Informaatioteknologian tiedekunnan julkaisuja
No. 83/2018

Martti Lehto ja Jukka Niemelä

Kyberalan tutkimus ja koulutus Suomessa 2019

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 83/2019

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7829-7 (verkkoj.)
ISSN 2323-5004
Jyväskylä 2019

Martti Lehto & Jukka Niemelä

KYBERALAN TUTKIMUS JA KOULUTUS SUOMESSA 2019

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Tässä raportissa kuvataan yliopistoissa ja ammattikorkeakouluissa annettavaa kyberturvallisuuden/informaatioturvallisuuden/tietoturvallisuuden tutkimusta ja koulutusta. Raportti on päivitys Jyväskylän yliopistossa vuonna 2015 julkaistuun raporttiin: *M. Lehto ja A. Kähkönen. Kyberturvallisuuden kansallinen osaaminen, Informaatioteknologian tiedekunnan julkaisuja, 20/2015*, https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/20-2015_kyber_kansallinen_osaaminen_verkko.pdf

Kyberturvallisuustutkimuksen osalta tämä raportti kuvaa vain yleisellä tasolla minkälaista tutkimusta eri korkeakouluissa tehdään menemättä syvälle eri tutkimusaiheiden kuvaamiseen.

Kyberturvallisuuden/informaatioturvallisuuden/tietoturvallisuuden koulutus on laajentunut edelleen. Koulutuksen toteuttamisessa on kaksi mallia: kyberturvallisuuteen keskittyvä koulutusohjelma tai kyberturvallisuuden opetuksen integroiminen osaksi eri koulutusohjelmia. Ensiksi mainittu malli on käytössä Jyväskylän ja Turun yliopistoissa sekä Jyväskylän ammattikorkeakoulussa ja Kaakkois-Suomen ammattikorkeakoulussa. Integroitua mallia käytetään muissa korkeakouluissa. Molemmat mallit ovat välttämättömiä alan osaamisen parantamiseksi.

Kyberturvallisuuden koulutusohjelma tuottaa kyberturvallisuuden kokonaisuutta hallitsevia alan ammattilaisia, jotka ovat profiloituneet jollekin erityisosaamisalueelle. 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. Nämä alustaratkaisut tehostavat erityisesti harjoittelua todenmukaisissa kyberympäristöissä.

Kansainvälinen vertailuanalyysi osoittaa, että kyberturvallisuutta opetetaan maisteriohjelmissa eri sisältöisenä: kyberturvallisuus itsenäisenä ohjelmana, kyberturvallisuus muiden informaatioteknologian eri tieteenalojen näkökulmasta tai kyberturvallisuus muiden tieteenalojen sisällä.

ABSTRACT

This report describes cyber security / information security / data security research and education in the universities and the universities of applied sciences. The report is an update to the report published by the University of Jyväskylä in 2015: M. Lehto and A. Kähkönen. National expertise in cyber security, Publications of the Faculty of Information Technology, 20/2015, https://www.jyu.fi/it/en/tutkimus/julkaisut/it-julkaisu/20-2015_kyber_kansallinen_osaaminen_verkko.pdf

In the case of cyber security research, this report only describes research on the general level, which is being carried out in different universities, without going deep into different research topics.

Cyber security / information security / data security education has expanded. There are two models for implementing education: a cyber security education program or the integration of cyber security education into various education programs. The first model is used in the universities of Jyväskylä and Turku, and in the Jyväskylä University of Applied Sciences and Southeast Finland University of Applied Sciences, the integrated model is used in other universities. Both models are indispensable for improving the industry's competence.

The Cybersecurity Education Program produces professionals in the cyber security community who are profiled in any of the specialty areas. The integrated model produces professionals who understand both the specific technology (information technology, telecommunications, automation technology, etc.) and relation to the cyber security issues.

Cybersecurity development environments have been built and are being built in Finland. In some universities and research institutes, development environments have been built by extending existing laboratory environments. In addition, new environments focused specifically on cyber security research and education has been built and is being built. These platforms solutions enhance training especially in realistic cyber environments.

International benchmarking shows that cyber security is taught in different curriculum in Master of Science programs. Models are cybersecurity as an independent program, cyber security in different disciplines of IT, or cybersecurity within other disciplines.

KUVIOT

KUVIO 1 NCWF-viitekehyksen kategoriat ja erityisalueet 11
KUVIO 2 Tutkimuksen ja koulutuksen tiekartta 15
KUVIO 3 Kyberturvallisuusosaaminen ja -kyvykkyys kattavat koko koulutusalan 26
KUVIO 4 Tärkeimmät vaadittavat kyberturvallisuuden osaamisalueet 32
KUVIO 5 Tärkeimmät työllistymiseen vaadittavat osaamisvaatimukset ja muodolliset pätevyysvaatimukset 33
KUVIO 6 Kyberturvallisuuden opetus seitsemässä yliopistoissa 50
KUVIO 7 Kyberturvallisuuden opetus ammattikorkeakouluissa 58

TAULUKOT

TAULUKKO 1 Yhteenveto maisteriohjelmista 72

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

TAULUKOT 4

SISÄLLYS 5

1 JOHDANTO 9
- 1.1 Aikaisempaa tutkimusta 9
- 1.2 Kyberturvallisuus 9
- 1.3 Kyberturvallisuus koulutusalana 10
- 1.4 Kyberturvallisuus tutkimusalana 12
- 1.5 Kyberturvallisuuden tutkimukselle ja opetukselle asetettuja vaatimuksia 13
  - 1.5.1 Euroopan unionin kyberturvallisuusstrategia 13
  - 1.5.2 Suomen kyberturvallisuusstrategia 13
  - 1.5.3 ICT-2015 työryhmän raportti 13
  - 1.5.4 Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen 14
  - 1.5.5 Suomen tietoturvallisuusstrategia 15
  - 1.5.6 Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 17
  - 1.5.7 Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020 17
  - 1.5.8 Kasvua digitaalisesta turvallisuudesta - Tiekartta 2019–2030 18
  - 1.5.9 Kyberturvallisuus Suomessa 2019-2029 19
  - 1.5.10 Digitaalinen Eurooppa -ohjelma vuosiksi 2021-2027 20
- 1.6 EU:n kyberturvallisuusalan huippuosaamisyksikkö 21
- 1.7 ENISA:sta EU:n Kyberturvallisuusvirasto 23

2 KYBERTURVALLISUUSKOULUTUKSEN KEHITTÄMINEN 25
- 2.1 Kyberturvallisuuskoulutuksen tavoitteita 25
- 2.2 Kyberturvallisuuskoulutuksen suunnittelu 27
  - 2.2.1 Interaktiivisten pelien mahdollisuuksia 27
  - 2.2.2 Psykologinen näkökulma koulutuksen suunnitteluun 29
- 2.3 Kyberturvallisuuden osaamisvaje kansainvälisesti 30
- 2.4 Kyberturvallisuuden osaamisvaje kansallisesti 33
  - 2.4.1 Kyberkoulutuksen tarjonta ja kehittäminen 33
  - 2.4.2 Kyberosaajien työmarkkinatilanne Suomessa 35
  - 2.4.3 Kyberammattilaisen osaamisprofiili 36
  - 2.4.4 Suomessa on kyberosaajapula 37
- 2.5 Johtopäätöksiä 38

3 YLIOPISTOT 39
3.1 Aalto yliopisto (Aalto) 39
3.1.1 Kyberalaan liittyvä opetus 39
3.1.2 Kyberalaan liittyvät kurssit 39
3.1.3 Kyberalaan liittyvä tutkimus 40
3.2 Helsingin yliopisto (HY) 40
3.2.1 Kyberalaan liittyvä opetus 40
3.2.2 Kyberalaan liittyvät kurssit 40
3.2.3 Kyberalaan liittyvä tutkimus 40
3.3 Itä-Suomen yliopisto (UEF) 41
3.3.1 Kyberalaan liittyvä opetus 41
3.3.2 Kyberalaan liittyvät kurssit 41
3.3.3 Kyberalaan liittyvä tutkimus 41
3.4 Jyväskylän yliopisto (JY) 41
3.4.1 Kyberalaan liittyvä opetus 41
3.4.2 Kyberalaan liittyvät kurssit 42
3.4.3 Kyberalaan liittyvä tutkimus 42
3.5 Lappeenrannan teknillinen yliopisto (LUT) 43
3.5.1 Kyberalaan liittyvä opetus 43
3.5.2 Kyberalaan liittyvät kurssit 43
3.5.3 Kyberalaan liittyvä tutkimus 43
3.6 Maanpuolustuskorkeakoulu (MPKK) 43
3.6.1 Kyberalaan liittyvä opetus 43
3.6.2 Kyberalaan liittyvät kurssit 44
3.6.3 Kyberalaan liittyvä tutkimus 44
3.7 Oulun yliopisto (OY) 45
3.7.1 Kyberalaan liittyvä opetus 45
3.7.2 Kyberalaan liittyvät kurssit 45
3.7.3 Kyberalaan liittyvä tutkimus 45
3.8 Tampereen yliopisto (TUNI) 46
3.8.1 Kyberalaan liittyvä opetus 46
3.8.2 Kyberalaan liittyvät kurssit 46
3.8.3 Kyberalaan liittyvä tutkimus 46
3.9 Turun yliopisto (TY) 48
3.9.1 Kyberalaan liittyvä opetus 48
3.9.2 Kyberalaan liittyvät kurssit 49
3.9.3 Kyberalaan liittyvä tutkimus 49

4 AMMATTIKORKEAKOULUT 51
4.1 Centria-ammattikorkeakoulu (Centria) 51
4.1.1 Kyberalaan liittyvä opetus 51
4.1.2 Kyberalaan liittyvät kurssit 51
4.1.3 Kyberalaan liittyvä tutkimus 51
4.2 Jyväskylän ammattikorkeakoulu (JAMK) 51
4.2.1 Kyberalaan liittyvä opetus 51
4.2.2 Kyberalaan liittyvät kurssit 52

4.2.3 Kyberalaan liittyvä tutkimus 52
4.3 Kaakkois-Suomen ammattikorkeakoulu (XAMK) 53
4.3.1 Kyberalaan liittyvä opetus 53
4.3.2 Kyberalaan liittyvät kurssit 53
4.3.3 Kyberalaan liittyvä tutkimus 53
4.4 Laurea ammattikorkeakoulu (Laurea) 53
4.4.1 Kyberalaan liittyvä opetus 53
4.4.2 Kyberalaan liittyvät kurssit 54
4.4.3 Kyberalaan liittyvä tutkimus 54
4.5 Metropolia ammattikorkeakoulu 54
4.5.1 Kyberalaan liittyvä opetus 54
4.5.2 Kyberalaan liittyvät kurssit 54
4.5.3 Kyberalaan liittyvä tutkimus 54
4.6 Oulun ammattikorkeakoulu (OAMK) 55
4.6.1 Kyberalaan liittyvä opetus 55
4.6.2 Kyberalaan liittyvät kurssit 55
4.6.3 Kyberalaan liittyvä tutkimus 55
4.7 Poliisiammattikorkeakoulu (POLAMK) 55
4.7.1 Kyberalaan liittyvä opetus 55
4.7.2 Kyberalaan liittyvät kurssit 55
4.7.3 Kyberalaan liittyvä tutkimus 55
4.8 Tampereen ammattikorkeakoulu (TAMK) 56
4.8.1 Kyberalaan liittyvä opetus 56
4.8.2 Kyberalaan liittyvät kurssit 56
4.8.3 Kyberalaan liittyvä tutkimus 57
4.9 Turun ammattikorkeakoulu (TURKUAMK) 57
4.9.1 Kyberalaan liittyvä opetus 57
4.9.2 Kyberalaan liittyvät kurssit 57
4.9.3 Kyberalaan liittyvä tutkimus 58

5 MUU KOULUTUS 59
5.1 Puolustusvoimien varusmieskoulutus 59
5.2 Maanpuolustuskoulutusyhdistys (MPK) 59
5.3 Yritysten tuottama kyberturvallisuuskoulutus 60
5.3.1 AlmaTalent 60
5.3.2 Cyber Security Academy 60
5.3.3 CyberWatch 60
5.3.4 F-Secure 61
5.3.5 Nixu Oyj 61
5.3.6 Saranen Consulting 62
5.3.7 Siverskin 62

6 MUU TUTKIMUSTOIMINTA 63
6.1 Tietotekniikan tutkimuslaitos 63
6.2 Valtion teknillinen tutkimuslaitos 63
6.3 Puolustusvoimien tutkimuslaitos 64

7 KYBERALAN KOULUTUS YHDYSVALLOISSA....65
7.1 Koonnos....65
7.2 MSc in Cyber Security....66
7.3 MSc in Computer Science (CS)....66
7.4 MSc in Information Systems (IS)....67
7.5 MSc in Computer Engineering (CE)....68
7.6 MSc in Information Technology (IT)....69
7.7 MSc in Information Assurance (IA)....71
7.8 Yhteenveto maisteriohjelmista....72

LÄHTEET....73

1 JOHDANTO

1.1 Aikaisempaa tutkimusta

Tässä raportissa esitellään kyberturvallisuuden tutkimuksen ja koulutuksen nykytilaa Suomessa. Päätavoite on ollut selvittää yleisellä tasolla kyberturvallisuuden koulutuksen toteutusta Suomessa. Raportti on koostettu tiedoista, jotka löytyvät yliopistojen ja ammattikorkeakoulujen verkkosivuilta. Tietoja on täydennetty kyselyjen avulla.

Kyberturvallisuusosaamisesta ja tarvittavista toimenpiteistä on julkaistu seuraavia tutkimuksia vuoden 2016 jälkeen:

- Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016, 15.02.2016
- Maailman luotetuinta digitaalista liiketoimintaa Suomen tietoturvallisuusstrategia, Liikenne- ja viestintäministeriön julkaisuja 7/2016, 19.4.2016
- Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, Valtioneuvoston kanslia, 17.2.2017
- Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, Turvallisuuskomitea, 10.4.2017
- Kasvua digitaalisesta turvallisuudesta - Tiekartta 2019–2030, Työ- ja elinkeinoministeriö, 8.3.2019

1.2 Kyberturvallisuus

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriintyneestä kybertoimintaympäristöstä riippuvat fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Keskeiset

tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden, määritellään Suomen kyberturvallisuusstrategiassa.[1]

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.

1.3 Kyberturvallisuus koulutusalana

Turvallisuuskomitean julkaisemassa toimeenpano-ohjelmassa (2017) on nostettu yhdeksi pääteemaksi kansalaisten, elinkeinoelämän ja hallinnon kyberosaamisen edistäminen tukemaan digitalisaation kehitystä. Keskeisinä osa-alueina mainitaan mm. kansalaisten ja ikääntyneiden ihmisten kyberosaamisen kehittäminen sekä kyberturvallisuuden ja digitaalisen toimintaympäristön perustaitojen edistäminen yleissivistävässä ja ammatillisessa koulutuksessa.[2] Kyberturvallisuuden edistämiseksi perus- ja jatkotutkintoon johtava yliopistojen ja ammattikorkeakoulujen toteuttama tutkimus- ja kehittämistoiminta, ja korkeakoulujen antama koulutus on välttämätön. Lisäksi tarvitaan alan opetusta myös II-asteen ammatillisessa koulutuksessa.

Koulutustoiminnan tehokkuuden kannalta on keskeistä, että siinä hyödynnetään jo olemassa olevaa osaamista ja resursseja, ja että koulutustoimintaa kehitetään toimijoiden välisenä yhteistyönä. On keskeistä luoda tavoitteet kyberturvallisuudelle yleissivistävälle koulutukselle, kyberalan tutkintoon johtavalle koulutukselle, muulle tutkintoon johtavalle koulutukselle, täydennyskoulutukselle sekä muulle osaamisen kehittämiselle (ikääntyneet, kansalaiskasvatus, lapset).[3]

National Initiative for Cybersecurity Education (NICE) on luonut tarvittavien kyberkompetenssien kuvaamiseen erityisen viitekehyksen. Tämä National Cybersecurity Workforce Framework -viitekehys (NCWF) on taksonomia ja sanasto, jolla voidaan kuvata kyberturvallisuusalan työtehtäviä. Sen tarkoituksena on helpottaa organisaatioita tunnistamaan kyberturvallisuusalan työn sisällölliset tarpeet. Tunnistamisen myötä henkilöstön rekrytointi, koulutus, harjoituttaminen ja kyvykkyyksien ylläpito voidaan organisoida tehokkaasti. Samalla se antaa työntekijälle mahdollisuuden tunnistaa omat kyvykkyytensä ja suunnitella omaa työuraansa. [4]

---

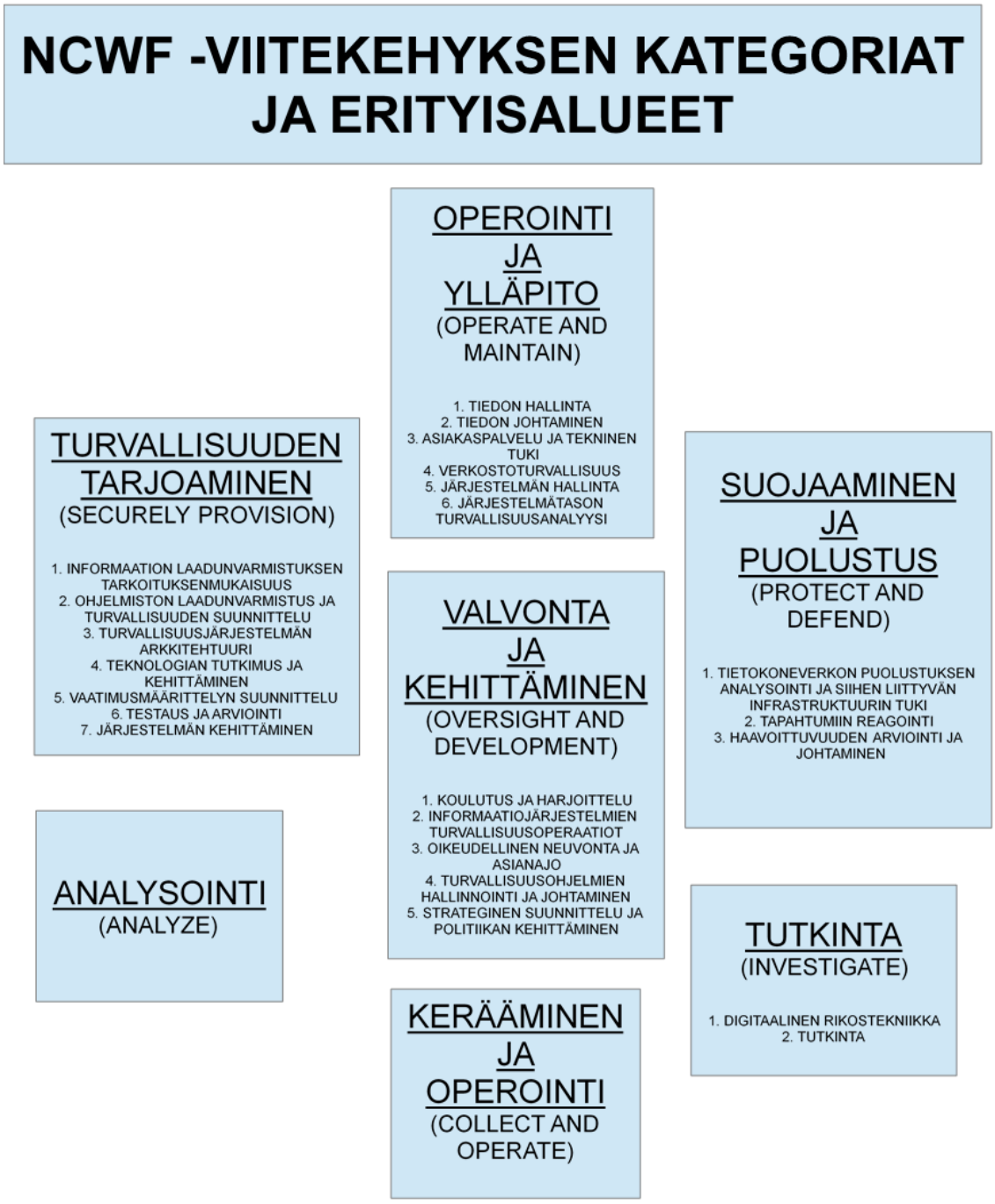
[1] Turvallisuuskomitea, Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013
Kyberturvallisuuden sanasto, turvallisuuskomitea 2018, http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

[2] Turvallisuuskomitea, Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, 10.4. 2017

[3] https://lausuntopalvelu.fi/SV/Proposal/ParticipationNonJsShowReport?proposalId=c31967a4-8364-44f0-b0f4-06953bd140f4

[4] Niemelä Jukka, Kyberturvallisuuden työvoiman tarve, saatavuus ja kehittäminen vastaamaan alan tarvetta Suomessa, pro gradu -työ, Jyväskylän yliopisto, IT-tiedekunta, 2019

Oheisessa kuviossa 1 on esitetty tiivistetysti NCWF-viitekehyksen seitsemän kategoriaa.[5]



KUVIO 1 NCWF-viitekehyksen kategoriat ja erityisalueet

NCWF-viitekehystä voidaan soveltaa tarvittavien kyberosaamisen ydinkompetenssin sisältöjen määrittelyyn ja sitä kautta opetussuunnitelmien ja kurssisisältöjen laatimiseen.

[5] Willberg Nils, Kyberosaamisen nykyiset ja tulevat tarpeet julkisen sektorin organisaatioissa, pro gradu -työ, Jyväskylän yliopisto, IT-tiedekunta, 2017

1.4 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 myös 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 sekä 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 tieteiden välisten 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 vahingoittumiselta. Osaamistarpeen perusta ulottuu tietojärjestelmätieteeseen, informaatioteknologiaan ja tietojenkäsittelytieteeseen.

1.5 Kyberturvallisuuden tutkimukselle ja opetukselle asetettuja vaatimuksia

1.5.1 Euroopan unionin kyberturvallisuusstrategia

Euroopan unionin kyberturvallisuusstrategian (2013) mukaan EU:n olisi turvattava verkkoympäristö, joka tarjoaa mahdollisimman laajan vapauden ja tietoturvan kaikkien hyödyksi. EU:n kyberturvallisuusstrategian tavoitteiden saavuttamiseksi komissio on pyytänyt jäsenvaltioita tehostamaan kansallisia toimia verkko- ja tietoturvaopetuksen ja -koulutuksen alalla aloittamalla kouluissa verkko- ja tietoturvaopetusta, antamalla tietotekniikan opiskelijoille opetusta verkko- ja tietoturvasta, tietoturvallisten ohjelmistojen kehittämisestä ja henkilötietojen suojasta sekä antamalla julkishallinnon työntekijöille peruskoulutusta verkko- ja tietoturvan alalla.[6]

1.5.2 Suomen kyberturvallisuusstrategia

Suomen kyberturvallisuusstrategian (2013) 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.[7]

1.5.3 ICT-2015 työryhmän raportti

Suomessa on pula kyberturvallisuusalan ammattilaisista. Tämän perusteella ICT 2015 -työryhmä (2013) 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.[8]

Tutkimus ja koulutus kytkevät entistä vahvemmin tiedonhallinnan ja tietointensiivisen osaamisen yritysten kilpailukykyyn ja kilpailuedun saavuttamiseen ja ylläpitämiseen.

[6] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final
[7] Turvallisuuskomitea, Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013
[8] TEM, 21 polkua Kitkattomaan Suomeen, ICT 2015 -työryhmän raportti 4/2013, 17.1.2013

Vahvistamalla alan tutkimusta ja opetusta edistetään tieteellisiä läpimurtoja, innovaatioiden syntymistä, teknologista kehitystä, tuottavuuden kasvua ja tätä kautta kansallista hyvinvointia.[9]

1.5.4 Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen

Kyberosaaminen Suomessa- raportin (2016) mukaan ”Nykytilanteessa yliopistojen ohjausmallissa painottuvat erilaiset suorituskykyindikaattorit, jotka painottavat esimerkiksi akateemista julkaisemista sen sijaan, että kannustaisivat ratkaisemaan yhteiskunnallisia ongelmia. Yliopistoilta edellytetään erikoistumista ja keskittymistä omiin vahvuusalueisiinsa. Kyberturvallisuuden alaa leimaa hajanainen tutkimuskenttä ja vähäinen yhteistyö eri tahojen välillä. Kyberturvallisuuden tutkimuksen ja koulutuksen suuntaamista ei koordinoida kansallisella tasolla. Alaa leimaa se, että kyberturvallisuus mielletään ensisijaisesti ja lähes pelkästään teknologiseksi erityisosaamiseksi.” [10]

Edelleen raportin mukaan ”tavoitteena on, että yliopistojen rooli yhteiskunnallisten haasteiden ratkaisussa vahvistuu ja uudet toimintamallit yritysten ja tutkimustoimijoiden yhteistyön vahvistamiseksi ovat vakiintuneet. Nopeasti muuttuviin vaatimuksiin vastaamiseksi on elinikäiselle oppimiselle luotu toimivat mahdollisuudet yhteiskunnallisella tasolla. Kyberturvallisuuskoulutus on toteutettu koordinoidusti eri koulutusasteilla varmistaen kansalaisten perusosaaminen, operatiivinen osaaminen ja riittävä erityisosaaminen. Tietoturvatietoisuudesta on kehittynyt lukutaitoon verrattava kansalaistaito ja erikoistunut kyberturvallisuusosaaminen on muodostunut erityisosaamisen alaksi, johon on oma koulutustarjontansa. Tavoitteen saavuttamiseksi tarvitaan ”kirkkaat strategiset valinnat ja valittuun suuntaan kohdistetut toimet”. [11]

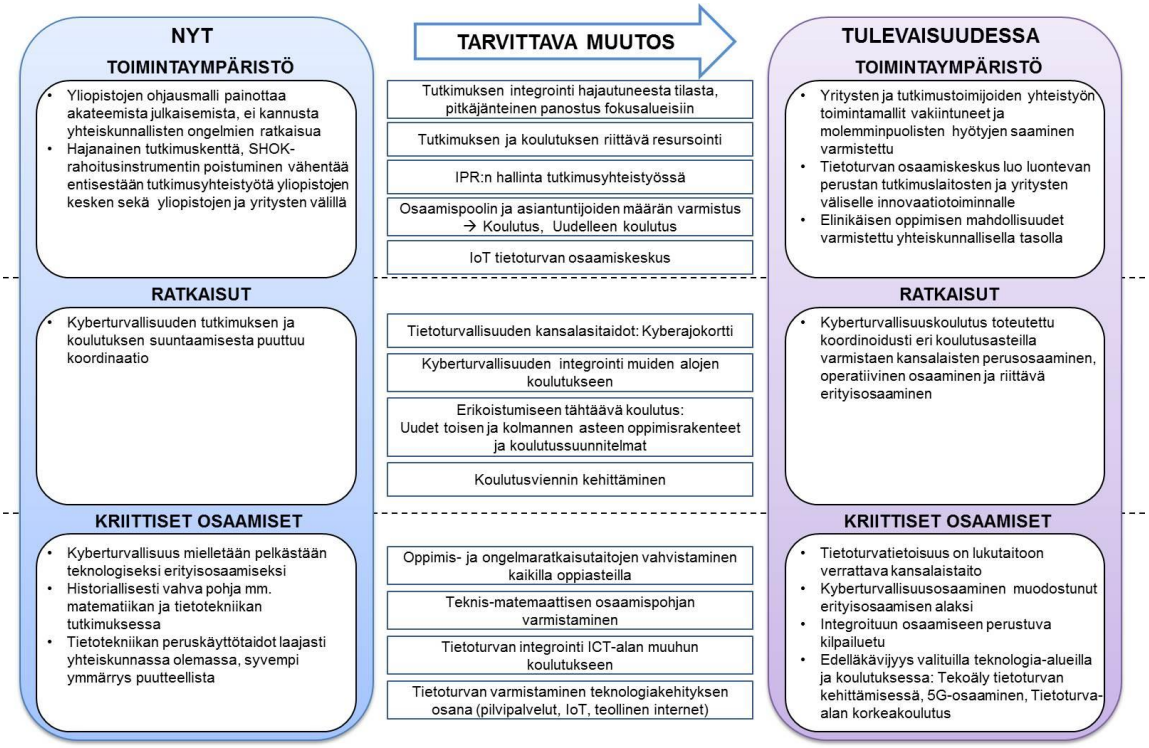
Tutkimuksen osalta ”muutoksen perusta liittyy toiminnan koordinointiin ja hajanaisen kentän järjestäytymiseen. Tutkimus ja koulutus tarvitsevat myös riittävästi resursseja ja rahoituksessa on varmistettava toiminnan pitkäjänteisyys valituilla alueilla. Kyberturvallisuusalan mahdollisuudet liittyvät suoraan osaajien määrään ja siten osaamispoolin ja asiantuntijoiden määrän varmistamiseksi on huolehdittava riittävästä koulutuksesta. Yhtä keskeistä on myös järjestää uudelleen koulutuksen mahdollistavat järjestelmät.”[12]

Kyberturvallisuuden koulutusta on ”tarpeen järjestää eri tasoilla ja erilaisilla painotuksilla alkaen tietoturvan kansalaistaidoista aina erikoistuneeseen korkeakoulutukseen asti. Kansalaistaitojen varmistamiseksi voidaan perustaa kyberajokortti, joka tarjoaisi perusymmärryksen henkilökohtaisesta kyberturvallisuudesta. Läpäisevyysperiaatteen mukaisesti kyberturvallisuustietoutta pitäisi integroida myös muiden alojen koulutukseen. Kyberturvallisuusalalla on tärkeää, että on saatavilla myös riittävän operatiivisen osaamisen omaavia ammattilaisia. Samanaikaisesti on tärkeää turvata erikoistumiseen

[9] Ibid.
[10] VNK, Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016, 15.02.2016
[11] Ibid.
[12] Ibid.

tähtäävä koulutus. Tätä varten tarvitaan uusia toisen ja kolmannen asteen oppimisrakenteita ja koulutussuunnitelmia.” [13]

Oheisessa kuviossa 2 on raportissa esitetty kyberturvallisuuden tutkimuksen ja koulutuksen tiekartta.



KUVIO 2 Tutkimuksen ja koulutuksen tiekartta[14]

1.5.5 Suomen tietoturvallisuusstrategia

Suomen tietoturvallisuusstrategian (2016) mukaan ”hallitakseen tietoturvariskejä, yritykset tarvitsevat erittäin monipuolista osaamista niin työntekijöiden kuin alihankkijoidensa piirissä. Järjestelmien ja niissä olevan tiedon suojaaminen perustuu teknisellä tasolla pitkälti tehokkaisiin tiedon salaus- ja suojaus- ja pääsynhallintamenetelmiin, joiden tuottamiseen ja hyödyntämiseen liittyvän osaamisen perusvalmiuksien kehittäminen edellyttää pitkäjänteistä tutkimusta ja opetusta.”[15]

”Kryptologisten menetelmien hallinta edellyttää kehittyneitä matemaattisia valmiuksia. Kryptologian opetus ja tutkimus Suomalaisissa yliopistoissa ja korkeakouluissa vaikuttaa olevan verrattain ohutta osaajien kysyntään nähden. Myös muulle teknologiselle osaa-

[13] Ibid.
[14] Ibid.
[15] LVM, Maailman luotetuinta digitaalista liiketoimintaa Suomen tietoturvallisuusstrategia, Liikenne- ja viestintäministeriön julkaisuja 7/2016, 19.4.2016

miselle sekä liiketaloudelliselle ja oikeudelliselle osaamiselle on tarvetta. EU:n tietosuoja-asetuksen ja verkko- tietoturvadirektiivin myötä tietosuojaan ja tietoturvaan liittyvän osaamisen kysyntä oletettavasti kasvaa."[16]

"Oikeanlaisten osaajien löytäminen on osoittautunut alan toimijoille haastavaksi myös siksi, etteivät parhaat osaajat välttämättä tule perinteisiä koulutusväyliä pitkin. Esimerkiksi osa huipputason koodareista saattaa olla täysin itseoppineita. Erityisesti tietoturva-ala onkin pyrkinyt käyttämään rekrytoinneissa myös perinteisestä poikkeavia keinoja ja yritykset ovat kehitelleet myös omia koulutusohjelmiaan potentiaalisille työntekijöille." Tietoturvallisuusstrategia esittää seuraavia toimenpiteitä tutkimukseen ja koulutukseen:[17]

- Kartoitetaan Suomessa toimivien yritysten tarpeet tietoturva- ja tietosuojaosaajille. Selvitetään keinoja osaajien saatavuuden parantamiseksi.
- Huolehditaan siitä, että tietoturvallisuuteen liittyvään koulutukseen on käytettävissä riittävästi resursseja.
- Järjestetään sarja kansallisten tietoturvaosaajien tunnistamista ja verkostoitumista tukevia tietoturvatapahtumia (Hackathon).

Suomen kyberturvallisuusstrategia (2019) luonnoksessa 4.3.2019 todetaan, että "Suomalainen yhteiskunta tarvitsee kyberturvallisuuden osaamista sekä julkisessa hallinnossa että elinkeinoelämässä. Kansallinen kyberturvallisuus rakennetaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä, jossa jokainen voi osaltaan vaikuttaa yhteiseen kyberturvallisuuteemme."[18]

Strategia luonnoksen mukaan kyberosaamista parannetaan: [19]

- Vahvistamalla ammattikorkeakoulujen ja yliopistojen kyber- ja tietoturvallisuuteen, ohjelmisto- ja sovelluskehitykseen sekä tietoverkkoihin ja tietoliikenteeseen liittyviä koulutusohjelmia
- Vahvistamalla kansallista kyberturvallisuuden tutkimus-, kehitys- ja testaustoimintaa
- Kehittämällä valtakunnallista digiturvallisuuden koulutus- ja harjoitusjärjestelmää osana julkisen hallinnon digitaalisen turvallisuuden koulutusta. Sillä kehitetään julkishallinnon, yritysten ja muiden sidosryhmien työntekijöiden sekä kansalaisten osaamista
- Varmistamalla kansallisesti kriittisten kyberosaamisalueiden edellyttämä korkeatasoinen koulutus. Tätä tuetaan sekä kansallisella että kansainvälisellä koulutuksella ja harjoitustoiminnalla

[16] Ibid.
[17] Ibid.
[18] Turvallisuuskomitea, Suomen kyberturvallisuusstrategia luonnos 1.0, 4.3.2019
[19] Ibid.

- Kehittämällä edelleen Kyberturvallisuuskeskuksen yhteistyötä viranomaisten ja elinkeinoelämän välillä. Tämä edistää Suomen kykyä tunnistaa tietoturvauhkia ja varoittaa niistä sekä parantaa edelleen elinkeinoelämän mahdollisuuksia varautua tietoturvauhkiin
- Lisäämällä julkisen hallinnon, elinkeinoelämän ja yksityisten ihmisten tietoisuutta uusien palveluiden ja tuotteiden tietoturvasta. Kyberturvallisuus on datatalouden ja tekoälyyn perustuvien sovellusten ehdoton edellytys. Tämä edellyttää valmistajien ja palveluntarjoajien luottamusta toisiinsa sekä kansalaisten luottamusta heille tarjottuihin palveluihin ja tuotteisiin.

1.5.6 Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi

Valtioneuvoston kanslialle tehdyssä kyberturvallisuusselvityksessä (2017) todetaan: ”Kyberturvallisuus on digitalisaation mahdollistaja. Suomella on vahva kansainvälinen luottamuspääoma ja tätä luottamusta sekä suomalaista kyberturvallisuuden osaamista on oleellista pystyä hyödyntämään.” [20] Edelleen selvityksessä todetaan, että ”Osaamisen taso on yksi keskeinen valtiollisen kyberturvallisuuden tason mittari. Suomella on hyvä kansainvälinen maine kyberturvallisuuden osaamisessa. VTT:n ”Kyberosaaminen Suomessa” -raportin ja tässä tutkimuksessa tehtyjen havaintojen perusteella suomalaisten osaamista on pystyttävä vahvistamaan kyberturvallisuuden edelläkävijyyden saavuttamiseksi. Kyse on myös tarvittavan osaamisen paremmasta tunnistamisesta (minkälaiselle osaamiselle on tarve) varsin nopeasti muuttuvassa teknologian kehityksessä. Osaavan henkilöstön puute ja rekrytointivaikeudet ovat kyberturvallisuusalan keskeisiä haasteita.”[21]

Raportin mukaan ”Kyberturvallisuuden osaajista käydään yhä kovenevaa kilpailua lähivuosina niin Suomessa kuin kansainvälisesti. Osaajien kouluttaminen edellyttää hajanaisen koulutuksen ja tutkimuksen nykyistä parempaa koordinaatiota oppilaitosten välillä sekä tutkimustoiminnan monipuolistamista. Samalla on kyettävä ketterään koulutuksen kehittämiseen ja osaamisen vahvistamiseen, sillä alan osaamisvaatimukset muuttuvat varsin nopeasti.”[22]

1.5.7 Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020

Turvallisuuskomitean julkaisemassa toimeenpano-ohjelmassa (2017) on esitetty seuraavia tavoitteita ja toimenpiteitä:[23]

[20] Lehto M. Limnéll J., Innola E., Pöyhönen J., Rusi T., Salminen M., Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, 17.2.2017
[21] Ibid.
[22] Ibid.
[23] Turvallisuuskomitea, Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, 10.4. 2017

- Julkisen hallinnon tieto- ja kyberturvallisuushenkilöstön osaamista on parannettu.
    - Tähän liittyvät kansalliset kyberturvallisuusharjoitukset ja julkisen hallinnon henkilöstön osaamisen kehittäminen ja kryptologian omavaraisuuden varmistaminen.
- Kansalaisten tieto- ja kyberturvallisuusosaaminen on edistynyt.
    - Maanpuolustuskoulutusyhdistys toteuttaa vuosittain kyberturvallisuuskoulutusohjelman, joka koostuu kaikille kansalaisille avoimista peruskursseista sekä ammattilaisille suunnatuista jatko- ja erikoiskursseista.
- Kansallinen tieto- ja kyberturvallisuusviikko on toteutettu vuosittain.
    - Toteutetaan lokakuussa osana Euroopan Unionin kyberturvallisuuskuukautta (ECSM).
- Kyberturvallisuuden ja digitaalisen toimintaympäristön perustaidot – yleissivistävä ja ammatillinen koulutus on edistynyt.
    - Opettajien täydennyskoulutuksessa kehitetään ja edistetään tieto- ja kyberturvallisuuteen liittyviä sisältöjä osana monilukutaitoa.
- Kyberturvallisuuden tutkimusyhteistyötä on tiivistetty viranomaisten ja tutkimusorganisaatioiden sekä elinkeinoelämän kesken.
    - Turvallisuuskomitean sihteeristö rakentaa yhdessä muiden tahojen kanssa tutkimustoiminnan yhteistyömallin.

1.5.8 Kasvua digitaalisesta turvallisuudesta - Tiekartta 2019–2030

TEM:n digitaalisen turvallisuuden kasvun tiekartan (2019) tavoitteena on edistää digitaaliseen turvallisuuteen ja osaamiseen liittyvää yritysvetoista kehitystä, kasvua ja kansainvälistymistä yritysten, julkisen sektorin ja tutkimuslaitosten yhteistyönä. Osaaminen ja jatkuva oppiminen -alueen toimenpiteiden tavoitteena on lisätä kansallista tietoisuutta digitaalisesta turvallisuudesta sekä korostaa digitaalisen turvallisuuden osaamisen roolia ja merkitystä osana uutta digitaalista yhteiskuntaa.[24]

Osaaminen ja jatkuva oppiminen -teeman visiossa ”Suomi on koulutuksen ja oppimisen mallimaa, jossa digitaalisen turvallisuuden peruskäsitteet ja kokonaisnäkemys omaksutaan jo nuorena ja osaamisen kehittymistä tuetaan jatkuvalla oppimisella läpi elämän. Digitaalisen turvallisuuden ymmärtäminen on kansalaistaito ja -velvollisuus, ja siihen liittyvät opetuksen ja osaamisen kehittämisen periaatteet ja menetelmät on tunnustettu parhaiksi maailmassa. Kokonaisnäkemykseen sisältyvät teknisten taitojen ja osaamisen ohella myös esimerkiksi etiikka, psykologia, systeeminen ajattelu ja liiketoimintaosaaminen. Jokaisella asukkaalla on yhdenvertaiset mahdollisuudet digitaalisten taitojen hankkimiseen ja oman osaamisensa jatkuvaan kehittämiseen. Digitaalinen luottamus ja turvallisuus nähdään yleisesti tulevaisuuteen suuntaavina investointeina, kansakunnan tu-

[24] TEM, Kasvua digitaalisesta turvallisuudesta - Tiekartta 2019–2030, Työ- ja elinkeinoministeriön julkaisuja 2019:17, 8.3.2019

kijalkoina sekä keskeisinä viennin ja kansainvälisen yhteistyön mahdollistajina. Koulutuksen ja tutkimuksen rahoitukselle on löydetty kestävä malli, joka mahdollistaa pitkäjänteisen osaamisen kehittämisen.” [25]

Tiekartan visio vuodelle 2030: ”**Vuonna 2030 Suomi on koulutuksen ja oppimisen mallimaa, jossa digitaalisen turvallisuuden peruskäsitteet ja kokonaisnäkemys omaksutaan jo nuorena ja osaamisen kehittymistä tuetaan jatkuvalla oppimisella läpi elämän**.”[26]

1.5.9 Kyberturvallisuus Suomessa 2019-2029

Tätä raporttia kirjoitettaessa valmisteilla oli Allied ICT Finlandin (AIF) CyberSec^{FIN} -kyberturvallisuusekosysteemin *Kyberturvallisuus Suomessa 2019-2029* strategia osana AIF:n strategiasarjaa. Siinä tarkastellaan seuraavia keskeisiä osa-alueita:[27]

1. Kyberturvallisuuden merkitys Suomelle
2. Kyberturvallisuuden positio Suomessa
3. Kyberturvallisuuden osaamisen hallinta
4. Kansallisen oppimisympäristön rakentaminen
5. Kansallisen kyberalan tutkimuksen vahvistaminen
6. Kyberturvallisuus Suomessa 2019-2029 -tavoitetila

Luonnoksen mukaan kyberturvallisuuteen tehtävät koulutus- ja tutkimuspanostukset lisäävät Suomen uskottavuutta kyberturvallisuuden edelläkävijämaana. Suomalainen kyberturvallisuuden johtamisen ja hallinnan osaaminen tulee olla kansainvälisesti merkittävällä tasolla. Myös kyberturvallisuuden tutkimuksen tulee olla kansainvälisesti tarkasteltuna huipputasoa.

Kyberturvallisuus tulee nähdä osana laajempaa kokonaisuutta luottamuksesta digitaalisiin palveluihin. Luottamus digitaalisiin palveluihin edellyttää teknisten taitojen lisäksi mm. median monilukutaitoa, ymmärrystä digitaalisen toimintaympäristön lainalaisuuksista ja tietoisuutta informaatiovaikuttamisesta. Digitaaliseen luottamukseen liittyvä osaaminen täytyy nähdä kansalaistaitona.

Koulutustavoitteiden toteutuminen edellyttää, että koulutuksen ja tutkimuksen rahoituksen taso on kunnossa ja pitkäjänteisesti turvattu.

Strategian mukaan kansallisen kyberturvallisuuden huippuosaamisen kehittäminen edellyttää riittävän osaamiskeskittymän muodostumista. Huippuosaamiskeskittymän muodostaminen edellyttää korkeakoulujen välistä yhteistyötä, monitieteellisyyttä ja usean muun eri sidosryhmän yhteistyötä. Kehittämiseen tulee sitouttaa mukaan opetus-

[25] Ibid.
[26] Ibid.
[27] https://alliedict.fi/

ja koulutusalan toimijat (yliopistot, ammattikorkeakoulut, peruskoulut, kunnat ja kaupungit), elinkeinoelämän keskeiset toimijat ja yhteistyöekosysteemit, yhteiskunnan kriittiseen infrastruktuuriin liittyvät toimijat sekä kyberalan yritykset ja toimijat.

Huippuosaamiskeskittymä tarvitsee digitaalisen alustan, jolla voidaan tarjota tietoa ja älykkäitä työkaluja opetuksen avuksi. Digitaalinen toimintaympäristö on jatkuvasti muuttuva ja siihen liittyvän opetus- ja koulutusmateriaalin tuottaminen sekä jakaminen on kyettävä tuottamaan siten, että kaikilla on yhtäläinen mahdollisuus tarvittavan tiedon omaksumiseen. Oleellisena osana skaalautuvaa oppimiskokonaisuutta on yhtenäinen digitaalinen alusta, joka mahdollistaa muuttuvan tiedon ja siihen liittyvän materiaalin jakamisen kouluille sekä oppilaitoksille. Alustan kautta pystytään tuottamaan työkaluja sekä opettajille että oppilaille, kaikkien erilaisiin tarpeisiin. Digitaalisen alustan lisäksi tarvitaan sisällön tuottamisen sekä jatkuvan oppimisen tukea muuttuvassa ympäristössä. Digitaalisen alustan ja sen sisältöjen tulee palvella kaikkia eri koulutustasoilla (varhaiskasvatus, peruskoulu, II-asteen koulutus (lukiot, ammattikoulut), yliopistot ja ammattikorkeakoulut, vapaaehtoistoiminta, aikuiskoulutus jne.).

CyberSec^{FIN} -kyberturvallisuusekosysteemin visiona on luoda Suomesta kansainvälisesti tunnustettu kyberturvallisuuden liiketoiminnan, tutkimuksen ja osaamisen sekä kyberuhkiin varautumisen maailmanlaajuinen edelläkävijä. Kyberturvallisuuden tutkimus ja opetus, alan teknologioiden kehittäminen sekä liiketoimintainnovaatiot ovat keskeisiä tulevaisuuden talouskasvun lähteitä ja kansallisia erottautumistekijöitä.

1.5.10 Digitaalinen Eurooppa -ohjelma vuosiksi 2021-2027

Tätä raporttia laadittaessa oli eduskunnan käsittelyssä Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston asetukseksi *Digitaalinen Eurooppa -ohjelman* perustamisesta. Osana monivuotiseen rahoituskehykseen liittyvää lainsäädäntöpakettia Euroopan komissio julkisti 6.6.2018 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi Digitaalinen Eurooppa -ohjelmasta (COM (2018) 434 final).[28]

Ehdotuksen tavoitteena on uuden Digitaalinen Eurooppa -ohjelman perustaminen ohjelmakaudelle 2021-2027 pyrkimyksenä parantaa EU:n kansainvälistä kilpailukykyä sekä kehittää ja vahvistaa Euroopan strategisia digitaalisia valmiuksia. Ohjelman avulla lisätään ja maksimoidaan digitaalisen murroksen hyödyt Euroopan kansalaisille, julkiselle hallinnolle ja yrityksille. Ohjelma jakautuu seuraaviin viiteen toisiinsa kytkeytyvään tavoitteeseen tai pilariin: suurteholaskenta, tekoäly, **kyberturvallisuus** ja luottamus, edistyneet digitaaliset taidot, sekä digitaaliteknologioiden hyödyntäminen, digitaalikyvykkyydet ja yhteentoimivuus. [29]

[28] https://eur-lex.europa.eu/legal-content/FI/HIS/?uri=COM%3A2018%3A0434%3AFIN
https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/U_69+2018.aspx
[29] Ibid.

Kyberturvallisuuden ja luottamuksen osalta tuetaan yhdessä jäsenvaltioiden kanssa kyberturvallisuuden edistyneiden työkalujen ja tietojärjestelmien hankintaa sekä kyberturvallisuuteen liittyvän eurooppalaisen osaamisen ja taitojen hyödyntämistä.[30]

Keskeisessä roolissa on ohjelman ensimmäisenä toteutusvuonna luotava, yrityksiä ja julkista sektoria digitalisaatiossa tukeva **digitaali-innovointikeskittymien (DIH) verkosto**. Digitaali-innovointikeskittymillä tarkoitetaan oikeudellisia toimijoita, jotka valitaan avoimen ja kilpailullisen menettelyn kautta toteuttamaan ohjelman toimenpiteitä, erityisesti tarjoamaan teknologista osaamista, kokeilualustoja ja digitaalisen murroksen edellyttämiä sovelluksia. [31]

Valtioneuvosto suhtautuu yleisellä tasolla myönteisesti ehdotukseen ja sen tavoitteisiin. Euroopan kilpailukykyä tulee vahvistaa ja siinä tärkeää on EU-tason panostus innovaatioihin, tutkimukseen, osaamiseen ja investointeihin. Valtioneuvosto näkee Digitaalinen Eurooppa -ohjelman EU:n olennaisena sitoumuksena digitaalisen muutoksen tukemisessa. Etenkin panostukset strategisiin hankkeisiin, kuten tekoäly ja kyberturvallisuus sekä digitaalisiin tietoihin ja taitoihin tukevat EU:n kasvua ja kilpailukykyä. [32]

Valtioneuvosto katsoo, että Digitaalinen Eurooppa -ohjelma kytkeytyy Suomelle tärkeisiin tavoitteisiin, jotka koskevat digitalisaation ja tekoälyn laajaa soveltamista yrityksissä ja yhteiskunnassa sekä digitaalisten taitojen ja osaamisen kehittämistä. Ohjelman tulee hyödyttää laajalti kansalaisia, yrityksiä, julkista sektoria sekä muita relevantteja toimijoita. Erityisesti tulisi huolehtia pk- ja mikroyritysten mahdollisuuksista kehittää osaamistaan. Tärkeää on edistää kaiken kokoisten yritysten osallistumista sekä yritysten ekosysteemejä ja kasvuohjelmia, joissa yritysten lisäksi mukana ovat esimerkiksi yliopistot, tutkimusorganisaatiot ja kaupungit. Nämä voivat osaltaan edistää tärkeällä tavalla digitalisaation hyötyjen kanavoimista. [33]

Yhtenä ohjelman painopisteenä oleva kyberturvallisuus muodostaa keskeisen perustan digitalisoituvalle yhteiskunnalle ja yritysten digitaaliselle liiketoiminnalle. Teknologisen kehittämisen päämääränä tulee olla koko yhteiskunnan etu ja innovointi, jolla lisätään laadukkaita työpaikkoja ja parannetaan elinoloja. [34]

1.6 EU:n kyberturvallisuusalan huippuosaamisyksikkö

EU parantaa kykyään suojella Eurooppaa kyberuhkilta luomalla uuden rakenteen, joka tukee sen osaamista kyberturvallisuusalan tutkimuksen, teknologian ja teollisuuden kehittämisessä. Neuvoston pysyvien edustajien komitea antoi 13.3.2019 Romanialle valtuudet käynnistää Euroopan parlamentin kanssa neuvottelut kyberturvallisuusalan

[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.

huippuosaamisyksikön, eli teollisuus-, teknologia- ja tutkimusalan kyberturvallisuutta käsittelevän eurooppalainen osaamiskeskuksen perustamisesta sekä kansallisten koordinointikeskusten verkoston luomisesta. Nämä rakenteet yhdessä auttavat turvaamaan digitaaliset sisämarkkinat ja lisäämään EU:n riippumattomuutta kyberturvallisuusalalla.[35]

Muodostettava **Kyberturvallisuuden tutkimus- ja osaamiskeskus** edistää kyberturvallisuutta koskevan tutkimuksen ja innovoinnin koordinointia. Se on myös tärkein väline, jolla EU voi yhdistää investointejaan kyberturvallisuusalan tutkimuksen, teknologian ja teollisuuden kehittämiseen. Valmisteilla oleva asetus määrittelee keskuksen toiminta-ajaksi 1.1.2021-31.12.2029, jonka jälkeen toiminnan jatkosta on päätettävä erikseen. [36]

Osaamiskeskuksen tehtävinä olisi: [37]

- Hallinnoida kyberturvallisuuteen ohjelmakaudella 2021-2027 Digitaalinen Eurooppa ja Horisontti Eurooppa -ohjelmista kohdennettavia varoja,
- Toteuttaa näiden ohjelmien kyberturvallisuuteen liittyviä osia,
- Auttaa koordinoimaan jäsenvaltioiden kansallisista keskuksista muodostuvaa verkostoa ja laajempaa yhteisöä kyberturvallisuusteknologiaan liittyvän agendan toteutuksessa,
- Vauhdittaa EU:n, jäsenvaltioiden ja teollisuuden yhteisiä investointeja ja tuotteiden ja ratkaisujen käyttöönottoa.
- Vahvistaa kyberturvallisuuteen liittyviä kyvykkyyksiä, tietoa ja infrastruktuuria teollisuuden, julkisten toimijoiden ja tutkimusyhteisöjen tukena,
- Edistää huippuluokan osaamista edustavien kyberturvallisuustuotteiden ja -ratkaisujen laajamittaista käyttöönottoa Euroopan Unionissa,
- Tukea kyberturvallisuuteen liittyvien osaamiskuilujen vähentämistä EU:n alueella,
- Edistää kyberturvallisuuden tutkimusta ja kehitystä,
- Vahvistaa siviili- ja puolustusalan yhteistyötä kaksikäyttöteknologioiden ja niiden sovellusten aloilla, sekä
- Vahvistaa synergioita siviili- ja puolustusalojen kesken ja Euroopan puolustusrahastoon liittyen.

Kyberturvallisuuden osaamisverkosto muodostuu jäsenmaiden nimeämistä **kansallisista koordinointikeskuksista**. Kansallisilla keskuksilla on kyberturvallisuusalan tekninen asiantuntemus tai mahdollisuus hyödyntää sitä esimerkiksi salausjärjestelmiin, tietomurtojen jäljitykseen tai inhimillisiin tekijöihin liittyvien turvallisuusnäkökohtien yhteydessä. Kyberturvallisuuden alalla keskus toimii yhteistyössä verkoston kanssa Euroopan horisontti -ohjelmasta ja Digitaalinen Eurooppa -ohjelmasta myönnettävän rahoitus-

[35] Valtioneuvosto, U-kirjelmä, U1022018 vp, 10.1.2019
Eurooppa neuvosto, EU yhdistää ja verkostoi kyberturvallisuusosaamistaan, tiedote 13.3.2019
[36] Ibid.
[37] Ibid.

tuen täytäntöönpanomekanismina. Ne auttavat yhdessä parantamaan EU:n kyberturvallisuusalan teollisuuden kilpailukykyä ja tekemään kyberturvallisuudesta kilpailuedun EU:n muille teollisuudenaloille. [38]

Ehdotus sisältää myös kolmannen rakenteen **kyberturvallisuuden osaamisyhteisön** perustamisen. Sen tarkoituksena on lähentää tärkeimpiä sidosryhmiä kyberturvallisuusosaamisen kehittämiseksi ja levittämiseksi EU:ssa. Siinä ovat mukana teollisuus, korkeakoulut ja voittoa tavoittelemattomat tutkimusorganisaatiot, operatiivisten ja teknisten kysymysten parissa toimivat julkisyhteisöt sekä muiden kyberturvallisuushaasteita kohtaavien alojen toimijat. [39]

1.7 ENISA:sta EU:n Kyberturvallisuusvirasto

Euroopan unionin verkko- ja tietoturvavirasto (ENISA) on tietoverkkoturvallisuuden osaamiskeskus Euroopassa. ENISA osallistuu aktiivisesti verkko- ja tietoturvan korkean tason saavuttamiseen unionissa.

ENISA perustettiin Euroopan parlamentin ja neuvoston asetuksella vuonna 2004, tavoitteena osaltaan varmistaa korkeatasoinen ja tehokas verkko- ja tietoturva unionissa ja luoda verkko- ja tietoturvakulttuuri, josta on hyötyä kansalaisille, kuluttajille, yrityksille ja julkishallinnoille. ENISAn toimikautta on jatkettu ulottuen nyt 19. päivään kesäkuuta 2020. ENISA:sta kehitetään EU:lle pysyvä kyberturvallisuusvirasto[40].

EU:n kyberturvallisuusasetus on ollut ensimmäisessä käsittelyssä 12.3.2019. Asetusluonnos perusteluosa määrittelee ENISA asemaa kyberturvallisuusvirastona, kyberosaamiseen liittyviä tekijöitä, joita ENISA:n tulisi edistää sekä EU-tason kyberturvallisuussertifiointiin liittyviä tekijöitä.[41]

Asetusluonnoksen mukaan ”Jotta ENISA voisi tukea asianmukaisesti jäsenvaltioiden operatiivista yhteistyötä, sen olisi vahvistettava entisestään sen teknisiä ja henkilöstöön liittyviä valmiuksia ja taitoja. ENISAn olisi parannettava osaamistaan ja valmiuksiaan. ENISA ja jäsenvaltiot voisivat kehittää vapaaehtoisuuden pohjalta ohjelmia kansallisten asiantuntijoiden lähettämiseksi ENISAan asiantuntijapoolien perustamiseksi ja henkilöstön vaihtamiseksi.[42]

[38] Ibid.
[39] Ibid.
[40] EU komissio, Unionin tila 2017 – Kyberturvallisuus, Bryssel 19. syyskuuta 2017
[41] EU parlamentti, Lainsäädäntöpäätöslauselma ehdotuksesta asetukseksi EU:n kyberturvallisuusvirasto ENISAsta, ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”), Bryssel, 12.3.2019
[42] Ibid.

”ENISAn olisi myös osallistuttava koulutusta ja koulutusmateriaalia koskevien tarpeiden kattamiseen, myös julkisten elinten tarpeiden osalta, ja tarvittaessa suuressa määrin ’koulutettava kouluttajia’ kansalaisille tarkoitetun eurooppalaisen digitaalisten taitojen puitekehyksen pohjalta, jotta jäsenvaltioita sekä unionin toimielimiä, elimiä ja laitoksia voidaan auttaa kehittämään omia koulutusvalmiuksiaan.” [43]

Lisäksi ”ENISAn olisi tuettava jäsenvaltioita kyberturvallisuutta koskevan tietoisuuden lisäämisen ja koulutuksen alalla helpottamalla tiiviimpää yhteistyötä ja parhaiden käytäntöjen vaihtoa jäsenvaltioiden välillä. Tällaiseen tukeen voisi kuulua muun muassa kansallisten **koulutusalan yhteyspisteiden verkoston ja kyberturvallisuuden koulutusfoorumin kehittäminen**. Kansallisten koulutusalan yhteyspisteiden verkosto voisi toimia kansallisten yhteyshenkilöiden verkostossa ja olla tulevan jäsenvaltioiden sisäisen koordinoinnin käynnistäjä.” [44]

[43] Ibid.
[44] Ibid.

2 KYBERTURVALLISUUSKOULUTUKSEN KEHITTÄMINEN

2.1 Kyberturvallisuuskoulutuksen tavoitteita

Kyberosaamisessa voidaan erottaa kaksi kokonaisuutta: kyberturvallisuus ammattina ja kyberturvallisuus taitona. Kyberturvallisuus ammattina kuvaa osaamista alan ammattilaisten kyvykkyytenä ja kyberturvallisuus taitona kuvaa kyvykkyyttä, jota tarvitaan erilaisissa työtehtävissä. Kyberturvallisuuden osaaminen ei ole vain erillinen ammatillinen osaamisalue vaan se kattaa kyvykkyyksiä kansalaistaidoista aina kansainvälisen tason professioon saakka. Tämän vuoksi kyberturvallisuuskoulutus tulee sisällyttää eri koulutusasteisiin (ks. kuvio 3).

1. Yleissivistävässä perusopetuksessa koulutuksella tulee varmistaa, että nuorilla on riittävät taidot toimia digitaalisessa toimintaympäristössä ja että he ymmärtävät kyberturvallisuusuhat ja osaavat suojautua niiltä. Lisäksi heille tulee antaa medialukutaidon perusteet ja ymmärrys informaatiovaikuttamisesta.

2. Lukiokoulutuksessa ja ammatillisessa koulutuksessa syvennetään em. taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa. Ammatilliseen koulutukseen voidaan sisällyttää kyberturvallisuuden alan perusammattitaitoon ja työelämässä tarvittavaan alan ammatilliseen pätevyyteen johtavaa koulutusta. Lisäksi ammatillisessa koulutuksessa turvallisen digitaalisen osaamisen pitää olla integroituna kaikkeen opiskeluun opiskeltavasta ammatista riippumatta.

3. Yliopistoissa tulee voida suorittaa kyberturvallisuuden alalta alempia ja ylempiä korkeakoulututkintoja sekä tieteellisiä jatkotutkintoja. Lisäksi tulisi tarjota aiheeseen liittyviä kursseja ja opintokokonaisuuksia kaikille opiskelijoille.

4. Ammattikorkeakouluissa tulee voida suorittaa kyberturvallisuusalalta sekä ammattikorkeakoulututkinto että ylempi ammattikorkeakoulututkinto. Kaikkeen korkeakouluopetukseen tulee liittää digitaalisten taitojen ja kyberturvallisuuden perusteet.

5. Aikuiskoulutukseen kyberturvallisuus tulee sisällyttää sen kiinteäksi osaksi. Kyberturvallisuuden aikuiskoulutus voi olla perustutkinto-opetusta, tutkintoon kuuluvia opintoja, näyttötutkintoihin valmentavaa koulutusta, oppisopimuskoulutusta, ammattitaitoa uudistavaa ja laajentavaa lisä- ja täydennyskoulutusta (muuntokoulutus) 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.

6. Kansanlaiskasvatus. Oppilaitosten ja yleissivistävän koulutuksen lisäksi kaikille kansalaisille on tarjottava avoin oppimisympäristö, jossa kyberturvallisuuden perusteita ja digitaitoja on mahdollisuus opiskella ilman oppilaitokseen kirjoittautumista. Tällainen oppimisympäristö tarjoaa myös mahdollisuuden ajan tasalla olevan tiedon saatavuuteen.

Kyberturvallisuuden koulutuksen yleisiä tavoitteita:

- Suomen koulutusjärjestelmään tukeutuva koko oppimispolun kattava kyberturvallisuuden opetusmalli mahdollistaa osaamisen tehokkaan kehittämisen ja koulutusviennin.
- Osaamisen ja jatkuvan oppimisen tavoitteena on rakentaa Suomesta digitaalisen luottamuksen mallimaa, jossa kyberturvallisuuden kokonaisnäkemys omaksutaan jo nuorena ja sen kehittymistä tuetaan jatkuvalla oppimisella läpi elämän.
- Osaamisen tason kasvaessa Suomessa julkisella sektorilla, yritysmaailmassa ja kansalaisten asenteissa saadaan aikaan merkittävä positiivinen kyberkulttuurin muutos.
- Laajasti koko korkeakoulusektorilla toteutettu kyberturvallisuuskoulutus tuottaa yhteiskunnan eri sektoreille alan huippuosaajia, joiden tiedot ja taidot vastaavat eri tehtäviin sisältyviä osaamisvaatimuksia.
- Digiyhteiskunnan tarpeisiin tulee kouluttaa laajan kyberosaamisen huippuammattilaisia, mikä mahdollistaa kansallisen kyberomavaraisuuden kehittymisen.
- Kyberturvallisuus tulee nähdä investointina tulevaisuuteen, yhteiskunnan kriittisen infrastruktuurin perustana ja keskeisenä liiketoiminnan varmistajana.

KUVIO 3 Kyberturvallisuusosaaminen ja -kyvykkyys kattavat koko koulutusalan

2.2 Kyberturvallisuuskoulutuksen suunnittelu

Tehokkaan kyberturvallisuuskoulutuksen perustana tulee olla laaja ymmärrys siitä, mitä halutaan kouluttaa (ts. mihin tehtäviin) ja millaiselle koulutettavalle. Koulutuksen kohdentamiseksi tulisi selvittää, mitkä ovat sellaiset kyberturvallisuusuhat, joiden ymmärtäminen auttaa suojautumaan ja ehkäisemään niitä tietyllä toimialalla. Järjestelmien ja koulutuksen näkökulmasta tärkeintä on kohteen alan mukaan realististen uhkien simuloiminen. Erilaisten uhkien simuloinnin lisäksi tulee myös pyrkiä yhdistämään teoriaa, käytäntöä sekä tietoa siitä, kuinka kehitystä ja suoriutumista voidaan mitata, jotta koulutus olisi riittävän laaja-alainen. Kyberkoulutusta suunnitellessa on tärkeää löytää soveltuvat tekniset opetuslaiteympäristöt ja -alustat sekä digitaaliset oppimisympäristöt, sekä pyrkiä valitsemaan ne niin koulutuksen tarkoituksen kuin koulutettavien henkilökohtaisten ominaisuuksien mukaisesti.[45]

2.2.1 Interaktiivisten pelien mahdollisuuksia

Kyberkoulutuksen keskeisessä roolissa ovat erilaiset järjestelmät ja digitaaliset oppimisympäristöt, sillä kybermaailman ilmiöitä on luonnollista tarkastella erilaisia kybermaailman keskeisiä teknologioita hyödyttäen. Sopivaa järjestelmää koulutusta varten valittaessa tulee ottaa huomioon useita eri tekijöitä, joiden avulla arvioidaan kunkin järjestelmän soveltuvuutta kyseisen koulutettavan osa-alueen simuloimiseksi. Järjestelmän ominaisuuksia onnistuneeseen kyberturvallisuuskoulutukseen ovat etenkin järjestelmän toimintojen ja logiikan yhteneväisyys todellisen maailman kyberilmiöihin, interaktiivisuus, pitkällä aikavälillä suoritettavat toimintokokonaisuudet, toimintokokonaisuuksien monipuoliset ratkaisumahdollisuudet ja koulutettavan oman suoriutumisen tarkastelun mahdollistaminen. Järjestelmän yhteneväisyys todellisen maailman kyberuhkien kanssa mahdollistaa koulutettavalle johdonmukaisen ymmärryksen kybertilanteiden etenemisestä, vaikka koulutusjärjestelmässä käytetään simuloitua peliä, eikä todellista hyökkäystä. Järjestelmän interaktiivisuus tarkoittaa käyttäjän kanssa vuorovaikuttavia pelejä, jotka mahdollistavat motivoivan koulutuksen sekä realistisen virtuaalisen toimintaympäristön. Uhkien simuloiminen kohteen kontekstin mukaan mm. interaktiivisten pelien avulla auttaa koulutettavaa hahmottamaan oman toimialan realistisimmat uhat ja kuinka ne vaikuttavat toteutuessaan.[46]

Interaktiiviset pelit tarjoavat koulutettavalle mahdollisuuden vuorovaikutuksellisesti ratkaista kohdatun ongelman, josta oikea ratkaisu palkitaan esimerkiksi pisteyttämällä suoritus. Interaktiivisuus voi myös tarkoittaa muun muassa resurssienhallinnan simulointia, jossa tarkoituksena on annetuilla resursseilla pyrkiä ratkaisemaan tietty ongelma, esimerkiksi torjua hyökkäys tietyssä ajassa tietyin työkaluin. Järjestelmän interaktiivisuuden yhtenä tärkeimpänä ominaisuutena voidaan pitää koulutettavan motivointia,

[45] Laukkarinen Emmi, Kokonaisvaltaisen kyberturvallisuuskoulutuksen suunnittelussa huomioitavia tekijöitä, julkaisematon ITKST41-kurssiraportti, 2019
[46] Ibid.

joka perustuu esimerkiksi koulutettavan ratkaisujen pisteytykseen tai oman koulutustason asteikolliseen arviointiin. [47]

Interaktiiviset pelit voidaan jakaa seitsemään eri kategoriaan, jotka ovat action-, rooli-, seikkailu-, strategia-, urheilu-, sota-, sekä niin sanotut sandbox-pelit. Moderniin kyberkoulutukseen suositellaan vuorovaikutuksellisuutta ja automatisoitua harjoitusympäristöä, joiden avulla pystytään jäljittelemään tehokkaasti hyökkäysten suorittamista ja vastaanottamista. Tämän takia useat alan tutkimukset suosittelevat koulutuksen tekniseen osa-alueen oppimisympäristöksi erilaisia pelejä. Sen lisäksi, että pelit mahdollistavat tilanteiden teknisen simulaation, ne myös saavat koulutettavassa aikaan luonnollisia reaktioita, ja pakottavat koulutettavan toimimaan parhaan osaamisensa mukaan tilanteiden ratkaisemiseksi. [48]

Action-pelejä suositellaan ennen kaikkea hyökkäysten torjunnan kouluttamisessa ja harjoittelussa. Niissä koulutettava on tapahtumien keskiössä ja vastaa täysin omien toimiensa mukaan tilanteiden edistymisestä. **Rooli- ja seikkailupelit** sisältävät erilaisia ratkaisumahdollisuuksia ja ratkaisuista seuraavia jatkotilanteita. Ne keskittyvät etenkin ongelmanratkaisuun, kuten hyökkäyksen jälkeisten palauttamistoimintojen kouluttamiseen. **Strategiapelit** on suunniteltu etenkin kahden tai useamman joukkueen välisten harjoitusten kouluttamista varten, joissa toinen joukkue hyökkää ja toinen puolustaa. **Urheilupelit** ovat pääasiassa tarkoitettu stressinhallinnan ja paineensietokyvyn kehittämiseen, ja niiden konteksti ei ole suoraan liitetty kybermaailmaan. Urheilupelien kautta voidaan pyrkiä kehittämään koulutettavan henkisiä ominaisuuksia. **Sotapelit** simuloivat suoraan esimerkiksi kybersodankäynnin tilanteita, joissa sekä tehdään erilaisia kyberhyökkäyksiä että puolustaudutaan niiltä. Tämän kaltaiset pelit sisältävät niin strategian kuin sodankäynnin toimintojen simuloimista. **Sandbox-peleissä** koulutettava osallistuu tapahtumiin ohjailevana osapuolena, mutta ei varsinaisesti osallistu pelin tapahtumiin. Tällaisia pelejä voidaan hyödyntää etenkin kybersodankäynnin eri operaatioiden toteuttamisen näkökulmasta, esimerkiksi vaikutusten havainnoinnissa tilanteissa, joissa järjestelmään asennetaan haittaohjelma ja tämän jälkeen seurataan tilanteen vaikutuksia kokonaisuudessaan. [49]

Tärkeintä sopivaa järjestelmää tai koulutusmenetelmää valittaessa on pyrkiä ottamaan huomioon järjestelmän logiikan yhteneväisyys todellisen kybermaailman ja sen ilmiöiden kanssa, järjestelmän vuorovaikutuksellisuus, koulutettavan ratkaisujen soveltamismahdollisuus sekä oman suoriutumisen reflektointi järjestelmän palautteen kautta. Järjestelmän tulee siis olla kuhunkin koulutustarkoitukseen teknisesti sopiva, mutta hyvältä järjestelmältä odotetaan myös interaktiivisuutta ja mahdollisuuksia tunnistaa erilaisia tapoja toimia ongelman ratkaisemiseksi.[50]

---

[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] Laukkarinen Emmi, Kokonaisvaltaisen kyberturvallisuuskoulutuksen suunnittelussa huomioitavia tekijöitä, julkaisematon ITKST41-kurssiraportti, 2019
Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. In 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, ss. 256-262

2.2.2 Psykologinen näkökulma koulutuksen suunnitteluun

Onnistuneen kyberkoulutuksen teknisen osa-alueen lisäksi tulisi kiinnittää huomiota myös psykologisiin tekijöihin etenkin koulutettavien toiminnan taustalla, sillä kyse on ihmisen ja teknologian välisen vuorovaikutuksen kouluttamisesta. Psykologinen ymmärrys auttaa hallitsemaan kokonaisuuksia järjestelmien kehittämistä ja käyttämistä kohtaan, mutta se myös toisaalta mahdollistaa järjestelmien ja niiden eri ilmiöiden aiheuttamien kognitiivisten seurausten tarkastelun laajemmin. Psykologinen näkökulma auttaa erilaisten kyberuhkien tunnistamisessa ja ymmärtämisessä, sillä on merkittävää tietää, kuinka ihmiset pyrkivät tunnistamaan ja ratkomaan havaitsemiaan ongelmia. Lisäksi psykologian avulla voidaan muun muassa rakentaa ymmärrystä ihmisen luottamuksen saavuttamisesta esimerkiksi phishing-hyökkäystilanteissa, tai pyrkiä ymmärtämään, miksi hyökkäävä osapuoli on päättänyt hyökätä juuri tiettyä järjestelmää tai yritystä kohtaan. Kyberkoulutuksen kokonaisuuden kannalta on myös hyvä katsoa taustoja teknisten ilmiöiden taustalla ja pyrkiä luomaan kognitiivista kokonaiskuvaa järjestelmän ja sen käyttäjän välisestä suhteesta.[51]

Psykologisten ilmiöiden merkitystä tulisi hyödyntää niin koulutettavien toiminnan tarkastelussa kuin kybermaailman eri toimijoiden ja osapuolten välisessä vuorovaikutuksessa. Taylor ym. (2017) mukaan psykologinen näkemys ja tietämys tulisi linkittää yhteen teknisen koulutuksen kanssa, jotta kyberkoulutuksessa säilyisi kuitenkin sen teknisesti ammatillinen konteksti. Sosiaalipsykologia tarjoaa näkökulmia teknologian vaikuttamiseen sosiaalisessa kanssakäymisessä, asenteissa sekä käyttäytymisessä. Sosiaalipsykologian tuntemuksen avulla voidaan esimerkiksi tarkastella koulutettavien ryhmädynamiikkaa joukkueena toimiessa, sekä tunteiden roolia ja vaikutusta järjestelmää käytettäessä, esimerkiksi kyberhyökkäystilanteessa. Koulutettavien toimintaa tarkastelemalla voidaan saada tärkeää informaatiota siitä, kuinka esimerkiksi ryhmässä toimimista tulisi kehittää, jotta teknisellä tasolla toimiminen olisi tehokkaampaa, tai kuinka päätöksenteko paineen alla vaikuttaa koulutettavan suoriutumiseen tehtävästä. Koulutuksen suunnittelun näkökulmasta sosiaalipsykologian tuntemusta voi hyödyntää etenkin koulutettavien työskentelyn tarkastelemisessa, ja havaintojen pohjalta voidaan esimerkiksi kehittää negatiivisten tunteiden hallintaa paineen alla toimiessa. Koulutettavien yksilöllisten erojen tarkastelemiseksi on myös tärkeää ottaa psykologiset tekijät huomioon. Esimerkiksi koulutettavan ikä ja persoonallisuus voivat vaikuttaa suoriutumiseen tietynlaisissa tehtävissä. Lisäksi koulutettavien kyky sietää stressiä on merkittävässä roolissa havainnoinnissa ja sitä kautta tehdyissä päätöksissä. On siis hyödyllistä luoda yleiskuva koulutettavista yksilöinä, jotta heidän käyttäytymistänsä ja valitsemiansa ratkaisuja esimerkiksi stressaavassa kyberhyökkäystilanteessa voidaan arvioida. Koulutusta suunniteltaessa olisikin erityisen tärkeää aloittaa suunnittelu perehtymällä koulutettavien taustoihin, jotta voidaan luoda kattava kuva siitä, millaiselle joukolle koulutusta ollaan järjestämässä. Koulutettavien ominaisuudet ja esimerkiksi toimiala vaikuttavat merkittäväsi myös koulutukseen sopivan järjestelmän valinnassa.[52]

[51] Laukkarinen Emmi, Kokonaisvaltaisen kyberturvallisuuskoulutuksen suunnittelussa huomioitavia tekijöitä, julkaisematon ITKST41-kurssiraportti, 2019

[52] Laukkarinen Emmi, Kokonaisvaltaisen kyberturvallisuuskoulutuksen suunnittelussa huomioitavia tekijöitä, julkaisematon ITKST41-kurssiraportti, 2019

Psykologia antaa myös näkökulmia kyberkoulutuksen ja kybermaailman ilmiöiden eettiseen puoleen. Pelkän teknisen ja järjestelmiin perustuvan osaamisen lisäksi koulutettavien tulee ymmärtää alan eettisiä näkökulmia ja ongelmia. Etiikan näkökulmasta voidaan tarkastella etenkin informaatioteknologian turvallisuutta ja siihen liittyviä teemoja, kuten yksityisyyttä, tiedon omistussuhteita sekä sen läpinäkyvyyttä ja avoimuutta, ja esimerkiksi vastuuta ja luotettavuutta tiedon keräämisen ja säilyttämisen osalta. Kattavassa kyberkoulutuksessa olisi siis tärkeää nostaa esille myös alalla esiintyviä eettisiä ongelmia ja niiden vaikutusta yksilöihin sekä yhteiskuntaan. Kattavan kyberkoulutuksen teknisten osa-alueiden hallitsemisen lisäksi koulutuksen suunnittelussa tulee ottaa huomioon, kuinka koulutettavan huomio saadaan säilytettyä olennaisissa asioissa, ja kuinka koulutettava saadaan sisäistämään koulutuksen sisältö halutulla laajuudella koulutettavan henkilökohtaisten ominaisuuksien sallimissa rajoissa. Psykologinen ymmärrys koulutuksen suunnittelun taustalla mahdollistaa osallistavan oppimisen järjestämisen, sekä myös mahdollisuuden arvioida koulutettavien tiedon omaksumista ja erilaisissa päätöksentekotilanteissa toimimista.[53]

2.3 Kyberturvallisuuden osaamisvaje kansainvälisesti

(ISC)² julkisti 17.10.2018 viimeisimmän kyberturvallisuuden työvoimatutkimuksensa tuloksia. Tutkimus osoittaa maailmanlaajuisen kyberturvallisuuden työvoimavajeen kasvavan lähes kolmeen miljoonaan Pohjois-Amerikassa, Latinalaisessa Amerikassa, Aasian ja Tyynenmeren alueella (APAC) ja Euroopassa, Lähi-idässä ja Afrikassa (EMEA). Tutkimus perustuu vajaan 1500:n kyberturvallisuusammattilaisen haastatteluun eri puolilla maailmaa. Näiden henkilöiden tehtävät kuvaavat kattavasti teollisuuden kyberturvallisuuden osaamista sekä suurissa että pienissä yrityksissä.[54]

Tutkimuksessa esille tulleet keskeiset havainnot ovat:[55]

- Kyberturvallisuuden työvoimatarve on tällä hetkellä noin 2,93 miljoonaa.
- Aasian ja Tyynenmeren alueilla on suurin osaamistarve: 2,14 miljoonaa, mikä johtuu ainakin osittain alueen kasvavista talouksista ja uudesta kyberturvallisuus- ja tietosuojalainsäädännöstä koko alueella.
- Pohjois-Amerikassa työvoimatarve on 498 000, kun taas EMEA ja Latinalaisen Amerikan osuus on 142 000 ja 136 000 henkilöä.
- 63 % vastaajista kertoo, että heidän organisaationsa on pulaa tietoturvaan liittyvästä tietoteknisestä henkilöstöstä.

Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., & Dale, J. (2017). Teaching psychological principles to cybersecurity students. In 2017 IEEE Global Engineering Education Conference (EDUCON), pp. 1782-1789

[53] Ibid.

[54] (ISC)², Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens Cybersecurity Workforce Study, October 17, 2018, www.isc2.org/research

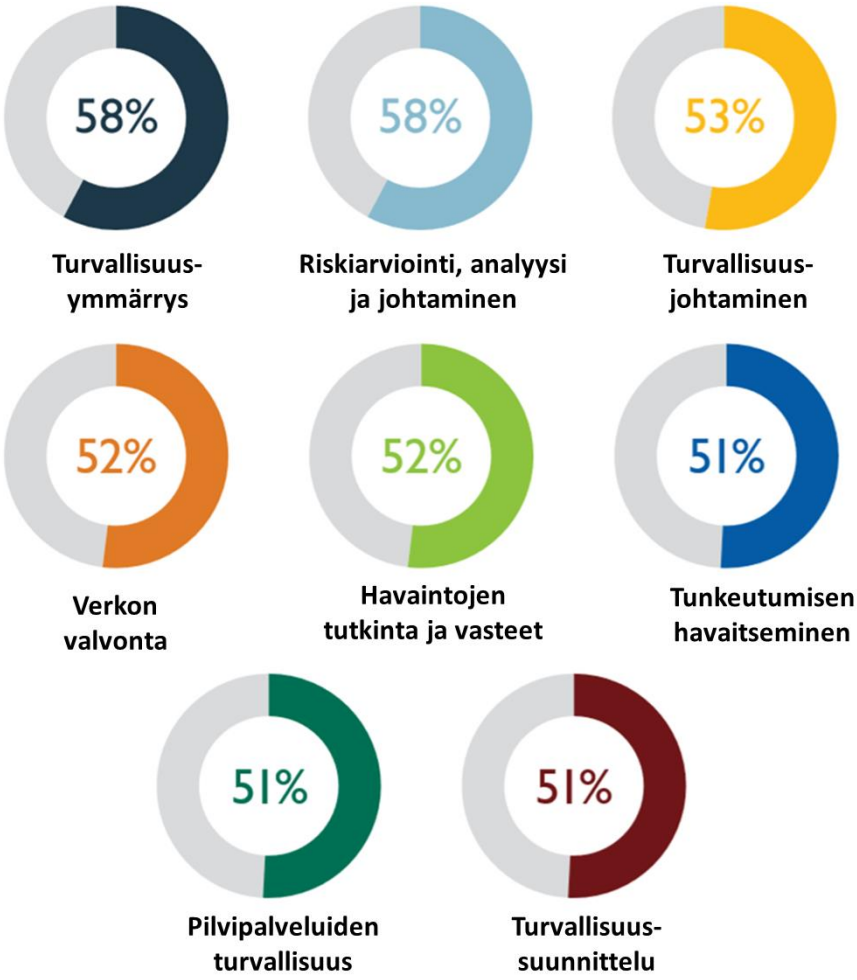
[55] Ibid.

- 59 % sanoo, että heidän yrityksensä ovat kohtalaisen tai hyvin suuressa vaarassa kyberturvallisuushyökkäyksistä tämän puutteen vuoksi.
- 48 % vastaajista sanoo, että heidän organisaationsa aikovat lisätä kyberturvallisuuden henkilöstöä seuraavien 12 kuukauden aikana.
- 68 % vastaajista sanoo olevansa hyvin tai jonkin verran tyytyväinen nykyiseen työhönsä.
- Yli puolet kaikista vastaajista (54 %) käyttää hyväkseen henkilön osaamista kuvaavia kyberturvallisuuden sertifikaatteja tai suunnittelee niiden käyttöä seuraavana vuonna.
- Suurimpia urakehityshaasteita, joista vastaajat raportoivat, ovat:
    - Epäselvät uramahdollisuudet (34 %)
    - Organisaation tietämyksen puute kyberturvallisuusosaamisestaan (32 %)
    - Koulutuksen kustannukset kyberturvallisuuden uralle valmistautumiseksi (28 %)
- Kyberturvallisuusosaajien mielestä heidän on kehitettävä eniten tai parannettava osaamistaan seuraavien kahden vuoden aikana seuraavilla neljällä osa-alueella, jotta he voivat edetä urallaan:
    - Pilvipalveluiden turvallisuus (Cloud computing security)
    - Tunkeutumistestaus (Penetration testing)
    - Uhka-analyysi (Threat intelligence analysis)
    - Forensiikka (Forensics)

Mihin koulutuksen tulisi siis keskittyä? Tutkimuksessa nousi esiin kahdeksan aluetta, joita yli puolet kyberturvallisuuden ammattilaisista pitää kriittisinä osaamistekijöinä kilpailukyvyn kannalta alallaan. Näihin kuuluvat turvallisuusymmärrys, riskiarviointi, turvallisuusjohtaminen, verkon valvonta, vaaratilanteiden tutkinta ja reagointi, tunkeutumisen havaitseminen, pilvipalveluiden turvallisuus ja turvallisuussuunnittelu. [56]

Kuviossa 4 on esitetty tärkeimmät vaadittavat kyberturvallisuuden osaamisalueet (%-osuus, jotka pitivät näitä osaamisalueita kriittisinä: [57]

[56] Ibid.
[57] Ibid.



KUVIO 4 Tärkeimmät vaadittavat kyberturvallisuuden osaamisalueet

Palkatessaan kyberturvallisuushenkilöstöä yritykset pyrkivät löytämään osaajia laajalta eri osaamisen sektoreilta. Relevantti työkokemus, tietämys edistyksellistä kyberturvallisuusratkaisuista ja kyberturvallisuusosaamista kuvaavat sertifikaatit ovat kolme tärkeintä. Yllätyksenä voidaan pitää sitä, että kyberturvallisuuteen liittyvät alempi ja ylempi tutkinto ovat kovin vähän merkittäviä palkkaamisen kannalta. Kuitenkin tutkimuksen mukaan kyberturvallisuushenkilöstö on hyvin koulutettua. Tutkimukseen osallistuneista ylempi korkeakoulututkinto oli 34 %:lla ja alempi korkeakoulututkinto 39 %:lla.[58]

Alan työntekijät saavat työpaikoilla työkokemusta, jolloin organisaatiot voivat keskittyä täyttämään osaamisvajetta tarjoamalla lisää koulutusmahdollisuuksia ja keskittymällä koulutuksessa kaikkein tarpeellisimpien taitojen kouluttamiseen. Kuviossa 5 on esitetty tärkeimmät työllistymiseen edellytettävät vaatimukset kyberturvallisuusalan tehtävissä:[59]

[58] Ibid.
[59] Ibid.

KUVIO 5 Tärkeimmät työllistymiseen vaadittavat osaamisvaatimukset ja muodolliset pätevyysvaatimukset

2.4 Kyberturvallisuuden osaamisvaje kansallisesti

2.4.1 Kyberkoulutuksen tarjonta ja kehittäminen

Jukka Niemelä tarkastelee pro gradu -työssään ”Kyberturvallisuuden työvoiman tarve, saatavuus ja kehittäminen vastaamaan alan tarvetta Suomessa” myös kyberkoulutuksen kehittämistä. [60]

[60] Niemelä Jukka, Kyberturvallisuuden työvoiman tarve, saatavuus ja kehittäminen vastaamaan alan tarvetta Suomessa, pro gradutyö, Jyväskylän yliopisto, IT-tiedekunta, 2019

Tutkimuksessa tehdyn koulutuskartoituksen kautta pyydettiin korkeakouluja antamaan tilannekuva heidän nykyisestä ja tulevasta kyberalan koulutuksesta. Sen lisäksi korkeakouluilta kysyttiin mielipidettä koulutuksen soveltuvuuteen työmarkkinoiden näkökulmasta. Kyselyssä esitettiin seuraavat kysymykset: [61]

1. Mihin suuntaan kyberalan opetus teidän oppilaitoksessanne on kehittymässä?
    a. Oppilasmäärät
    b. Opetustarjonta
    c. Erikoistuminen tiettyyn kyberturvallisuuden osa-alueeseen tai sen linkittäminen toiseen alaan
2. Tulisiko kyberalan opetusta Suomen mittakaavassa keskittää tai jakaa ohjatusti?
3. Miten hyvin kyberturvallisuuden koulutus mielestänne valmistaa oppilaita työmarkkinoiden tarpeisiin?

Kyselyn perusteella oppilasmäärät ovat pääsääntöisesti vakiintuneet tietylle tasolle. Aalto yliopisto, Helsingin yliopisto sekä Centria Ammattikorkeakoulu pyrkivät kasvattamaan sisään otettavien ja valmistuvien oppilaiden määriä. Turun yliopisto koki tarvetta kasvattaa kryptografiaan suuntautuvien oppilaiden määrää.[62]

Kyberopetuksen opetustarjonta laajenee oppilaitosten vastausten perusteella alan kehityksen ja tarpeen mukaan. Yleisesti suuntaus on laajentaa opetusta muiden koulutusalojen kanssa tai suunnata koulutusta kunkin korkeakoulun omille vahvuusalueille. Kyberala tulee kiinteäksi osaksi muuta IT-alan koulutusta sekä entistä vahvemmin sivuaineena muiden alojen opiskelijoille. Verkkokurssien määrä todennäköisesti tulee entisestään lisääntymään ja esimerkiksi Helsingin yliopiston kaikille avoimet verkkokurssit ovat olleet hyvin suosittuja.[63]

Kyberalan opetuksen keskittäminen tietyille osa-alueille ei ole laajasti suunnitelmissa. Osa oppilaitoksista tarjoaa kyber- tai tietoturva-alan opetusta perustasolla kaikille opiskelijoille. Kyberalaan voimakkaasti keskittyneet oppilaitokset pyrkivät tarjoamaan mahdollisimman laajan kirjon alan opetusta. Osa oppilaitoksista omaa vahvaa osaamista tietyiltä osa-alueilta ja se näkyy erikoistumisena. Näistä esimerkkeinä Turun yliopiston kryptografia, Jyväskylän yliopiston laajeneva tiedusteluopetus sekä Aalto yliopiston hallinnollinen tietoturva sekä alkava liiketoimintaosaamiseen liittyvä yhteistyö Kauppakorkeakoulun kanssa.[64]

Kyberalan keskitettyyn ohjaukseen Suomessa oppilaitokset suhtautuvat pääosin kielteisesti. Siitä huolimatta vastaukset osoittavat, että osaamiskeskittymiä on jo muodostunut ja kilpailu Suomen kokoisessa markkinassa ei kuitenkaan ole mielekästä. Yhteistyö ja yhteinen koordinointi toistui vastauksissa. Yhteistyön kautta oppilaitokset voivat yhdistää vahvuuksiaan ja siten luoda uusia innovaatioita ja tutkimusideoita poikkitieteelli-

[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Ibid.

sesti. Osaamisen keskittyminen nähdään myös vahvuutena, jolla voidaan luoda parempaa opetusta ja korkeatasoisempaa tutkimusta. Vastauksissa näkyy kolme suuntausta: [65]

1. Kyber on kaikkialla, joten opetusta tarvitaan kaikkialla.
2. Keskittäminen koetaan uhkaksi omalle toiminnalle, erityisesti, jos oma kyberopetuksen suunta ja asema ei ole vielä vakiintunut.
3. Keskittäminen koetaan vahvuutena, jolloin isommissa yksiköissä saadaan tehtyä laadukkaampaa tutkimusta. Suuntaus korreloi oppilaitoksen tämän hetken asemaa kyberalan koulutuksen järjestäjänä. Vakiintuneet toimijat ovat myönteisempiä keskittämiselle. Kyberalan suuntaa hakevat oppilaitokset ja uudet kyberopetusta tarjoavat tulokkaat suhtautuvat kielteisemmin keskittämiseen.

2.4.2 Kyberosaajien työmarkkinatilanne Suomessa

Oppilaitosten mielestä koulutus vastaa hyvin työmarkkinoiden tarpeita. Tästä todisteena oppilaitokset käyttävät yrityksistä saatua palautetta sekä valmistuneiden tai kesken opintojen työllistyneiden oppilaiden tilastoja. Oppilaitokset näkevät kuitenkin haasteena nopeasti muuttuvan ympäristön, johon on vaikea reagoida. Kyberala ja tekniikka kehittyy, joten muutoksen perässä on vaikea pysyä. Samalla tulisi pystyä tarjoamaan uusien ja nousevien tekniikoiden koulutusta, jota työnantajat toivovat. Opetuksen tulee olla joustavaa ja mukautua ajan myötä. Tutkimuksen ja kehityksen tulee suuntautua enenevissä määrin nouseviin trendeihin. Muina laadullisina huomioina nousivat esiin oppilaitoksien liian pienet resurssit ja koulutusmäärä. Samoin täydennyskoulutuksen tarve. [66]

Vaikka opiskelijat työllistyvät hyvin, on koulutuksen vastaavuus silti laitettava tarkempaan tarkasteluun. Työmarkkinoilla on suuri pula alan osaajista ja koulutusta on ollut suhteellisen vähän aikaa tarjolla, joten työmarkkinat eivät ole kylläisiä. Tästä osoituksena voi ottaa esimerkiksi kesken opiskelun töihin siirtyvien määrän. Työnantajat ottavat sen minkä saavat, jopa kesken koulutuksen varmistaakseen edes tyydyttävän osaamistason rekrytointitilanteessa. Koulutuksen ei siis tule tyytyä nykytilanteeseen vaan jatkuvasti pyrkiä mukautumaan ja kehittämään toimintaansa. Koulutuksen tasoa ja onnistumista tulisi työllistymisen sijaan mitata entistä enemmän työnantajapalautteista sekä käydä avointa keskustelua työnantajien kanssa. [67]

Yritysten näkemyksen mukaan tämän hetken tarpeen perusteella koulutusta pitäisi muuttaa seuraavasti: [68]

- Vahvistaa tekniikan perusosaamista ja ymmärrystä.
- Syventää käytännön osaamista.

[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Ibid.

- Kehittää IoT laitteiden tietoturvan koulutusta ja laitteiden penetraatiotestausta.
- Oppilaitosten tulisi olla trendien edelläkävijöitä, joiden kautta saadaan uutta osaamista.
- Pitäisi tehdä enemmän yhteistyötä mm. tarjota lopputöiden aiheita sekä pitää luentoja ja opetusta oppilaitoksissa.
- Lopputöiden tulisi olla laadukkaita ja tehty tarpeeseen/toimeksiannosta.
- Tietoturvan perusteita tulisi kouluttaa aktiivisesti, jonka kautta tulisi kiinnostus ja riittävä osaaminen/uskallus lähteä opiskelemaan lisää.
- Opetetaan muitakin kuin teknisiä taitoja, kuten liiketoiminnan ymmärrystä.
- Pääosin ohjelmistokehitys ongelmana, kuten turvallinen ohjelmointi.
- Virtualisointi, Linux -osaaminen ja tietoturva ovat osaamiskapeekoita.
- Verkostoituminen esim. YAMK koulutuksen kautta.

2.4.3 Kyberammattilaisen osaamisprofiili

Niemelän tutkimuksen mukaan kyberalan työntekijän profiili muodostuu seuraavista ominaisuuksista: [69]

- Tiedot: *matemaattisesti kyvykäs ja kielitaitoinen, ymmärtää liiketoiminnan vaatimukset, pystyy osoittamaan tiedonlähteen (koulutus, sertifikaatit, työhistoria)*
- Taidot: *ohjelmointitaitoinen sekä osaa tietojärjestelmien ja -verkkojen hallinnan sekä suojaamisen, valmis kouluttautumaan*
- Kyvyt: *oma-aloitteinen ja vuorovaikutustaitoinen*
- Muut persoonallisuustekijät: *motivoitunut sekä omaa analyyttisen ja systemaattisen ajattelutavan*

Toisin sanoen yritykset etsivät ”hyvää tyyppiä”, jolla on kyky omaksua uutta tietoa.

Koulutuksen kehittämiseen liittyvä palaute yrityksiltä tuo ilmi laadullisen puutteen; koulu ei valmista suoraan työelämään. Tämä yritysten kokema kuilu johtaa määrälliseen puutteeseen, koska osalta hakijoista puuttuu oleellisia kykyjä. Haastateltavat arvioivat koulutuksen vastaavan odotuksia melko hyvin (ka 3,0) asteikolla 1-5 (1 Erittäin huonosti - 2 Huonosti - 3 Melko hyvin - 4 Hyvin - 5 Erittäin hyvin). Vastaukset jakaantuivat tasaisesti 2-4 välille. Sen sijaan perustelut erosivat vastaajien kesken merkittävästi. Yhdessä ääripäässä todettiin, että soveltuvaa koulutusta ei Suomessa ole lainkaan, keskikastissa koettiin puutteita matemaattisten taitojen opetuksessa sekä koulutuksen hitaudessa tarpeeseen nähden ja toisessa ääripäässä koulutuksen tason koettiin olevan hyvä, mutta määrällisesti osaavia henkilöitä valmistuu liian vähän. Myös koulutuksen tason osalta haastateltavat olivat laskeneet odotuksia. Opiskelun jälkeen tulisi päästä työelämään kasvamaan kohti huippuasiantuntijuutta ja kouluttautua eteenpäin. Työnantajien tarve on voimakkaammin korkean asiantuntijuuden vaativissa, ns. seniortason, tehtävissä. [70]

[69] Ibid.
[70] Ibid.

Opiskelijoiden tulisikin itse suunnitella omat opintonsa tarkemmin ja kohdentaa osaamistaan tietyille alueille. Syvempi osaaminen jostakin kyberturvallisuuden osasta on työnantajien toiveena. Työnhakijoilta edellytetään tutkimushaastattelujen perusteella ainakin yhden osa-alueen syvää asiantuntemusta sekä yhden tai useamman muun osa-alueen hyvää tietämystä. Tämä johtui pääosin kahdesta seikasta: työtehtävässä menestyminen edellyttää laajempaa tietämystä alasta sekä organisaatiolla ei ole resursseja tai halua palkata useampaa henkilöä hoitamaan määriteltyjä työtehtäviä. [71]

Nykyisen työvoiman osaamisen tulee jatkuvasti pysyä kehityksen mukana. Se vaatii paljon resursseja, joita työnantaja ei aina tarjoa. Eteneminen omalla uralla vaatii siis myös vapaa-ajan uhraamista uuden oppimiseen. Kaikki tutkimukseen haastatellut yritysten edustajat kokivat työnhakijan oman aktiivisuuden, harrastuneisuuden ja alan seuraamisen oleelliseksi osaksi uuden työntekijän valintaa tehtäessä sekä tärkeänä osana oman olemassa olevan henkilökunnan kehitystä. Kaikki olivat myös valmiita tukemaan jollakin tavalla omien työntekijöidensä ammatillista kehitystä tarjoamalla mm. aikaa tai oppimista tukevaa materiaalia. [72]

2.4.4 Suomessa on kyberosaajapula

Jukka Niemelän tutkimus osoittaa selvästi soveltuvan työvoiman puutteen kyberalalla Suomessa. Työnantajien odotukset hakijoiden osaamisen tasosta eivät täyty. Lyhyellä aikavälillä tulisi keskittyä jatko- ja muuntokoulutukseen ja sen kautta uuden ja osaavamman työvoiman kehittymiseen alalle. Koulutusta tulee laajentaa kautta linjan ja lisätä alan houkuttelevuutta, jotta saadaan riittävästi hakijoita ja siten nostettua oppilaitosten koulutusmääriä. Siten voidaan vastata alan määrälliseen vajeeseen pitkällä aikavälillä. Työnantajien tulee tarjota työntekijöille mahdollisuuksia lisätä osaamista tukemalla oppimista työpaikoilla. [73]

Erityisesti pulaa on alan huippuosaamisesta sekä osaamisesta erikoisaloille, joille kyber laajentuu. Puutteita havaitaan perustason matemaattisessa osaamisessa ja ohjelmointitaidoissa sekä useilla eri osa-alueilla, joille kaivataan korkeampaa osaamista. Laadukasta teknologista osaamista tarvitaan voimakkaimmin pilvipalveluiden, turvallisen ohjelmoinnin ja rajapintojen tuntemuksessa sekä korkean turvatason palvelinympäristöjen osaamisessa. Työnantajat odottavat koulutuksen tuottavan valmiimpia osaajia. Erityisesti uusien tekniikoiden osalta oppilaitoksilta odotetaan edelläkävijyyttä. [74]

[71] Ibid.
[72] Ibid.
[73] Ibid.
[74] Ibid.

2.5 Johtopäätöksiä

Kattavan kyberturvallisuuskoulutuksen suunnittelussa tulee huomioida useita eri tekijöitä, jotka vaikuttavat koulutuksessa käytettävien järjestelmien ja digitaalisten oppimisympäristöjen valintaan, sekä koulutuksen rakenteen muodostamiseen. Teknisestä näkökulmasta suositellaan otettavan huomioon järjestelmien osalta niiden toimintalogiikan yhteneväisyys todellisen kybermaailman ja sen ilmiöiden kanssa, järjestelmän vuorovaikutuksellisuus, koulutettavan ratkaisujen soveltamismahdollisuus sekä oman suoriutumisen reflektointi järjestelmän palautteen kautta. Teknisen ja toiminnallisen sopivuuden lisäksi järjestelmän tulee haastaa koulutettavaa ja olla interaktiivinen, eli tarjota erilaisia vastauksia erilaisten ratkaisumahdollisuuksien mukaisesti. [75]

Psykologisesta näkökulmasta koulutukseen ja sen suunnitteluun voidaan saada lisähyötyä muun muassa koulutettavien henkilökohtaisten ominaisuuksien tarkastelussa osana koulutuksen onnistumista tai koulutettavien toimimista, sekä koulutuksen erilaisten osa-alueiden suunnittelussa yhteistyössä sosioteknisten järjestelmien kanssa, jotta digitaalinen koulutus antaisi kattavan kuvan kybermaailman ilmiöistä ja uhista. Koulutusta suunniteltaessa tulee selvittää koulutettavien henkilökohtaisten ominaisuuksien vaikutusta koulutukseen valittavien järjestelmien kanssa. On tärkeää valita teknisesti sopivin kyseistä koulutuksen osa-aluetta simuloiva järjestelmä, mutta tulee myös tuntea koulutettavat ja heidän henkilökohtaiset ominaisuutensa ja esimerkiksi ryhmätyöskentelytaitonsa, jotta järjestelmien ja koulutettavien yhteistyö olisi koulutuksen sisäistämisen kannalta paras mahdollinen. Psykologinen näkemys auttaa luonnollisesti myös koulutettavien tuntemisessa, joten myös koulutukseen valittavien henkilöiden henkilökohtaisia ominaisuuksia tulee selvittää, jotta persoonallisten ominaisuuksien hyödyt voitaisiin saada käyttöön alalla, joka vaatii hyvin suurta paineensietokykyä monimukaisessa ja -ulotteisessa sekä hektisessä toimintaympäristössä. Kattavan kyberturvallisuuskoulutuksen suunnittelussa tulee ottaa huomioon niin teknisiä kuin psykologisiakin tekijöitä määrällisten tarpeiden ohella, jotta koulutuksella voidaan tuottaa osaamiskyvyiltään, asenteiltaan ja motivaatioltaan mahdollisimman sopiva henkilöstö kuhunkin tehtävään eri toimialoilla.[76]

[75] Laukkarinen Emmi, Kokonaisvaltaisen kyberturvallisuuskoulutuksen suunnittelussa huomioitavia tekijöitä, julkaisematon ITKST41-kurssiraportti, 2019
[76] Ibid.

3 YLIOPISTOT

Tässä luvussa kuvataan yleisellä tasolla yliopistoissa annettavaa kyberturvallisuuskoulutusta ja niissä tehtävää kyberturvallisuuden/tietoturvallisuuden tutkimusta aakkosjärjestyksen mukaan. Myös muissa, kuin tässä esitetyissä yliopistoissa on kyber/tieto/informaatioturvallisuutta sisällytetty opintoihin. Myös tutkielmia, pro gradu -töitä ja väitöskirjoja on laadittu monissa muissakin yliopistoissa.

3.1 Aalto yliopisto (Aalto)

3.1.1 Kyberalaan liittyvä opetus

Aalto-yliopistossa opiskellaan Tietoliikenne- ja tietoverkkotekniikan laitoksella tekniikan kandidaatiksi ja siitä edelleen diplomi-insinööriksi. Tietoturvallisuutta opiskellaan osana opintoja. Kyberturvallisuudesta ei ole erikseen koulutusohjelmaa tai pääainetta. Informaatioverkostot-opintojen tarkoituksena on kouluttaa tietoyhteiskunnan laaja-alaisia osaajia. Tietotekniikan opinnoissa on mahdollista keskittyä mm. teknologiaoikeuteen, mobiilisovelluksiin, tiedonlouhintaan, salaustekniikoihin sekä sulautettuihin järjestelmiin. Maisteriohjelmista kyberturvallisuutta lähimpänä ovat:

- Computer, Communication and Information Sciences: Computer Science
- Computer, Communication and Information Sciences: Security and Cloud Computing.

AaltoPro:n PD-ohjelmassa on *Diploma in Digital Security* -koulutusohjelma, jossa annetaan tiedot ja työkalut digitalisoituvan liiketoiminnan turvallisuuden johtamiseen. Koulutusohjelma käsittelee organisaatioiden valmiuksia toimia osana kyberympäristöä.

3.1.2 Kyberalaan liittyvät kurssit

- CS-E4320 Cryptography and Data Security 5 op
- CS-C3130 Information Security 5 op
- CS-E4300 Network Security 5 op
- CS-E4160 Laboratory Works in Networking and Security 5 op
- CS-E4310 Mobile Systems Security 5 op
- CS-E4330 Special Course in Information Security 2-10 op
- CS-E4520 Computer Aided Verification and Synthesis 5 op

3.1.3 Kyberalaan liittyvä tutkimus

Tietoliikenne- ja tietoverkkotekniikan laitoksen tutkimus jakautuu kolmeen osa-alueeseen: Communication ecosystems, Communication and networking technology sekä Information and Communications theory. Tutkimus keskittyy mm. tietoliikenteeseen, kyberturvallisuuden johtamiseen, kyber- ja hybridisodankäyntiin, kehittyviin internet-teknologioihin, verkkoarkkitehtuuriin, tietoverkkoliiketoimintaan, verkkoturvallisuuteen ja -luottamukseen, käyttöliittymiin sekä mobiiliin pilvilaskentaan.

3.2 Helsingin yliopisto (HY)

3.2.1 Kyberalaan liittyvä opetus

Helsingin yliopistossa opiskellaan Matemaattis-luonnontieteellisessä tiedekunnassa filosofian maisteriksi. Siellä tietojenkäsittelytiede ja datatiede ovat osa maisteriohjelmia. Opinnot keskittyvät algoritmeihin, ohjelmistotuotantoon, hajautettuihin järjestelmiin ja koneoppimiseen. Näissä tarjotaan tietoturvan ja kyberturvallisuuden kursseja. Kyberturvallisuudesta ei ole erikseen koulutusohjelmaa tai pääainetta.

3.2.2 Kyberalaan liittyvät kurssit

- TKT20009 Introduction to Cyber Security Intermediate studies
- CSM13202 Cryptography in Networking Advanced studies
- CSM13204 Cyber Security II Advanced studies
- DATA16001 Network Analysis Advanced studies
- CSM13282 Seminar on Advanced Topics in Networking and Security

3.2.3 Kyberalaan liittyvä tutkimus

Tutkimusta tehdään Matemaattis-luonnontieteellisessä tiedekunnassa, erityisesti Tietojenkäsittelytieteen osastossa. Tutkimusaloja on neljä: algoritmit, tekoäly, tietoverkot ja ohjelmistot. Tutkimusryhmiä on kullakin alalla useita, esim. Secure Systems. Osa tutkimuksesta tapahtuu erityisissä keskuksissa, joita ovat Finnish Center for Artificial Intelligence (FCAI), Helsinki-Aalto Center for Information Security (HAIC), Helsinki Centre for Data Science (HiDATA), ja Nokia Center for Advanced Researcher (NCAR). Tutkimuksen pääkohteita ovat mm. data-analytiikka, koneoppimisalgoritmit, tekoäly, hajautetut järjestelmät sekä suuret tietoaineistot. Osaston yhteydessä toimii Aalto-yliopiston kanssa yhteinen Tietotekniikan tutkimuslaitos HIIT. Useimmat em. keskuksista ovat HIIT:n ohjelmia.

3.3 Itä-Suomen yliopisto (UEF)

3.3.1 Kyberalaan liittyvä opetus

Itä-Suomen yliopiston Luonnontieteiden ja metsätieteiden tiedekunnan tietojenkäsittelytieteen laitos on keskittynyt opetusteknologiaan, tekoälyyn ja koneoppimiseen, joissa painopisteenä on ohjelmointi ja suunnittelu. Kyberalan opintoja ei ole tarjolla perustason tietoturvaa lukuun ottamatta.

3.3.2 Kyberalaan liittyvät kurssit

- 3621418 Johdatus tietoturvaan (JTI) 5 op

3.3.3 Kyberalaan liittyvä tutkimus

Tietojenkäsittelytieteen laitoksen tutkimus jakautuu kahteen ryhmään. Älykäs medialaskenta pitää sisällään laskennallisen älykkyyden, spektrisen väritutkimuksen sekä koneoppimisen tutkimusalat. Opetus- ja kehitysteknologiat keskittyvät opetukseen ja vuorovaikutukseen.

3.4 Jyväskylän yliopisto (JY)

3.4.1 Kyberalaan liittyvä opetus

Jyväskylän yliopiston Informaatioteknologian tiedekunnassa opintoja voi suorittaa tietojärjestelmätieteiden, tietotekniikan, kognitiotieteen ja kyberturvallisuuden aloilla. Näistä valmistuu kauppatieteen ja filosofian kandidaatteja ja maistereita.

Jyväskylän yliopisto on ainoa Suomen yliopisto, jolla on kyberturvallisuudesta oma maisteriohjelma. Kyberturvallisuuden maisteriohjelman tavoitteena on tarjota opiskelijalle vankka osaaminen työskentelyyn kyberturvallisuuden kokonaishallintaa vaativissa johtamis- ja kehittämistehtävissä. Koulutuksessa tarkastellaan kybermaailmaa ja sen turvallisuutta yhteiskunnallisesta, toiminnallisesta, teknologisesta ja systeemisestä näkökulmasta. Maisteriohjelmassa kyberturvallisuutta tarkastellaan kokonaisturvallisuuden kontekstissa ottaen huomioon kansainvälistyvään ja digitalisoituvaan yhteiskuntaamme liittyvät kehityskulut, toiminta- ja huoltovarmuus sekä reagointi- ja riskinsietokyky.

Kyberturvallisuuden maisteriohjelman opinnot koostuvat vähintään 80 op laajuisista maisteriohjelman syventävistä opinnoista (joihin sisältyy 30 op laajuinen opinnäyte), vähintään 5 op laajuisista viestintä- ja kieliopinnoista sekä vähintään 35 op laajuisista muista opinnoista, joiden sisältö vaihtelee opiskelijan taustatutkinnon ja opiskelijan itselleen asettamien tavoitteiden mukaisesti.

3.4.2 Kyberalaan liittyvät kurssit

- TJTSM51 Information Security Management 5 op
- TJTSM56 Advanced Course on Information Security Management 5 op
- ITKST50 Secure Systems Design 5 op
- TJTSM65 Information Privacy 5 op
- ITKST41 Kybermaailma ja turvallisuus 5 op
- ITKST56 Järjestelmähaavoittuvuudet 5 op
- TIES327 Tietoverkkoturvallisuus 3-5 op
- KYBS1201 Kyberturvallisuusteknologiat 5 op
- ITKST45 Introduction to Cyber Conflict 5 op
- ITKST55 Kyberhyökkäys ja sen torjunta 5 op
- KYBS7011 Kyberturvallisuus, yhteiskunta ja henkinen kriisinkestävyys 5 op
- ITKST40 Yhteiskunta ja informaatioturvallisuus 5 op
- ITKST44 Kybermaailma ja kansainvälinen oikeus 5 op
- KYBS7021 Viestinnän ja vaikuttamisen teoreettisia perusteita 5 op
- KYBS7022 Informaatiovaikuttamisen keskeisiä kysymyksiä 5 op
- KYBS7031 Informaation hallinta ja tiedustelu I 5 op
- KYBS7032 Informaation hallinta ja tiedustelu II 5 op
- KYBS7033 Informaation hallinta ja tiedolla johtaminen 5 op
- KYBS7041 Anomalian havaitseminen 5 op
- KYBS7042 Anomalian havaitsemisen jatkokurssi 5 op

3.4.3 Kyberalaan liittyvä tutkimus

Informaatioteknologian tiedekunnan neljä päätutkimusaluetta ovat Computational Sciences, Software and Telecommunication Technology, Information Systems sekä Congnitive Science and Educational Technology. Lisäksi Cyber Security sekä Computational thinking and decicsion-making tutkimusalat risteävät edellä mainittujen päätutkimusalojen kanssa.

Kyberturvallisuuden tutkimus jakautuu neljään päätutkimusalueeseen:

1. Cyber Security and Networking
    a. Detection of Zero-Day Network Attacks
    b. Advanced Data Analysis
2. Information Security Management
    a. Cyber security management
    b. Cyber security investments
    c. Cyber security strategies and policies in enterprises
    d. Privacy
3. Cyber Defence
    a. Development cyber warfare capabilities
    b. Electronic warfare and cyber security
    c. Information operation management

   d. Cyber threat intelligence
   e. Hybrid warfare environment
4. Critical infrastructure protection.
   a. Cyber security in critical environment
   b. Cyber security in energy systems
   c. Cyber security in civil aviation
   d. IoT and cyber security
   e. Cyber security situational awareness
   f. Cyber security in healthcare system

3.5 Lappeenrannan teknillinen yliopisto (LUT)

3.5.1 Kyberalaan liittyvä opetus

Lappeenrannan teknillisen yliopiston School of Engineering Science:ssa voi opiskella tekniikan kandidaatiksi ja diplomi-insinööriksi. Myös kaksoistutkinto yhteistyöyliopistoissa Venäjällä on mahdollista. Tietotekniikan ohjelmassa opinnon kohdentuvat pääosin digitalisaatioon ja ohjelmistotuotantoon. Englannin kielinen Software Engineering and Digital Transformation -maisteriohjelma jakautuu niemensä mukaan ohjelmistojen suunnitteluun ja määrittelyyn sekä digitaaliseen muutokseen.

3.5.2 Kyberalaan liittyvät kurssit

- CT30A3500 Tietoturvan perusteet 3 op
- CT60A5500 Quality Assurance in Software Development 6 op

3.5.3 Kyberalaan liittyvä tutkimus

LUT:n tutkimus keskittyy ajankohtaisiin energiakysymyksiin ja tarvittaviin ratkaisuihin. Tutkimuksella tuotetaan uusia menetelmiä datan jalostamiseen entistä nopeammin ja monipuolisemmin. Tekniikan tutkimus on kohdentunut konenäköön ja hahmontunnistukseen sekä älykkäisiin digitaalipalveluihin.

3.6 Maanpuolustuskorkeakoulu (MPKK)

3.6.1 Kyberalaan liittyvä opetus

Maanpuolustuskorkeakoulun pääaineita ovat johtaminen, sotilaspedagogiikka, sotataito ja sotatekniikka. Ylemmän korkeakoulun suorittaneista tulee sotatieteiden maistereita. Kyberturvallisuuden osalta opiskeltavat alat keskittyvät kyberpuolustukseen, ky-

bertilannekuvan luomiseen sekä kriittisen infrastruktuurin suojaamiseen. Kyberturvallisuudesta ei ole erikseen koulutusohjelmaa tai pääainetta vaan koulutus on sisällytetty opintojaksoina eri moduuleihin.

Maanpuolustuskorkeakoulun tarjoamista tutkinnoista tiedot on koottu sotatieteiden kandidaatin (vuoden 2018) ja -maisterin (vuoden 2018 tutkintojen opetussuunnitelmista. Sotatieteiden kandidaatin tutkinnossa (laajuus 180 opintopistettä) on neljä eri koulutusohjelmaa: maa-, meri-, ja ilmavoimien sekä lentoupseerien koulutusohjelmat.

3.6.2 Kyberalaan liittyvät kurssit

1. Maavoimien koulutusohjelmaan kuuluvat seuraavat kyberturvallisuusopinnot:
Johtamisjärjestelmäopintosuunnan moduuli: Operaatioturvallisuus (3 op)

2. Merivoimien koulutusohjelmaan kuuluvat seuraavat kyberturvallisuusopinnot:
Johtamisjärjestelmäopintosuunnan moduuli: Kyberturvallisuuskurssi (3 op)

3. Ilmavoimien koulutusohjelmaan kuuluvat seuraavat kyberturvallisuusopinnot:
Johtamisjärjestelmän opintosuunta: Tietoverkkopuolustuksen perusteet (3 op) ja Kyber ilmapuolustuksessa (2 op).
Ilmavoimien johtokeskusopintosuunta: Tietoverkkopuolustuksen perusteet (3 op)

Tämän lisäksi kyberturvallisuutta on sisällytetty eri moduulien ja opintojaksojen sisälle.

3.6.3 Kyberalaan liittyvä tutkimus

Tutkimuksen tehtävänä on kehittää sotatieteitä kansallisesti sekä kansainvälisesti ja palvella Puolustusvoimille laissa asetettuja kolmea päätehtävää. Tutkimuksen painopiste on ennen kaikkea tulevaisuuden uhkakuvissa ja Suomen puolustusjärjestelmän kehittämisessä. Maanpuolustuskorkeakoulun kolmessa eri ainelaitoksissa harjoitettava sotatieteellinen tutkimustoiminta jaetaan kahdeksaan tutkimusalueeseen, joita ovat:

1. Operaatiotaito ja taktiikka
2. Sotahistoria
3. Johtaminen
4. Sotilaspedagogiikka
5. Sotatekniikka
6. Sotatalous
7. Strategia
8. Sotilassosiologia

Kyberturvallisuuden ja kybersodankäynnin tutkimusta toteutetaan näiden tutkimusalojen sisällä.

3.7 Oulun yliopisto (OY)

3.7.1 Kyberalaan liittyvä opetus

Oulun yliopiston Tieto- ja sähkötekniikan tiedekunta tarjoaa tietojenkäsittelyn, tietotekniikan ja tietoliikenteen koulutusta, joista voi valmistua tekniikan kandidaatiksi ja diplomi-insinööriksi. Tietotekniikan koulutuksessa on mahdollista perehtyä mm. data-analyysiin, esineiden internetiin ja signaalikäsittelyyn. Luonnontieteellisessä tiedekunnassa laskennallisen matematiikan ja datatekniikan opinnoissa voi opiskella mm. kryptografiaa, tiedonlouhintaa, massadatan käsittelyä ja salaustekniikoita. Kyberturvallisuudesta ei ole erikseen koulutusohjelmaa tai pääainetta.

3.7.2 Kyberalaan liittyvät kurssit

- 811168P Tietoturva 5 op
- 813623S Information Security Policy Management in Organizations 5 op
- 521155S Computer Security 5 op
- 801698S Kryptografia 5 op
- 802336A Salausmenetelmät 5 op

3.7.3 Kyberalaan liittyvä tutkimus

Yliopiston tutkimus sijoittuu kaikkialla läsnä olevaan (eng. ubiquitous) tietotekniikkaan, empiiriseen ohjelmistotuotantoon ja ihmiskeskeiseen digitalisaatioon sekä informaatiotekniikkaa tukevaan matematiikkaan, kuten kryptografiaan ja salausmenetelmiin sekä informaation visualisointiin.

Suomalaiset ja yhdysvaltalaiset perustivat Oulun yliopiston yhteyteen kyberturvallisuuden tutkimusyksikön. Taustalla on monivuotinen suomalaisyliopistojen ja yritysten yhteistyö yhdysvaltalaisen tiedesäätiö National Science Foundationin (NSF) kanssa. Perustettu tutkimusyksikkö *Cyber Security and Software Engineering Research Site* on osa NSF:n kyberturvallisuusaiheista tutkimusta. Tutkimusyksikkö on avoin kaikille suomalaisille yliopistoille ja tutkimuslaitoksille. Yksikkö toimii osana *Security and Software Engineering Research Center* -keskusta, joka on tutkinut 13 yliopiston ja yli 20 teollisen ja julkishallinnollisen partnerin voimin ohjelmistojen ja järjestelmien turvallisuutta Yhdysvalloissa vuodesta 2010 alkaen.

3.8 Tampereen yliopisto (TUNI)

3.8.1 Kyberalaan liittyvä opetus

Tampereen yliopistossa Informaatioteknologian- ja viestinnän tiedekunnassa voi opiskella tekniikan kandidaatiksi ja diplomi-insinööriksi. Tietotekniikan kandidaatin tutkinnossa voi suuntautua ohjelmistotekniikkaan, signaalinkäsittelyyn ja koneoppimiseen, elektroniikkaan ja sulautettuihin järjestelmiin sekä tietoliikennetekniikkaan. Kyberturvallisuus I -opintojakso on pakollisena kaikilla tietotekniikan opiskelijoilla kandivaiheessa. Tietoturvallisuus on tarjolla syventävänä kokonaisuutena DI-vaiheessa. Näitä syventäviä opintoja voi painottaa kryptologisesti, hallinnollisesti, ohjelmistoteknisesti, ihmiskeskeisesti tai verkkoteknisesti.

Tietoturvallisuus sisältää opintojaksoja, joissa käsitellään kyberturvallisuutta, identiteetin- ja pääsynhallintaa, kryptografiaa, verkon tietoturvaa, ohjelmoinnin turvallisuutta, hallinnollista tietoturvaa sekä automaation tietoturvaa.

3.8.2 Kyberalaan liittyvät kurssit

Tietotekniikka

- TIE-30151 Kyberturvallisuus I: perusteet 5 op
- TIE-30302 Kyberturvallisuus II: syventävä 5 op
- TIE-30201 Tietoturva-arki 5 op
- TIE-30501 Identiteetin ja pääsynhallinta 5 op
- TIE-30601 Turvallinen ohjelmointi 5 op
- TIE-30406 Network Security 5 op
- TIE-31106 Cryptography Engineering 5 op

Automaatiotekniikka

- ASE-7610, Automaation turvallisuus 5 op

Tietojohtaminen

- TLO-35236, Information Security Management 4 op

3.8.3 Kyberalaan liittyvä tutkimus

NISEC eli Network and Information Security Group on vuodesta 1996 alkaen toiminut tietoturvallisuuden ja yksityisyydensuojan asiantuntijaryhmä. NISEC-ryhmän nykyiset tutkimusalueet ovat seuraavat:

A. Tietoverkkojen turvallisuus

Tärkeä osa tietoverkkojen turvallisuutta on TUT Cyber Labs -laboratorio, joka on suunniteltu tutkimuksen ja opetuksen tarpeisiin. Tutkimuksen pääalueet ovat:

- SDN-turvallisuus
- Identiteetin- ja pääsynhallinta hajautetuille järjestelmille
- Tietoturvalliset protokollat
- Tapaustenhallinta ja reagointi
- Tekoäly kyberturvallisuudessa Esineiden internetin tietoturvallisuus

B. Esineiden internet (Internet of things, IoT)
Tutkimus keskittyy IoT-laitteiden ja niiden komponenttien turvalliseen kommunikointiin ja elinkaaren hallintaan. Tutkimuksen pääalueet ovat:

- Tietoturvallisuus ja yksityisyydensuoja esineiden Internetissä ja älykkäissä ympäristöissä
- IoT-laitteiden ja yhdysväylien tietoturvallinen provisiointi, alustaminen ja päivittäminen
- Autentikointi ja pääsynhallinta rajoitetuissa IoT-ympäristöissä
- IoT-yhdyskäytävälle asennettavien sovellusten turvallinen alustaminen

C. Laitteistoavusteinen tietoturvallisuus
Laitteistoavusteisen tietoturvallisuuden tutkimus on yhdistelmä teoriaa ja käytäntöä kryptografiassa. Tutkimuksen pääalueet ovat:

- Sovellettu kryptografia
- Sivukanavahyökkäykset
- Sulautetut järjestelmät ja niiden tietoturva
- Tietokonearkkitehtuurit

D. Yksityisyydensuoja ja käytettävä tietoturvallisuus
NISEC kehittä ja suunnittelee tärkeimpiin protokolliin sekä muuhun tekniikkaan ratkaisuja, jotka auttavat parantamaan käyttäjien yksityisyydensuojaa ja tietoturvallisuutta:

- Yksityisyydensuoja ja turvallisuus sähköisen äänestämisen järjestelmissä
- Tietoturvallisuus ja yksityisyydensuoja pilvijärjestelmissä, erityisesti tietoturvallinen tiedon säilöminen ja tiedon jakaminen
- Yksityisyyden säilyttävät terveydenhuollon järjestelmät
- Luotettu tietojenkäsittely (eng. trusted computing)
- Tutkimuskohteena käytettävä tietoturva ja yksityisyydensuoja

3.9 Turun yliopisto (TY)

3.9.1 Kyberalaan liittyvä opetus

Turun yliopiston Luonnontieteiden ja tekniikan tiedekunta tarjoaa luonnontieteen ja tekniikan kandidaatin sekä filosofian maisterin ja diplomi-insinöörin tutkintoihin johtavaa koulutusta. Keskeisin kyberturvallisuuteen liittyvä tutkinto-ohjelma on monitieteinen **Master's Degree Programme in Information Security and Cryptography**. Tässä ohjelmassa on tarjolla kaksi pääainetta, DI-tutkintoon johtava Security of Networked Systems sekä FM-tutkintoon johtava Cryptography and Data Security. Pakollisiin pääaineopintoihin kuuluvat kyberturvateknologian (Tulevaisuuden teknologioiden laitos), matemaattisen kryptografian (Matematiikan ja tilastotieteen laitos) sekä tietoturvajohtamisen (Turun kauppakorkeakoulun johtamisen laitos) kurssit. Lisäksi erikoiskursseina voi vuosittain vaihtelevasti olla tarjolla oikeustieteellisiä sekä valtiotieteellisiä kyberturvallisuuskursseja.

Information Security and Cryptography -maisteriohjelma (ja sen pääaine Security of Networked Systems) on ainoa suomalainen kyberturvallisuusalan tutkinto-ohjelma, joka on hyväksytty osaksi yhteiseurooppalaista EIT Digital Master School in Cyber Security -yhteistutkinto-ohjelmaa. EIT (European Institute of Innovation & Technology) Digital Master School on kahdenkymmenen eurooppalaisen yliopiston yhteistyönä järjestettävä kaksoistutkintoon johtava maisterikoulu. Turun yliopisto toimii Cyber Security -ohjelmassa sekä ”entry”- että ”exit”-yliopistona.

Information Security and Cryptography -maisteriohjelman lisäksi kyber-/informaatioturvallisuuteen keskittyviä opintoja on sisällytetty myös mm. tietotekniikan, tietojenkäsittelytieteiden ja matematiikan tutkinto-ohjelmiin. Nämä tutkinto-ohjelmat käsittävät tietotekniikan, tietojenkäsittelytieteen, tietojärjestelmätieteen, matematiikan ja tilastotieteen aloja.

Information Security and Cryptography -tutkinto-ohjelman rakenne on seuraava:

Pääaine: Security of Networked Systems (DI) 120 ECTS:

1. Network and Cyber Security module 20 ECTS
2. Cryptography and Security Management module 20 ECTS
3. Master's Thesis module 40 ECTS (thesis 30 ECTS, Finnish course 5 ECTS for non-Finnish speakers and/or courses supporting thesis, internship/work placement recommended, 5-10 ECTS)
4. Elective studies in Major subject 20 ECTS (valinnaisia pääaineopintoja)
5. Thematic module 20 ECTS (vapaasti valittava sivuaine: Cryptography and Data Security, Information Technology Management, Innovation and Business Creation, IoT Systems and Security, Applications of Interaction Design, Data Science, Software Engineering)

Pääaine: Cryptography and Data Security (FM) 120 ECTS:

1. Cryptography module 20 ECTS
2. Security of Networked Systems and Security Management module 20 ECTS
3. Master's Thesis module 40 ECTS (thesis 30 ECTS, elective major subject studies 10 ECTS)
4. Elective studies 20 ECTS (Finnish course 5 ECTS for non-Finnish speakers and/or elective studies in major subject)
6. Thematic module 20 ECTS (vapaasti valittava sivuaine tai matematiikan pääaineopintoja: Security of Networked Systems, Information Technology Management, Discrete Mathematics, IoT Systems and Security, Applications of Interaction Design, Data Science, Software Engineering)

3.9.2 Kyberalaan liittyvät kurssit

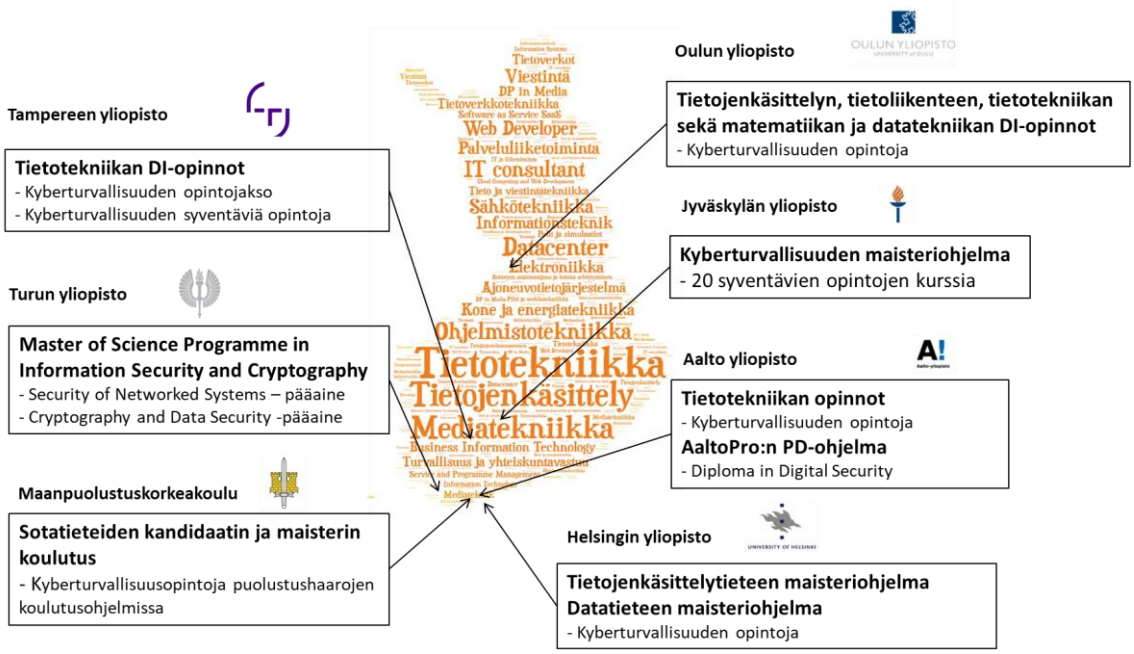
- DTEK1068 Opiskelun ja työelämän tietotekniikka, Tieto- ja kyberturvallisuus 1 op
- DTEK1064 Tietoyhteiskunta ja kyberturvallisuus 4 op
- DTEK8025 System and Application Security 5 op
- DTEK8063 Firewall and IPS Technology 5 op
- DTEK0039 Security Engineering 5 op
- DTEK2029 Human Element in Information Security 5 op
- DTEK8060 Protocol Processing and Security 5 op
- DTEK8096 Network Infrastructure Technologies and Security 5 op
- DTEK8097 Secure Sensor Network Systems 5 op
- DTEK2034 Communication Technologies and Security in IoT 5 op
- MATE5341 Foundations of Cryptography 5 op
- MATE5396 Cryptography I 5 op
- MATE5397 Cryptography II 5 op
- MATE5344 Algebraic Structures in Cryptography 5 op
- MATE5345 Selected Topics in Cryptography 5 op
- DTEK8098 Software Development and Software Security 5 op
- DTEK8102 Privacy and Security for Software Systems 5 op
- TJ093150 TJS13 Management of Information System Security 6 op
- TJ093222 TJS16 Information Technology and Ethics 6 op

3.9.3 Kyberalaan liittyvä tutkimus

Kyberalan tutkimusta tehdään monessa laitoksessa eri tiedekunnissa monialaisessa yliopistossa. Tulevaisuuden teknologioiden laitoksessa kyberalan tutkimus keskittyy tietoturvateknologiaan erityisinä fokusalueinaan terveydenhuollon, älykkäiden ympäristöjen, verkkojärjestelmien (ml. IoT ja sensoriverkot) ja ohjelmistojen turvallisuus. Tutkimusaiheina ovat myös tietoyhteiskunnan kyberturvallisuus sekä kyberturvallisuuden inhimillinen elementti (Human Element in Cyber Security).

Matematiikan ja tilastotieteen laitoksella tutkitaan muun muassa koodausteoriaa, ja kryptografian tutkimuksen osalta laitos tekee yhteistyötä Helsingin yliopiston Tietojenkäsittelytieteen osaston kanssa. Turun kauppakorkeakoulun Johtamisen laitoksella kyberturvallisuuden tutkimus keskittyy tietoturvajohtamisen ja liiketoiminnan jatkuvuuden hallinnan tutkimukseen. Valtiotieteessä tutkitaan muun muassa Kiinan verkkosensuuria ja internet-hallintaa.

Kuviossa 6 on esitetty kyberturvallisuuden opetus seitsemässä yliopistoissa.



KUVIO 6 Kyberturvallisuuden opetus seitsemässä yliopistoissa

4 AMMATTIKORKEAKOULUT

Tässä luvussa kuvataan yleisellä tasolla ammattikorkeakouluissa annettavaa kyberturvallisuuskoulutusta ja niissä tehtävää kyberturvallisuuden/tietoturvallisuuden tutkimusta. Myös muissa, kuin tässä esitetyissä ammattikorkeakouluissa on kyber/tieto/informaatioturvallisuutta sisällytetty opintoihin. Myös tutkielmia ja opinnäytetöitä on laadittu monissa muissakin ammattikorkeakouluissa.

4.1 Centria-ammattikorkeakoulu (Centria)

4.1.1 Kyberalaan liittyvä opetus

Centrian informaatioteknologian opinnot keskittyvät ohjelmistotuotantoon ja viestintäteknologioihin. Centriasta valmistuu tieto- ja viestintätekniikan alan insinööriksi.

4.1.2 Kyberalaan liittyvät kurssit

- ITK1055 Cisco Networking Academy II 4 op
- ITK1056 Cisco Networking Academy III 3 op
- ITK1059 Cisco Networking Academy IV 3 op
- ITK1041 IP-Networks 4 op
- SAY1209 Tietoturva 4 op
- MTY1102 Tietoturvan rakentaminen 5 op
- MTY1114 CSNA: Security 5 op

4.1.3 Kyberalaan liittyvä tutkimus

Centrian tutkimus ja kehitys on keskittynyt langattomien verkkojen, paikkatiedon, tietoturvan ja sulautettujen järjestelmien ympärille. Esimerkkeinä CyberWI-projekti, joka työskentelee tunkeutumiseneston, autentikoinnin ja pääsynhallinnan sekä turvallisen datasiirron parissa.

4.2 Jyväskylän ammattikorkeakoulu (JAMK)

4.2.1 Kyberalaan liittyvä opetus

Jyväskylän ammattikorkeakoulussa voi valmistua tietojenkäsittelyn tradenomiksi tai tieto- ja viestintätekniikan alan insinööriksi. Näissä suuntautumisvaihtoehtoina ovat mm.

kyberturvallisuus, media-, ohjelmisto- ja tietoverkkotekniikka. Ylemmässä ammattikorkeakoulussa (YAMK) on myös oma englanninkielinen Cyber Security -linja. JAMK tarjoaa kattavan kyberturvallisuuden opintokokonaisuuden. Kyberturvallisuuden ydinopinnot muodostavat 14 kurssin ja 58 opintopisteen kokonaisuuden, jonka lisäksi on 15 op:n kyberharjoituskokonaisuus ja yleisiä kyberturvallisuusopintoja.

Jyväskylän ammattikorkeakoulun IT-instituutin Jyväskylä Security Technology (JYVSECTEC) on kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus. Se järjestää mm. kyberturvallisuusharjoituksia.

4.2.2 Kyberalaan liittyvät kurssit

- YTCP0100 Security Management in Cyber Domain 5 op
- YTCP0200 Cyber Security Implementation in Practice 10 op
- YTCP0300 Auditing and Testing Technical Security 5 op
- YTCP0400 Cyber Security Exercise 5 op
- TTZC0600 Kyberturvallisuus 4 op
- TTKS0100 Data Network Protocols 3 op
- TTKS0600 Encryption Techniques and Systems 5 op
- TTKS0700 Data Security Testing 3 op
- TTKS0800 Tietoturvateknologiat 6 op
- TTKS0900 Tietoturvallisuus palvelunhallinnassa 3 op
- TTKS1000 Tunkeutumis- ja puolustamismenetelmät 4 op
- TTKW0110 Tietoturvakontrollien suunnittelu ja toteutus 8 op
- TTKW0210 Web Application Security 5 op
- TTKW0220 Software Exploitation 5 op
- TTKW0230 Reverse Engineering 5 op
- TTKW0310 Kyberharjoituksen suunnittelu ja valmistelu 10 op
- TTKW0320 Kyberharjoituksen toteutus 5 op

4.2.3 Kyberalaan liittyvä tutkimus

JAMK:ssa kyberalaan liittyvä tutkimus ja kehitys painottuu sovellettuun kyberturvallisuuteen. Siinä järjestelmien testauksen ja arvioinnin kautta luodaan suojausmekanismeja kyberhyökkäyksiä vastaan. Lisäksi JAMK:ssa tutkitaan toimialaspesifejä kyberturvallisuusuhkia, niiden analysointia ja uhkien torjumista. Sovelletun tutkimuksen osa-alueena myös organisaation kyberturvallisuusosaamisen kehittäminen.

4.3 Kaakkois-Suomen ammattikorkeakoulu (XAMK)

4.3.1 Kyberalaan liittyvä opetus

Kaakkois-Suomen ammattikorkeakoulussa tietoteknistä alaa voi opiskella Kotkassa ja Mikkelissä. Vaihtoehtoina ovat mm. insinööriopinnot kyberturvallisuudesta ja tietotekniikasta, Bachelor of Engineerin opinnot informaatioteknologiasta sekä tradenomin opinnot tietojenkäsittelystä. YAMK opinnoissa on Älykkäät tietojärjestelmät ja Cybersecurity - Kyberturvallisuus -koulutusohjelmat. Kyberturvallisuudessa perehdytään tietoturvauhkien tunnistamiseen ja torjuntaan sekä tietoturva-auditointiin. Kaiken kaikkiaan tarjolla on laaja kirjo kyberturvallisuuden opintoja.

4.3.2 Kyberalaan liittyvät kurssit

- TI00BI12 Tietoturva 5 op
- TI00BI22 Kyberturvallisuuden matematiikka ja fysiikka 5 op
- TI00BI23 Kyberturvallisuus 5 op
- TI00BI25 Pentesting 5 op
- TI00BI26 Secure Enterprise Networks 5 op
- TI00BI27 Cyber Security Project 5 op
- TI00BI31 Advanced secure operating systems 5 op
- TI00BI33 Advanced cyber security 5 op
- IT00CO77 Security fundamentals 5 op
- IT00CO89 Information and network security 5 op
- BY00CW36 Introduction to cybersecurity 5 op
- CS00CU77 Services in cybersecurity 5 op
- CS00CU78 Networks and cybersecurity 5 op
- CS00CU79 Defensive cybersecurity 5 op
- CS00CU80 Offensive cybersecurity 5 op

4.3.3 Kyberalaan liittyvä tutkimus

XAMK:n kyberturvallisuuden tutkimus lähestyy kyberturvallisuutta järjestelmäkokonaisuuksien hallinnan kautta.

4.4 Laurea ammattikorkeakoulu (Laurea)

4.4.1 Kyberalaan liittyvä opetus

Laurea tarjoaa tietojenkäsittelyn tradenomin opintoja. Tarjolla on useita kyberturvallisuuteen suuntautuvia opintojaksoja.

4.4.2 Kyberalaan liittyvät kurssit

- R0242 Tietoverkot ja tietoturva 5 op
- R0318 Introduction to Information Security 5 op
- R0319 Information Security Management 5 op
- R0320 Information Security Development Project 5 op
- R0385 Internet Infrastructure and Security 5 op
- R0386 Contemporary Issues in Networking and Network Security 5 op
- R0321 Cybersecurity 5 op
- R0322 Systems Security 5 op
- R0324 Network Security 5 op
- R0323 Enterprise Application Security 5 op
- R0325 Cyber Security in Emerging Environment 5 op
- R0326 Cyber Security Applied Project 5 op

4.4.3 Kyberalaan liittyvä tutkimus

Laurean kyberturvallisuuden tutkimus, kehitys ja innovaatiot sitoutuvat yhteen yhtenäisen turvallisuuden kehyksessä. Se huomioi turvallisuus-, rikosseuraamus-, sosiaali- ja terveys-, sekä tietojenkäsittelyalan. Avainsanoina konfliktien esto, kriisinhallinta, rikoksentorjunta sekä auditointi.

4.5 Metropolia ammattikorkeakoulu

4.5.1 Kyberalaan liittyvä opetus

Metropolia ammattikorkeakoulu tarjoaa työelämässä toimiville ammattilaisille kyberturvallisuuden erikoistumiskoulutusta. Kyberturvallisuuden erikoistumiskoulutus on laajuudeltaan 30 opintopistettä ja se koostuu kuudesta kyberturvallisuuden kurssista.

4.5.2 Kyberalaan liittyvät kurssit

- Johdatus kyberturvallisuuteen 5 op
- Kyberturvallisuusliiketoiminta 5 op
- Puolustava kyberturvallisuus 5 op
- Offensiivinen kyberturvallisuus 5 op
- Tietoverkkojen kyberturvallisuus 5 op
- Kyberturvallisuusprojekti 5 op

4.5.3 Kyberalaan liittyvä tutkimus

Metropoliassa on ICT-alaan liittyvää TKI-toimintaa seuraavilla aloilla:

- Ketteriä asiakaslähtöisiä menetelmiä ja uusien digitaalisten teknologioiden soveltaminen
- IoT ja Pilvidata-analyysi
- Robotiikka

4.6 Oulun ammattikorkeakoulu (OAMK)

4.6.1 Kyberalaan liittyvä opetus

Oulun AMK:n tietojenkäsittelyn koulutusohjelma tarjoaa perustason opetusta tietoturvasta.

4.6.2 Kyberalaan liittyvät kurssit

- T252003 Tietosuoja- ja tietoturvateknologia 3 op

4.6.3 Kyberalaan liittyvä tutkimus

OAMK tutkimus ja kehitys suuntautuu tuote- ja järjestelmäkehitykseen, mutta ei suoranaisesti kyberturvallisuusalan näkökulmasta.

4.7 Poliisiammattikorkeakoulu (POLAMK)

4.7.1 Kyberalaan liittyvä opetus

Poliisiammattikorkeakoulu keskittyy kyberturvallisuuden osalta tietojärjestelmien hyödyntämiseen sekä tietoverkkoihin kohdistuvaan rikostorjunta- ja tutkintaosaamiseen.

4.7.2 Kyberalaan liittyvät kurssit

Poliisiammattikorkeakoulun vahvistamassa vuosia 2018-2020 koskevassa opetussuunnitelmassa on kuvattu kyberturvallisuusopintoja. Opetuksen tavoitteet on kirjattu rikostorjunta- ja tutkintaosaamisen opintokokonaisuuden alaisuuteen kuuluvaan esitutkinta -opintojakson pakkokeinot ja tiedonhankinta -osajaksoon (laajuus 3,5 opintopistettä).

4.7.3 Kyberalaan liittyvä tutkimus

Polamkin tutkimus- ja kehitys suuntautuu laajempaan turvallisuuskäsitykseen, missä osana on kybermaailma ja siihen liittyvät ilmiöt sekä uhat.

4.8 Tampereen ammattikorkeakoulu (TAMK)

4.8.1 Kyberalaan liittyvä opetus

Tampereen ammattikorkeakoulussa tietoteknisiin opintoihin on kaksi linjaa. Tieto- ja viestintätekniikan insinööriopinnoissa suuntautumisvaihtoehtoina ovat ohjelmistotekniikka, sulautetut järjestelmät ja elektroniikka, tietoverkot ja tietoliikennetekniikka sekä älykkäät koneet. Tietojenkäsittelyn tradenomiopinnoissa vaihtoehtoina ovat ohjelmistotuotanto, tietoverkkopalvelut, ICT-alan yrittäjyys, Web-palvelut sekä Game Production.

Lisäksi tarjolla ovat kyberturvallisuuden erikoistumisopinnot (30 op), englannin kielinen tietotekniikan insinöörikoulutus Software Engineering ja YAMK-tutkintokoulutukset. Mukana ovat tietojärjestelmäosaaminen, Information Technology sekä SOTE-alalle suunnattu hyvinvointiteknologia, joissa käsitellään tietoteknisiä asioita.

Talotekniikan ja sähkötekniikan opinnoissa on mukana kyberturvallisuuteen liittyviä opintoja ja tietosuoja-asioita.

4.8.2 Kyberalaan liittyvät kurssit

- 5G00BM49 Tietoturvan perusteet 4 op
- 4A00CN79 IP-verkkojen vianmääritys ja ylläpito 5 op
- 4A00CQ19 Verkon tietoturva 5 op
- 4A00CQ30 Tietoturvan yleiset perusteet 3 op
- 4A00DM18 Kyberturvallisuuden perusteet 3 op
- Kyberturvallisuustoiminnot 5 op
- Johdatus tietoturvalliseen ohjelmistotuotantoon 3 op
- Johdatus kyberturvallisuuteen 3 op
- Tietoturvalliset järjestelmät 5 op
- Turvalliset tietoverkot 5 op
- Tietoliikennetekniikan ja -verkkojen uudet suuntaukset 5 op
- Introduction to Cybersecurity 5 op

Erikoistumiskoulutuksen opintojaksot:

- Johdatus kyberturvallisuuteen 5 op
- Tunkeutumistestaus ja haavoittuvuusanalyysi 5 op
- Verkkopalveluiden ja palvelinten kyberturvallisuus 5 op
- Tietoverkkojen kyberturvallisuus 5 op
- Tietosuoja ja kyberturvallisuuteen liittyvä juridiikka 5 op
- Kehitystehtävä 5 op

4.8.3 Kyberalaan liittyvä tutkimus

Tampereen ammattikorkeakoulun tutkimuksen painoaloja ovat:

- Energiatehokas ja terveellinen rakennettu ympäristö
- Kehittyvä pedagoginen osaaminen
- Sosiaali- ja terveyspalvelujen uudet toimintamallit
- Yrittäjyys ja uusi liiketoiminta
- Älykkäät koneet ja laitteet

Digitalisaatio, älykkyys ja turvallisuus ovat vahvasti mukana TAMK:n tki-toiminnassa.

4.9 Turun ammattikorkeakoulu (TURKUAMK)

4.9.1 Kyberalaan liittyvä opetus

Turun ammattikorkeakoulu tarjoaa mm. tieto- ja viestintätekniikan insinöörikoulutusta sekä tietojenkäsittelyn tradenomikoulutusta. Molemmissa tietoturva on osana koulutusta. Insinööriopinnoissa osaamispolkuna on valittavissa Tietoverkkojen ja kyberturvallisuuden -suunta. Tradenomiopinnoissa on mukana hallinnollinen ja sovellusten tietoturva. Tutkintoon johtavan koulutuksen lisäksi TurkuAMK tarjoaa kyberturvallisuuden erikoistumiskoulutusta, jonka laajuus on 30 op YAMK-tasoisia opintojaksoja.

4.9.2 Kyberalaan liittyvät kurssit

- 5051215 Tietoverkkojen ja tietoturvan perusteet 5 op
- 5051252 Tietoturva ja tietosuoja 5 op
- 5051244 Information Security Testing and Assessment 5 op
- 5051245 Operational Security 5 op
- 3011580 Data protection and Privacy 5 op
- 3011366 Information Security 5 op
- 3011640 Application Security 5 op
- 3011369 Information Security Risk Management 5 op
- 3011468 Network Security 5 op

Kyberturvallisuuden erikoistumiskoulutuksen (30 op) kuuluvat kurssit ovat:

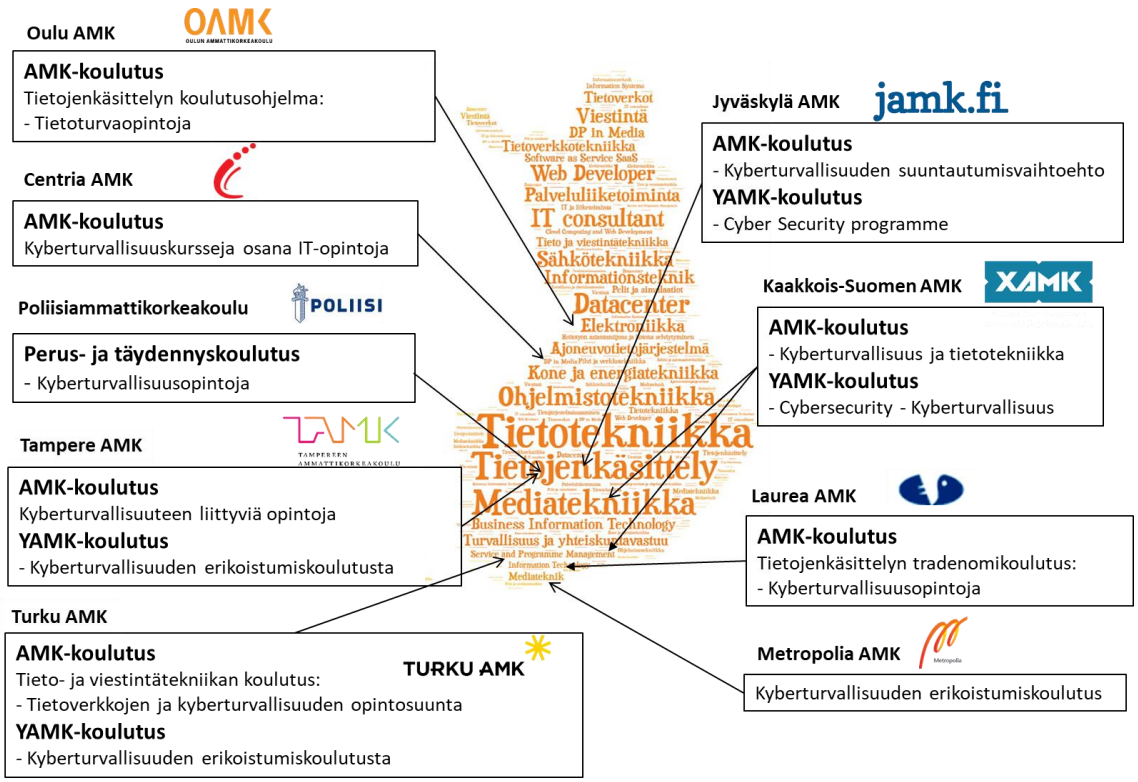
- Johdanto kyberturvallisuuteen 5 op
- Hyökkäävä kyberturvallisuus 5 op
- Puolustava kyberturvallisuus 5 op
- Tietoverkkojen kyberturvallisuus 5 op
- Kyberturvallisuus ja liiketoiminta 5 op
- Kyberturvallisuuden projekti 5 op

4.9.3 Kyberalaan liittyvä tutkimus

TurkuAMK:n tutkimus, kehitys ja innovaatiot sisältävät tietoliikenteen ja tietoturvan tutkimusta. Siellä liiketoimintaan liittyvät tietojärjestelmät, -verkot ja niiden tietoturva ovat tutkimuksen keskiössä.

Tutkimushankkeissa kehitetään Salon IoT Campukselle IoT-laitteiden ja -järjestelmien kyberturvallisuuden testauslaboratoriota. Tutkimuksessa TurkuAMK pyrkii profiloitumaan langattoman teknologian kyberturvallisuuteen.

Kuviossa 7 on esitetty kyberturvallisuuden koulutus ammattikorkeakouluissa.



KUVIO 7 Kyberturvallisuuden opetus ammattikorkeakouluissa

5 MUU KOULUTUS

5.1 Puolustusvoimien varusmieskoulutus

Puolustusvoimien johtamisjärjestelmäkeskus kouluttaa kybervarusmiehiä, joille annetaan peruskoulutus mm. tietoturvatestauksesta, tietoliikenteestä ja blue team vs. red team -harjoitustoiminnasta.[77]

Kybervarusmiehen tehtävässä osallistutaan blue team vs. red team -harjoitustoimintaan, rakennetaan palveluita ja testataan niiden turvallisuutta sekä suoritetaan ohjelmointiprojekteja. Parhaat edellytykset tehtävään antaa tieto-, tietoliikenne- tai tietoturvatekniikan perusteiden osaaminen niin teoriassa kuin käytännössä ja tietotekninen harrastuneisuus. Kybervarusmiespalvelus antaa hyvät valmiudet tietoturva-alalla työskentelyyn ja monet ovat työllistyneet kehitys-, ylläpito- tai testaustehtäviin.[78]

5.2 Maanpuolustuskoulutusyhdistys (MPK)

Kyberkoulutus on yksi MPK:n uusimmista koulutusmahdollisuuksista. Koulutus perustuu kolmeen kurssitasoon: Peruskursseille voivat tulla kaikki, ilman ennakkotietoja. Jatko- ja erikoistason kursseilla tarvitaan jo pohjatietoa, joka voi olla esimerkiksi siviiliammatin kautta hankittua tai MPK:n omalta, nousujohteiselta kurssipolulta saatua. Kyberturvallisuuskoulutus nähdään laajana kokonaisuutena ja se kattaa muun muassa elektronisen sodankäynnin, informaatioturvallisuuden ja tietoturvallisuuden.[79]

Kyberturvallisuuskoulutuksessa on tarjolla seuraavia kursseja:

- Informaatioturvallisuuskurssi
- Tietoturvakurssi
- Kansalaisen kyberturvallisuus
- Kyberturvallisuuden peruskurssi
- Kyberkurssi lukiolaisille
- Kyber-jatkokurssi 1 / SOC tier 1 - poikkeamien havainnointi
- Kyber-jatkokurssi 2 / SOC tier 2 - poikkeamien hallinta
- OSINT (Open Source Intelligence)

[77] https://varusmies.fi/palvelustehtavat-ja-paikat/-/services/506
[78] Ibid.
[79] https://mpk.fi/koulutukset/kyberturvallisuus/

5.3 Yritysten tuottama kyberturvallisuuskoulutus

Ohessa on esimerkinomaisesti kuvattu muutamien yksityisten yritysten tuottamaa kyberturvallisuuskoulutusta.

5.3.1 AlmaTalent[80]

Alma Talent tuottaa asiantuntijoille koulutuksia, kirjallisuutta ja sisältöpalveluja ammattitaidon ylläpitoon ja kehittämiseen. Alma Talent on asiantuntijoille suunnattujen koulutusten ja seminaarien palveluntuottaja. Aihealueina ovat juridiikka, robotiikka, ICT, talous- ja henkilöstöhallinto, markkinointi, viestintä ja esimiestyö.

Esimerkkeinä tieto/kyberturvallisuutta käsitteleviä koulutuksia ovat:

- Tietosuojavastaavan koulutusohjelma
- Kyberrikollisuuden menetelmät
- Kyberjohtaja

5.3.2 Cyber Security Academy

Cyber Security Academy on yhdistelmä tietoturvakoulutusta ja käytännön työssäoppimista. Koulutus muodostuu lähiopetuksesta, itsenäisestä opiskelusta sekä työssäoppimisesta yhteistyöyrityksessä. Ohjelman aikana voi myös suorittaa CompTIA Security+ -sertifioinnin. Koulutusohjelma on tarkoitettu ICT-alan osaajille, jotka haluavat päivittää osaamistaan ja löytää uuden työpaikan.[81]

5.3.3 CyberWatch

Cyberwatch Finland tuottaa kybermaailmasta strategisia tilannekuva-analyyseja, jotka asiantuntijat muodostavat avoimista lähteistä tekoälyn avustuksella. Johtavat asiantuntijat jalostavat ne erityisesti suomalaisille päättäjille hyödyllisiksi havainnoiksi ja johtopäätöksiksi. Lisäksi Cyberwatch Finland tarjoaa e-koulutuspalveluita ja konsultointia kybertietoisuuden ja -osaamisen parantamiseksi kaikilla organisaation tasoilla. Kyberjohtamisen peliharjoituksen avulla tuotetaan osaamista kyberturvallisuuden strategisella tasolla. Heillä on mahdollisuus tarjota myös yrityskohtaisesti räätälöityjä koulutuspaketteja.[82]

[80] https://www.almatalent.fi/koulutukset
[81] http://www.rekrytointikoulutus.fi/cyber-security-academy/
[82] https://www.cyberwatchfinland.fi/koti/

5.3.4 F-Secure[83]

F-Secure ja Helsingin yliopisto jatkavat yhteistyötään kyberturvallisuuskoulutuksessa. F-Securen ja Helsingin yliopiston avoin tietoturvaverkkokurssi (MOOC) auttaa tulevaisuuden tietoturva-asiantuntijoita löytämään potentiaalinsa opintokurssin **Cyber Security Base:n** avulla. Kurssi on suunniteltu antamaan opiskelijoille tietoturva-alan vaatimat käytännön taidot ja tiedot, ja se hyödyntää yritysten ja asiantuntijoiden kehittämiä aitoja menetelmiä. Cyber Security Base paketoi F-Securen ja Helsingin yliopiston tietojenkäsittelytieteen laitoksen osaamisen helposti omaksuttavan verkkokurssin muotoon. Kurssisisältö sisältää laajan valikoiman aiheita, jotka tietoturvaosaajan täytyy hallita. Kurssiin kuuluu myös hakkerointitehtäviä sekä muita käytännön harjoituksia, joiden avulla opiskelijat pääsevät soveltamaan oppimaansa käytännössä.

Vuonna 2016 ensimmäistä kertaa järjestetty kurssi on kiinnostanut kymmeniä tuhansia opiskelijoita ympäri maailmaa, ja sen ovat läpäisseet sadat ihmiset, joista osa on saanut yliopistotutkintoon vaadittavia opintopisteitä. Vaikka kurssin ensisijainen tavoite on varustaa yliopisto-opiskelijat perustason tietoturvaosaamisella, siitä hyötyvät myös jo työelämässä olevat IT-osaajat, jotka haluavat lisäoppia tietoturvasta.

5.3.5 Nixu Oyj

Yritykset ovat lähteneet kasvattamaan tulevaisuuden osaajia harjoitteluohjelmansa avulla. Kasvustrategiaansa tukeakseen Nixu etsii jatkuvasti joukkoonsa niin kokeneita kuin uransa alkuvaiheessa olevia kyberturvaosaajia. Nixulla huippuammattilaisista koostuva henkilöstö nähdään elintärkeänä kilpailuvalttina globaalilla pelikentällä ja yhtiössä halutaan edistää päämäärätietoisesti uusien asiantuntijoiden kasvattamista alalle. Nixun arvojen mukaisesti intohimo kyberturvallisuuteen on kuitenkin edellytys tuleville ammattilaisille, ja tämä ominaisuus löytyy usein muiden kanavien kuin perinteisen koulutusputken kautta.

Hyvä esimerkki oman harrastuneisuuden merkityksestä alalla ovat tapahtumat, kuten Disobey, joissa on mahdollista tavata taitavia nuoria harrastajia. Näillä nuorilla on suuri potentiaali toimia tulevaisuudessa eettisen hakkeroinnin parissa kyberturvallisuuden alalla.

Nixu Challenge -harjoitteluohjelma antaa nuorille mahdollisuuden päästä työskentelemään aitoihin kyberturva-alan töihin Nixun kokeneiden huippuammattilaisten rinnalla. Haku harjoitteluohjelmaan käynnistyy teknisen haasteen ratkaisemisella, jonka avulla hakijat osoittavat tekniset taitonsa ja ongelmanratkaisukykynsä.[84]

[83] https://fi.press.f-secure.com/2018/11/06/suosittu-maksuton-kyberturvallisuuden-verkkokurssi-kaynnistyy-kolmannen-kerran/
[84] https://thenixuchallenge.com/entry/

5.3.6 Saranen Consulting

Data Protection Specialist -koulutusohjelman kautta kehittymishaluisia osaajia ovat kouluttamassa ja rekrytoimassa mm. Azets Insight, E-It, Fiarone, Granite, GRC Nordic, Iodata, Midpointed, Multi Support, Tieto sekä useat muut yritykset. Data Protection Specialist koulutusohjelmassa opiskelijan ja rekrytoivan yrityksen välille tehdään puolen vuoden koulutussopimus, jonka tavoitteena on työsopimus ohjelman jälkeen. Koulutusaiheita ovat mm. tietosuoja-asetuksen (GDPR) perusperiaatteet, henkilötietojen käsittely, tietoturvallisuuden hallinta osana yritysturvallisuutta, tietoturvalainsäädäntö sekä kansalliset tietosuojaa ja tietoturvaa koskevat lait. [85]

5.3.7 Siverskin[86]

Silversikin Academy tarjoaa tietoturvatietoisuutta lisääviä koulutuksia työntekijöille sekä tarkasti kohdennettua tietoturvakoulutusta hallinnolle sekä teknisille spesialisteille. Awareness-harjoitukset kehittävät yksilön motivaatiota ja kykyä havaita kyberriskejä sekä toimia turvallisesti arjessa.

Hallinnolle ja asiantuntijoille räätälöidyt koulutukset on suunniteltu kehittämään organisaation kyvykkyyttä ja taitoja puolustautua. Koulutuksen seurauksena niin organisaation hallintotavat kuin tekninen osaaminenkin kehittyvät kohti parempaa kyberhyökkäysten vastustuskykyä.

Top 10 Academy-kurssia ovat:

- Cyber Stalking and Reconnaissance
- Cyber Attacks and Offensive Measures
- Cyber Security Management
- Investigations, Audits and Compliance
- Secure Software Development
- Cyber Security Awareness
- GDPR Compliance
- Secure Web Application Development
- Secure Agile Project Management
- Secure Mobile Development

[85] http://www.rekrytointikoulutus.fi/avoimet-tehtavat/10-tietoturva-asiantuntijaa-projektipaallikkoa/
[86] https://www.silverskin.com/fi/academy.html

6 MUU TUTKIMUSTOIMINTA

6.1 Tietotekniikan tutkimuslaitos[87]

Helsinki Institute for Information Technology (HIIT) on Aalto-yliopiston ja Helsingin yliopiston yhteinen tutkimuslaitos. Tutkimuksen fokuksessa on tietokonemallintaminen ja data-analyysi sekä kaikkialla oleva ICT sekä niiden vaikutus ihmisiin ja yhteiskuntaan.

HIIT tukee seuraavia tutkimuskeskuksia ja -ohjelmia:

- Finnish Center for Artificial Intelligence (FCAI)
- Foundations of Computational Health (FCHealth)
- HAIC Research Program (HAIC-R)
- Helsinki Centre for Data Science (HiDATA)

HAIC (Helsinki-Aalto Center for Information Security) on Aalto-yliopiston ja Helsingin yliopiston kesäkuussa 2016 perustama strateginen aloite tietoturvallisuuden tutkimuksen ja koulutuksen huippuosaamisen varmistamiseksi. Viime vuosina Aalto-yliopisto ja Helsingin yliopisto ovat luoneet vahvat tutkimusryhmät ja koulutusohjelmat tietoturvallisuuteen ja yksityisyyden suojaan liittyen. HAIC:n tutkimusyksikön tehtävä vuoteen 2025 mennessä on mahdollistaa hajautettujen suurten järjestelmien suunnittelu, rakentaminen ja käyttöönotto, jossa kukin solmu (komponentti, laite, verkkoelementti jne.) auttaa varmistamaan koko järjestelmän luotettavuuden. Jokainen solmu voisi myös tarkistaa, onko jokin muu solmu tai jopa koko järjestelmä luotettava.

6.2 Valtion teknillinen tutkimuslaitos[88]

Valtion teknillinen tutkimuslaitos (VTT) tarjoaa kyberturvallisuustestausta ja riskianalyysejä, jotka varmistavat laitteen tai ohjelmiston tietoturvallisuuden elinkaaren kaikissa vaiheissa – suunnitteluvaiheen vaatimuksista käytönaikaiseen ylläpitoon. VTT:n tarjoamat palvelut auttavat varmistamaan teollisen tuotannon kyberturvallisuuden ja häiriöttömän jatkuvuuden. VTT tarjoaa teollisen tuotannon kyberturvallisuuskartoituksia, kybersuojaustason parannussuunnitelman ja kybersuojauksen toteutuksen. Lisäksi VTT auttaa rakentamaan turvallisia sulautettuja järjestelmiä. VTT suunnittelee ja toteuttaa turvalliset ympäristöt eri laitteille kuten älypuhelimille, reitittimille, ympäristöantureille tai älykkään sähköverkon komponenteille.

VTT:llä on laaja kyberturvallisuuden tutkimusryhmä Suomessa. Ryhmä tarjoaa tutkimus- ja tuotekehityspalveluita asiakkailleen mm. seuraavilla osa-alueilla:

- Teollisuusautomaation tietoturva

[87] https://www.hiit.fi/research/
[88] https://www.vtt.fi/palvelut/digitaalinen-maailma/kyberturvallisuus

- Tietoturvan mittaaminen ja mittareiden kehitys
- Tunkeutumisen havainnointi
- Mukautuvat tietoturvaratkaisut
- Tietoturvan varmistaminen ja testaus
- Tietoturvalliset alustat
- Tietoliikenteen tietoturva sekä yksityisyydensuoja

Ryhmän laaja-alainen kokemus kyberturvallisuuden tutkimuksesta sekä pitkäaikainen yhteistyö sitä soveltavien ja hyödyntävien yritysten kanssa mahdollistavat kyvyn ymmärtää ja soveltaa ajantasaisia tutkimustuloksia asiakkaiden tarpeisiin.

6.3 Puolustusvoimien tutkimuslaitos[89]

Puolustusvoimien tutkimuslaitos (PVTUTKL) on monitieteinen organisaatio, joka tuottaa vaativia puolustusalan tutkimus-, kehittämis- ja testauspalveluja strategian ja sotataidon sekä käyttäytymistieteiden ja useiden eri teknologioiden alueille.

Informaatiotekniikkaosasto Riihimäellä on yksi laitoksen viidestä osastosta. Osasto tukee Puolustusvoimien yhteisten suorituskykyjen rakentamista ja tuottaa tutkittua tietoa tukemaan taistelua verkosta ja spektristä. Informaatiotekniikkaosasto tutkii:

- Radiotaajuisia sensori- ja vaikuttamisjärjestelmiä
- Elektronista sodankäyntiä
- Tietoverkkosodankäyntiä
- Johtamisjärjestelmiä

Osasto tarjoaa laskennallisen tieteen ja mallinnuksen asiantuntijaosaamista sekä laskenta- ja järjestelmälaboratorion palveluita.

[89] https://puolustusvoimat.fi/tietoa-meista/tutkimuslaitos

7 KYBERALAN KOULUTUS YHDYSVALLOISSA

7.1 Katsaus

Kiinnostavaa on selvittää millaista kyberkoulutusta muissa maissa annetaan. Benchmarking-näkökulmasta tehtiin analyysi käyttäen 112 maisteritason kyberturvallisuuskoulutusta antavan Yhdysvaltain yliopiston ja collegen tietoja. Ne tarjoavat yhteensä 120 erilaista kyberturvallisuuden maisteriohjelmaa.

Tämän tutkimuksen perusteella yhdysvaltalaiset maisteriohjelmat voidaan jakaa kolmeen kokonaisuuteen. Ensimmäisen kokonaisuuden muodostavat kyberturvallisuuden tai informaatioturvallisuuden maisteriohjelmat. Ohjelmat ovat kokonaisuudessaan keskittyneet kyberturvallisuuteen tai informaatioturvallisuuteen kuten Jyväskylän yliopistossa. Osa ohjelmista ovat erityisesti suuntautuneet kyberturvallisuuden hallintaan tai yksityisyyden suojaan.

Toinen kokonaisuus koostuu kybersuuntautuneista maisteriohjelmista eri informaatioteknologian alueilla kuten tietojenkäsittelytieteessä, tietojärjestelmätieteessä ja tietotekniikassa. Näissä tapauksissa kyberturvallisuutta lähestytään kunkin tieteenalan näkökulmasta ja koulutusohjelmissa on mukana tieteenalaan perustuvaa tutkimusta.

Kolmas koostuu kyberturvallisuuteen keskittyneistä maisteriohjelmista muilla tieteenaloilla kuten hallintotieteet, kauppa- ja taloustieteet, laskentatoimi ja oikeustiede.

Tutkitut 120 maisteriohjelmaa jakautuivat seuraavasti:

- MSc In Cyber Security 35 ohjelmaa
- MSc In Computer Science (CS) 37 ohjelmaa
- MSc in Information Systems (IS) 13 ohjelmaa
- MSc In Information Technology (IT) 7 ohjelmaa
- MSc In Computer Engineering (CE) 13 ohjelmaa
- MSc In Information Assurance (IA) 5 ohjelmaa
- Other disciplines + Cyber security 10 ohjelmaa

Tutkimuksessa kävi ilmi, että kyberturvallisuuden maisterikoulutuksessa ei ole yhtenäistä tai yleistä opetussuunnitelmaa. Sitä opetetaan monien eri tieteenalojen pohjalta ja opetusohjelmilla on hyvin erilainen painotus. Lisäksi yliopistoilla on omat painopistealueensa riippuen niille tärkeistä kohde- tai sidosryhmistä. Kyberturvallisuuteen fokusoituneiden maisteriohjelmien kaikille yhteisenä ja yleisenä tavoitteena on kehittää tarvittavia kyvykkyyksiä, joita tarvitaan suojaamaan organisaation elintärkeitä toimintoja (engl. assets) tai aineettomia oikeuksia (engl. Intellectual Property Rights, IPR).

Seuraavissa alaluvuissa on kuvattu englanniksi kukin maisteriohjelman keskeinen sisältö esimerkkien avulla. Opintopisteiden osalta yleissääntönä voidaan pitää, että 1 opintopiste = 0.5 US Credit.

7.2 MSc in Cyber Security

An MSc in Cyber Security digs deeper into the security issues addressed in a bachelor's degree. This includes methods related to data integrity, disaster recovery, business continuity planning and risk management. Courses might deal with advanced tools and techniques (e.g. forensics, cryptography/cryptanalysis) and important organizational practices (e.g. access control). Universities often make a point of emphasizing technical skills instead of theoretical concepts.

Example: Webster University

MSc in Cybersecurity: The 39 credit hours required for the MSc degree in cybersecurity must include the required core courses.

Program Curriculum:

Core Courses (21 credits):

- CSSS 5000 Introduction to Cybersecurity (3 credits)
- CSSS 5110 Cybersecurity Communications (3 credits)
- CSSS 5120 Cybersecurity Infrastructures (3 credits)
- CSSS 5130 Cybersecurity Intelligence/Counterintelligence (3 credits)
- CSSS 5140 Cybersecurity Strategic Operations (3 credits)
- CSSS 5160 Encryption Methods and Techniques (3 credits)
- CSSS 6001 Practical Research in Cybersecurity (3 credits)

Elective Courses (18 credits), 4 elective courses chosen from the following:

- CSSS 5210 Cybersecurity Law and Policy (3 credits)
- CSSS 5220 Cybersecurity Threat Detection (3 credits)
- CSSS 5230 Cybersecurity Forensics (3 credits)
- CSSS 5240 Pre-emptive Deterrence (3 credits)
- CSSS 5250 Use and Protection of Space Assets (3 credits)
- CSSS 5270 Cybersecurity in Cloud Computing (3 credits)
- CSSS 5280 Social Engineering (3 credits)
- CSSS 5990 Advanced Topics in Cybersecurity (3 credits)
- CSSS 6500 Cybersecurity Internship (3 credits)

7.3 MSc in Computer Science (CS)

Instead of creating a separate degree program in cyber security, some universities have chosen to stick with an MS in Computer Science and offer an elective/concentration in security. First the student might be required to complete high-level computing courses

(e.g. programming, algorithm analysis, operating systems, software engineering) before student are allowed to concentrate on subjects like cryptography/cryptanalysis, network security and digital forensics.

Example: Southern Connecticut State University

MS in Computer Science, Network and Information security program sequence: The Master of Science degree in Computer Science is a 36-credit program in which all students must complete 30 credits of course work in addition to a 6-credit capstone requirement.

Program Curriculum:

Required Core Requirements (12 credits):

- CSC 540 Database Systems (3 credits)
- CSC 543 Web Programming (3 credits)
- CSC 563 Multithreaded Distributed Programming (3 credits)
- CSC 565 Computer Networks (3 credits

Concentration Requirements (12 credits):

- CSC 555 Principles of Information Security (3 credits)
- CSC 558 Network Security (3 credits)
- CSC 568 Ethical Hacking and Penetration Testing (3 credits)
- CSC 578 Secure Systems (3 credits)

7.4 MSc in Information Systems (IS)

Some universities offer an interdisciplinary Master of Science in Information Systems and Cyber Security, IS and Security Management, and IS and Information Assurance. The education is interdisciplinary and includes courses in subjects ranging from business and public policy and management to human-computer interaction. Curriculum is drawn from fields such as accounting, economics, finance, management, and information systems.

Example: Pennsylvania State University

MS in Information Systems and Technology – Security Focus: The MS in IST is a 30-credit degree program, which takes two years to complete on a full-time basis.

Program Curriculum:

Core courses (6 credits):

- IST 504 Foundations of Theories and Methods of Information Sciences (3 credits)
- IST 505 Foundations of Research Design in Information Sciences and Technology (3 credits)

Specialty courses: complete a minimum of 12 credits of specialty area coursework. A specialty area course could be in IST, law, business, education, engineering, the liberal arts or any area that is linked to the information sciences.

A. Cybersecurity Concentration
Sample Courses (minimum 12 credits):

- IST 543 Foundations of Software Security (3 credits)
- IST 554 Network Management and Security (3 credits)
- IST 564 Crisis, Disaster, and Risk Management (3 credits)
- IST 815 Foundations of Information Security and Assurance (3 credits)
- IST 820 Cybersecurity Analytics (3 credits)

B. Data Sciences Concentration
Sample Courses:

- IST 557 Data Mining: Techniques and Applications, (3 credits)
- IST 558 Data Mining II, (3 credits)
- IST 597 Special Topics: Machine Learning (3 credits)
- STAT 500 Applied Statistics (3 credits)

C. Human-Centered Design Concentration
Sample Courses:

- IST 520 Foundations in Human-Centered Design (3 credits)
- IST 521 Human-Computer Interaction: The User and Technology (3 credits)
- IST 525 Computer-Supported Cooperative Work (3 credits)
- IST 526 Development Tools and Visualizations for Human-Computer Interaction (3 credits)

7.5 MSc in Computer Engineering (CE)

Like the MSc in Computer Science, this is a general degree where student can choose to specialize in cyber security. Computer engineering degrees are concerned with both hardware development (e.g. microelectronics, digital systems) and software development. So in the case of security, courses might focus on topics like microprocessor and embedded systems, advanced data structures, security software development, reverse engineering and network security.

Example: University of Washington

MSc in Cyber Security Engineering: To fulfill degree requirements, students must complete a total of 51-54 credits of coursework including: core (31-34 credits), electives (10 credits) and project or thesis (10 credits).

Program Curriculum:

Core courses (31-34 credits):

- CSS 517 Information Assurance and the Secure Development Lifecycle (5 credits)
- CSS 519 Incident Response and Risk Management (5 credits)
- CSS 527 Cryptography and Information Assurance (5 credits)
- CSS 537 Network and System Security (5 credits)
- CSS 577 Secure Software Development (5 credits)
- CSS 578 Ethical Penetration Testing (5 credits)

Elective courses (minimum 10 credits):

- CSS 579 Malware and Attack Reverse Engineering (5 credits)
- CSS 538 Security in Emerging Wireless and Mobile Networks (5 credits)
- CSS 539 Cyber Security in Emerging Environments (5 credits)
- CSS 545 Mobile Computing (5 credits)
- CSS 553 Software Architecture (5 credits)
- CSS 581 Machine Learning (5 credits)
- CSS 600 Independent Study or Research (1-5, max. 6 credits)

7.6 MSc in Information Technology (IT)

Although it's not a hard and fast rule, an MSc in Information Technology with a concentration in security tends to be a little less technical and a little more MBA than a degree like CS and Cyber Security. This is a qualification that CTOs and IT Managers may be interested in. Courses often deal with security risks, regulatory issues, organizational objectives and IT best practices.

Example: University of Kansas

Master of Science in Information Technology (MSIT) with a focus area in information security and assurance has three focus areas: Cyber security, Software Engineering and IT Project Management

A. Focus area: Cyber Security
Core courses:

- IT710: Information Security and Assurance

- IT711: Security Management and Audit
- IT712: Network Security
- IT780: Communication Networks
- IT811: IT Project Management

Electives course: five of the following courses:

- IT746: Database Management Systems
- IT714: Information Security and Cyber Laws
- IT810: Principles of Software Engineering
- IT814: Software Quality Assurance
- IT818: Software Architecture
- EMGT806: Finance for Engineers
- EMGT821: Strategic Analysis of Technology Projects

B. Focus area: Software Engineering
Core courses:

- IT810: Principles of Software Engineering
- IT814: Software Quality Assurance
- IT818: Software Architecture
- IT780: Computer Networks
- IT811: IT Project Management

Electives course: five of the following courses:

- IT746: Database Management Systems
- IT710: Information Security and Assurance
- IT714: Information Security and Cyber Laws
- IT711: Security Management and Audit
- IT712: Network Security
- EMGT806: Finance for Engineers
- EMGT821: Strategic Analysis of Technology Projects

C. Focus area: IT Project Management
Core courses:

- IT811: IT Project Management
- IT711: Security Management and Audit
- EMGT806: Finance for Engineers
- EMGT821: Strategic Analysis of Technology Projects
- IT810: Principles of Software Engineering

Electives course: five of the following courses:

- IT746: Database Management Systems

- IT710: Information Security and Assurance
- IT712: Network Security
- IT714: Information Security and Cyber Laws
- IT780: Communication Networks
- IT814: Software Quality Assurance
- IT818: Software Architecture

7.7 MSc in Information Assurance (IA)

Information assurance and cyber/information security are usually paired together in degree titles (e.g. MS in Information Assurance and Security). Information assurance is concerned with both the technical and managerial aspects of protecting and controlling information and information systems. In addition to technical courses on forensics, auditing, intrusion detection, etc., student may be examining security policies, best practices, cyber law and other management issues.

Example: Oklahoma State University

M.S. in Information Assurance (MSIA): Core classes engage the student in the study of information assurance, both from a hands-on technical approach and from a business-oriented managerial perspective. The MSIA program is a minimum 35-36 credit hour program includes 30 hours of core of courses and 5-6 credits of electives in approved courses (this may include an approved internship or practicum).

Program Curriculum:

Core courses (30 credits):

- ECEN 5553 Telecommunications Systems (3 credits)
- MSIS 5213 Information Assurance Management (3 credits)
- MSIS 5773 The Upper Layers of Telecommunications Systems (3 credits)
- MSIS 5233 Applied Information Systems Security (3 credits)
- MSIS 5713 Scripting Essentials (3 credits)
- MSIS 5253 Advanced System Certification and Accreditation (3 credits)
- MSIS 5273 Legal and Ethical Issues in Information Technology (3 credits)
- MSIS 5263 Information Assurance Offense (3 credits)
- MSIS 5283 Secure Information Systems Administration (3 credits)
- MSIS 5293 Information Assurance Capstone (3 credits)

In addition, elective courses (minimum 5-6 credits), credit courses of electives in business or other appropriate disciplines

7.8 Yhteenveto maisteriohjelmista

Analyysiin on käytetty tietoja 112 yhdysvaltalaisesta yliopistosta ja collegesta. Ne tarjoavat 120 eri sisältöistä ja eri tyyppistä kyberturvallisuusalan maisteriohjelmaa. Taulukossa 1 on esitetty maisteriohjelmien taksonomia:

TAULUKKO 1 Yhteenveto maisteriohjelmista

Maisteriohjelman tieteenala	**Maisteriohjelma**	**Maisteriohjelmien määrä**
MSc In Cyber Security		
	Cyber/Information security	29
	Cyber security Management	4
	Cyber security and privacy	2
MSc In Computer Science (CS)		
	Computer Science + Cyber security	19
	Computer Science + Information Assurance	7
	Computer Science + Forensic	3
	Computer Science + Network security	8
MSc in Information Systems (IS)		
	Information Systems + Cyber security	3
	Information Systems + Information Assurance	6
	Information Systems + Cyber security management	4
MSc In Information Technology (IT)		
	Information Technology + Cyber Security	7
MSc In Computer Engineering (CE)		
	Computer Engineering + Cyber Security	13
MSc In Information Assurance (IA)		
	Information Assurance	5
Other disciplines + Cyber security		10

LÄHTEET

Aalto yliopisto (2018a). Koulutus. Haettu osoitteesta http://www.aalto.fi/fi/studies/education/.

Aalto yliopisto (2018b). Tutkimus. Haettu osoitteesta http://comnet.aalto.fi/en/research/.

Allied ICT Finland (2019). CyberSec^{FIN} -kyberturvallisuusekosysteemin strategia: Kyberturvallisuus Suomessa 2019-2029, valmisteilla oleva raportti toukokuu 2019

Centria ammattikorkeakoulu (2018a). Koulutus. Haettu osoitteesta https://soleops.cou.fi/opsnet/disp/fi/ops_KoulOhjOps/tab/tab/sea?ryhma_id=5303193&koulohj_id=2003952&valkiel=en&stack=push.

Centria ammattikorkeakoulu (2018b). Tutkimus. Haettu osoitteesta https://tki.centria.fi/hankkeet/digitalisaatio.

European Commission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final

EU komissio, Unionin tila 2017 – Kyberturvallisuus, Bryssel 19. syyskuuta 2017

EU parlamentti (2019). Lainsäädäntöpäätöslauselma ehdotuksesta asetukseksi EU:n kyberturvallisuusvirasto ENISAsta, ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”), Bryssel, 12.3.2019

Eurooppa neuvosto, EU yhdistää ja verkostoi kyberturvallisuusosaamistaan, tiedote 13.3.2019, https://www.consilium.europa.eu/fi/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/

Helsingin yliopisto (2018a). Koulutus. Haettu osoitteesta https://www.helsinki.fi/fi/koulutustarjonta.

Helsingin yliopisto (2018b). Tutkimus. Haettu osoitteesta https://www.helsinki.fi/fi/tietojenkasittelytiede/tutkimus.

(ISC)² (2018). Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens Cybersecurity Workforce Study, October 17, 2018, www.isc2.org/research

Itä-Suomen yliopisto (2018a). Tietojenkäsittelytieteiden laitos. Koulutus. Haettu osoitteesta http://www.uef.fi/fi/web/cs/cs .

Itä-Suomen yliopisto (2018b). Tietojenkäsittelytieteiden laitos. Tutkimus. Haettu osoitteesta http://www.uef.fi/web/cs/tutkimus.

Jyväskylän ammattikorkeakoulu (2018a). Insinööri, tieto- ja viestintätekniikka. Koulutus. Haettu osoitteesta https://www.jamk.fi/fi/Koulutus/tekniikan-ala/insinoori-tieto-ja-viestintatekniikka/.

Jyväskylän ammattikorkeakoulu (2018b). Tutkimus. Haettu osoitteesta https://www.jamk.fi/fi/Tutkimus-ja-kehitys/vahvuusalat/Kyberturvallisuus/.

Jyväskylän yliopisto (2018a). Koulutus. Haettu osoitteesta https://www.jyu.fi/it/fi.

Jyväskylän yliopisto (2018b). Tutkimus. Haettu osoitteesta https://www.jyu.fi/it/en/research.

Jyväskylän yliopisto (2018c). Tutkimus, kyberturvallisuus. Haettu osoitteesta https://www.jyu.fi/it/en/research/research-areas/cyber-security.

Kaakkois-Suomen ammattikorkeakoulu (2018a). Cybersecurity – kyberturvallisuus, ylempi AMK. Koulutus YAMK. Haettu osoitteesta https://www.xamk.fi/koulutukset/insinoori-ylempi-amk-tieto-ja-viestintatekniikka/.

Kaakkois-Suomen ammattikorkeakoulu (2018b). Koulutus AMK. Haettu osoitteesta https://www.xamk.fi/koulutus/tutkinto-amk/.

Kaakkois-Suomen ammattikorkeakoulu (2018a). Koulutus YAMK. Haettu osoitteesta https://www.xamk.fi/koulutus/tutkinto-yamk/.

Kaakkois-Suomen ammattikorkeakoulu (2018b). Tutkimus. Haettu osoitteesta https://www.xamk.fi/digitaalisen-talouden-osaamiskarjet/.

Kyberturvallisuuden sanasto (2018), Turvallisuuskomitea, http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Lappeenrannan teknillinen yliopisto (2018a). Koulutus. Haettu osoitteesta https://www.lut.fi/opiskelu/kandidaattiohjelmat/tietotekniikka.

Lappeenrannan teknillinen yliopisto (2018b). Tutkimus. Haettu osoitteesta https://www.lut.fi/web/en/research.

Laukkarinen Emmi (2019). Kokonaisvaltaisen kyberturvallisuuskoulutuksen suunnittelussa huomioitavia tekijöitä, julkaisematon ITKST41-kurssiraportti

Laurea ammattikorkeakoulu (2018a). Koulutus. Haettu osoitteesta https://www.laurea.fi/opiskelu-ja-hakeminen/amk-tutkinnot/tietojenkasittely.

Laurea ammattikorkeakoulu (2018b). Tutkimus. Haettu osoitteesta https://www.laurea.fi/tutkimus-kehitys-ja-innovaatiot/tki-toiminta-laureassa/yhtenainen-turvallisuus.

Lehto M., Kähkönen A. (2015). Kyberturvallisuuden kansallinen osaaminen, Jyväskylän yliopisto, Informaatioteknologian tiedekunta, tutkimusraportti 20/2015

Lehto M. Limnéll J., Innola E., Pöyhönen J., Rusi T., Salminen M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, 17.2.2017, ISBN 978-952-287-368-2 (verkkoj.)

LVM (2016). Maailman luotetuinta digitaalista liiketoimintaa Suomen tietoturvallisuusstrategia, Liikenne- ja viestintäministeriön julkaisuja 7/2016, 19.4.2016

Maanpuolustuskorkeakoulu (2018a). Haettu osoitteesta http://maanpuolustuskorkeakoulu.fi/opiskelu

Maanpuolustuskorkeakoulu. (2018b). Opinto-opas 2018. Sotatieteiden kandidaatin tutkinto ja sen lisäksi suoritettavat sotilasammatilliset opinnot. 105./88. Kadettikurssi. Tampere. 2018. https://www.doria.fi/bitstream/handle/10024/161363/MPKK_SK_opintoopas_2018_web.pdf?sequence=1&isAllowed=y

Maanpuolustuskorkeakoulu. (2018c). Opinto-opas 2018. Sotatieteiden maisterin tutkinto. Upseerien koulutusohjelma SM9. Lentoupseerien koulutusohjelma SM LENTOUPS 18. Viranomaisyhteistyön koulutusohjelma SMVIR18. Tampere. 2018. https://www.doria.fi/bitstream/handle/10024/161145/MPKK%20Sotatieteiden%20maisterin%20tutkinnon%20opinto-opas_2018.pdf?sequence=1&isAllowed=y

Maanpuolustuskoulutusyhdistys, MPK (2018). Kyberturvallisuus. Haettu osoitteesta https://www.mpk.fi/Kyberturvallisuus.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. In 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, pp. 256-262

Niemelä J. (2019). Kyberturvallisuuden työvoiman tarve, saatavuus ja kehittäminen vastaamaan alan tarvetta Suomessa, pro gradutyö, Jyväskylän yliopisto, IT-tiedekunta, 2019

Oulun yliopisto (2018a). Koulutus. Haettu osoitteesta http://www.oulu.fi/yliopisto/hakijalle/kandidaatti-ja-maisterikoulutus.

Oulun yliopisto (2018b). Tutkimus. Haettu osoitteesta http://www.oulu.fi/tst/yksiköt.

Oulun yliopisto (2018c). Tutkimus. Haettu osoitteesta http://www.oulu.fi/matematiikka/tutkimus.

Oulun ammattikorkeakoulu (2018a). Koulutus. Haettu osoitteesta http://www.oamk.fi/opinto-opas/opintojen-sisalto/opetussuunnitelmat.

Oulun ammattikorkeakoulu (2018b). Tutkimus. Haettu osoitteesta https://www.oamk.fi/fi/tutkimus-ja-kehitys/hankkeet/

Poliisiammattikorkeakoulu (2018a). Koulutus. Haettu osoitteesta https://www.polamk.fi/amk/koulutus_ja_opiskelu.

Poliisiammattikorkeakoulu (2018b). Tutkimus. Haettu osoitteesta https://www.polamk.fi/tki/tutkimus.

Rekrytointikoulutus (2018). Cyber Security Academy. Haettu osoittteesta http://www.rekrytointikoulutus.fi/cyber-security-academy/.

Tampereen ammattikorkeakoulu (2018a). Tieto- ja viestintätekniikan koulutus. Haettu osoitteesta http://opinto-opas-ops.tamk.fi/index.php/fi/167/fi/49583.

Tampereen ammattikorkeakoulu (2018b). Tietojenkäsittelyn koulutus. Haettu osoitteesta http://opinto-opas-ops.tamk.fi/index.php/fi/167/fi/49535.

Tampereen yliopisto (2018a). Koulutus. Haettu osoitteesta http://www.tut.fi/opinto-opas/2018-2019.

Tampereen yliopisto (2018b). Tutkimus. Haettu osoitteesta https://www.tuni.fi/fi/tutkimus.

Tampereen yliopisto (2017). Tampereen uusi korkeakouluyhteisö syntyy vuoden 2019 alussa. Haettu osoitteesta http://www2.uta.fi/ajankohtaista/uutinen/tampereen-uusi-korkeakouluyhteiso-syntyy-vuoden-2019-alussa.

Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., & Dale, J. (2017). Teaching psychological principles to cybersecurity students. In 2017 IEEE Global Engineering Education Conference (EDUCON), pp. 17821789

TEM (2013). 21 polkua Kitkattomaan Suomeen, ICT 2015 -työryhmän raportti 4/2013, 17.1.2013

TEM (2019). Kasvua digitaalisesta turvallisuudesta - Tiekartta 2019–2030, Työ- ja elinkeinoministeriön julkaisuja 2019:17, 8.3.2019

Turku AMK (2018a). Koulutus. Haettu osoitteesta https://ops.turkuamk.fi/opsnet/disp/fi/ops_PuuHierValOpas/tab/nop/clr?menuid=2.

Turku AMK (2018b). Tutkimus. Haettu osoitteesta https://www.turkuamk.fi/fi/tutkimus-kehitys-ja-innovaatiot/tutkimusryhmat/tietoliikenne-ja-tietosuoja/.

Turun yliopisto (2018a). Koulutus. Haettu osoitteesta http://www.utu.fi/fi/yksikot/sci/opiskelu/koulutustarjonta/ohjelmat/Sivut/home.aspx.

Turun yliopisto (2018b). Tutkimus. Haettu osoitteesta https://tech.utu.fi/en/information-security-and-cryptography/.

Turvallisuuskomitea (2013). Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013

Turvallisuuskomitea (2017). Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, Turvallisuuskomitea, 10.4.2017

Turvallisuuskomitea (2019). Suomen kyberturvallisuusstrategia luonnos 1.0, 4.3.2019

Valtioneuvosto, U-kirjelmä, U1022018 vp, 10.1.2019

Varusmies (2018). Puolustusvoimat, palvelustehtävät, kybervarusmies. Haettu osoitteesta http://varusmies.fi/palvelustehtavat-ja-paikat/-/services/506.

VNK (2016). Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016, 15.02.2016

Willberg Nils (2017). Kyberosaamisen nykyiset ja tulevat tarpeet julkisen sektorin organisaatioissa, pro gradu -työ, Jyväskylän yliopisto, IT-tiedekunta, 2017

Verkkojulkaisut:
https://alliedict.fi/
https://eur-lex.europa.eu/legal-content/FI/HIS/?uri=COM%3A2018%3A0434%3AFIN
https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/U_69+2018.aspx
https://www.hiit.fi/research/
https://mpk.fi/koulutukset/kyberturvallisuus/
http://www.rekrytointikoulutus.fi/cyber-security-academy/
https://thenixuchallenge.com/entry/
https://www.almatalent.fi/koulutukset
https://www.cyberwatchfinland.fi/koti/
https://fi.press.f-secure.com/2018/11/06/suosittu-maksuton-kyberturvallisuuden-verkkokurssi-kaynnistyy-kolmannen-kerran/
http://www.rekrytointikoulutus.fi/avoimet-tehtavat/10-tietoturva-asiantuntijaa-projektipaallikkoa/
https://www.silverskin.com/fi/academy.html
https://www.vtt.fi/palvelut/digitaalinen-maailma/kyberturvallisuus
https://puolustusvoimat.fi/tietoa-meista/tutkimuslaitos

Informaatioteknologian tiedekunnan julkaisuja
No. 83/2019

ISBN 978-951-39-7829-7 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO