöltä riittäviä tietoyhteiskunta- ja mediataitoja. Tietoyhteiskunnan kannalta on tärkeä varmistaa lasten ja nuorten tulevaisuuden osaaminen ja kyky toimia digitaalisessa ympäristössä. Tämä edellyttää lasten huoltajien, opettajien ja muiden kasvattajien tietoteknisen osaamisen, digitaalisten palvelujen käytön, mediakasvatustietoisuuden ja sosiaalisen pääoman vahvistamista.

Tietoyhteiskunnan nopea muutos luo jatkuvan tarpeen poikkitieteelliselle tietoyhteiskunnan tutkimustiedolle. Koulutuksen kehittämisessä tarvitaan sekä puhtaasti pedagogista tutkimusta että tutkimusta tieto- ja viestintätekniikan vaikutuksista oppimiseen. Suomalainen tutkimus ja tutkimusta palveleva tutkimusinfrastruktuuri on kansainvälisesti korkeatasoista. Suomalainen tutkimus- ja innovaatiojärjestelmä edellyttää jatkossakin panostusta tieto- ja viestintätekniikan tutkimukseen ja huippuosaamiseen.

1.2.3 Suomen kyberturvallisuusstrategia 2013

Kyberturvallisuusstrategian mukaan Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden kärkimaaksi. Kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana. Kyberturvallisuuden kehittämisessä panostetaan voimakkaasti kybertoimintaympäristön tutkimukseen, koulutukseen, työllistymiseen ja tuotekehitykseen, jotta Suomi voisi kehittyä yhdeksi kyberturvallisuuden johtavista maista. Strategiseksi tavoitteeksi asetettiin, että lisätään panostuksia tutkimukseen, tuotekehitykseen ja koulutukseen sekä toimenpiteitä kyberturvallisuuden osaamisen kehittämiseksi koko yhteiskunnan osalta.

1.2.4 Suomen kyberturvallisuusstrategian toimeenpanosuunnitelma 2014

Kyberturvallisuusstrategian toimeenpanosuunnitelman mukaan ”kyberturvallisuuden tutkimus ja opetus, alan teknologioiden kehittäminen sekä innovaatiot ovat talouskasvun lähteitä ja kansallisia erottautumistekijöitä. Viranomaisten välistä tutkimusyhteistyötä vahvistetaan osana turvallisuustutkimuksen toimeenpano-ohjelmaa. Poikkihal-

linnollisia tutkimustarpeita ja -prioriteetteja johdetaan yhteisiksi tutkimusteemoiksi ja vuositason tutkimushankkeiksi.” ”Suomalaisissa yrityksissä ja tutkimusyksiköissä on kyber- ja tietoturvallisuuden huippukyvykkyyttä, mutta osaaminen on pirstaleista. Kattavuuden parantamiseksi yksiköiden, laitosten ja muun yhteiskunnan yhteistyöhön on panostettava.” Toimeenpanosuunnitelma esittää kehittämiskohteena aiheen: ”Kokonaiskuva kyberosaamisen nykytilasta ja toimenpiteet alan tutkimus- ja kehitystyön sekä innovaatiotoiminnan kapasiteetin kehittämiseen”. Kokonaiskuvan tuottamiseksi selvitetään kyberturvallisuuteen liittyvän osaamisen ja tutkimustoiminnan kannalta keskeisten osa-alueiden tilanne ja arvioidaan kypsyystaso, erityisenä kohteena korkeakoulutasoisen tieto- ja kyberturvallisuuden koulutuksen sekä tutkimus- ja kehitystyön edistäminen.

1.2.5 ICT-2015 työryhmän raportti 2013

Suomessa on pula kyberturvallisuusalan ammattilaisista. Tämän perusteella ICT 2015 -työryhmä on tunnistanut Suomen menestymisen kannalta teknologiseen osaamiseen liittyvinä kehityskohteina syvällisen tietojenkäsittelyn osaamisen kehittämisen ja kriittisten avainteknologioiden osaamiskeskittymän luomisen (digitaaliset palvelut ja sisällöt, pelillisyys, tietoturva, mobiliteetti ja big data). Kansainvälisesti kilpailukykyisen ja turvallisen ICT-intensiivisen tuotteen ja palvelun kehittämiseen tarvitaan laajaa osaamista. Onnistuminen edellyttää, että yrityksillä on käytettävissään kyberturvallisuusteknologian huippuosaajien ydintiimi, joka hallitsee syvällisesti alan keskeiset osa-alueet.

Tutkimus ja koulutus kytkevät entistä vahvemmin tiedonhallinnan ja tietointensiivisen osaamisen yritysten kilpailukykyyn ja kilpailuedun saavuttamiseen ja ylläpitämiseen. Vahvistamalla alan tutkimusta ja opetusta edistetään tieteellisiä läpimurtoja, innovaatioiden syntymistä, teknologista kehitystä, tuottavuuden kasvua ja tätä kautta kansallista hyvinvointia.

1.2.6 Innovatiiviset kaupungit 2014–2020 (INKA) kyberturvallisuusteema

INKA 2014–2020 -kyberturvallisuusteeman visiona on luoda Suomesta kansainvälisesti tunnustettu kyberturvallisuuden liiketoiminnan ja osaamisen sekä kyberuhkiin varautumisen maailmanlaajuinen edelläkävijä. Teeman tavoitteena on luoda kansallinen koulutuksen, tutkimuksen ja yritystoiminnan sekä kansainvälisen toiminnan yhteistyöverkosto, jonka avulla kehitetään alan osaamista ja liiketoimintaa, luodaan uusia alan yrityksiä ja saadaan ulkomaisia yrityksiä etabloitumaan Suomeen sekä muodostetaan kansallinen kyberturvallisuuden innovaatiokeskittymä.

Kyberturvallisuusteema vahvistaa alan osaamista ja tutkimusta sekä käynnissä olevia ja alkavia kehittämishankkeita, joiden avulla Suomessa mahdollistetaan uusien tuote- ja palveluinnovaatioiden kehittäminen kansalaisille, yrityksille ja julkiselle sektorille. Kyberturvallisuudesta muodostuu yrityksille niiden liiketoiminnan varmistaja ja kilpailuetu sekä lisäksi se on oma kasvava liiketoiminta-alansa.

Kyberturvallisuusteema rakentuu kahden pilarin varaan, jotka ovat kyberliiketoiminta ja kyberosaaminen. Kyberturvallisuuden innovaatiokeskittymä muodostaa Suomeen kansainvälisen huipputason tutkimus- ja koulutusosaamista sekä kansainvälisesti houkuttelevan ja kilpailukykyisen toimintaympäristön kyberturvallisuusalan huippuosaajille ja yrityksille.

Kyberturvallisuuden huippuosaamista tarvitaan, jotta voidaan saada aikaan ja kehittää kybertilannetietoisuutta, tehokasta varautumista kyberuhkatilanteisiin, luoda kriittisiä infrastruktuureita suojaavia järjestelmiä ja kehittää vaikuttavia kyberturvallisuusratkaisuja.

Kyberturvallisuuskoulutus on määritelty INKA-hankkeessa yhdeksi kärkiteemaksi, jonka mukaan jatketaan kyberturvallisuuden maisteri- ja jatkokoulutuksen kehittämistä laajentamalla ja syventämällä opetustarjontaa ja luomalla kansallinen alan osaamisverkosto tuottamaan huippuopetusta ja vahvistamalla kansallista osaamispääomaa. Kehittämisessä etsitään uusia tapoja toteuttaa koulutusta eri seutukuntien yhteistyönä kehittäen innovatiivisia etäopetusmenetelmiä ja internetin hyödyntämistä opetuksessa.

1.3 Kyberturvallisuus tutkimusalana

Kyberturvallisuuden tutkimukselle on keskeistä monitieteellinen lähestymistapa. Kyberturvallisuutta voidaan lähestyä matemaattisten mallien käytön ja kehittämisen näkökulmasta kehitettäessä anomalioiden havaitsemista ja poikkeamien hallintaa. Laskennallisen tieteen lähestymistavalla voidaan tehokkaasti saavuttaa tutkimustuloksia, kun erilaisia kompleksisia järjestelmiä (tekniset, ihmislähtöiset) voidaan mallintaa ja optimoida entistä tarkemmin. Yhä monimutkaisempien kyberturvallisuuden eri ilmiöiden tutkimuksessa soveltavan matematiikan ja laskennallisen tieteen käyttäminen mahdollistaa aikaisempaa hankalampien ongelmien tai yhteiskunnan monimutkaisten turvallisuusongelmien ratkaiseminen. Laskennallisen tieteen avulla ratkotaan haastavia tutkimusongelmia hyvin monilla tieteenaloilla sekä poikkitieteellisesti. Laskennallisten menetelmien soveltamisessa tarvitaankin paitsi menetelmäosaamista, myös syvällistä sovellusalueen ymmärrystä. Avaintekijöinä laskennallisen tieteen läpimurrolle on ollut tietotekniikan nopea kehitys, erityisesti tietokoneiden laskenta- ja tiedonhallintakapasiteetin erittäin voimakas kasvu, menetelmäosaamisen kehittyminen ja laajeneminen eri tutkimusalueilla.

Kognitiotieteen tutkimusmenetelmien avulla voidaan yhdistää erilaisia ihmistieteellisiä ja teknistaloudellisia tutkimusaloja. Kognitiotieteellinen lähestymistapa antaa mahdollisuuden tutkia kybermaailman toimintaympäristöä ongelmalähtöisesti ja monitieteellisesti integroimalla eri lähitieteiden osaamista tieteidenvälisten kysymysten ratkaisemiseksi. Tutkimuksessa keskitytään luotettavan ja validin mallin kehittämiseen, jolla voidaan määritellä relevantteja ihmisen suorituskyvyn kriteereitä digitaalisessa toimintaympäristössä. Tutkimuksessa korostuvat ne mekanismit, jotka vaikuttavat havaitsemiseen, oppimiseen, muistamiseen, ymmärtämiseen, ajatteluun ja vuorovaikutukseen.

Tavoitteena on pyrkiä selittämään millaiset digitaalisen tilannekuvaympäristön tietojen representaatiot ja tiedonkäsittelyprosessit tuottavat optimaalisen ja adaptiivisen käyttäytymisen erityisesti poikkeusoloissa.

Tietojenkäsittelytiede tieteenalana tutkii tietotekniikkaan ja sen käyttöön liittyviä ongelmia. Perinteisessä tietojenkäsittelytieteessä tutkitaan kaikkia tietoon liittyviä laskennallisia kysymyksiä, mutta nykyään tutkimusala on hyvin laaja. Kyberturvallisuus on koko tieteenalaa läpileikkaava ja se ulottuu laajaan skaalaan teknologioita ja prosesseja suojattaessa verkkoja, tietokoneita, ohjelmia, dataa ja sovelluksia kyberhyökkäyksiltä ja vahingoittumisilta. Osaamistarpeen perusta ulottuu tietojärjestelmätieteeseen, informaatioteknologiaan ja tietojenkäsittelytekniikkaan.

1.4 Kyberturvallisuus koulutusalana

Kyberturvallisuuden osaaminen ei ole vain erillinen ammatillinen osaamisalue vaan se kattaa kyvykkyyksiä kansalaistaidoista aina kansainvälisen tason professioon saakka. Tämän vuoksi kyberturvallisuus tulisi sisällyttää eri koulutusasteisiin. Yleissivistävässä perusopetuksessa koulutuksella tulee varmistaa, että nuorilla on riittävät taidot toimia kybermaailmassa ja he ymmärtävät sen uhat ja osaavat suojautua niiltä. Lukiokoulutuksessa ja ammatillisessa koulutuksessa syvennetään näitä taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa. Ammatilliseen koulutukseen voidaan sisällyttää kyberturvallisuuden alan perusammattitaitoon ja työelämässä tarvittavaan alan ammatilliseen pätevyyteen johtavaa koulutusta.

Yliopistoissa korostuu kyberturvallisuuden tieteellinen tutkimus ja siihen perustuva opetus. Ammattikorkeakoulut tarjoavat käytännönläheistä ja työelämän tarpeita vastaavaa kyberturvallisuuskoulutusta.

Yliopistoissa tulisi voida suorittaa kyberturvallisuuden alalta alempia ja ylempiä korkeakoulututkintoja sekä tieteellisiä jatkotutkintoja. Vastaavasti ammattikorkeakouluissa tulisi voida suorittaa kyberturvallisuusalalta sekä ammattikorkeakoulututkintoja ja että ylempiä ammattikorkeakoulututkintoja. Laajasti koko korkeakoulusektorilla toteutettu kyberturvallisuuskoulutus tuottaa yhteiskunnan eri tasoille alan huippuosaajia, joiden tiedot ja taidot vastaavat eri tehtäviin sisältyviä osaamisvaatimuksia.

Kyberturvallisuus tulee sisällyttää osaksi aikuiskoulutusta. Kyberturvallisuuden aikuiskoulutus voi olla perustutkinto-opetusta, tutkintoon kuuluvia opintoja, näyttötutkintoihin valmentavaa koulutusta, oppisopimuskoulutusta, ammattitaitoa uudistavaa ja laajentavaa lisä- ja täydennyskoulutusta sekä kansalais- ja työelämätaitoihin valmentavia yhteiskunnallisia opintoja ja harrastusopintoja.

Aikuiskoulutusta järjestetään nuorten koulutusjärjestelmään kuuluvissa oppilaitoksissa, yksinomaan aikuiskoulutusta järjestävissä oppilaitoksissa, yrityksissä sekä henkilöstökoulutuksena työpaikoilla. Tämä edellyttää kyberturvallisuuden opettajakoulutuksen

toteuttamista, jotta mahdollisimman tehokkaasti voidaan tuottaa opetusresursseja eri koulutusasteille.

2 KYBERTURVALLISUUSALA SUOMESSA

2.1 Yliopistot ja tutkimuslaitokset

2.1.1 Aalto-yliopisto

Kyberturvallisuuden alan tutkimus ja koulutus on jaettu Aalto-yliopistossa Sähkötekniikan korkeakouluun ja Perustieteiden korkeakouluun. Aalto-yliopistolla tehtävä kyberturvallisuusalan tutkimus on laaja-alaista. Se ulottuu sekä yhteiskunnallisiin että teknisiin kysymyksiin. Riskien ja impaktien analyysi, mallintaminen, erilaisten järjestelmien turvallisuuskysymykset ja julkishallinnon kyberturvallisuutta koskevien kysymysten lisäksi tutkimukset kattavat myös lainsäädännöllisen näkökulman.

2.1.2 Helsingin yliopisto

Kyberturvallisuusalan tutkimusta ja koulutusta toteutetaan Helsingin yliopistolla pääasiassa Matemaattis-luonnontieteellisessä tiedekunnassa Tietojenkäsittelytieteiden laitoksella ja Fysiikan laitoksella.

2.1.3 Jyväskylän yliopisto

Informaatioteknologian tiedekunnassa kyberturvallisuuden tutkimusta ja koulutusta toteutetaan tietotekniikan ja tietojenkäsittelytieteiden laitoksilla. Kyberturvallisuuden teemaopintoja on toteutettu vuodesta 2009 ja oma maisterikoulutusohjelma alkoi tammikuussa 2015.

Informaatioteknologian tiedekunnassa tietojenkäsittelyoppia on opiskeltu Jyväskylän yliopistossa jo vuodesta 1967 alkaen. Tiedekunta vastaa kehittyvän informaatioteknologian sekä digitalisoitumisen tuomiin tutkimus- ja koulutushaasteisiin. Tiedekunta yhdistää kokonaisvaltaisesti teknologian, informaation, organisaatioiden ja liiketoiminnan sekä ihmisen näkökulmat niin tutkimuksessa, koulutuksessa kuin sidosryhmäyhteistyössä.

2.1.4 Maanpuolustuskorkeakoulu

Maanpuolustuskorkeakoulun keskeisenä tehtävänä on tuottaa korkeasti koulutettua henkilökuntaa Puolustusvoimille ja Rajavartiolaitokselle. Sotatieteet on laaja käsite ja monialainen kokonaisuus, jota sitovat yhteen sodat, kriisit ja niihin liittyvät turvallisuusuhat sekä pyrkimykset näiden ehkäisemiseen. Tämän päivän maailmassa sotatie-

teiden on kyettävä ymmärtämään sotilaallista turvallisuutta ja puolustusta laaja-alaisesta turvallisuusviitekehyksestä.

Maanpuolustuskorkeakoululla tehdään vuosittain useita opinnäytetöitä, jotka käsittelevät kyberturvallisuutta. Sotatieteiden kandidaatin ja maisterin opetusohjelmaan kuuluu lisäksi joitakin yksittäisiä kursseja. Kyberturvallisuuden tutkimusta tekevät eri ainelaitosten tutkijat erityisesti ja sotatieteiden tohtoriohjelman opiskelijat.

2.1.5 Oulun yliopisto

Oulun yliopistossa keskitytään erityisesti tekniikkaan ja luonnontieteisiin, informaatioteknologian ollessa yksi Oulun yliopiston tutkimuksen painoaloista. Kyberturvallisuutta käsitellään Tieto- ja sähkötekniikan tiedekunnan Tietojenkäsittelytekniikan osastolla ja kryptologian osalta Matematiikan laitoksella.

Tietotekniikan osaston tutkimus keskittyy mm. konenäön, lääketieteellisen tekniikan älykkään informaationkäsittelyn, tietoturvan ja ubiikki internet aihealueisiin. Tietoturvan alueella tutkitaan tietoturvallista ohjelmointia, digitaalista vesileimausta ja biometristä tunnistusta.

2.1.6 Puolustusvoimien tutkimuslaitos

Puolustusvoimien tutkimuslaitos (PVTUTKL) on Pääesikunnan alainen sotilaslaitos, joka tuottaa asiakaslähtöisesti puolustusvoimien tarvitsemat vaativat tutkimus-, kehittämis-, testaus- ja evaluaatiopalvelut. Se on monialainen tutkimusorganisaatio, joka kokoaa yhteen sotataitoon ja käyttöperiaatteisiin, puolustusmateriaaliin ja -teknologiaan sekä ihmisen toimintakykyyn liittyvää tutkimus- ja kehittämistoimintaa.

Puolustusvoimien tutkimuslaitoksen tietoverkkosodankäynnin tutkimusalalla tutkitaan muun muassa haavoittuvuustestauksen menetelmiä ja kryptologiaan liittyviä kysymyksiä. Ulkopuolista opetusta ei laitoksessa anneta, mutta varusmiespalveluksen tai työharjoittelun voi suorittaa tässä yksikössä.

2.1.7 Tampereen teknillinen yliopisto

Tieto- ja sähkötekniikan tiedekunnassa tutkitaan pilvipalveluiden tietoturvaa, identiteetin- ja pääsynhallintaa, avaintenhallintaa, kryptograafisia protokollia ja turvallista ohjelmointia. Kyberturvallisuuden tutkimus ja koulutus ovat osa eri laitosten toimintaa. Ongelmakenttää lähestytään sekä automaation tietoturvan että tietojenkäsittelytieteiden näkökulmasta.

2.1.8 Turun yliopisto

Turun yliopisto tarjoaa monialaisen tutkimusympäristön tietoturva-aiheeseen nivoen yhteen asiantuntijoita tietotekniikasta, matemaattisesta kryptografiasta ja tietojärjestelmätieteestä. Tutkimuskohteita ovat muun muassa kryptologia, mobiilin viestinnän tietoturva ja tietosuoja, ohjelmistoturvallisuus, sulautettujen järjestelmien turvallisuus, tietoverkkojen turvallisuus, ihmisläheiset aspektit tietoturvassa sekä tietoturva ja liiketoiminnan jatkuvuuden turvaaminen.

2.1.9 Valtion teknillinen tutkimuslaitos

VTT on kansainvälisesti verkottunut, moniteknologinen tutkimuskeskus, joka tuottaa korkeatasoisia teknologisia ratkaisuja ja innovaatiopalveluja. VTT lisää asiakkaidensa kansainvälistä kilpailukykyä ja edistää näin yhteiskunnan kestävää kehitystä, työllisyyttä ja hyvinvointia. Teollisuuden automaation tietoturva ja siihen liittyvät auditoinnit ovat olleet pitkään VTT:n toimialueella. Kyberturvallisuuden osuutta tutkimuslaitoksen kokonaisuudessa kasvatetaan.

2.2 Ammattikorkeakoulut

2.2.1 Centria-ammattikorkeakoulu

Centria-ammattikorkeakoulu profiloituu työelämälähtöisyyteen ja turvallisuuteen. Pyrkimyksenä on jatkuvasti tuoda ja luoda uutta tietoa, osaamista ja teknologioita. Centrian profiloituminen turvallisuuteen tuo alueelle uutta osaamista, jolla vahvistetaan elinkeino- ja työelämän laatua, tuottavuutta ja kilpailukykyä.

Centria-ammattikorkeakoulun painoaloilla teollisuusprosessien ja tuotantoteknologioiden kehittäminen, tietoverkot ja niihin liittyvä sisällöntuotanto sekä moniammatillinen palvelu- ja liiketoimintaosaaminen kyberturvallisuus kohdistuu seuraaviin aloihin: teollisen internetin ja langattomien järjestelmien tietoturva, kriittisten järjestelmien tietoturva, IoT ja tietoturva sekä älyliikenteen tilannetietoisuus ja yksityisyyden suoja.

2.2.2 Jyväskylän ammattikorkeakoulu

Kyberturvallisuus on yksi JAMKin strategiassa määritellyistä viidestä painoalasta. Painoalalla edistetään koulutuksen ja TKI-toiminnan keinoin kyberturvallisuuteen pohjautuvaa osaamista ja liiketoimintaa sekä lisätään yrittäjyyttä. Kyberturvallisuuden painoala on geneerinen osaamisalue, joka ylittää JAMKin tulosyksiköiden rajat. Kyberturvallisuuden tutkimus-, koulutus- ja kehitystoimintaa toteutetaan IT-instituutin JYVSECTEC tutkimus-, koulutus ja kehityskeskuksessa. Tämän lisäksi IT-instituutissa toteutetaan englanninkielistä kyberturvallisuuden YAMK-koulutusohjelmaa.

2.2.3 Kymenlaakson ammattikorkeakoulu

Kymenlaakson ammattikorkeakoulun tavoitteena on yhdistää peliohjelmointi-, kyberturvallisuus- ja datakeskusosaaminen yhdeksi kokonaisuudeksi, jonka osaamistavoitteet ovat datakeskusten, tietoverkkoratkaisujen ja käyttöjärjestelmien tietoturvallisessa toteuttamisessa, penetraatiotestauksessa ja tunkeutumisen havaitsemisessa. Osa kyberturvallisuuskoulutuksesta toteutetaan pelillistämisen keinoin.

2.2.4 Laurea ammattikorkeakoulu

Laurea ammattikorkeakoulussa voi suorittaa tradenomin tutkinnon YAMK-tutkinnon yhteiskuntatieteiden, liiketalouden ja hallinnon alan liiketalouden, turvallisuuden ja tietojenkäsittelyn ohjelmissa. Turvallisuusalan koulutus tähtää monialaiseen turvallisuusosaamiseen kuten kiinteistöjen turvallisuuteen, henkilöjen turvallisuuteen, toiminnan turvallisuuteen, yhteiskunnan turvallisuuteen, tietoturvallisuuteen ja turvallisuusjohtamiseen liittyvää osaamista.

2.2.5 Oulun ammattikorkeakoulu

Oamk on monialaisuutta, alueen vahvaa tieto- ja viestintäteknologiaosaamista hyödyntävä osaaja, alueen innovaatiotoiminnan aktiivinen kehittäjä. YAMK:n Tietotekniikan tutkinto-ohjelmaan sisältyy tietoturvallisuuden suunnitteluosaamisen opintojakso.

2.2.6 Poliisiammattikorkeakoulu

Poliisiammattikorkeakoulussa tehdään yksittäisiä väitöskirjatutkimuksia kyberturvallisuudesta. Kurssivalikoimassa ja opinnäytetöissä on myös mukana joitakin aiheeseen liittyviä tarkasteluita. Lisäksi Poliisiammattikorkeakoulu järjestää kyberturvallisuuteen liittyvää ammatillista täydennyskoulutusta poliisihallinnossa työskentelevien ammattitaidon ylläpitämiseksi ja kehittämiseksi.

2.2.7 Turun ammattikorkeakoulu

Turun ammattikorkeakoulun profiilina on monialaisuuteen perustuva innovaatiopedagogiikka, jossa yrittäjyys, soveltava T&K-toiminta ja kansainvälisyys kytketään opetukseen. Soveltava ICT on yksi ammattikorkeakoulun tutkimus- ja kehitys- ja innovaatio (TKI)-ohjelmista. Tieto- ja viestintätekniikan insinöörikoulutuksessa sekä Tietojenkäsittelyn IT-tradenomikoulutuksessa yksi opintopoluista on Tietoturva. Lisäksi kansainvälisessä Degree Program in Information Technology -koulutusohjelmassa Data Networks and Information Security on yksi opintopoluista.

3 KYBERTURVALLISUUSALAN TUTKIMUS SUOMESSA

3.1 Yliopistot ja tutkimuslaitokset

Turvallisuus ja kyberulottuvuus kattavat lukuisia elämänaloja ja tutkimuskohteita. Useat tieteenalat käsittelevät kyberturvallisuuteen liittyviä teemoja. Tietotekniikassa, tietojärjestelmätieteissä, tietojenkäsittelytieteissä, informaatiotekniikassa ja systeemitekniikassa on tutkittu pitkään kysymyksiä, jotka liittyvät kyberturvallisuuteen.

Yliopistoilla on perinteisesti omat laitoksensa tietotekniikalle, tietojenkäsittelytieteille ja systeemitekniikalle. Näiden lisäksi on kasvatettu muun muassa big datan, pilvipalveluiden, käytettävyyden ja sulautettujen järjestelmien tutkimusta, joissa on mukana myös kyberturvallisuusnäkökulmia.

3.1.1 Aalto-yliopisto

Kyberturvallisuuden alan tutkimusta tehdään Aalto-yliopistossa Perustieteiden korkeakoulussa ja Sähkötekniikan korkeakoulussa. Tutkimusaiheita ovat muun muassa:

- Ethernet-verkkojen turvallisuus
- Software-define Network (SDN) ja sen turvallisuuskysymykset ja mahdollisuudet
- Hyökkäyskohteiden automaattinen etsintä ja identifointi julkisista verkoista
- Hyökkäystentorjuntajärjestelmien (Intrusion Prevention/Detection System, IPS/IDS) testaus ja kehitys uudenlaisia uhkia vastaan
- Pilviteknologian avulla toteutettavat turvapalvelut
- Teollisuusautomaation turvallisuus
- Riski- ja impaktianalyysi
- Geneettisten algoritmien käyttö hyökkäyksien mallintamisessa
- Älykkäiden sähköverkkojen turvallisuus ja yksityisyyden suoja
- Julkishallinnon kyberkyvykkyys
- Lainsäädännön soveltuvuus kyberyhteiskuntaan
- Hajautettujen automaatiojärjestelmien uudet ohjelmointitekniikat
- Internetin ja tietoverkkojen turvallisuus
- Palvelunestohyökkäyksiltä suojautuminen
- Tulevaisuuden Internet-protokollien turvallisuus
- Tietotekniikan ja tietoverkkojen uusien sovellusalueiden tietoturva
- NFC-kommunikaation ja maksujärjestelmien turvallisuus
- Pilvipalveluiden turvallisuus
- Laitteiden välisen kommunikaation (Internet of Things) turvallisuus

- Yksityisyyden suoja
- Symmetristen salausmenetelmien analyysimenetelmät
- Salausmenetelmille tehokkaiden ja turvallisten ohjelmisto- ja laitepohjaisten toteutusten kehittäminen

3.1.2 Helsingin yliopisto

Helsingin yliopistossa kyberturvallisuusalan tutkimusta tehdään pääasiassa Matemaattis-luonnontieteellisessä tiedekunnassa. Siihen kuuluvissa Tietojenkäsittelytieteiden laitoksessa ja Fysiikan laitoksessa on tutkijoita, joiden tutkimuskohteisiin kuuluu kyberturvallisuuden kysymyksiä. Tutkimusaiheita ovat:

- Mobiilitietoturva
- Luottamuksen hallinta
- Tietoturva ja käytettävyys
- Esineiden Internet
- Tietoliikenneprotokollat
- Big Data
- Hajautettujen järjestelmien luotettavuus
- ICT-sektorin sovellusten kehittäminen
- Kasvavien tietomassojen hyödyntäminen ja jalostaminen moderneilla tavoilla

3.1.3 Jyväskylän yliopisto

Tietotekniikanlaitoksen tutkimus perustuu pääosin analyyttis-konstruktiivisten menetelmien käyttöön teknisestä, laskennallisesta, matemaattisesta tai pedagogisesta näkökulmasta. Sen tutkimusaloja ovat kybertilannekuva ja -tilannetietoisuus, kriittisen infrastruktuurin suojaaminen kyberhyökkäyksiltä, identiteetin ja tekijäoikeuksien suojaaminen, anomalioiden havaitseminen, APT-hyökkäysten havaitseminen ja torjunta sekä kyberpuolustus.

Tietojenkäsittelytieteiden laitoksen tutkimuksessa tarkastellaan tietojärjestelmiä ja tietojenkäsittelyä neljästä näkökulmasta: teknologinen, ihmiskeskeinen, liiketoiminnallinen ja informaatiokeskeinen. Nämä näkökulmat muodostavat laitoksen yleisen tehtävän: ymmärtää, kehittää, suunnitella ja hallita tietojärjestelmiä ja tietojenkäsittelyä sekä niiden vaikutuksia kokonaisvaltaisesti käyttökontekstissaan.

Laitoksen tutkimuksessa kyberturvallisuuden tutkimusaloja ovat tieto- ja kyberturvallisuusstrategian kehitysmenetelmät, tietoturvan johtaminen ja hallinta, turvallisten tietojärjestelmien kehitysmenetelmät, tietoturvakäyttäytymisen ja tietoturvakulttuurin parantaminen, tietoturvainvestoinnit, social engineering ja phishing -teemat.

3.1.4 Lappeenrannan teknillinen yliopisto

Lappeenrannan teknillisessä yliopistossa sivutaan kyberturvallisuutta osana ohjelmistotuotannon ja tiedonhallinnan tutkimusta. Näillä tutkimusaloilla keskitytään ohjelmistotyön tehostamiseen käyttäjälähtöisistä ratkaisuista organisaatiokeskeiseen kehittämiseen.

3.1.5 Maanpuolustuskorkeakoulu

Kyberturvallisuutta tutkitaan Maanpuolustuskorkeakoulussa sen eri laitoksissa.
Sotataidon, johtamisen ja sotilaspedagogiikan sekä sotatekniikan laitokset tuovat tutkimuskenttään erilaisia lähestymistapoja. Tutkimuksia tehdään osana sotatieteiden tohtorin opintoja ja lisäksi sekä perustutkinto-opiskelijat että yleisesikuntaupseerikurssilaiset ovat tarkastelleet kyberturvallisuutta opinnäytetöissään.

Sotatekniikan laitoksella tutkitaan erityisesti teemoja, jotka liittyvät tilannekuvan luomiseen, kriittisen infrastruktuurin suojaamiseen ja verkostoavusteiseen puolustukseen.

3.1.6 Oulun yliopisto

Tietoturvallisen ohjelmoinnin tutkimusryhmä on kansainvälisesti arvostettu tutkimusryhmä, joka on profiloitunut tietoturvahaavoittuvuuksien löytäjänä. Ryhmä on osa Tieto- ja sähkötekniikan tiedekuntaa ja tietotekniikan osastoa. Samassa tiedekunnassa on myös tietojenkäsittelytieteiden laitos ja tietojärjestelmien tietoturvallisuuden tutkimuskeskus.

Oulun yliopistossa tutkitaan:

- Processes and quality
- Agile & Lean methods
- Software development methodologies
- Requirements engineering
- Software and system architectures
- Cloud based development and systems (in and for cloud)
- Innovation processes
- Service design methods and tools
- Computer Security at Nuclear Facilities
- Integration of information security to the information systems and software development methods
- Behavioral aspects of information security at the organizational and home contexts-effect of information security training and awareness for employees

Tietotekniikan osastolla tehdään huippututkimusta konenäön, lääketieteellisen tekniikan, älykkään informaationkäsittelyn, tietoturvan sekä ubiikin internetin alueilla.

Sulautettujen järjestelmien tutkimuksen tavoitteena on luoda valmiudet suunnitella sulautettuja järjestelmiä muun muassa matkapuhelimiin, puhelinverkkoihin, autoihin, päälle puettaviin laitteisiin, kodinkoneisiin ja viihde-elektroniikkaan.

Informaatiotekniikan tutkimuksessa kohteina ovat mm. laskennallisesti älykkäiden järjestelmien keskeiset menetelmät ja tekniikat kuten tekoäly, tietämystekniikka, digitaalinen signaalinkäsittely ja konenäkö.

Soveltavan tietotekniikan alueella luodaan valmiuksia tutkia ja kehittää uusinta teknologiaa hyödyntäviä ohjelmistoja käyttäjien ja yritysten tunnistamiin tarpeisiin, kuten jokapaikan tietotekniikka, Internet-teknologiat, mobiili ja sosiaalinen laskenta.

3.1.7 Puolustusvoimien tutkimuslaitos

Puolustusvoimien tutkimuslaitoksen Informaatiotekniikkaosastossa kasvatetaan tietoverkkosodankäynnin tutkimusalaa osana kansallista puolustusta. Tutkimusta suoritetaan kiinteässä yhteistyössä eri yliopistojen ja muiden tutkimuslaitosten kanssa.

Informaatiotekniikkaosasto tutkii radiotaajuisia sensori- ja vaikuttamisjärjestelmiä, tietoverkkosodankäyntiä ja johtamisjärjestelmiä. Vaikuttamiseen, tiedusteluun ja suojautumiseen keskittyvän analyysin kohteena ovat järjestelmien vaikuttavuus ja kokonaissuorituskyky elektronisella taistelukentällä. Kehittyvä laskentalaboratorio ja tietoverkkosodankäynnin suuntaan laajeneva toiminta perustuvat osaston elektronisen sodankäynnin, tiedonsiirron, johtamisjärjestelmien ja tutkatekniikan sekä radiotaajuisten aseiden tutkimukseen.

3.1.8 Tampereen teknillinen yliopisto

Tampereen teknillisessä yliopistossa tutkitaan kyberturvallisuutta pääasiassa kahdella laitoksella: Tietotekniikan laitoksella ja Systeemitekniikan laitoksella. Tutkimusaiheita ovat:

- Pilvipalveluiden tietoturva
- Security Service Level Agreements
- Identiteetin- ja pääsynhallinta
- Avaintenhallinta
- Kryptograafiset protokollat
- Turvallinen ohjelmointi
- Hardware-orientoitunut tietoturva
- Automaation tietoturva

3.1.9 Tietotekniikan tutkimuslaitos

Tietotekniikan tutkimuslaitos (Helsinki Institute for Information Technology, HIIT) on Helsingin yliopiston ja Aalto-yliopiston yhteinen tutkimuslaitos, jossa sivutaan kyber-

turvallisuutta osana muuta tutkimusta. Tietotekniikan tutkimuslaitokset tutkimusohjelmia ovat:

- Algorithmic Data Analysis
- Computational Inference
- Distributed and Mobile Cloud Systems
- Future Internet
- Network Society

Tietotekniikan tutkimuslaitos HIIT ja Helsingin yliopiston oikeustieteellinen tiedekunta tekevät kyberturvallisuuteen liittyvää oikeudellista tutkimusta etenkin henkilötietojen suojan osalta. Käynnissä on yhteinen Emil Aaltosen säätiön rahoittama tutkimusprojekti "*Henkilötietojen suoja digitalisoituvassa yhteiskunnassa"*.

3.1.10 Turun yliopisto

Tietoturva-alan tutkimus on nimetty Turun yliopiston strategiassa yhdeksi yliopiston neljästä voimakkaan kehitysvaiheen tutkimusalasta, ja on tätä kautta yliopiston strategisen hankerahoituksen piirissä. Turun yliopisto tarjoaa monialaisen tutkimusympäristön tietoturva-aiheeseen nivoen yhteen asiantuntijoita tietotekniikasta, matemaattisesta kryptografiasta ja tietojärjestelmätieteestä.

Tutkimusalat ovat:

- Man-In-Browser -hyökkäysten olemus ja torjuminen
- Turvallisuusmonitorien upottaminen aspekti-pohjaisin tekniikoin ohjelmiin
- Tietoverkkoreitityksen turvallisuus
- Tietoturva-algoritmien suorittamiseen optimoitujen ohjelmoitavien prosessorien suunnittelu
- Sähköisen äänestyksen turvallisuus
- Kryptografinen tutkimus
- Monitieteellinen kyberturvallisuuden tutkimus
- Tietoturvan ihmiselementin tutkimus
- Cryptography and data security
- Networked systems security
- Business continuity management

3.1.11 Turun tietotekniikan tutkimus- ja koulutuskeskus

Turun tietotekniikan tutkimus- ja koulutuskeskus (Turku Centre for Computer Science, TUCS) on Turun yliopiston ja Åbo Akademin yhteinen tutkimuslaitos, jonka Software Development Laboratory:ssa (SwDev) tutkimus kohdistuu laaja-alaisesti ohjelmistokehitykseen. Tutkimuksessa on mukana kyberturvallisuusnäkökulma. Tutkimusaloja ovat mm:

- Cloud service architectures and business models
- Game development and gamification
- Software business, special focus on start-ups

- Software development methodologies and processes
- Software ecosystems
- Software metrics, testing and security
- Software production
- Software techniques, especially related to parallelism
- Software technology-enabled services and managing technology-service convergences

3.1.12 Valtion teknillinen tutkimuslaitos

Valtion teknillinen tutkimuslaitos (VTT) on kansainvälisesti verkottunut, soveltavaa tutkimusta tekevä moniteknologinen tutkimuskeskus. VTT:n tutkimusvisiota ohjaavat digitalisoituminen ja kestävä kehitys. Tiedon digitalisoituminen ohjaa tieto- ja viestintäteknologian lisäksi kaikkien sen sovellusalueiden kehittymistä. Kestävä kehitys puolestaan edellyttää ympäristön huomioimista niin tuotteissa, palveluissa kuin valmistusprosesseissakin.

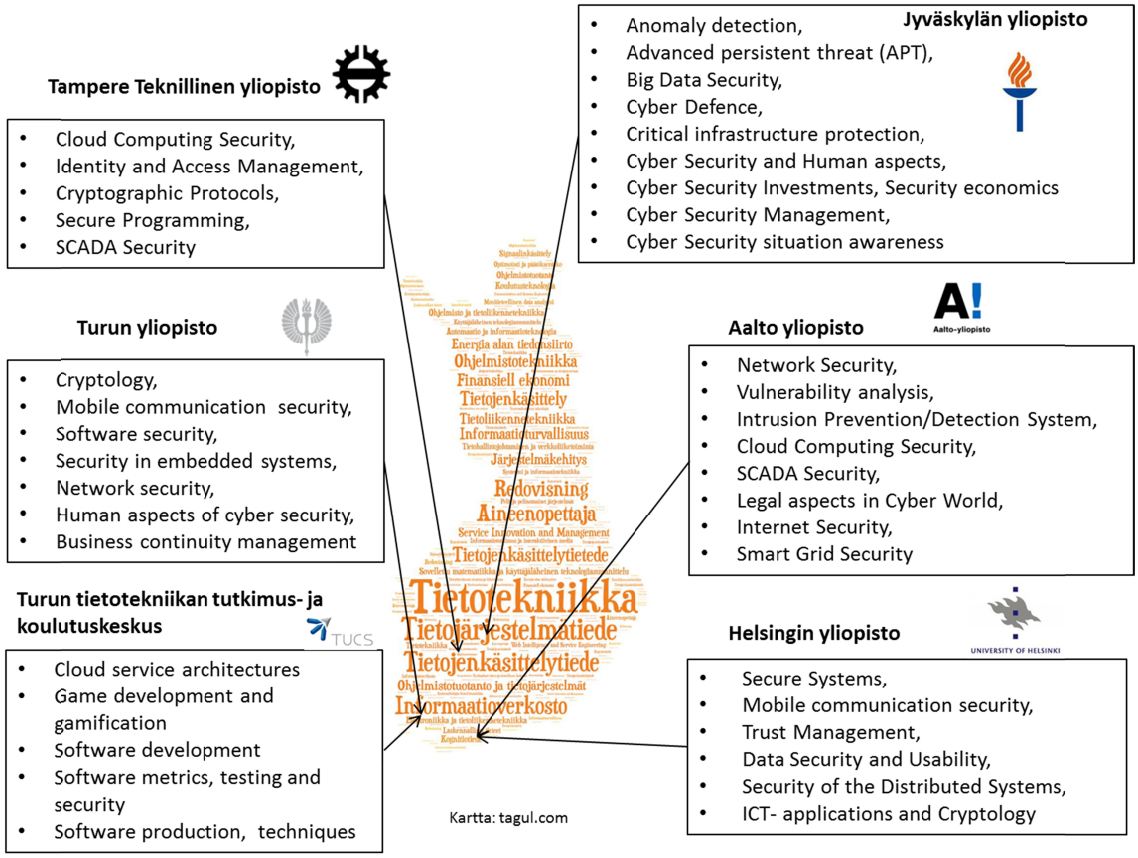
VTT:llä tietoturvatutkimus on laaja kokonaisuus, johon sisältyy tutkimustyötä ja kehitystyötä alkaen tutkimuksellisista ongelmanasetteluista aina käytännöllisiin ja käyttökelpoisiin tietoturvaratkaisuihin saakka.

VTT tutkii ja kehittää ICT-teollisuuden tarpeisiin sopivia menetelmiä ohjelmistointensiivisten järjestelmien ja tuotteiden tietoturvan varmistamiseen. Tällä alueella päätutkimuskohteita ovat: tietoturvan analysointimenetelmät, ohjelmiston tietoturvan varmistaminen, operatiivisen järjestelmän tietoturvan seuranta ja varmistaminen sekä tietoturvametriikat. Tutkimusaloja ovat:

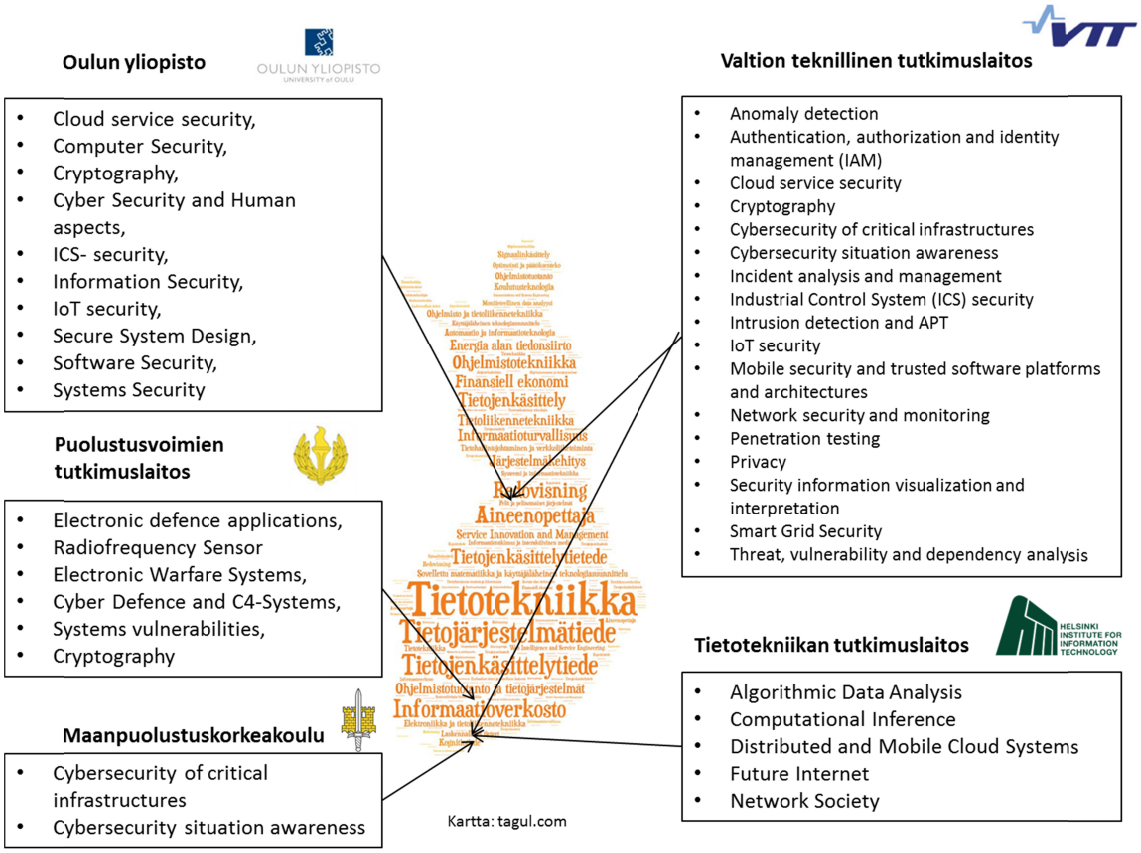
- Adaptive security
- Android platform security
- Anomaly detection
- Authentication, authorization and identity management (IAM)
- Built-in security
- Cloud service security
- Cryptography
- Cybersecurity of critical infrastructures
- Cybersecurity situation-awareness
- Incident analysis and management
- Industrial Control System (ICS) security
- Intrusion detection and APT
- IoT security
- Mobile security and trusted software platforms and architectures
- Network security and monitoring
- Penetration testing
- Piracy prevention
- Privacy
- Risk analysis and risk-driven design
- Secure services

- Security architectures and communication protocols
- Security assurance: security analysis, testing and monitoring, auditing
- Security economics
- Security information visualization and interpretation
- Security metrics and data aggregation
- Security standardization activities
- Security testing
- Smart Grid Security
- Strengthening legacy systems
- Threat, vulnerability and dependency analysis
- Trust management
- Trust relationships in networks
- Usable security

Kuvissa 2 ja 3 on esitetty kyberturvallisuuden tutkimusta eri yliopistoissa ja tutkimus-laitoksissa.



KUVA 2 Kyberturvallisuuden tutkimusta yliopistoissa ja tutkimuslaitoksissa



KUVA 3 Kyberturvallisuuden tutkimusta yliopistoissa ja tutkimuslaitoksissa

3.2 Ammattikorkeakoulut

3.2.1 Centria-ammattikorkeakoulu

Centria-ammattikorkeakoulun kyberturvallisuuteen liittyviä tutkimus-, kehitys- ja innovaatiotoiminnan aloja ovat:

- Teollisen internetin tietoturva
- Kriittisten järjestelmien tietoturva
- IoT ja tietoturva
- Älyliikenteen tilannetietoisuus ja yksityisyyden suoja
- Tietoturva sosiaali- ja terveysalalla

3.2.2 Jyväskylän ammattikorkeakoulu

Jyväskylän ammattikorkeakoulussa kyberturvallisuuden tutkimusta tehdään osana kyberturvallisuuden JYVSECTEC tutkimus-, koulutus- ja kehityskeskuksen toimintaa.

Tutkimusaiheita ovat:

- Cyber security situation picture
- Security information's visualization
- Cyber security situation awareness
- Visualization of security risk management
- Cloud service security
- Security testing
- Penetration testing
- Security training
- Security pre-auditing
- Threat analysis
- Security protocols

3.2.3 Kymenlaakson ammattikorkeakoulu

Kyberturvallisuusalan tutkimus on keskittynyt Kymenlaakson ammattikorkeakoulussa datakeskusten ja pilvipalvelujen tietoturva-, tunkeutumisenhavaitsemis- ja tunkeutumisista toipumistilanteiden tutkimiseen.

3.2.1 Turun ammattikorkeakoulu

Turun ammattikorkeakoulun tutkimus-, kehitys- ja innovaatiotoiminta (TKI) on laajaa ja monipuolista. Lähes 30 erilaista tutkimusryhmää työskentelee eri tutkimusalueilla. Työn tukena ammattikorkeakoululla on alueellisten verkostojen lisäksi vahvat kansalliset ja kansainväliset kumppaniverkostot.

Tietoturva-aiheinen TKI-toiminta on tutkimusryhmän Tietoliikenne ja tietoturva vastuulla. Tutkimusryhmän tavoitteena on kattaa laajasti yritysten liiketoimintaan liittyvät tietojärjestelmät, -verkot ja niiden käyttöön liittyvät tietoturvahaasteet. Erityisenä tavoitteena on tietoturvatietoisuuden lisääminen. Erityisesti keskitytään PK-sektorin yritysten liiketoimintaedellytysten parantamiseen ICT:n avulla. Tämän lisäksi osallistutaan kansallisiin ja kansainvälisiin tutkimushankkeisiin. Toimintaan kuuluu mukaan vuosittainen PK-yrityksille suunnattu Tietoturvapäivä sekä Kansalaisen mikrotuki, joka tukee kaikkia turkulaisia tietoturvaan liittyvissä jokapäiväisissä ongelmissa.

4 KYBERTURVALLISUUSALAN KOULUTUS SUOMESSA

4.1 Yliopistot

4.1.1 Aalto-yliopisto

Aalto-yliopistossa tietoturvallisuutta opiskellaan aina jonkin sovellusalueen rinnalla, eikä erillisenä pääaineena tai ohjelmana. Keskeisenä sovellusalueena ovat tietoverkot, mutta tietoturvallisuuden opintoja on mahdollista yhdistää DI-opintojen sivuaineeksi minkä tahansa tekniikan alan rinnalle. Tietotekniikan laitoksella opetus keskittyy tekniseen tietoturvallisuuteen, koska myös tutkimus painottuu tekniikkaan.

Automaatio- ja informaatioteknologian hakukohteen kautta valitut opiskelijat suorittavat tekniikan kandidaatin tutkinnon sähkötekniikan kandidaattiohjelmassa pääaineenaan joko automaatio- ja systeemitekniikka tai informaatioteknologia. Tutkintoon kuuluvat kandidaattiohjelman yhteiset perusopinnot, pääaineen opinnot, sivuaineen opinnot sekä valinnaiset opinnot. Tarjolla olevia kursseja ovat muun muassa:

- Tietoverkkojen turvallisuuden peruskurssi
- Automaatiojärjestelmien turvallisuus
- Kyberturvan jatko-opiskelijaseminaari ja
- Kyberturvallisuuden moduuli (opintokokonaisuus)

Ohjelmista valmistuu vuosittain yhteensä yli 30 diplomi-insinööriä, joista 10–15 tekee opinnäytteensä tietoturvallisuuden alueelta.

Aalto-yliopiston tietojenkäsittelytieteen laitoksen pääaineessa on mahdollisuus suorittaa kryptologian kursseja sekä kirjoittaa diplomityö kryptologian alalta. Opetusohjelmassa tarjotaan seuraavat kurssit:

- Cryptography and Data Security
- Cryptology
- Advanced Course in Cryptology

4.1.2 Helsingin yliopisto

Tietojenkäsittelytieteen laitoksella on Hajautettujen järjestelmien ja tietoliikenteen erikoistumislinja. Linjalla keskitytään alan keskeisiin aihepiireihin sekä kiinteän verkon palveluiden että mobiililaitteiden näkökulmasta. Internet-teknologiat ovat linjan keskiössä kuten myös hajautettujen järjestelmien teoria sekä käytännön toteutus moderneissa ohjelmistoratkaisuissa.

Ryhmän erityisosaamisiin kuuluvat Internet-teknologiat ja palvelut, liikkuvuus (teknologia- ja paikkariippumattomuus, langaton kommunikointi), vuorovaikutteiset järjestelmät, kontekstitietoisuus ja interaktiiviset järjestelmät. Alueella yhdistyy laitoksella perinteikäs langattoman ja liikkuvan tietojenkäsittelyn tutkimus uusiin, kasvaviin tutkimusteemoihin. Tutkimuksen painopiste on laajentunut protokollista sovelluskerroksen ongelmiin ja ratkaisuihin. Linjan syventävät opinnot (80 op) sisältää seuraavat kyberturvallisuuteen liittyvät kurssit:

- Tietoturvan perusteet
- Cryptography and Network Security
- Software Security
- Mobile Platform Security

4.1.3 Jyväskylän yliopisto

Informaatioturvallisuuden maisteriohjelma (120 op) on Informaatioteknologian tiedekunnan ainelaitosten yhteinen koulutusohjelma, mikä mahdollistaa sekä tietojenkäsittelytieteiden laitoksen että tietotekniikan laitoksen kandidaattitutkinnon suorittaneille opiskelijoille opiskelun tässä FM-tutkintoon johtavassa maisteriohjelmassa. Maisteriohjelman pääaineena on tietojenkäsittelytiede ja siihen valitaan vuosittain 20 opiskelijaa.

Informaatioturvallisuuden maisteriohjelman yleisenä tavoitteena on antaa opiskelijalle johdatus informaatioturvallisuuden kokonaisuuteen sekä syventäviä opintoja informaatioturvallisuuden eri osa-alueilta. Informaatioturvallisuuden opetus muodostuu opintokokonaisuudessa, jossa tarkastellaan kybermaailmaa ja sen turvallisuutta yhteiskunnallisesta, toiminnallisesta, teknologisesta ja systeemisestä näkökulmasta.

Teknologialähtöisestä suuntautumisvaihtoehdosta valmistunut maisteri kykenee määrittelemään tietoon, tietoverkkoihin, ja -liikenteeseen sekä tieto- ja ohjausjärjestelmiin sekä toimintaprosesseihin liittyviä informaatioturvallisuusriskejä. Hän tuntee kybermaailman eri uhkamallit ja tuntee uhkien torjuntaan liittyvät toiminnalliset ja teknologiset ratkaisumallit. Hänellä on hyvät valmiudet suunnitella, toimeenpanna ja johtaa informaatioturvallisuuden teknologista suunnittelua ja kehittämistä.

Organisaatiolähtöisestä suuntautumisvaihtoehdosta valmistunut maisteri erikoistuu erityisesti tietoturvallisuuden suunnitteluun, johtamiseen ja tietoturvallisuusriskien hallintaan. Hän tuntee kybermaailman eri uhkamallit ja tuntee uhkien torjuntaan liittyvät ratkaisumallit. Hän kykenee johtamaan erilaisten organisaatioiden tietoturvatoimintoja.

4.1.4 Maanpuolustuskorkeakoulu

Maanpuolustuskorkeakoulussa voidaan opiskella kyberturvallisuutta eri laitoksilla osana sotatieteiden kandidaatin, maisterin ja tohtorin opintoja.

4.1.5 Oulun yliopisto

Oulun yliopiston tieto- ja sähkötekniikan tiedekunnan Tietotekniikan osastolla toteutetaan tietotekniikan koulutusohjelma, jossa tietoturva on osa opintoja.

Tietojenkäsittelytieteiden laitoksen tietojenkäsittelytieteiden koulutusohjelma sisältää tietoturvaan liittyvää koulutusta.

Matemaattisten tieteiden laitoksella maisteriksi voi valmistua pääaineenaan matematiikka, sovellettu matematiikka tai tilastotiede. Laitoksella voi opiskella kryptografiaa ja salaustekniikoita.

Tietoliikennetekniikan osastolla tietoliikenteen opetus on sijoitettu pääasiassa kahteen koulutusohjelmaan, jotka ovat sähkötekniikan koulutusohjelma ja englanninkielinen kansainvälinen maisteriohjelma Wireless Communication Engineering.

4.1.6 Tampereen teknillinen yliopisto

Tietoturvallisuutta opetetaan Tietoliikennetekniikan laitoksella, Ohjelmistotekniikan laitoksella ja Systeemitekniikan laitoksella.

Tietoturvallisuuden sivuaineen sisältönä ovat ohjelmat, verkko, hallinto ja kryptologia. Sivuaineen suorittajien määrä on ollut jatkuvasti kasvussa. DI-tutkintonsa pääaineeksi nämä opiskelijat ovat tyypillisesti valinneet tietoliikenneverkoihin, ohjelmistotekniikkaan tai automaatiotekniikkaan liittyvän syventävän opintokokonaisuuden.

Ohjelmistotekniikan laitoksella on tarjolla turvalliseen ohjelmointiin keskittyvä syventävä kurssi.

Systeemitekniikan laitos on integroinut tietoturvaopetuksen laitoksen perusopetukseen sekä automaation tietotekniikan ammattiainesuuntaukseen. Kyberturvallisuutta on lähestytty näkemyksellä "tietoturva, tietoliikennetekniikka, ohjelmistotekniikka sekä ohjelmistotuotannon menetelmät ovat työkaluja luotettavan automaation tuottamisessa". Kursseja on yhteensä kuusi.

Automaation turvallisuutta ja muissa kursseissa tietoturva on yhdistettynä joko luentoihin, soveltaviin harjoitustöihin tai molempiin. Aihealueelta valmistuu vuodessa useita automaation diplomi-insinööriä, joiden opintoihin automaation tietoturva on sisällytetty. Automaation tietotekniikkaa pääaineenaan lukevia valmistuu vuodessa 5-10 henkeä.

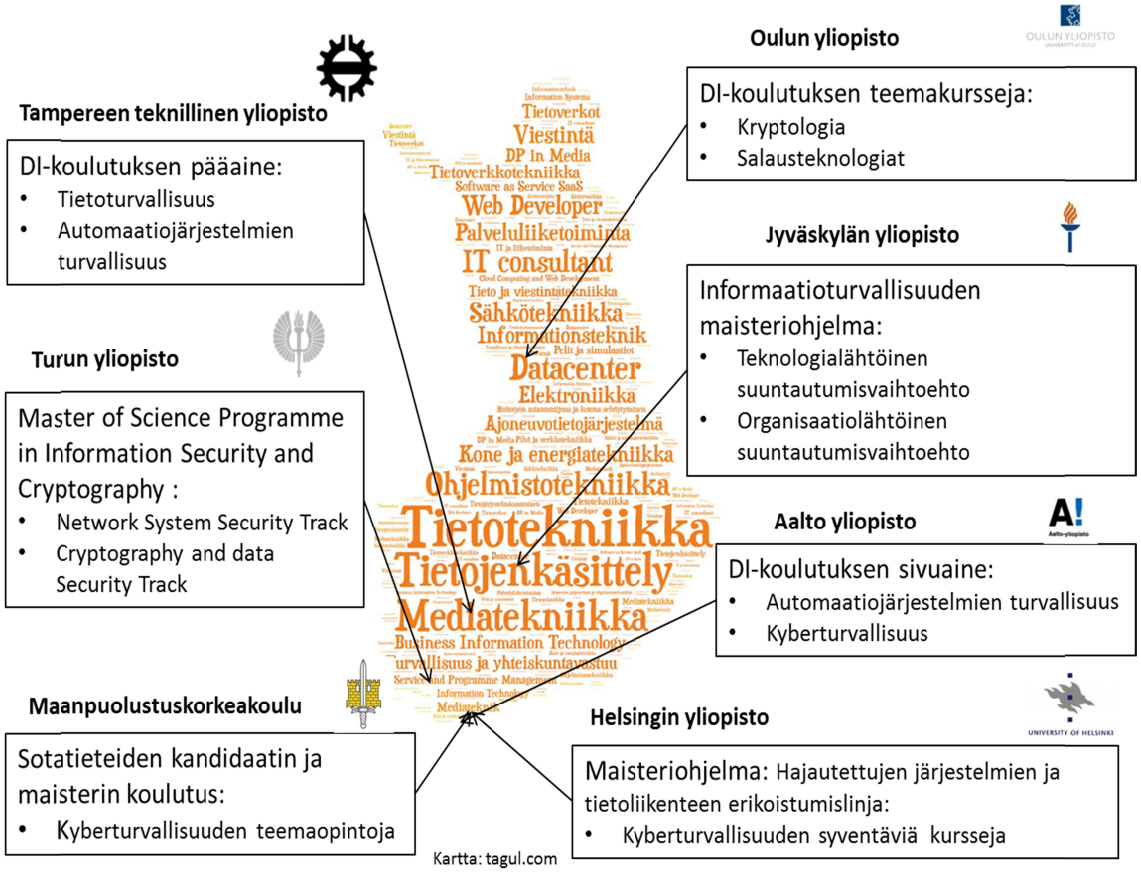
4.1.7 Turun yliopisto

Master's Programme in Information Security and Cryptography maisteriohjelmassa on kaksi suuntautumisvaihtoehtoa: Networked System Security ja Cryptography and Data Security.

Ohjelmaan valitaan vuosittain 20 alemman korkeakoulututkinnon suorittanutta opiskelijaa. Ohjelmasta valmistutaan joko diplomi-insinööriksi (pääaine Networked Systems Security) tai filosofian maisteriksi (pääaine Cryptography and data security).

Tietoturvajohtamisen opintoja tarjotaan Master's Degree Programme in Global Information Technology Management -ohjelmassa. Tässä maisteriohjelmassa opiskelija voi sisällyttää opintoihinsa tietoturvajohtamisen opintoja 25 op (Information Security Management, Business Continuity Management). Ohjelmasta valmistutaan kauppatieteen maisteriksi. Ohjelmaan valitaan vuosittain 25 alemman korkeakoulututkinnon suorittanutta opiskelijaa.

Kuvassa 4 on esitetty kyberturvallisuuden opetusta eri yliopistoissa.



KUVA 4 Kyberturvallisuuden opetusta yliopistoissa

4.2 Ammattikorkeakoulut

4.2.1 Centria-ammattikorkeakoulu

AMK -insinöörikoulutus sisältää seuraavia opintokokonaisuuksia:

- Käyttäjän tietoturva: kokonaisuus tietoturvasta työntekijän ja yksilön näkökulmasta
- Tietoturvan rakentaminen: kokonaisuus tietoturvan teknisestä toteuttamisesta verkkoihin
- Basis of cryptography

Tietoturvaopetus on kiinteänä osana sovellusalakohtaista opetusta. Esimerkiksi seuraavissa opintojaksoissa:

- Tietoturva sosiaali- ja terveysalalla: Luentosarja tietosuoja-asioista sosiaali- ja terveysalan tietojärjestelmien kanssa toimiville
- Tietoturvaopetusta sensoriverkkoihin liittyen kursseihin ”Mobile Networks” ja ”Langattomat järjestelmät”
- Tietoturvaopetusta ohjelmistotekniikassa

4.2.2 Jyväskylän ammattikorkeakoulu

Kyberturvallisuuden ja tietoturvallisuuden koulutusta Jyväskylän ammattikorkeakoulussa toteuttaa IT-instituutti. Valmistuneiden loppututkinnot ovat: Tekniikan ammattikorkeakoulu tutkinto; insinööri (AMK) 240 op ja ylempi ammattikorkeakoulututkinto; Master of Engineering 60 op.

AMK-insinöörikoulutus tarjoaa kyberturvallisuuden koulusta kolmessa koulutusohjelmassa omina erillisinä opintojaksoina ja eri opintojaksojen sisään integroituina kokonaisuuksina. Erityisesti kyberturvallisuus korostuu käyttöjärjestelmien, ohjelmoinnin ja tietoverkkojen opintojaksoissa. Erillisinä kyberturvallisuuteen keskittyvinä opintojaksoina opiskelijoille tarjotaan Tietoturva ja palveluiden hallinta sekä Tietoturvan toteutus.

YAMK-insinööritutkintoon johtavassa englanninkielisessä Master´s Degree Programme in Information Technology -ohjelmassa koulutetaan tietoturvallisen ympäristön rakentamista, testaamista ja evaluointia nykymaailman kyberturvallisuusuhkia huomioon ottaen. Opintokokonaisuuksissa opitaan turvalliset/oikeat toteutustavat ja parhaita käytäntöjä osana opintosisältöä. Opitut asiat kootaan yhteen viimeisessä opintojaksossa, jossa suunnitellaan ja harjoitellaan kyberturvallisuuteen liittyviä skenaarioita realistisessa ympäristössä eri rooleissa. Pelkästään kyberturvallisuuteen keskittyviä opintoja

on 25 opintopistettä. Valinnaisia opintoja on 5 op ja opinnäytetyö on 30 opintopisteen laajuinen.

4.2.3 Kymenlaakson ammattikorkeakoulu

Kymenlaakson ammattikorkeakoulu tarjoaa kyberturvallisuuden opetusta osana tietotekniikan koulutusta. Osaamistavoitteina ovat datakeskusten, erilaisten tietoverkkojen ja käyttöjärjestelmien tietoturvallinen toteuttaminen, penetraatiotestaus ja tunkeutumisen havaitseminen. Osa kyberturvallisuusopetuksesta toteutetaan pelien keinoin.

Tietoverkkotekniikka koulutuksen uudet osaamiskokonaisuudet mahdollistavat kyberturvallisuuteen ja konesalitekniikkaan perehtymisen. Kyberturvallisuudessa perehdytään erityisesti tietojärjestelmien haavoittuvuuksien paikantamiseen.

4.2.4 Laurea ammattikorkeakoulu

Turvallisuusalan koulutusohjelman opinnoissa käsitellään turvallisuuden ja riskienhallintaa niin kansallisissa kuin kansainvälisissä ympäristöissä. Valmistuneen tradenomin ydinosaamisalueita ovat riskienhallinta, turvallisuusjohtaminen, liiketoimintaosaaminen, henkilöturvallisuus, tietoturvallisuus sekä toiminnan, toimitilojen ja ympäristön turvallisuus kansainvälisessä liiketoiminta-/toimintaympäristössä.

4.2.5 Oulun ammattikorkeakoulu

YAMK-tason tietotekniikan tutkinto-ohjelmaan sisältyvän Tietoturvallisuuden suunnitteluosaaminen osaamisalueen tavoitteena on, että opiskelija:

- Ymmärtää tietoturvallisuuden, tunnistamisen ja paikantamisen asettamat vaatimukset ohjelmistosuunnittelussa
- Osaa suunnitella, toteuttaa ja testata tietoturvallisia ohjelmistoratkaisuja ja tietokantasovelluksia
- Tuntee tietoturvalliset ohjelmistokehitysmenetelmät
- osaa suunnitella ja toteuttaa turvallisia ja luotettavia tietoverkkoja

4.2.6 Poliisiammattikorkeakoulu

Poliisiammattikorkeakoulun täydennyskoulutusohjelmassa on tarjolla tietotekniikkarikosten opintokokonaisuus.

4.2.7 Turun ammattikorkeakoulu

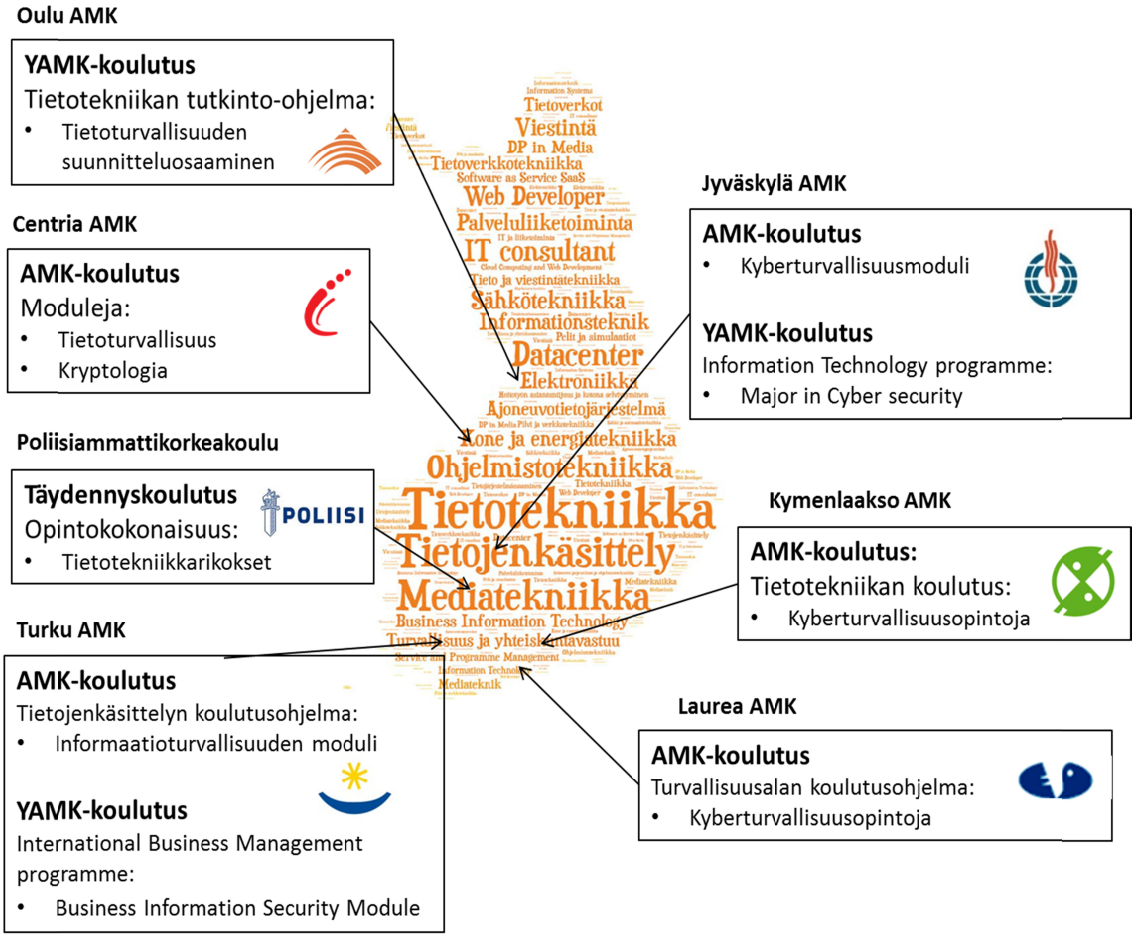
International Business Management YAMK-ohjelmassa on mahdollisuus erikoistua Business Information Security and Information Risk Management -aihepiiriin.

Tieto- ja viestintätekniikan insinööriopinnoissa annetaan valmiudet toimia esimerkiksi elektroniikkalaitteiden tutkimus- ja tuotekehitystehtävissä, hyvinvointia edistävien järjestelmien kehittäjänä, pelisuunnittelijana, ohjelmistokehittäjänä, tietoliikenneasiantuntijana tai itsenäisenä yrittäjänä.

Tietojenkäsittelyn IT-tradenomiopinnoissa opiskelija saa valmiudet yritysten tietoverkko- ja palvelinratkaisujen sekä tietoturva-asioiden ylläpitämiseen ja kehittämiseen. Opinnot koostuvat ammattiaineista, joiden keskeisenä sisältönä ovat tietoliikenne- ja laitetekniikka, erilaiset palvelinratkaisut sekä tietoturvallisuus.

Insinööri- ja IT-tradenomi opintojen yhteisessä Tietoverkot ja tietoturva -osaamispolun opinnoissa keskitytään erityisesti IP-pohjaisten tietoverkkojen ja palvelimien teknisten sisältöjen hallintaan, yritystason tietoturvan ja riskienhallinnan kokonaisuuteen sekä IT-palvelutoiminnan prosesseihin.

Kuvassa 5 on esitetty kyberturvallisuuden opetusta eri ammattikorkeakouluissa.



KUVA 5 Kyberturvallisuuden opetusta ammattikorkeakouluissa

5 KYBERTURVALLISUUSALAN INFRASTRUKTUURI SUOMESSA

5.1 Yliopistot ja tutkimuslaitokset

5.1.1 Aalto-yliopisto

Aalto-yliopistossa on seuraavat laboratorioympäristöt:

- verkkojen tietoturvalaboratorio (Laaja opetus- ja koulutusyhteistyö Stonesoftin kanssa)
- SDN-teknologian testauslaboratorio
- Laajat tietoverkkojen ja palvelinkeskusten laboratoriojärjestelmät
- Alusta automaatiolaitteiden automaattiseen etsintään ja analysointiin
- IPS-järjestelmien testausympäristö

5.1.2 Helsingin yliopisto

Mobiilitietoturvan tutkimusinstituutti toimii yhteistyössä Intel Securityn kanssa. Instituutti keskittyy kehittämään ja vahvistamaan mobiilialustojen tietoturvateknologioita, erityisesti niiden käytettävyyttä.

Nodes laboratorio on kokeellisen tietojenkäsittelytieteen erityisesti tietoverkkojen ja joka paikan sekä liikkuvan tietotekniikan (Ubiquitous and Mobile Computing) tutkimusinfrastruktuuri. Laboratoriossa on keskeistä infrastruktuuria alueen tutkimukseen, kuten uusien tietoverkkoprotokollien ja reititysalgoritmien kehittämiseen tarkoitetut tietoverkot ja testikehikot, häiriösuojattu huone langattomiin mittauksiin, sekä vuorovaikutteisen tietojenkäsittelyn tarvitsemat älynäytöt ja sensorit.

5.1.3 Jyväskylän yliopisto

Jyväskylän yliopiston IT-tiedekunnan ylläpitämä laboratorioinfrastruktuuri muodostuu tiedekuntatasolla ylläpidetyistä laskentaympäristöstä, oppimisympäristöstä ja luovuuslaboratoriosta ns. Pekan pajasta sekä laitosten omista laboratorioista.

Tietoliikennelaboratoriossa on käytössä verkkosimulaattoreita (private / open source) sekä erilaisia virtuaaliverkkoja, joissa voidaan mallintaa ja kehittää tietoverkkojen luotettavuutta ja turvallisuutta. Virtuaaliympäristöt ovat hyvin dynaamisia ja keveitä kehittää sekä ylläpitää erilaisiin opetuksen ja tutkimuksen tarpeisiin.

5.1.4 Maanpuolustuskorkeakoulu

Maanpuolustuskorkeakoulun sotatekniikanlaitoksella on tutkimusympäristö kyberturvallisuuden tutkimusta varten.

Suomessa havaittujen krypto-osaamisen vakavien puutteiden korjaamiseksi Puolustusvoimat perustaa kansallisen kryptolaboratorion. Laboratorio on kryptologian osaamiskeskus, jonne luodaan tekninen ympäristö osaamisen kehittämiseksi sekä salausteknisten ratkaisuiden ja tuotteiden testaamiseksi ja niiden vahvuuden verifioimiseksi. Kryptolaboratorio tekee lisäksi yhteistyötä tiedeyhteisön kanssa tukemalla kryptologian tutkimustyötä sekä tarjoamalla teknisen laboratorioympäristön resursseja tutkimuskäyttöön. Yhteistyöverkostossa on myös alan palveluja tuottavia yrityksiä.

5.1.5 Oulun yliopisto

Tietoliikennelaboratorio vastaa langattoman tietoliikenteen koulutuksesta ja opetuksesta Oulun yliopistossa. Tietoliikennelaboratorio ja sen tutkimusyksikkö CWC ovat osa sähkö- ja tietotekniikan osastoa.

5.1.6 Tampereen teknillinen yliopisto

TUTCyberLabs on uusi tutkimus- ja opetusympäristö, jossa simuloidaan kyberhyökkäyksiä ja niiltä puolustautumista sekä testataan laitteistojen ja ohjelmistojen tietoturvaominaisuuksia. Syksyllä TUTCyberLabs aloittaa kyberturvallisuuskoulutuksen TTY:n opiskelijoille, jotka opiskelevat tietoturvaa pääaineenaan.

TUTCyberLabs on kolmen eri TTY:n laitoksen välinen yhteishanke, johon osallistuvat tietotekniikan, systeemitekniikan ja sähkötekniikan laitokset. Kyseessä on ainutlaatuinen ja rajoja rikkova yhdistelmä tietotekniikka-, teollisuusautomaatio- ja Smart Grid älyverkko-osaamista. Se tarjoaa monipuolisen ympäristön, jossa voi tehdä aktiivisia kyberhyökkäyksiä, harjoitella eri kyberpuolustustekniikoita, etsiä haavoittuvuuksia ja testata laitteiden, ohjelmistojen, sovellusten sekä järjestelmäarkkitehtuurien tietoturvaa. Tämän lisäksi TUTCyberLabissa voi emuloida valtakunnallisen sähköverkon ja tietoliikenneverkkojen tapaisten kriittisten infrastruktuurien välisiä riippuvaisuuksia sekä tuottaa tilannekuvaa verkkojen toiminnasta. Siellä pystytään tunnistamaan erityyppisiä kyberuhkia ja keräämään niistä tietoa, ja myös osoittamaan käytännössä riittämättömän kyberturvan seuraukset.

TUTCyberLabs koostuu kolmesta laboratoriosta,
jotka ovat
- Networking laboratory
- Industrial automation cybersecurity laboratory
- Smart grid ICT laboratory

5.1.7 Valtion teknillinen tutkimuslaitos

VTT on perustanut erityisen Cyber War Room -laboratorion, jossa kyberturvallisuustestausta voidaan tehdä hallitusti, luotettavasti ja luottamuksellisesti. Cyber War Roomissa on mm. käytössä täysin kaikesta muusta tietoliikenteestä eristetty pienoisinternetympäristö, jossa testattavia laitteita tai ohjelmistoja kohtaan voidaan tehdä hallittuja ja riittävän todenmukaisia kyberhyökkäyksiä. Cyber War Roomissa voidaan toteuttaa esimerkiksi järjestelmien haltuunottoon tähtääviä hyökkäyksiä, tyypillisiä hakkereiden käyttämiin menetelmiin perustuvia hyökkäyksiä ja bottihyökkäyksiä. Tehokkaiden hyökkäysten monitoroinnin ja tilannekuvan työkalujen kehittäminen on myös tärkeässä roolissa Cyber War Roomissa.

VTT:n Converging Networks Laboratory käsittää kehitys- ja testauspalveluita (mm. IMS), monipuolisesta konfiguroitavissa olevassa verkkoympäristössä, kuten 3G/HSDPA, Wi-Fi and WiMAX.

WILLAB on langattomien verkkojen tutkimusympäristö ja ATLAS laboratoriossa voidaan testata LTE/LTE-A verkkojen turvallisuutta.

5.1.8 FISC kyberlaboratorio

Suomalaisten tietoturva-alan yritysten yhteenliittymä (Finnish Information Security Cluster, FISC) perusti vuonna 2013 Cyberlab Oy:n, jonka tehtävänä on kaupallistaa pk-yritysten ja julkisten toimijoiden osaaminen vientituotteiksi ja -palveluiksi. FISC ry:n tavoitteena on vahvistaa suomalaista tietoturvaosaamista ja houkutella investointeja Suomeen. Cyberlab-toiminta tähtää myös kansallisen "kyberomavaraisuuden" kehittämiseen.

5.2 Ammattikorkeakoulut

5.2.1 Centria-ammattikorkeakoulu

Centria-ammattikorkeakoululla on laboratorioympäristöjä eri toimialoille. Tietoliikennelaboratorio toimii tulevaisuuden tietoverkkojen tietoturvan tutkimusympäristönä ja tuotantotekniikan laboratoriossa tutkitaan teollisen internetin tietoturvaa. Sähkö- ja energiatekniikan laboratorion tutkimusympäristöä hyödynnetään kriittisen sähköjakeluverkon tietoturvaan liittyen. Chemplant - kemian minitehdas sekä puutuotelaboratorio varustettuna automaatiolla, kenttäväylällä ja prosessiohjauksella soveltuvat prosessiteollisuuden tutkimusympäristöiksi kyberturvallisuuteen liittyen. Centrialla on osaamista ja ympäristöjä erilaisten langattomien järjestelmien tietoturvaan ja tiedonsiirron luotettavuuteen.

5.2.2 Jyväskylän ammattikorkeakoulu

Jyväskylän ammattikorkeakoulun IT-instituutin JYVSECTEC (Jyväskylä Security Technology) kyberturvallisuuden tutkimus-, koulutus- ja kehityskeskuksessa tuotetaan huipputason palveluja osana kansallista ja kansainvälistä yhteistyöverkostoa. JYVSECTEC toteuttaa mm. testaustoimintaa, koulutuksia ja kyberharjoituksia, joissa eri toimijat voivat harjoitella todenmukaisessa ympäristössä toimintaa erilaisia kyberuhkia ja hyökkäysmenetelmiä vastaan. Ympäristön avulla voidaan myös toteuttaa tuotekehitystä sekä kouluttaa kyberturvallisuutta kolmansille osapuolille yksityisellä ja julkishallinnollisella sektorilla.

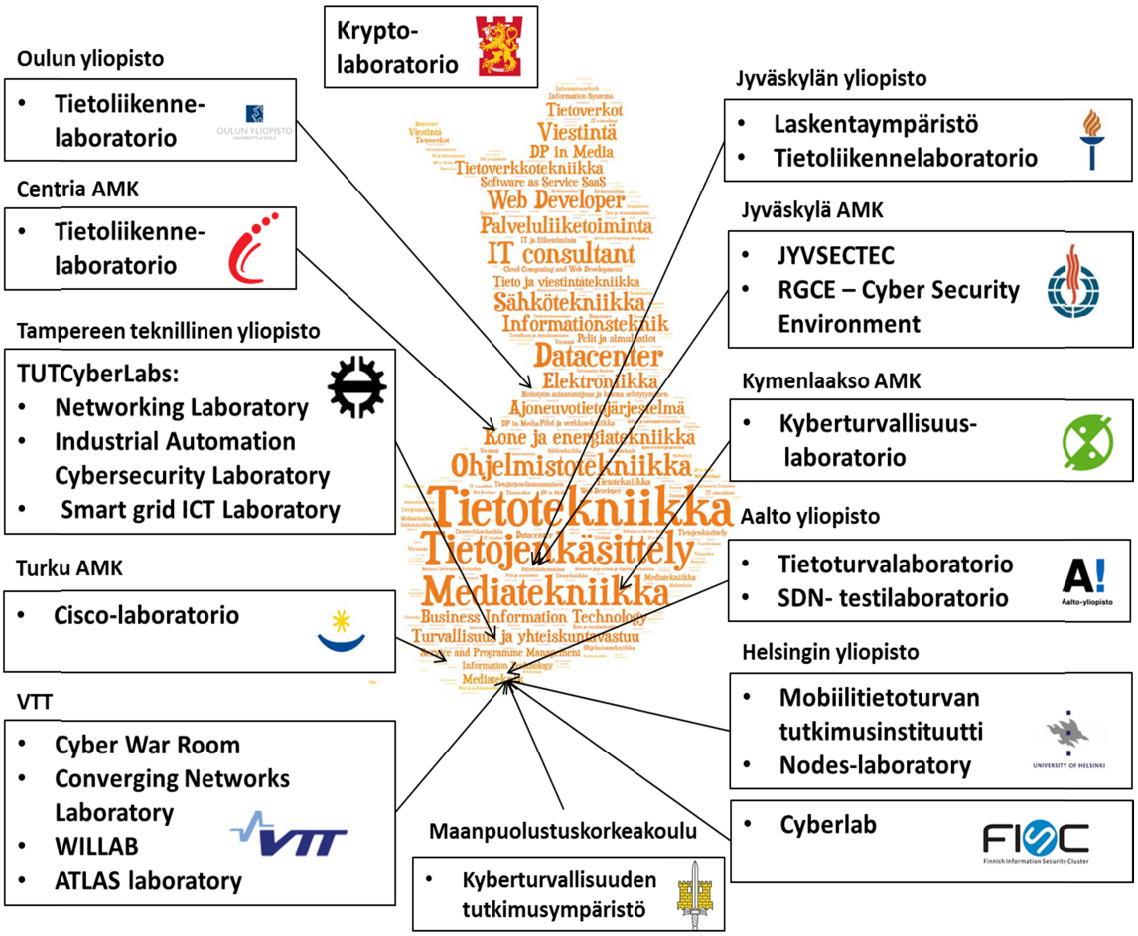
JYVSECTEC:n RGCE (Realistic Global Environment) ympäristössä tapahtuvan toiminnan tavoitteena on parantaa toimijoiden häiriönsietokykyä, mahdollisuuksia havaita oman toimintansa ja järjestelmiensä haavoittuvuuksia, kykyä havaita ja torjua kyberuhkia sekä kehittää henkilöstön osaamista. Esimerkkinä tästä Puolustusvoimat hyödynsi IT-instituutin JYVSECTEC:n osaamista kyberturvallisuusharjoituksessa 9.6.–13.6.2014. JYVSECTEC mahdollisti todenmukaisen teknisen harjoitusympäristön, jota hyödyntäen harjoitettavat tilanteet toteutettiin joukoille.

5.2.3 Kymenlaakson ammattikorkeakoulu

Vuoden 2014 aikana uutena osaamisalueena mukaan tulee kyberturvallisuus ja siitä erityisesti tunkeutumistestaus. Kyberturvallisuuden osaamisen varmistamiseksi on rakenteilla kokonaan uusi kyberturvallisuuslaboratorio.

5.2.4 Turun ammattikorkeakoulu

Turun ammattikorkeakoulussa on Cisco-laboratorio, jossa annetaan tietoverkko-opetusta sekä tietoturvalaboratorio, jossa on käytössä StoneGate ja tunkeutumistestausympäristö.



KUVA 6 Kyberturvallisuuden kehitys- ja laboratorioympäristöjä

6 KYBERTURVALLISUUSALAN KANSAINVÄLINEN TOIMINTA

Yliopistoilla ja ammattikorkeakouluilla on laaja kansainvälinen yhteistyöverkosto, jonka piirissä toteutetaan kyberturvallisuusalan tutkimus- ja opetustoimintaa, järjestetään konferensseja ja erilaista opettaja- ja opiskelijavaihtoa. Tässä luvussa on esitetty otos yliopistojen ja ammattikorkeakoulujen kyberturvallisuuteen liittyvästä kansainvälisestä yhteistoiminnasta.

6.1 Yliopistot ja tutkimuslaitokset

6.1.1 Aalto-yliopisto

Yliopisto	Kyberturvallisuuden osaamisalue
Northern Arizona University, USA	Human-cyber-physical systems with a focus on wireless sensor networks for environmental and ecosystems monitoring, cyber intelligence and analysis
University of Auckland, New Zealand	Security of information systems, Cyber- crime, cyber- terrorism and cyberwar , Cloud computing, Big Data computing, Radio spectrum management
Luleå Technical University, Sweden	Information security, cyber-physical systems, information management
University of Cambridge, UK	Network security, security engineering
Cyber Security Centre of Oxford University, UK	Cloud Internal Threat Detection, future Home Networks and Services, identity security, information security, mobile security, network security , security protocols for ad hoc networks
University of Glamorgan, UK	Intrusion detection, Intrusion prevention, digital forensics
Ecrypt II Network of Excellence	Maintain and strengthen the excellence of European research and industry in the area of cryptology and obtain a durable integration which lasts beyond the funding of the NoE provided by the European Commission

6.1.2 Helsingin yliopisto

Yliopisto	Kyberturvallisuuden osaamisalue
International Computer Science Institute (ICSI), USA	Novel management approaches to network defenses, cybercrime, troubleshooting, and measurement and characterization
University of Califor-	Cryptography, cyber policy analysis, trustworthiness of computer sys-

nia at Berkeley, USA	tems and appropriately balance rights of privacy, needs of data security
Cambridge University, Computer Laboratory, UK	Computer security along with related topics such as cryptology, formal methods, hardware design, biometrics, and the robustness of distributed systems in general
Tsinghua University, China	Electric power systems and automation security and stability analysis, intelligent control
Technische Universität Darmstadt, Germany	Cryptographic Protocols, Network Security, Privacy and Identity Management, Secure Engineering, Security and Privacy in Cloud Computing, Security and Privacy in Smart Home

6.1.3 Jyväskylän yliopisto

Yliopisto	Kyberturvallisuuden osaamisalue	Yhteistoimintamuodot
University of British Columbia, Canada	Cyber security in operating systems and distributed systems, communications security	Professorivierailuja Hankeyhteistyötä
Deakin University, Melbourne, Australia	Critical Infrastructure Protection, SCADA Security	Professorivierailuja
Edith Cowan University, Perth, Western Australia	Network Security and Forensics, Intrusion Detection Systems, and SCADA Security	Professorivierailuja Jatko-opiskeluvierailuja
Carnegie Mellon University, USA	Cyber-physical systems, Adaptive Cyber-Learning, Privacy and cyber security, Trustworthy Computing Platforms and Devices, Software Security	Professorivierailuja Hankeyhteistyötä
Florida State University, USA	Digital and Network Forensics, Cybersecurity and Cybercrime	Professorivierailuja Luennoitsijavaihtoa
City University of Hong Kong, China	Cryptography, wireless security, Cyber Physical Systems,	Professorivierailuja Hankeyhteistyötä
University of the Aegean, Greece	Security and Privacy Economics, Secure eCommerce, eBusiness, eGovernment, eHealth, Privacy Technologies, Development of Secure Information Systems, Security and Privacy Legal and Regulatory issues, Forensics Investigation; Internet Telephony Security, Wireless and Mobile Communications Security, Privacy and Trust in Wireless Sensor Networks	Professorivierailuja Hankeyhteistyötä
George Mason University, USA	Cyber Security engineering, Cyber security economics	Professorivierailuja Hankeyhteistyötä
University of Nevada Las Vegas, USA	Developing anti-spam and anti-phishing tools, Computing and Network Forensics	Professorivierailuja Hankeyhteistyötä
Newcastle University, UK	Cryptography, secure system engineering, information, and operational assurance techniques, quantitative security	Professorivierailuja Hankeyhteistyötä
Massachusetts Institute of Technology MIT, USA	Internet of Things, Anti-Counterfeiting, Fraud Detection, Big Data and Visualization, Future Proofing Systems – Simula-	Professorivierailuja Kursseille osallistumista

	tor, Negative Authentication, HTML5 Attack Surface, Password cracking	
University of Memphis, USA	Intrusion Detection and Responses	Professorivierailuja Konferenssiyhteistyötä
University of Gjövik	Cryptography and security mechanisms, network security, intrusion detection and prevention, digital and computational forensics, security management, information warfare, wireless communication security, legal aspects of information security, organizational and human aspects of information security	Professorivierailuja Luennoitsijavaihtoa
Universität der Bundeswehr München, Germany	Algebraic Number Theory, Arithmetic Geometry, Algorithmic, Cyber Defence, Cyber War and Peace, Cyber-attacks and weapons	Tutkimusyhteistyötä
Tallinn University of Technology, Estonia	Cyber Defence, Legal Aspects of Cyber Security, Malware Foundations and Management of Cyber Security	Vierailleva professori
Tel Aviv University, Israel	Anomaly Detection	Vierailleva professori Hankeyhteistyötä
University of Virginia, USA	Cyber Security Management, Security Policy Development and Assessment, Designing Dynamic Security Architecture, Cybercrime, Cyber Law, Regulation, and Ethics, Securing the Internet of Things	Professorivierailuja Hankeyhteistyötä
Yale University, USA	Secure hardware-software architectures Sensor networks for monitoring and security Data center architecture and security	Vierailleva professori Hankeyhteistyötä

6.1.4 Turun yliopisto

Yliopisto	Kyberturvallisuuden osaamisalue	Yhteistoimintamuodot
Luleå Tekniska Universitet, Sweden	Information security, cyber-physical systems, information management	Professori/luennoitsijavaihtoa
RMIT University, Australia	Information security and protection	Vierailleva professori, intensiivikurssi

6.2 Ammattikorkeakoulut

6.2.1 Centria-ammattikorkeakoulu

Yliopisto	Kyberturvallisuuden osaamisalue
University of East London, UK	Security management, computer security, cybercrime and digital forensics

Ochanomizu University, Japan	Cyber-physical systems
Gwangju Institute of Science and Technology (GIST), South-Korea	Research activities have focused on theoretical and empirical studies on wireless / optical communication and network systems including hardware and software component and system development
University of California at Berkeley, USA	Cryptography, cyber policy analysis, trustworthiness of computer systems and appropriately balance rights of privacy, needs of data security
Chungbuk National University, South Korea	
Blekinge tekniska högskola, Karlskrona, Sweden	Machine learning techniques and anomaly detection, telecommunications systems focus on performance and efficiency issues, the evaluation and treatment of mobile multimedia, web services, and virtual environments such as cloud computing and cloud networking
University of Lodz, Poland	Information Technology

6.2.2 Jyväskylän ammattikorkeakoulu

Yliopisto	Kyberturvallisuuden osaamisalue	Yhteistoimintamuodot
University of Arizona, USA	Hacker behaviours analysis	Koulutusyhteistyö
Tallinn University of Technology, Estonia	Formal methods in system verification and testing, network applications and cyber security.	Hankeyhteistyö
Industrial Cybersecurity Center, Spain	Improve Industrial Cybersecurity by developing analysis, studies and information exchange and sharing about practices, processes and technologies	Hankeyhteistyö
The University of Worcester, UK	Information Assurance	Hankeyhteistyö
Athlone Institute of Technology, Ireland	Conducts research in the areas of connected and interactive media and in infrastructure performance management	Hankeyhteistyö
Baltic Defence College, Estonia	Trends in war and warfare, new security issues and the armed forces, strategic culture, change management and military transformation, armed forces and society	Vierailevia luennoitsijoita, hankeyhteistyö

6.2.3 Turun ammattikorkeakoulu

Yliopisto	Kyberturvallisuuden osaamisalue	Yhteistoimintamuodot
University of Ontario Institute of Technology, Canada	Biometrics, Security and privacy in wireless sensor and ad hoc networks	Tutkijavaihto, opiskelijavaihto, yhteiset T&K-hankkeet

7 ESIMERKKEJÄ ULKOMAISESTA KYBERTURVALLISUUDEN KOULUTUKSESTA

7.1.1 University of Gjøvik, Norway

The Master of Science in Information Security provides the students with knowledge and theoretical background, as well as with the skills and attitudes necessary to succeed in this challenging yet eminently rewarding field.

The goals of the study program are achieved through the research-based courses that reflect the research results of the teaching staff to a large extent. In such a way, the students are always offered top-quality courses through which they acquire knowledge that gives them many advantages in their careers.

The study program is closely related to the research community Norwegian Information Security Laboratory (NISlab), which also offers bachelor and PhD studies in information security. This research environment consists of professors that are active in research and internationally recognized as experts in their respective fields. NISlab is a member of Forum for Research and Innovation in Security and Communication (FRISC), a Norwegian network of institutions dedicated to cutting-edge research in information security. NISlab also has strong international relations and its collaboration network includes more than 20 research institutions worldwide.

The programme has three tracks:

- Technology
- Digital forensics
- Management

Major areas of study

- Cryptography and security mechanisms
- Network security
- Intrusion detection and prevention
- Digital an computational forensics
- Security management
- Biometric authentication
- Information warfare
- Wireless communication security
- Legal aspects of information security
- Organizational and human aspects of information security
- Risk analysis

There are three laboratories for the students:

1. The Norwegian Information Security Laboratory consists of professors and scientists widely known for their work in information security.
2. Testimon - Digital forensics laboratory
3. The Norwegian Biometrics Laboratory

This two-year master program (120 ECTS credits) contains four main elements:

1. Mandatory courses, 60 ECTS
2. Elective courses, 25 ECTS
3. Research Project Planning, 5 ECTS
4. Master's Thesis, 30 ECTS

Table 1 Mandatory courses, 60 ECTS

Technology track	Digital Forensics track	Management track
Scientific Methodology	Scientific Methodology	Scientific Methodology
Cryptology 1	Cryptology 1	Cryptology 1
Applied Information Security	Applied Information Security	Applied Information Security
IT Governance	IT Governance	IT Governance
Legal Aspects of Information Security	Legal Aspects of Information Security	Legal Aspects of Information Security
Digital Forensics 1	Digital Forensics 1	Digital Forensics 1
Socio-technical Security Risk Modeling and Analysis 1	Machine Learning and Pattern Recognition 1	Socio-technical Security Risk Modeling and Analysis 1
Network Security	Network Security	Network Security
Foundations of Information Security	Computational Forensics	Security as Continuous Improvement
Cryptology 2	Digital Forensics 2	Security Management Dynamics
Biometrics	Software Security Trends	Security Planning and Incident Management
Software Security Trends		

At least 25 ECTS must be chosen from the following courses:

Table 2 Elective courses, 25 ECTS

Course	ECTS
Ethical Hacking and Penetration Testing	5
Discrete Mathematics	5
Information Warfare	5
Machine Learning and Pattern Recognition 2	5
Organizational and Human Aspects of Infor-	5

mation Security	
Behavioral Biometrics	5
Intrusion detection and prevention	5
Wireless communication security	5
Risk Management 1	5
Risk Management 2	5
Information Security Economics 1	5
IT Rhetorics for Security Risk Management	5
Socio-technical Security Risk Modeling and Analysis 2	5
Specialization Course 1	5
Specialization Course 2	10

7.1.2 Deakin University, Australia

Deakin's Bachelor of IT Security provides a thorough knowledge and understanding of general issues, concepts and practices in IT security. There is an emphasis on analysis, investigation, problem-solving, development and technical skills related to IT security in addition to hands-on experiential learning.

The Bachelor of IT Security is professionally accredited with the Australian Computer Society (ACS). The course also assist students in completing the material required to become a Certified Information Systems Security Professional (CISSP).

Career options include work as a security analyst, project manager, security system manager, cryptographer, consultant, security system developer or programmer, information security auditor, business continuity or IT security engineer.

The student gain practical and theoretical knowledge in this critical aspect of IT with an emphasis on understanding and assessing the need for IT security in a working environment, knowledge of the security solutions available, as well as understanding the business, ethical and legal implications of risk management. The student will learn in a leading-edge study environment and graduate as a qualified IT professional.

Course Curriculum:

- Advanced Digital Forensics
- Advanced Topics in Digital Security
- Communications Network Security
- IT Security Management

7.1.3 University of Washington Tacoma, USA

The Master in Cybersecurity and Leadership (MCL) program leverages the resources of the University of Washington's mission Center for Information Assurance and Cybersecurity and the Milgard School of Business MBA program to create the newest program at UWT. By identifying, addressing, and promoting solutions for issues of information assurance and cybersecurity, MCL will serve as an educational foundation for invention, innovation, and entrepreneurship in the state of Washington, giving its graduates the path to success in in the cybersecurity field.

The MCL is designed for professionals with a minimum of three year's work experience, IT managers, and military personnel with an accredited bachelor's degree. Applicants are seeking a competitive advantage for advancement in the military, in government agencies, and in the private sector for leadership positions in the growth area of cybersecurity operations. The MCL program provides graduates with the managerial skills and technical competencies necessary for leading technology professionals and organizations in the 21st century.

The Master in Cybersecurity and Leadership is a non-thesis, 40 credit-hour cohort based program, with a balance between a technically-oriented curriculum focused on understanding the basic operations and functionality of cybersecurity systems and information assurance and a more behaviorally-oriented curriculum focused on the management of technical professionals and organizational leadership.

Student learning outcomes include a practical understanding of the principles of data protection, network security and counter cyber-terrorist techniques; as well as a solid understanding of how to ethically lead, communicate and effect strategic change in technical departments and in organizations. Graduates of the MCL program will be well versed in advanced information assurance knowledge and they will be effective leaders who are able to contribute to their organization's effectiveness.

Program Learning Objectives

- Identify and critically assess issues and concepts related to the protection of information and information systems.
- Use risk management principles to assess threats, vulnerabilities, countermeasures and impact contributions at risk in information systems.
- Create policies and standard operating procedures for organizations that are ethically, morally and legally sound.
- Illustrate and explain fundamental architectures of networks and the Internet, as well as their underlying protocols.
- Understand the concepts inherent in information security architectures.
- Understand the key functions and challenges of organizational communication, including the factors that can hinder and facilitate effective communication in business settings.
- Recognize ethical dilemmas and social responsibilities.
- Formulate and implement strategy and effectively manage change.

Course Curriculum

- Principles of Cybersecurity
- Business Essentials
- Networking and Internet Security
- Strategic Organization Change
- Information Assurance, Risk Management and Security Strategies
- Leadership and Team Dynamics
- Cybersecurity Management
- Project Management

LIITE 1 Kyberturvallisuuden tutkimusaloja Suomen yliopistoissa ja tutkimuslaitoksissa

	Aalto yliopisto	Helsingin yliopisto	Jyväskylän yliopisto	MPKK ja PVTT	Oulun yliopisto	Tampereen teknillinen yliopisto	Turun yliopisto	VTT
Anomaly detection			X					X
APT analyze			X					X
Authentication, authorization &identity management (IAM)						X		X
Big Data Security	X	X	X					
Cloud service security	X				X	X		X
Computer Security	X		X		X			
Cryptography	X	X		X	X	X	X	X
Cyber Defence			X	X				
Cyber Security legal aspects	X							
Critical infrastructure protection	X		X	X		X		X
Cyber Security and Human aspects			X		X		X	
Cyber Security Investments			X					
Cyber Security Management			X					
Cyber Security situation awareness	X		X	X				X
Data mining and analysis and Cyber Security		X	X					
Dos/DDos attack protection	X		X					
Incident analysis and management								X
Identity and access management	X					X		
Identity protection			X					
Industrial Control System (ICS) security	X				X			X
Information Assurance		X						X
Information Security		X	X		X	X		
Intrusion detection	X		X					X

Intrusion Prevention	X		X					
IoT security	X	X	X		X	X		X
Machine learning methods for Cyber analysis			X					
Mobile security	X	X	X			X	X	
Network security and monitoring	X	X	X			X	X	
Privacy	X							X
Risk analyze	X							X
SCADA security	X		X	X		X		X
Secure services			X				X	X
Secure System Design	X		X		X	X		
Security architectures and communication protocols	X	X			X			X
Security economics			X				X	X
Security information visualization and interpretation			X	X				X
Security metrics and data aggregation			X					X
Security standardization								X
Security testing			X		X			X
Smart Grid Security	X					X		X
Software Security		X	X		X		X	
Systems Security	X	X			X	X	X	
Threat, vulnerability and dependency analysis	X		X	X			X	X
Trust management	X	X	X			X		X

LIITE 2 Kyberturvallisuuden yliopistokursseja

Aalto-yliopisto

- T-110.4206 Information Security Technology, 5 op
- T-110.5102 Laboratory Works in Networking and Security, 5-10 op
- T-110.5220 Information Security and Usability P, 3 op
- T-110.5241 Network Security, 5 op
- T-110.5291 Seminar on Network Security P, 5 op
- T-110.6101 Special Assignment in Networking and Security P, 1-10op
- T-110.6220 Special Course in Information Security P, 2-10 op
    - Reverse Engineering Malware, 5 op
- CSE-C3400 Information Security, 5 op
- T-79.4502 Cryptography and Data Security, 5 op
- T-79.5501 Cryptology, 5 op
- T-79.5502 Advanced Course in Cryptology, 5 op
- S-38.3153 Security of Communication Protocols, 4 op
- AS-116.3181 Automaatiojärjestelmien turvallisuus, 5 op

Helsingin yliopisto

- 582704 Mobile Platform Security, 3 op
- 582708 Software Security, 4 op

Jyväskylän yliopisto

- ITKST 40 Yhteiskunta ja informaatioturvallisuus, 5 op
- ITKST 41 Kybermaailma ja turvallisuus, 5 op
- ITKST 42 Anomaly Detection, 5 op
- ITKST 44 Kybermaailma ja kansainvälinen oikeus, 5 op
- ITKST 45 Introduction to cyber conflict, 5 op
- ITKST 47 Advanced Anomaly Detection, 5 op
- ITKST 48 Advanced Persistence Threat, 5 op
- ITKST 49 Cyber Security and Critical Information Infrastructure Protection, 5 op
- ITKST 50 Secure Systems Design, 5 op
- ITKST 51 Operating system security 1, 5 op
- ITKST 52 Operating system security 2, 5 op
- ITKST 53 Ohjelmistoturvallisuus, 5 op
- ITKST 54 Mobiilijärjestelmien informaatioturvallisuus, 2 op
- ITKST 55 Kyberhyökkäys ja sen torjunta, 5 op
- ITKST 56 System vulnerabilities, 5 op
- ITKST 57 Cyber defence strategy analysis, 5 op

- TJTSM51 Information Security Management, 5 op
- TJTSM56 Advanced Course on Information Security Management, 5 op
- TJTSM65 Information privacy, 5 op
- TIES327 Tietoverkkoturvallisuus, 5 op
- KAOPXXX, Oikeudet informaatioturvallisuudessa, 5 op

Maanpuolustuskorkeakoulu

- 4A09B Johtamisjärjestelmä- ja tiedonsiirtotekniikan perusteet
- 4C06BV Tieto- ja tietoliikennejärjestelmät
- 124 Tietoverkkosodankäynti
- Sotatekniikan jatko-opintoseminaari

Tampereen teknillinen yliopisto

- TIE-03100 Tietoverkot ja tietoturva, 4 op
- TIE-30101 Tietoturvallisuuden perusteet, 2 op
- TIE-30200 Tietoturva-arki, 4 op
- TIE-30300 Tietoturvallisuuden jatkokurssi, 8 op
- TIE-30400 Verkon tietoturva, 5 op
- TIE-30500 Identiteetin- ja pääsynhallinta, 4 op
- TIE-30600 Turvallinen ohjelmointi, 3-6 op
- TIE-13100 Tietotekniikan projektityö, 5-10 op
- TIE-11400 Tietotekniikan seminaari, 3 op
- ASE-7610 Automaation turvallisuus, 5 op (Systeemitekniikan laitoksen kurssi)
- TLO-35236 Information Security Management, 4 op (Tiedonhallinnan ja logistiikanlaitoksen kurssi)
- MAT-63256 Mathematical cryptology, 7 op (Matematiikan laitoksen kurssi)

Turun yliopisto

- Foundations of Cryptography
- Cryptography I
- Cryptography II
- Algebraic Structures in Cryptography
- Selected Topics in Cryptography
- Coding Theory
- Algorithmic Complexity
- Automata and Formal Languages
- System and Application Security
- Firewall and IPS Technology
- Human element in information security
- Security Engineering
- Advanced Internet Technologies
- Management of Information System Security, 6 op
- Knowledge Management - Information Security, 6 op
- Proactive Law and the Prevention and Resolution of Disputes, 5-8 op

- Information technology and ethics, 5 op
- Management of ICT Services, 6 op
- Management of IS Projects, 6 op
- ProActive Contracting and Risk Management, 5-8 op

LIITE 3 Kyberturvallisuuden ammattikorkeakoulukursseja

Jyväskylän AMK

- Security Management in Cyber Domain, 5 op
- Auditing and Testing Technical Security, 5 op
- Cyber Security Implementation in Practice, 10 op
- Cyber Security Exercise, 5 op
- Tietoturva ja palveluiden hallinta, 7 op
- Tietoturvan toteutus, 8 op

Turun AMK

- Information Security, 5 op
- Cryptology, 5 op
- Web Application Security, 5 op
- Tietosuoja ja yksityisyys, 5 op
- Enterprise Information Security -moduuli, 15 op
    - CCNA Security, 5 op
    - Operational Security, 5 op
    - Information Security Risk Management, 5 op
- Internet Services and Security -moduuli, 15 op
    - Storage Systems, 5 op
    - Server Technology, 5 op
    - Cloud Computing, 5 op
- Information Security and Information Security Risk Management -moduuli, 15 op (YAMK)
    - Information Security Management 5 op
    - Data Protection 5 op
    - Information Security Risk Management 5 op

LÄHTEET

[1] ENISA, Threat Landscape, Responding to the Evolving Threat Environment, September 2012

[2] Euroopan parlamentin päätöslauselman Euroopan unionin kyberturvallisuussuunnitelmasta – avoin, turvallinen ja vakaa verkkoympäristö (2013/2606(RSP)) 6.9.2013, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B7-2013-0386+0+DOC+XML+V0//FI

[3] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final Brussels, 7.2.2013, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[4] INKA - innovatiiviset kaupungit 2014–2020, kyberturvallisuusteeman toimintasuunnitelma 2.1, 18.1.2014

[5] Libicki Martin C. (2007), Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New

[6] Turvallisuuskomitea, Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma, 11.3.2014, http://www.turvallisuuskomitea.fi/index.php/fi/20-ajankohtaista/45-kyberturvallisuusstrategian-toimeenpano-ohjelma-on-valmis

[7] Työ- ja elinkeinoministeriö, 21 polkua Kitkattomaan Suomeen, ICT 2015 -työryhmän raportti 17.1.2013, http://www.tem.fi/ajankohtaista/julkaisut/julkaisujen_haku/21_polkua_kitkattomaan_suomeen.98249.xhtml

[8] Valtioneuvoston periaatepäätös, Suomen kyberturvallisuusstrategia, 24.1.2013, www.yhteiskunnanturvallisuus.fi.

[9] Yhteiskunnan turvallisuusstrategia, valtioneuvoston periaatepäätös 16.12.2010

Informaatioteknologian tiedekunnan julkaisuja
No. 20/2015

ISBN 978-951-39-6105-3 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO