KYBERTURVALLISUUS SUOMALAISESSA PERUSOPETUKSESSA

Suomalaisessa peruskoulussa tapahtuvan kyberturvallisuuden opetuksen nykytila ja opetussuunnitelmien perusteiden tulevaisuuden suuntaviivat

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Insinööri opinnäytetyö

Tieto- ja viestintätekniikka

2022

Miiro Pyysing

Sari Kaipainen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikan koulutusohjelma
Tekijä Miiro Pyysing ja Sari Kaipainen
Työn nimi Kyberturvallisuus suomalaisessa perusopetuksessa
Ohjaaja Ismo Turve

Tiivistelmä
Vuosi 2022

Opinnäytetyön tavoitteena oli kerätä tietoa siitä, missä määrin kyberturvallisuuteen liittyviä tietoja ja taitoja opetetaan suomalaisessa peruskoulussa. Lisäksi haluttiin kartoittaa kyberturvallisuusalan asiantuntijoiden näkemyksiä siitä, mitä kyberturvallisuuden osa-alueita olisi olennaista opettaa suomalaisessa peruskoulussa. Opinnäytetyö tilaajana toimi Opetushallitus.

Opinnäytetyön teoriaosuus koostuu kyberympäristön määrittelystä, aiheen ajankohtaisuuden hahmottelusta sekä kyberturvallisuuteen liittyvien peruskäsitteiden avaamisesta. Opinnäytetyö on tyypiltään tutkimuksellinen. Opinnäytetyössä tehtiin kaksi erillistä kyselytutkimusta. Ensimmäinen kyselytutkimus suunnattiin peruskoulun opettajille koskien kyberturvallisuuden opetuksen nykytilaa ja toinen kyberturvallisuusammattilaisille liittyen siihen, miten he kokevat kyberturvallisuuden opetuksen tulevaisuuden näkymät ja opetettavat teemat.

Opettajille suunnattuun kyselyyn saatiin lopulta 9 vastausta ja ammattilaisten kyselyyn 149. Kysely toteutettiin verkkolomakkeella ja kyselytutkimukset olivat puolistrukturoituja. Kyselyiden avoimet vastaukset analysoitiin teemoittelun, tyypittelyn, koodauksen ja kategorisoinnin avulla. Numeerisia vastauksia käsiteltiin webropol-työkalun avulla.

Toteutettujen kyselytutkimusten perusteella kyberturvallisuuden opetus peruskoulussa on tällä hetkellä melko hajanaista ja järjestäytymätöntä. Aihealuetta opetetaan osana laaja-alaista osaamista sekä tieto- ja viestintäteknologisia taitoja. Kyselyiden perusteella opettajat tarvitsevat lisäkoulutusta sekä konkreettisia ohjeita opetuksen tueksi. Sekä ammattilaiset että opettajat näkevät, että peruskoulussa tapahtuvaa kyberturvallisuuden opetusta voitaisiin tukea monenlaisilla ratkaisuilla.

Tutkimuksen perusteella voidaan todeta, että kyberturvataitoja voidaan pitää kansalaistaitona, jota tulisi opettaa suomalaisessa peruskoulussa. Jotta kyberturvallisuuden opetusta voidaan toteuttaa tarvittavalla tavalla, pitää opettajille taata riittävä osaaminen sekä resurssit. Tutkimukseen perustuen kyberturvallisuuteen liittyvien asioiden tarkentaminen peruskoulun opetussuunnitelmien perusteissa olisi suositeltavaa. Lisäksi eri tahojen yhteistyöllä voitaisiin tuottaa materiaalia opetuksen tueksi sekä täydennyskouluttaa peruskouluopettajia.

Avainsanat kyberturvallisuus, peruskoulu, perusopetus, opetussuunnitelmien perusteet
Sivut 63 sivua ja liitteitä 24 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Information and Communication Technology

Abstract

Author Miiro Pyysing and Sari Kaipainen
Year 2022
Subject Cyber security in the Finnish basic education
Supervisor Ismo Turve

The aim of the thesis was to examine how cyber security related topics are currently taught in the Finnish comprehensive school. The other objective was to find out the views of cyber security professionals about what cyber security related themes are relevant in basic education. The thesis was commissioned by the Finnish national agency for education.

The theoretical part consists of defining the cyber environment, specifying how topical the theme is, and explaining the mainline cyber security related terms. The thesis is research-based and contains two separate surveys. One of them is directed at comprehensive school teachers in order to examine what the current state of cyber security education is and the other for cyber security professionals aiming to map how they view the outlook of cyber security education in the next few years to be carried out and what the themes should be.

The survey targeted to comprehensive school teachers was answered by 9 people and the survey for cyber security professionals was answered by 149 people. The survey was conducted via a web form and the questions were half structured by their type. The open format survey answers were analyzed by arranging them into the themes and types using coding and cathegorizing.The numerical answers were processed with webropol tool.

According to the surveys, cyber security education in the Finnish comprehensive school is currently quite fragmented and unorganized. The theme is being taught as a part of the wide transversal competence and information and communication technology skills. Based on the surveys the teachers need further education and concrete instructions to support their teaching. Both the cyber security professionals and the teachers find that the comprehensive school education could be supported by various solutions.

Based on the study, cyber security skills can be considered as civic skills, which should be taught in the Finnish comprehensive school. In order to carry out the cyber security education in praxis, it is necessary to ensure that the teachers have adequate knowledge and resources. Based on the research it is recommended to define the cyber security related topics more closely in the national core curriculum. Furthermore, material to support the comprehensive school education could be produced and teachers educated in collaboration with different organizations.

Keywords Cyber security, comprehensive school, basic education, national core curriculum

Pages 63 pages and appendices 24 pages

Sisällys

1 Johdanto 1

2 Kyberturvallisuus 2

2.1 Kyber 2

2.2 CIA-malli 3

2.3 Kyberturvallisuuden ominaispiirteet 4

2.4 Kyberympäristö ja kyberresilienssi 5

3 Kyberympäristö 5

3.1 Mikä on kyberympäristö 6

3.2 Vaikutukset yksilö, yhteisö ja yhteiskunta 6

3.3 Kyberympäristö lasten ja nuorten näkökulmasta 9

4 Perusopetus Suomessa 11

4.1 Suomalainen peruskoulu 11

4.2 Kyberturvallisuus opetussuunnitelmien perusteissa 12

4.3 Kyberturvallisuus osana laaja-alaista osaamista 13

4.4 Kyberturvallisuuden opettaminen 15

5 Ajankohtaisuus 16

5.1 Kansalaisten taidot 16

5.2 Yleistyvä verkkorikollisuus 17

5.3 Suomen kansalliset kyberturvallisuusohjelmat 21

5.4 Suomen kyberturvallisuus osana Euroopan unionia 22

6 Aiemmat tutkimukset 23

7 Tutkimuksen näkökulmat 26

8 Tutkimuksen toteutus 26

8.1 Tutkimuskysymykset ja tutkimuksen tarkoitus 27

8.2 Kvantitatiivinen tutkimus 27

8.3 Tutkimusmenetelmät ja kohderyhmä 28

8.4 Tutkimuksen rajaukset ja aineiston keruu 30

8.5 Analysointi 31

8.6 Eettisyys ja luotettavuus 32

9 Tulokset 33

9.1 Kyberturvallisuuden opetuksen nykytila 33
9.1.1 Opettajien valmiudet kyberturvallisuuden opetukseen 34
9.1.2 Opetus ja opetuksen sisällöt 36
9.1.3 Opetuksen merkityksellisyys 38
9.2 Kyberturvallisuuden opetuksen teemat ja tulevaisuus 39
9.2.1 Tietoisuus kyberturvallisuuden opetuksesta peruskoulussa 39
9.2.2 Kansalaistaitojen merkitys 42
9.2.3 Opetettavat teemat 44
9.2.4 Opetuksen järjestäminen 45
10 Johtopäätökset 50
10.1 Kyberturvallisuuden opetuksen nykytila 50
10.2 Kyberturvallisuuden opetuksen teemat ja tulevaisuus 52
11 Pohdinta 53
Lähteet 56

Liitteet

Liite 1 Aineistonkäsittelysuunnitelma
Liite 2 Perusopetuksen opettajille suunnattu kysely
Liite 3 Kyberturvallisuuden ammattilaisille suunnattu kysely

1 Johdanto

Peruskouluikäisten internetin käytön lisääntymisen sekä päätelaitteiden käyttömahdollisuuksien muutoksen myötä jokapäiväiseen toimintaympäristöömme on syntynyt uudenlaisia haasteita, joihin vastatakseen tulisi lasten ja nuorten kyberturvallisuuden perustaitojen olla ajan tasaiset. Halusimme selvittää missä määrin suomalaisessa peruskoulussa opetetaan näitä taitoja ja mitä kyberturvallisuuden ammattilaiset ajattelevat taitojen opettamisen tulevaisuudesta.

Opetushallituksen toimeksiannosta lähdimme opinnäytetyössä selvittämään kyberturvallisuuden opetuksen toteutumista suomenkielisessä peruskoulussa sekä kyberturvallisuuden ammattilaisten näkemyksiä siitä, mitä kyberturvallisuuden teemoja perusopetuksessa olisi olennaista opettaa. Opinnäytetyö on teemaltaan erittäin ajankohtainen, koska viimeistään COVID-19-pandemian myötä erilaiset tietotekniset laitteet sekä internetin mahdollistamat etäyhteydet tulivat osaksi jokaisen, myös lasten- ja nuorten arkea. Pandemian jälkeisen Euroopan poliittisen tilanteen kiristymisen myötä myös erilaiset kyberturvallisuuteen liittyvät skenaariot ja uhat, niin yksilö- kuin valtiotasoiset, ovat nousseet yleiseen keskusteluun.

Opinnäytetyössä käsitellään kyberturvallisuuteen liittyvän toimintaympäristön (jäljempänä kyberympäristö) olennaisia käsitteitä, määritelmiä sekä lainalaisuuksia. Lisäksi tarkastellaan nykyisten opetussuunnitelmien perusteiden sisältämiä mainintoja kyberturvallisuuden opetukseen liittyen. Tästä kokonaisuudesta muodostuu pohja tutkimukselle, joka koostuu kahdesta osasta: Ensimmäisessä osassa selvitetään suomalaisessa peruskoulussa tapahtuvaa kyberturvallisuuden opetuksen nykytilaa. Kyselytutkimus suunnataan peruskoulun opettajille. Toisen osan tavoitteena on selvittää, mitä kyberturvallisuuden osa-alueita suomalaisessa peruskoulussa tulisi opettaa. Myös toinen osuus toteutetaan kyselytutkimuksella ja se on suunnattu kyberturvallisuuden parissa työskenteleville henkilöille. Tutkimuksien tuloksia on mahdollista hyödyntää suunniteltaessa kyberturvallisuuden opetukseen liittyviä mainintoja opetussuunnitelmien perusteissa ja siten opinnäytetyöllä voi olla vaikutusta kyberturvallisuuden opetuksen tulevaisuuteen.

2 Kyberturvallisuus

Niin kyberturvallisuus kuin muutkin kyber-alkuiset sanat ovat ilmestyneet suomen kieleen toden teolla viimeistään vuoden 2013 alussa julkaistun ensimmäisen kyberturvallisuusstrategian myötä. Tässä kappaleessa ja sen alaluvuissa käydään läpi kyberturvallisuuteen liittyvää termistöä sekä keskeisiä käsitteitä. Tarkasteluun tulee myös CIA-malli, jonka avulla pystytään tarkastelemaan kyberturvallisuuden tilaa, sekä ATTAT-malli, jolla pystymme tarkastelemaan kyberympäristön lainalaisuuksia.

2.1 Kyber

Vuoden 2013 alussa julkaistussa kyberturvallisuuden strategiassa käytiin läpi termistöä ja huomioitiin myös se, että sanasto on vasta kehittymässä suomen kieleen ja kulttuuriin. (Limnéll 2014, 16) Etuliite *kyber* on peräisin kreikkalaisesta sanasta *kybereo*, joka viittaa suomeksi sanoihin ”*ohjata*”, ”*opastaa*” ja ”*hallita*”. *Kyber*-etuliitteellä viitataan digitaalisuuteen ja usein myös tietokone- ja informaatiojärjestelmiin. (Turvallisuuskomitea, 2018, s. 21)

Kyberturvallisuus sanana kuvaa useita toimenpiteitä, joita toteutetaan, jotta voidaan hallita erilaisia riskejä ja uhkia, joita toimintaympäristöön liittyy. Olennaista on ehkäistä kyberuhkia ja niiden vaikutuksia yksilöön ja yhteiskuntaan. Erilaiset haitalliset tapahtumat tai teot, joilla voi olla vaikutusta kyberympäristön toimintaan ovat kyberuhkia. Myös ympäristössä liikkuvien tietojen suojaaminen eli tietoturvallisuudesta huolehtiminen on osa kyberturvallisuutta. (Turvallisuuskomitea, 2018, ss. 22, 25)

Osana kyberturvallisuuden kokonaisuutta on syytä mainita myös termit tietosuoja sekä GDPR (General Data Protection Regulation eli yleinen tietosuoja-asetus). GDPR on henkilötietojen käsittelyyn liittyvä laki, joka otettiin käyttöön EU-maissa vuonna 2018. Sen tarkoituksena on säännellä henkilötietojen käsittelyä siten, että henkilötiedot on paremmin suojattu ja lisätä kunkin mahdollisuuksia omien henkilötietojensa käytön hallintaan. GDPR:n myötä rekisterinpitäjien (esimerkiksi palveluntuottaja) on täytettävä tietyt vaatimukset henkilötietojen käsittelyssä. (Tietosuojavaltuutetun toimisto, 2022a.)

Tietosuojalla taas tarkoitetaan ihmisen perusoikeutta omiin tietoihinsa. Tietosuojalla tarkoitetaan myös henkilön oikeuksien sekä vapauksien huomioimista silloin, kun henkilötietoja käsittelee jokin taho tai organisaatio. Tietosuoja määrittelee sen, missä tilanteessa ja milloin henkilötietoja voidaan käsitellä ulkopuolisen tahon toimesta. Henkilötietoja ovat esimerkiksi ihmisen nimi, osoite ja puhelinnumero. Käsitteellä tietoturva viitataan käytännön keinoihin esimerkiksi tekniset toimenpiteet, joilla suojataan tietoja esimerkiksi tietojärjestelmissä. (Tietosuojavaltuutetun toimisto, 2022b.)

2.2 CIA-malli

Yleensä tietoturvan ja kyberturvallisuuden tilan arviointiin liittyviä kolmea peruskäsitettä hahmotetaan kolmion kautta. Samalla nämä kolme peruskäsitettä ilmentävät perushaasteita, joita turvallisuuden parissa kohdataan kybermaailmassa. Kolmion kolme elementtiä ovat *Confidentiality/Luottamuksellisuus, Integrity/Eheys* sekä *Availability/Saatavuus.* Luottamuksellisuudella viitataan siihen, että tiedon tulee olla vain niiden tiedossa, joille se kuuluu. Tietoon annetaan siis oikein määritellyt pääsyoikeudet sekä näkyvyys. On olemassa useita tekniikoita, joilla hyökkääjät voivat yrittää murtaa luottamuksellisuutta. Tällaisia ovat muun muassa man-in-the-middle -hyökkäykset ja erilaiset tietojenkalasteluhuijaukset, joissa pääsyoikeuksia omaavat tunnukset pyritään hankkimaan luvattomaan käyttöön. (Fortinet, 2022)

Eheydellä puolestaan viitataan siihen, että talletettuja tietoja ei pystytä luvattomasti manipuloimaan vaan säilytys tapahtuu luotettavasti. Hyökkääjät voivat monella tapaa yrittää ohittaa havainnointijärjestelmiä sekä päästä sisään uhrin järjestelmään ja sitä kautta muuttamaan järjestelmään talletettuja tietoja. Erilaiset digitaaliset allekirjoitukset, kryptaus ja hash-arvojen käyttö, voivat auttaa varmistamaan tiedon oikeellisuuden ja muuttumattomuuden. (Fortinet, 2022)

Saatavuus mahdollistaa tietojen käsittelyn silloin, kun tiedon saannille on tarve. Käyttöoikeudet omaavilla käyttäjillä täytyy siis olla pääsy tietoihin, jotta niitä voidaan käyttää tarkoituksen mukaisesti. Saavutettavuus voi olla uhattuna esimerkiksi sähkökatkon tai DOS-hyökkäyksen (denial-of-service eli palvelunestohyökkäys) tai kiristyshaittaohjelman takia.

Palvelunestohyökkäyksellä tarkoitetaan sellaista tietoverkkoihin kohdistuvaa tahallisesti tuotettua liikennettä, jonka tarkoituksena on kuormittaa kohdetta, esimerkiksi verkkosivustoa tai palvelua. Haittaohjelmiin luokiteltava kiristyshaittaohjelma sen sijaan ujutetaan hyökkääjän toimesta kohdejärjestelmään ja sillä pyritään esimerkiksi tietojen lukitsemiseen sekä tilanteen hyödyntämiseen kohdetahon kiristämiseksi. Saavutettavuutta voidaan parantaa huomioimalla varmuuskopioiden saatavuus sekä suunnittelemalla toipumissuunnitelmia erilaisten tilanteiden varalle. (Fortinet, 2022; Kyberturvallisuuskeskus 2022a)

CIA-mallin avulla voidaan yksinkertaisella tavalla havainnollistaa kyberturvallisuuden tilaa yksilön, yrityksen tai muun toimijan kohdalla. Mallia voidaan myös hyödyntää kyberturvallisuuden kehittämisessä sekä ihmisten kouluttamisessa, kun mietitään, miten voidaan paremmin valmistautua erilaisiin poikkeustilanteisiin. (Fortinet, 2022)

2.3 Kyberturvallisuuden ominaispiirteet

ATTAT-mallin avulla (aika, tila, tunnistamattomuus, asymmetrisyys ja tehokkuus) voidaan kuvata niitä dynaamisen kyberympäristön lainalaisuuksia, jotka vaikuttavat selviytymiseen kyseisessä ympäristössä niin yksilön, yhteisön kuin yhteiskunnankin kannalta. Asioita voi tapahtua kybermaailmassa välittömästi fyysisestä etäisyydestä riippumatta. Toisaalta kybermaailmassa voidaan toimia huomaamattomasti pitkiäkin aikoja. Tilan merkitys katoaa, ei ole väliä missä olet ja minne asti tarvitset yhteyden, eivätkä kyberuhat ole sidoksissa paikkaan tai aikaan. Tilan merkitys kybermaailmassa on myös siitä näkökulmasta erilainen, että sitä voidaan manipuloida ja muokata esimerkiksi päivitysten muodossa. (Limnéll ym., 2014, ss. 63–66)

Yksi kybermaailman ominaispiirre on tunnistamattomuus. Kybermaailmassa on yleistä se, että tekijää tai teon alkuperää voi olla vaikea jäljittää. Tästä syystä myös kiinnijäämisen ja seurauksien riski esimerkiksi rikollisille on pieni. (Limnéll ym., 2014, s. 67) Kybermaailmassa valitsee myös asymmetrisyys: näennäisesti heikompi osapuoli voikin pystyä hyvin kyvykkäisiin tekoihin. Tämä mahdollistaa monimuotoisemman toimijajoukon sekä sen, että pienemmilläkin resursseilla voi saada aikaan merkittäviä asioita. (Limnéll ym., 2014, s. 68)

Kybermaailmassa toiminta on tehokasta siinä mielessä, että yksi toimija voi tehdä useita asioita samanaikaisesti. Samalla tämä tuo puolustajalle haasteita: miten suojata monimutkaisia sekä verkottuneita systeemejä useammalla tasolla samanaikaisesti? (Limnéll ym., 2014, s. 69)

2.4 Kyberympäristö ja kyberresilienssi

Kyberympäristöllä tarkoitetaan erilaisista laitteista, verkoista, ohjelmista sekä tietojärjestelmistä muodostuvaa kokonaisuutta, jossa tieto liikkuu sähköisessä muodossa. Kyberturvallisuus on tila, jossa kybermaailmassa toimivaan ympäristöön voidaan luottaa ja sen toiminta on turvallista. Turvallisen toiminnasta tekee hallittavuus ja ennakointi sekä se, miten hyvin ongelmatilanteessa pystytään toimimaan. (Varmuuden vuoksi, n.d.)

Tietoturvallisuudella taas viitataan hieman suppeampaan kokonaisuuteen ja nimenomaan tietoihin, joita kybermaailmassa liikkuu. Tietoturvan piiriin liittyviä tietoja ovat esimerkiksi erilaiset viestit ja henkilötiedot. Tietoturvaan liittyy olennaisesti se, että tiedot on suojattu, ne ovat saatavilla, kun niitä tarvitaan ja että ne pysyvät eheinä koko niiden elinkaaren ajan. (Varmuuden vuoksi, n.d.)

Vuoden 2019 valtioneuvoston periaatepäätöksessä on todettu tarve kansallisen kyberturvallisuuden kokonaistilan kohentamiseksi. (Paananen, 2021a, s. 7) Kansallisen kokonaistilan kuvaamiseksi käytetään usein käsitettä kyberresilienssi, jota voidaan kuvata myös sanalla kriisinkestävyys. Sillä tarkoitetaan toimintakyvyn tasoa, joka yksilöllä tai yhteiskunnalla on muuttuvissa tilanteissa tai poikkeustilan sattuessa. Resilienssiä tuottavat tiedot, taidot, joustavuus ja palautumiskyky. (Turvallisuuskomitea, 2018, s. 14)

3 Kyberympäristö

Jotta kyberturvallisuus käsitteenä voidaan laajemmin ymmärtää, täytyy ensin perehtyä siihen, mitä kyberympäristöllä tarkoitetaan. Tässä kappaleessa keskitytään tarkastelemaan, mikä on kyberympäristö, mitä vaikutuksia sillä on elämäämme ja miltä kyberympäristö näyttää, kun sitä tarkastellaan erityisesti lasten ja nuorten näkökulmasta.

3.1 Mikä on kyberympäristö

Sanoilla *kybermaailma* tai *kyberympäristö* viitataan tässä opinnäytetyössä niihin ympäristöihin, joissa on käytössä monenlaisia digitaalisia ratkaisuja informaation muokkausta, varastointia sekä siirtoa varten. Käytännön esimerkkejä kyberympäristöjen osakokonaisuuksista ovat esimerkiksi erilaiset tietojärjestelmät, tietoverkot sekä laitteet, joita näiden yhteydessä käytetään. (Turvallisuuskomitea, 2018, s. 21) Erityisesti internetin kaupallistuminen ja sosiaaliset ulottuvuudet nivovat nämä monimutkaiset ympäristöt osaksi meidän jokapäiväistä arkeamme. (Limnéll ym., 2014, s. 95).

Kyberympäristö, joka perustuu tietotekniikkaan sekä erilaisiin yhteyksiin, on toiminnassa jatkuvasti, eikä se ole riippuvainen esimerkiksi maantieteellisestä sijainnista tai kellon ajasta. (Limnéll ym., 2014, s.16) Erityisesti lasten ja nuorten kohdalla korostuu konkreettisen fyysisen maailman sekä kybermaailman saumaton erottamattomuus. Heille on luontevaa toimia molemmissa vuorotellen tai yhtä aikaa. Voi olla, että lasten ja nuorten on vaikeampi hahmottaa, mitä kaikkea konkreettista internetin taustalla on, kun se on aina ollut heidän elämässään läsnä ja lähes aina toiminut toivotulla tavalla. Tosiasiassa internetin taustalla vaikuttavat monimutkaiset tekniset ratkaisut sekä fyysiset laitteet. (Limnéll ym., 2014, s.32-33)

Pohjatoimija kybermaailmassa ei kuitenkaan ole tietokone tai muu tekninen laite. Ennen kuin kalasteluviesti lähetetään, haittaohjelma ohjataan uhrin järjestelmiin tai kyberpuolustusta rakennetaan, on joku päättänyt toimia valitulla tavalla. Kybermaailman keskiössä on siis ihminen. (Limnéll ym., 2014, s. 76) Kyberympäristön jatkuva laajeneminen näkyy myös siinä, että yhä useammat kodinkoneet, lämmitysjärjestelmät sekä muut etäohjattavat laitteet ovat yhteydessä internetiin tai vähintäänkin sisältävät jonkun tietoteknisen komponentin. (Limnéll ym., 2014, s. 32)

3.2 Vaikutukset yksilö, yhteisö ja yhteiskunta

Kybermaailmassa tapahtuvilla asioilla on moninaisia vaikutuksia arkeemme. Limnéll, Majewski ja Salminen kirjoittavat kirjassaan *Kyberturvallisuus*, että kyberturvallisuuden

perustaitojen tulisi olla kansalaistaitoja samoin kuin lukemisen, laskemisen ja kirjoittamisen ajatellaan olevan. (Limnéll ym., 2014, s. 14) Kyberturvallisuuteen liittyvät ilmiöt voivat vaikuttaa jopa perusturvallisuuden tunteeseemme (Limnéll, 2022). Yksilöiden näkökulmasta ajateltuna, kyberympäristön laajenemisen myötä, myös erilaiset uhat lisääntyvät. Yksi tavallisimmista uhista, joita kansalaiset yksilöinä kohtaavat kybermaailmaan liittyen ovat verkkorikolliset. Käytännössä rikollisuus voi näkyä esimerkiksi tietojenkalasteluna, valtiollisena tiedusteluna kohdistuen työntekijään tai erilaisina muina huijauksina. (Limnéll ym., 2014, s. 49)

Uhkien yleistyessä, kyberturvallisuudesta on suomalaisessa yhteiskunnassa alettu myös viime vuosina tuottamaan kaikkien saatavilla olevaa materiaalia. Esimerkiksi Maanpuolustuskoulutusyhdistyksen (MPK) julkaisema K*yberin taskutieto* -opas sisältää kansalaisen 10 + 1 kyberkäskyä, jotka nostavat esiin olennaisia seikkoja, joita kansalaisen tulee huomioida toimiessaan digitaalisessa maailmassa. (Lönnqvist & Moilanen, 2017) Kybermaailma mullistaa yksilön todellisuutta siitäkin näkökulmasta, että hänen ei välttämättä tarvitse olla verkossa täysin oma itsensä. Ihmisen on siis mahdollista luoda erilaisia identiteettejä ja hahmoja, joina toimia verkossa. Kybermaailman luonteen vuoksi voi olla helppo häivyttää henkilöllisyyttään ja haasteena on vahvistaa annetut tiedot tosiksi tai valheellisiksi. (Limnéll ym., 2014, s. 96) Lisäksi yhteiskunnan näkökulmasta katsottuna kyberympäristön tapahtumat liittyvät myös konkreettisiin asioihin: sähköjen toimivuuteen, energian toimitukseen, rahajärjestelmien toimintaan ja elintarvikehuoltoon. Tästä syystä kyberympäristön tila ja varsinkin toimintahäiriöt vaikuttavat vahvasti arkeemme. (Limnéll ym., s. 32)

Sosiaalinen media ja muut uudet verkkoalustat mahdollistavat yhä useampien yksilöiden ja yhteisöjen äänen kuulumisen julkisessa keskustelussa. Moniäänisyyden lisääntyessä voi olla vaikea määritellä, mikä saatavilla olevasta informaatiosta on oikeaa tietoa ja sellaista tietoa, johon voi luottaa. Tässä arvioinnissa painottuu jokaisen yksilön oma arviointikyky ja taito kriittiseen ajatteluun. (Limnéll ym. 2014, s.53) Järjestelmällinen viestintä, jolla pyritään vaikuttamaan kohteeseen, tämän mielipiteeseen tai käyttäytymiseen on informaatiovaikuttamista. Sen yhteydessä käsitellään yleisesti myös termejä misinformaatio (tahattomasti levitettyä väärää tietoa) ja disinformaatio (tahallisesti levitettyä väärää tietoa).

Valeuutisella taas tarkoitetaan uutisenomaista tekstiä, jolla pyritään tahallisesti johtamaan lukijaa harhaan. Informaatiovaikuttamista voi yhtä lailla olla tavanomainen markkinointiviestintä kuin sotapropagandakin. (Vehkoo, 2021)

Internetin ja kyberympäristöjen yleistyessä myös yhteisöllisyyden ja muut yksilöiden sekä yhteisöjen kanssakäymisen muodot muovautuvat uudelleen ja synnyttävät uutta. Verkossa keskustellaan, luodaan uusia ystävyyssuhteita ja toimitaan yhdessä esimerkiksi pelaamalla tai luomalla virtuaalisia alustoja. Samaistumisen kohteiden löytäminen saattaa helpottua ja sosiaalinen verkosto on lähellä. Toisaalta yhteisöjen ja yksilöiden välisissä suhteissa on ollut aina myös haasteita, jotka myös ottavat uudet muodot kybermaailmassa. (Limnéll ym. 2014, ss. 95-96) Myös tietoa tuotetaan kybermaailmassa yhdessä. Voidaankin nähdä, että yksilöllä on monta roolia samanaikaisesti niin tiedon tai muun sisällön vastaanottajana kuin sisällöntuottajanakin. (Limnéll ym., 2014, s.97)

Jotta yhteiskunnan eri tasoilla esimerkiksi valtionjohdossa ja yrityksissä pystytään tekemään oikea-aikaisia, perusteltuja ja oikein mitoitettuja toimenpiteitä kybermaailmaa koskien, on ihmisten tietoisuutta aiheesta lisättävä. (Limnéll ym., 2014, s. 16) Vuonna 2019 päivitetyssä *Suomen kyberturvallisuusstrategiassa* todetaan, että merkittävä osa kybermaailman riskeistä kohdistuu ihmisten tekemiin virheisiin. (Turvallisuuskomitea, 2019, s. 4) Jokaisella kansalaisella on siis mahdollisuus omalla toiminnalla sekä muiden huomioimisella vaikuttaa Suomen kyberturvallisuuden tilaan. Vuoden 2019 kyberturvallisuusstrategiassa korkeatasoinen osaaminen on nostettu yhdeksi kärkitavoitteeksi ja juuri yksilön kouluttaminen on tätä tavoitetta lähestyttäessä avainasemassa. (Turvallisuuskomitea, 2019, ss. 8-10)

Kyberympäristö on joutunut ainakin jo kertaalleen todella koetukselle COVID-19-pandemian lähtiessä liikkeelle 2020 alkuvuodesta. Silloinkin kyberturvallisuuteen liittyvät uudet kysymykset ja pohdinnat koskivat nopealla tempolla lähes kaikkia kansalaisia riippumatta iästä tai muusta taustasta. (Paananen, 2021b) Yrityksien sekä yhteiskunnallisten toimijoiden toiminnot ovat siis riippuvaisia digitalisaatiosta ja myös lopulta siitä, kuinka turvallisesti kybermaailmassa pystytään navigoimaan ja toimimaan. (Limnéll ym. 2014, s. 20)

Digitalisoituvat palvelut ja kyberympäristö luovat erilaisille instituutioille mahdollisuuksia esimerkiksi tuotannon tehostamiseen, toiminnan laajentamiseen, uusien innovaatioiden synnyttämiseen sekä kustannustehokkuuteen. (Limnéll ym. 2014, s.15) On todettu, että kyberturvallisuus tulisikin nähdä luonnollisena osana yhteiskunnallista vastuuta yksilöiden ja yrityksien toiminnassa. (Paananen, 2021a, s. 10) Kyberturvallisuuden pitäisi olla siis sisäänrakennettu osa erilaisia uusia toimintoja sekä rakentamista, oli kyse fyysisistä rakennelmista tai digitaalisista järjestelmistä. Näin myös yhteiskunnan tasolla pystytään parhaiten vastaamaan muuttuviin tilanteisiin ja lisäämään toimintavarmuutta. (Limnéll ym. 2014, ss. 14-15)

3.3 Kyberympäristö lasten ja nuorten näkökulmasta

Lasten ja nuoren Internetin käyttö on muuttunut erityisesti mobiililaitteiden yleistymisen myötä. Tilastokeskus julkaisee vuoden 2022 marraskuussa tuoreimman Internetin käyttöön liittyvän tilastokokonaisuuden. Edellisen kerran Internetin käyttöä on laajemmassa kokonaisuudessa selvitetty vuonna 2015. On kuitenkin selvää, että muun muassa Internetin käyttö, päätelaitteiden määrä, erilaisten verkkopalveluiden, mobiilisovellusten ja verkkokaupan käyttöuseus sekä tavoittavuus ovat muuttuneet merkittävästi seitsemässä vuodessa. Tilastokeskuksen ajankäyttötutkimuksen mukaan vuonna 2017 lähes jokaisella 10–14-vuotiaalla nuorella on ollut käytössään älypuhelin, tietokone vastaavasti arviolta 70 prosentilla. Laite ei välttämättä ole henkilökohtainen, vaan esimerkiksi perheen yhteiskäyttölaitteet lasketaan mukaan. (Pitkänen & Saarenmaa, 2021) On kuitenkin oletettavaa, että laitteiden saavutettavuus on lisääntynyt edelleen vuodesta 2017 vuoteen 2022.

Huomionarvoista on se, että lapset ja nuoret hyödyntävät Internetiä muun muassa tiedonhakuun, musiikin kuunteluun, videosisältöjen katseluun, pelaamiseen, yhteydenpitoon tai sisällön tuottamiseen. Internet on tullut osaksi lasten ja nuorten vapaa-aikaa ja siinä, missä aikaisemmin keskusteltiin internetiin käytetystä ajasta, tämän hetken peruskouluikäiset lapset ja nuoret viettävät aikaansa verkossa. (Salasuo, 2020, s. 97) He eivät erittele internetin mahdollistamia toimintoja muusta toiminnasta.

Kun internetin mahdollistamia palveluita käytetään aktiivisesti ja usealla osa-alueella, on perusteltua nostaa esille turvataitojen merkitys. Tilannetta voidaan ajatella myös hyökkäyspinta-alan kasvuna: mitä enemmän erilaisia tarpeita Internetin avulla tyydytetään, mitä kauemmin aikaa sen parissa kuluu sekä mitä useampia palveluita hyödynnetään, sitä laajemmalta alueelta yksilö voi tulla uhatuksi. Turvataitojen opetuksen tarvetta voidaan lähestyä esimerkiksi seuraavien Lasten ja nuorten vapaa-aikatutkimuksessa esiin nousseiden ajanvieteteemojen kautta: verkkopalveluihin rekisteröityminen, tiedon hakeminen ja videosisältöjen katseleminen, sosiaalinen media, sisällön jakaminen ja verkkohuijaukset. (Salasuo, 2020, s. 97) Näistä esimerkkeinä muun muassa seuraavat osa-alueet:

- verkkopalveluihin rekisteröityminen (esimerkiksi ikärajat, salasanat, palvelun käyttöperiaate)
- tiedon hakeminen ja videosisältöjen katseleminen (esimerkiksi ikätasoiset sisällöt, lähdekriittisyys)
- sosiaalinen media (esimerkiksi väärennetyt tilit, yhteydenottopyynnöt, grooming, identiteettivarkaudet)
- sisällön jakaminen (esimerkiksi mitä jaat, kenelle ja missä – datan joutuminen vääriin käsiin)
- verkkohuijaukset (esimerkiksi huijausviestin tunnistaminen, hälytysmerkit, identiteettivarkaudet).

Mediakasvatusseura on julkaissut jo vuonna 2007 katsauksen median vaikutuksista lapsiin ja nuoriin sekä kansainvälisestä mediakasvatuksen tilanteesta. Tästä 15 vuoden takaisesta katsauksesta voidaan havaita, että jo tuolloin on pidetty tärkeinä niitä teemoja, joita tässä opinnäytetyössä käsitellään. Katsauksessa suositetaan mediakasvatusmateriaalin tuottamista niin vanhemmille kuin kasvatuksen ammattilaisillekin, viitaten myös eri oppiaineiden aineopetukseen. Katsauksessa pidetään tarpeellisina myös peruskoululaisille kohdennettuja ohjeistuksia liittyen kriittiseen medialukutaitoon, turvataitoihin, nettikiusaamiseen, uhkien havaitsemiseen sekä havaittujen rikosten ilmiantamiseen. Turvataitokasvatuksella pyritään lisäämään lasten ja nuorten kykyä havaita ja suojautua uhkaavia sekä vahingollisia tilanteita verkossa. (Mustonen & Salokoski, 2007, s. 140)

Katsauksessa ehdotetun mediakasvatusmateriaalin ohella tulisi media- ja turvataitokasvatusta kyetä tarjoamaan hyödyntäen monipuolisesti lasten ja nuorten mediakenttää. Esimerkiksi YouTube-videoita seurataan ikäluokassa aktiivisesti. Lasten ja nuorten ajankäyttöä selvittäneen tutkimuksen mukaan yli puolet peruskouluikäisistä seuraa aktiivisesti jonkun YouTube-sisällöntuottajan videoita (Salasuo, 2020, s. 99). Näistä sisällöntuottajista muodostuu lapsille ja nuorille esikuvia, joilla voi olla vahva vaikutus seuraajiinsa ja, joiden avulla voitaisiin myös välittää turvataitokasvatusta.

Mikäli peruskouluikäiset halutaan mediateitse tavoittaa, tulisi sisällön olla tarjolla heille luontevassa mediassa – tai osana perusopetusta. Tyypillistä on, että lapset eivät yleensä kerro vanhemmilleen mitä tekevät internetissä. Koulussa tapahtuvan opetuksen kautta myös vanhemmat voisivat saada vinkkejä siitä, miten keskustella aiheesta lasten kanssa ja miten tehdä tarvittaessa rajoituksia esimerkiksi laitteiden käyttöön. (Amankwa, 2021)

4 Perusopetus Suomessa

Tässä luvussa käsitellään perusopetuksen rakentumista Suomessa sekä sitä, minkälaisia sisältöjä tieto- ja viestintätekniikasta opetussuunnitelmien perusteiden mukaan tulisi opettaa eri vuosiluokilla ja, miltä osin sisällöt liittyvät kyberturvallisuuden aihepiiriin.

Alaluvuissa perehdytään myös perusopetuksen perusteisiin eli valtakunnalliseen ohjeistukseen, jonka perusteella paikalliset koulut järjestävät perusopetuksen. Tällä hetkellä käytössä oleva ohjeistus on otettu käyttöön 2016 ja sen käyttöönotto on tapahtunut vaiheittain. (Opetushallitus, 2022a)

4.1 Suomalainen peruskoulu

Vuoden 2020 tilastojen mukaan Suomessa on 2 276 peruskoulua (Tilastokeskus, 2021a). Suomessa peruskoulujen opetus pohjautuu perusopetuksen opetussuunnitelmien perusteisiin. Perusteilla pyritään varmistamaan koulutuksen tasalaatuisuus sekä edellytykset oppimiselle. Muita opetuksen järjestämistä koskevia sekä ohjaavia instrumentteja ovat perusopetuslaki, perusopetusasetus sekä paikalliset opetussuunnitelmat ja

lukuvuosisuunnitelmat. Opetussuunnitelmien perusteet antavat raamit sille, miten perusopetusta järjestetään paikallisesti eri kouluissa. (Opetushallitus, 2016, ss. 9–13) Perusopetuksen tavoitteena on oppijan laaja-alainen osaaminen. Laaja-alaisella osaamisella tarkoitetaan sitä kokonaisuutta, joka syntyy tietojen, taitojen, arvojen, asenteiden sekä tahdon yhteisvaikutuksesta. (Opetushallitus, 2016, s. 20)

Kuntien järjestämisvastuulla oleva perusopetus luo Suomessa perustan kansalaisten tasavertaiselle yleissivistykselle. Opetuksessa tulee ottaa huomioon oppijan ikätaso sekä muut edellytykset. (Opetushallitus, 2016, ss.14-15) Suomalainen opetus- ja koulutusjärjestelmä on maailmalla arvostettu. Sen ominaisuuksia ovat ajantasaisuus, korkea koulutustaso sekä julkisrahoitteisuus. Nämä ovat ehdottomia vahvuuksia ajatellen kyberturvallisuuden opetusta suomalaisessa peruskoulussa. (Lehto ym., 2019, ss. 22-23)

4.2 Kyberturvallisuus opetussuunnitelmien perusteissa

Opetussuunnitelmien perusteissa todetaan, että perusopetuksen on tarkoitus ohjata oppijaa toimimaan myös teknologisoituneessa arjessa ja että oppilaat tarvitsevat perustiedot teknologiasta sekä sen kehityksestä ja vaikutuksesta heidän omaan elämäänsä. Huomiota suunnataan erityisesti järkevien teknologisten ratkaisujen tekemisen oppimiseen sekä toimintaperiaatteiden, eettisyyden ja vastuullisuuden ymmärtämiseen. (Opetushallitus, 2016, s. 22) Perusopetus on olennainen komponentti yhteiskunnan kehityksessä ja rakentamisessa. (Opetushallitus, 2016, s. 18) Onnistunut kyberturvallisuuden opetus ja tavoitetaso vaatii toteutuakseen sen, että koulutukseen sekä tutkimukseen ohjataan riittävästi rahoitusta ja, että näitä toteutetaan pitkäjänteisesti. (Lehto ym., 2019, s. 29) Varsinaisten kyberturvallisuustaitojen lisäksi lapsilla ja nuorilla olisi hyvä olla perusymmärrys informaatiovaikuttamisesta sekä medialukutaidosta. (Lehto ym., 2019, s. 26)

Opetussuunnitelmien perusteissa on erikseen nostettu osaamisalueeksi tieto- ja viestintäteknologinen osaaminen. Sen perusteella perusopetuksessa tulee huomioida oppijoiden mahdollisuus tieto- ja viestintäteknologisen osaamisen kehittämiseen. Perusopetuksessa tulisi myös pyrkiä siihen, että jokainen oppii keskeisistä käsitteistä,

turvallisuudesta sekä erilaisten sovelluksien ja laitteiden käytöstä. Esille nostetaan myös riskien ja merkityksien hahmottaminen globaalissa maailmassa. (Opetushallitus, 2016, s. 23)

Vuoden 2016 opetussuunnitelmien perusteissa tietoturvaan liittyvä opetus on sidottu osaksi laaja-alaista osaamista. Tämä tarkoittaa, että se ei ole itsenäinen oppiaine vaan sen aihealueet sisällytetään muuhun opetukseen ja opetettaviin aineisiin. Helsingin Sanomien artikkelissa vuodelta 2016 todetaan, että luultavasti opetuksen taso vaihtelee niin opettajan oman osaamisen ja kiinnostuksen mukaan, kuin myös alueellisesti ja koulujen välillä. (Silfverberg & El-Khoury, 2016) Huomion arvoista on myös se, että opetus perustuu paljolti juuri tietoturvaan liittyviin asioihin eikä kokonaisvaltaisesti kyberturvallisuuteen. Perusteissa on mainintoja mm. tietoturvariskeiltä suojautumisesta ja tekijänoikeuksista. Perusteissa ohjataan siihen, että opetuksen ansiosta oppilaat osaisivat toimia vastuullisesti ja turvallisesti tieto- ja viestintätekniikan ympäristössä. (Silfverberg & El-Khoury, 2016)

4.3 Kyberturvallisuus osana laaja-alaista osaamista

Siirryttäessä peruskouluun lähtötasona tietojen ja taitojen oppimiselle toimii varhaiskasvatuksessa ja esiopetuksessa saadut taidot. (Opetushallitus, 2016, s. 98) 1–2 vuosiluokilla tietoturvallisuuden opetukseen liittyviä mainintoja löytyy muun muassa *itsensä huolehtiminen ja arjentaidot (L1)* alta. Tässä aihealueessa tulisi oppilaiden kanssa tutkia arjen teknologiaa ja sen turvallisen käytön edellytyksiä ja merkitystä arjessa. Myös *monilukutaito (L4)* sisältää mainintoja tiedon hankkimisen taidoista sekä kuvitteellisen maailman ja todellisen maailman suhteiden hahmottamisesta. Suurin osa tietoturvan opetuksen maininnoista on sisällytetty *Tieto- ja viestintäteknologinen osaaminen (L5) (TVT)* alle. 1–2-vuosiluokilla korostuvat leikinomainen asioiden opettelu sekä perustaitojen harjoittelu. Perustaitoja ovat muun muassa laitteiden käyttö, käyttötarkoitukset ja peruskäsitteet. Erikseen esille nostetaan vastuullinen ja turvallinen toiminta, johon kuuluvat muun muassa hyvät käytöstavat ja laitteiden turvalliset käyttötavat. (Opetushallitus 2016, ss. 100–101) Ympäristöopin kokonaisuudessa puhutaan luonnosta ja rakennetusta ympäristöstä sekä ihmisten tekemien valintojen vaikutuksesta ympäristölle. Tässä kohtaa tieto- ja viestintätekniikan luomasta internet-maailmasta ei mainita mitään, vaikka se on

kiistämättömästi olennainen osa nykyarkeamme ja sosiaalista toimintaa. (Opetushallitus 2016, ss. 130-131)

Vuosiluokilla 3–6 vahvistetaan aiemmin opittuja perustaitoja ja opetellaan uutta. Jälleen laajin tietoturvallisuuden opetusta koskeva kokonaisuus löytyy *TVT-osaamisen (L5)* alta. Oppilaita opetetaan käyttämään laitteita, palveluita sekä erilaisia toimintalogiikoita. Turvallista ja vastuullista toimintaa korostetaan. (Opetushallitus 2016, ss. 154, 157) Tietoturvaopetuksen voisi nähdä myös osana *Ajattelun ja oppimaan oppimisen (L1) taitoja*, koska internet-maailmassa navigoidessa korostuu *yksilön harkintakyky sekä kriittinen ajattelu (L1). Kulttuurinen osaaminen, vuorovaikutus ja ilmaisun (L2)* osa-alueella korostetaan medialukutaitoa sekä median luomien vaikutusten tunnistamista. Faktan, fiktion ja mielipiteen erottamisen taito näkyy myös *monilukutaito (L4*) osalta. (Opetushallitus 2016, ss. 155–156). *Itsestä huolehtiminen ja arjen taidot (L3)* osa-alueessa puhutaan paljon ympäristössä turvallisesti toimimisesta sekä toiminnasta vaaratilanteissa. Esiin nostetaan myös teknologian monimuotoisuus, tutustuminen teknologin kehitykseen ja pohdinta sen vaikutuksista elämään ja ympäristöihin. Oppilaita tulisi myös ohjata teknologian turvallisuuteen ja eettiseen toimintaan liittyviin pohdintoihin sekä taitoihin. (Opetushallitus 2016, s. 156)

Vuosiluokilla 7–9 opetuksen pääpainotus on siinä, että oppilas saisi edellytykset siirtyä perusopetuksen jälkeisiin opintoihin. Yleensä oppilaiden väliset tasoerot alkavat erottua tässä kohtaa. 7–9-vuosiluokkien opetuksen perusteet tietoturvallisuuden osalta jäljittelevät edellisten luokka-asteiden sisältöjä ja tavoitteita syventävällä otteella. (Opetushallitus 2018, ss. 280, 283) *TVT (L5)* -taitojen osalta kuvataan, että tieto- ja viestintäteknologian tulisi olla luonteva osa oppilaan oppimista. Lisäksi todetaan, että oppilaalla olisi käsitys siitä, miten hyödyntää jo opittua myöhemmin työelämässä sekä yhteiskunnassa. (Opetushallitus, 2016, s. 284)

Ensimmäinen suora ja muihin osa-alueisiin verrattaessa huomiota herättävän laaja viittaus kyberturvallisuuden opetukseen on kirjattu 7–9-vuosiluokkien kohdalle osion *vastuullinen ja turvallinen toiminta* alle kohdassa *Tieto- ja viestintätekniset taidot (L5)*:

> ” *Oppilaita ohjataan turvalliseen ja eettisesti kestävään tieto- ja viestintäteknologian käyttöön. He oppivat, miten suojaudutaan mahdollisilta tietoturvariskeiltä ja vältytään tiedon häviämiseltä. Vastuulliseen toimintaan ohjataan pohtimalla, mitä esimerkiksi käsitteet tietosuoja ja tekijänoikeus tarkoittavat, ja mitä seurauksia vastuuttomasta ja lainvastaisesta toiminnasta voi olla.”* (Opetushallitus, 2016, s. 284)

Yllä olevassa lainauksessa huomataan, että lainaus sisältää melko laajojakin kokonaisuuksia. Jotta oppilas voi ymmärtää ”*miten suojaudutaan mahdollisilta tietoturvariskeiltä*” tai mitä on ”*lainvastainen toiminta*” täytyy hänellä olla kattavat perustiedot kyberturvallisuudesta sekä kyberympäristön erilaisista osa-alueista. Jo vuonna 2014 Limnéll, Majewski ja Salminen ovat todenneet kirjassaan, että monissa valtioissa on keskusteltu kyberturvallisuuden opetuksen järjestämisestä ja sisällöistä. (Limnéll ym., 2014, s. 62) Yllä kuvatut kohdat ovat ne asiat, joita suomalaisen perusopetuksen opetussuunnitelmiin on tällä hetkellä sisällytetty. Löytyneet kohdat ovat kuitenkin huomattavia, ottaen huomioon se, että ne on lisätty opetussuunnitelmien perusteisiin vasta viimeisimmän vuoden 2016 uudistuksen yhteydessä.

4.4 Kyberturvallisuuden opettaminen

Haastavaksi kyberturvallisuuden opetuksen tekee se, että kyberturvallisuus on laaja kokonaisuus, johon opetussuunnitelmien perusteista ei löydy seikkakohtaista ohjeistusta. Opettajien voi olla vaikea hahmottaa sitä, mikä on missäkin yhteydessä olennaista. Tärkeää olisi myös esittää asia niin, että jokainen voi sen oppia erilaisista lähtötasoista huolimatta. (Merilehto, 2019, s.31) Opettajilla on kuitenkin merkittävä rooli tieto- ja viestintätekniikan opetuskäytännöissä. Loppujen lopuksi heistä on myös paljon kiinni, miten oppilaiden mielissä tieto- ja viestintätekniikan ja sitä kautta myös kyberturvallisuuteen liittyvät merkitykset tunnistetaan ja miten näistä opitut asiat konkretisoituvat. Opetussuunnitelmien perusteet luovat puitteet tämän toteutumiselle. (Säntti, 2020, ss. 74–75)

Tampereen yliopistossa tehdyn kehittämistutkimuksen mukaan opettajat tarvitsevat konkreettisia esimerkkejä ja työkaluja tieto- ja viestintäteknologian hyödyntämisestä. Lisäksi tutkimuksessa saatiin selville, että opettajien työtä helpottaisi myös se, että tieto- ja

viestintäteknologiaa kohtaan asetetut tavoitteet olisivat saatavilla tiiviissä muodossa, oppiainekohtaisesti listattuna. Tutkimuksessa tuotettiin myös tukimateriaalia, johon saadun palautteen perusteella toivottiin erityisesti lisäohjeistusta liittyen tietoturvallisuuteen. (Luukka, 2018) Turun yliopiston koulutussosiologisen tutkimuskeskuksen tutkimuksessa on havaittu, että opettajien osaamisessa tietoturvasta on selkeitä puutteita. Tutkimuksessa monilukutaidosta ja ohjelmoinnillisesta ajattelusta 2018 havaittiin, että tietoturvan kannalta olennaisia osa-alueita painotetaan opetuksessa aika vähän, vaikka ne ovat olennaisia. (Leino ym., 2019, ss. 58, 47)

5 Ajankohtaisuus

Kyberturvallisuuden opetuksen tutkimuksen ajankohtaisuutta voidaan perustella monin tavoin. Tässä luvussa pohdimme selvityksen tekemistä yksittäisen kansalaisen näkökulmasta, kansallisten ohjelmien sekä rikostilastojen kautta. Viimeisessä alaluvussa käsittelemme Suomen positiota osana Euroopan unionin kyberturvallisuuden kehitystä.

5.1 Kansalaisten taidot

Kun teknologiset ratkaisut yleistyvät ja yksityishenkilöt pääsevät yhä laajemmin kiinni verkottuneeseen maailmaan sekä tuottamaan sisältöä, voidaan samalla nähdä jokaisen henkilön vastuun laajenevan. Toistaiseksi on melko vähän tutkimusta siitä, minkälaisessa arvossa ihmiset näkevät kyberturvallisuustaidot ja miten tärkeänä he pitävät kyberturvallisuus osaamisen kehittämistä. Usein tietoisuuden herättämisen eteen on tehty työtä erilaisten kampanjoiden kautta, mutta suurta muutosta ei ole vielä ehtinyt tapahtua. Usein teemat ovat ehkä liiaksi keskittyneet luomaan pelkoja. (Dutton, 2017)

Vuoden 2020 digibarometrin teemana oli kyberturva sekä digitaalinen luottamus. Selvityksessä kävi ilmi, että yhä useampi kansalainen on jättänyt käyttämättä digitaalisia tuotteita tai palveluita kyberturvallisuutta koskevien huolien takia. (Mattila ym., 2020, s.15) Pohjoismaissa digitalisaatio ja digipalvelut ovat yleisesti koreatasoisia ja laajasti saatavilla. Tutkimuksissa on kuitenkin havaittu, että yleisten digitaitojen opetuksen lisäksi tarvetta on myös digitaalisen turvallisuuden opetukselle. On arvioitu, että tietotaidon lisäksi on

olennaista, että ihmiset osaavat toimia konkreettisten tekojen kautta turvallisemmin arki elämässään. (Anthony ym., 2019, ss. 11,20)

Maailman digitalisoituminen vaikuttaa myös monella tapaa opiskeluun sekä työelämään. Konkreettinen esimerkki on etätyön ja -opiskelun lisääntyminen sekä siihen liittyvät ratkaisut. Vaikka työelämän joustaminen tällä tavalla on monesti työntekijä etu, tuo se myös mukanaan uusia kyberturvallisuusriskejä. Riskit korostuvat, kun siirrytään yrityksien sisältä jokaisen omaan ympäristöön, joka ei ole yhtä hallittavissa. Työelämässä ja yritysmaailmassa eri toimijoiden välillä on usein monenlaista yhteistyötä. Kyberturvallisuuden näkökulmasta tällöin on erityisen tärkeää huolehtia omasta osaamisesta ja teknisistä ratkaisuista, koska niillä on suora vaikutus myös muihin yrityksiin, työntekijöihin ja yhteistyökumppaneihin. (Limnéll ym. 2014, s. 54–56) Yksilöillä, jotka eivät ole koulutuksen tai työelämän piirissä, ei ole samanlaista ohjaavaa verkosto- ja koulutusmahdollisuutta, vaikka kaikki kansalaiset ovat samalla tavalla alttiita kybermaailma uhille. (Sandroos, 2021, s. 1)

5.2 Yleistyvä verkkorikollisuus

Verkkorikollisuutta voidaan jaotella esimerkiksi, sillä perusteella, onko kyseessä internetin hyödyntäminen rikosten toteuttamiseen, vai tietoverkkoihin tai -järjestelmiin suoraan kohdistuvat rikokset (Sisäministeriö, 2017, ss. 20-21). Internetin välityksellä tapahtuvia rikoksia ovat esimerkiksi kunnianloukkaus, laiton uhkaus, yksityiselämää loukkaavan tiedon levittäminen, erinäiset huijaukset ja petokset sekä seksuaalirikokset (Riku, 2019a). Rikostilastoja käsiteltäessä tulee ottaa huomioon, että todelliset toteutuneet rikosmäärät ovat todennäköisesti huomattavasti suurempia kuin rikosilmoitusten perusteella voitaisiin olettaa, koska osasta rikoksia ei kirjata rikosilmoitusta lainkaan. Lisäksi on huomioitava, että rikosilmoitusten määrän muutos voi olla osittain seurausta myös yleisestä tietoisuuden lisääntymisestä, minkä seurauksena ilmoituksia tehdään enemmän.

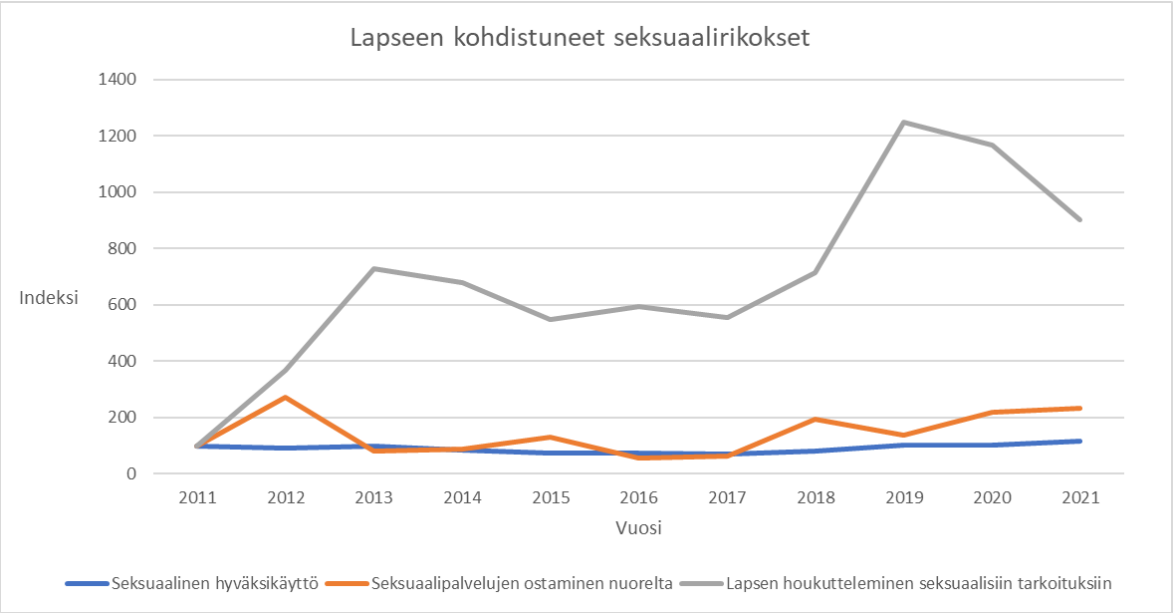
Kuten kappaleessa 4.3 (Kyberturvallisuus osana laaja-alaista osaamista) todettiin, olisi tärkeää, että oppilaat alkavat jo peruskoulussa hahmottaa laajemmin, mihin internetiä ja siihen kytkettyjä laitteita voidaan käyttää sen lisäksi, että tämä kykenisi erottamaan itseen

kohdistuvat riskitilanteet. Usein tilanteet voivat olla monimutkaisia ja vaikeasti hahmotettavia myös aikuisen näkökulmasta.

Internet mahdollistaa yhteydenpidon tuttaviin ja sukulaisiin erilaisten sosiaalisen median alustojen kautta, mutta samalla mahdollistuu myös se, että lapsi tai nuori kohtaa sosiaalisessa mediassa tai pelialustoilla tuntemattomia ihmisiä, jotka saattavat esiintyä toisena henkilönä tai esimerkiksi valehdella ikänsä. Alaikäisen keskustellessa itsensä ikäiseksi esiintyvän henkilön kanssa, on mahdollista, että lapsi tai nuori houkutellaan lähettämään itsestään tietoa tai kuvia, joiden avulla tätä esimerkiksi voidaan kiristää (Riku, 2019b).

Tilastokeskuksen julkaisemasta rikos- ja pakkokeinotilastosta selviää, että lapsiin kohdistuneista seksuaalirikoksista kirjattujen rikosilmoitusten määrissä on havaittavissa kasvava trendi. Kun lasketaan mukaan kaikki kirjatut lapsen seksuaaliseen hyväksikäyttöön ja hyväksikäytön yritykseen liittyvät rikosilmoitukset, on vuoden 2021 lukema (1967 kpl) viiden sekä kymmenen viimeisimmän vuoden keskiarvoihin nähden yli kolmanneksen suurempi ja vuoteen 2020 nähden noin 18 prosenttia. (Tilastokeskus, 2021b) Alla olevasta kaaviosta voidaan havaita, miten rikosilmoitusten määrät ovat vaihdelleet kymmenen viimeisimmän vuoden aikana (Kuva 1). Vuosi 2011 on asetettu vertailukohdaksi (indeksiluku 100).

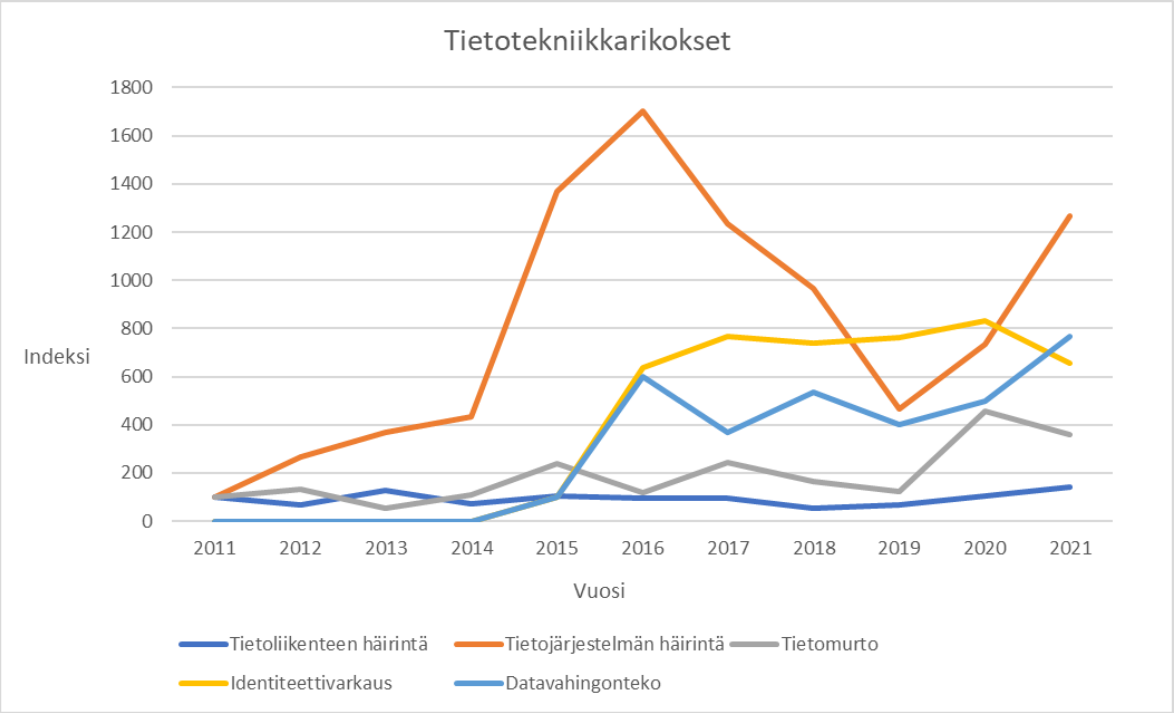
Kuva 1. Lapseen kohdistuneiden seksuaalirikosten rikosilmoitusten määrän kehitys vuosina 2011-2021 (Tilastokeskus, 2021b)



Seksuaalipalveluiden ostaminen nuorelta sekä ostamisen yritys -nimikkeen alle on kirjattu vuodelle 132 rikosilmoitusta ja kasvua viiden sekä kymmenen vuoden keskiarvoihin nähden on tullut yli 70 prosenttia. Muutos vuodesta 2020 oli reilu 6 prosenttia. Lapsiin kohdistuneita seksuaalirikoksia kirjataan myös muiden nimikkeiden alle, kuten lapsen houkutteleminen seksuaalisiin tarkoituksiin. Näiden rikosilmoitusten määrä on niin ikään lisääntynyt viiden (noin viidellä prosentilla) sekä kymmenen vuoden (noin 34 prosenttia) keskiarvoihin nähden, joskin edellisvuodesta ilmoitusten määrä väheni noin 20 prosentilla. (Tilastokeskus, 2021b)

Tietotekniikkarikosten määrässä on tapahtunut muutosta vuodesta 2011, jolloin rikosilmoituksia kirjattiin yhteensä 957 kappaletta, kun taas vuodelle 2021 kirjattiin 5656 ilmoitusta. Seuraavasta kaaviosta nähdään tietotekniikkarikosten sekä datavahingontekojen rikosilmoitusten määrän kehitys vuodesta 2011 (indeksiluku 100) vuoteen 2021 (Kuva 2). Identiteettivarkauksien osalta vertailuvuotena on käytetty vuotta 2015, jolloin valitusta datasta löytyi ensimmäiset kirjaukset tehdyistä rikosilmoituksista. (Tilastokeskus, 2021b)

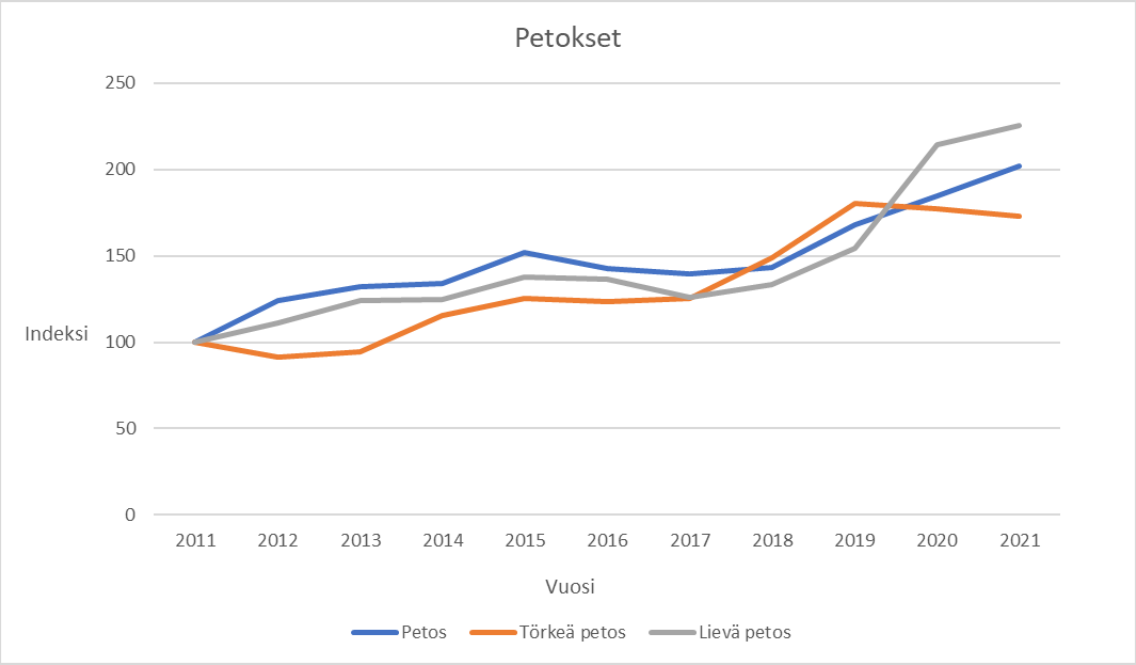
Kuva 2. Tietotekniikkarikosilmoitusten määrän kehitys vuosina 2011-2021 (Tilastokeskus, 2021b)



Vaikka vuosina 2016–2019 on havaittavissa eri rikosnimikkeiden ilmoitusmäärien vähenemistä suhteessa vertailuvuoteen, on trendi silti nouseva. Kaiken kaikkiaan valittujen tietotekniikkarikosten ilmoitusmäärät ovat viiden vuoden keskiarvoon verrattuna noin 10 prosenttia matalammat ja kymmenen vuoden keskiarvoon nähden noin 70 prosenttia korkeammat, datavahingonteon osalta kasvua on tapahtunut noin 60 prosenttia, kymmenen viimeisimmän vuoden havainnot rajoittuvat vuoteen 2015, joten vertailua kymmenen vuoden keskiarvoon ei ole järkevää tehdä. Tietotekniikkarikosten osalta muutosprosentit selittyvät sillä, että identiteettivarkauksien rikosilmoitusmäärissä on tapahtunut vuonna 2016 huomattavaa kasvua (516 ilmoituksesta runsaaseen 3000:een). Edellisvuoteen nähden tietotekniikkarikosilmoitusten ilmoitusmäärissä on havaittavissa noin 20 prosentin lasku, kun taas datavahingontekojen ilmoitusmäärät kasvoivat 53 prosenttia. (Tilastokeskus, 2021b)

Tietoteknisten laitteiden välityksellä tehtävistä huijauksista ja petoksista, sekä niiden yrityksistä, kirjataan rikosilmoitus petosrikokseksi. Seuraavasta kaaviosta nähdään petosrikosten sekä petosyritysten rikosilmoitusten määrän muutos vuodesta 2011 (vertailuvuosi, indeksi 100) vuoteen 2021 (Kuva 3). Petoksiin liittyvät rikosilmoitukset sisältävät kaikki petokset, ei siis ainoastaan verkkohuijauksia tai -petoksia (Riku 2019c).

Kuva 3. Petosrikosilmoitusten määrän kehitys (Tilastokeskus, 2021b)



Petosrikosten ja niiden yritysten yhteenlasketut määrät ovat kasvaneet suhteellisen tasaisesti vuodesta 2011 vuoteen 2021. Petoksiin liittyvien rikosilmoitusten määrät ovat muuttuneet seuraavasti (Kuva 4).

Kuva 4. Petosrikokset 2011-2021 (Tilastokeskus, 2021b)

	2011 (kpl)	2021 (kpl)
Petos 36:1§1-2	8878	17384
Petoksen yritys 36:1§3	1195	2960
Petos yhteensä	10073	20344
Törkeä petos 36:2§1/1-4	1013	1610
Törkeän petoksen yritys 36:2§2	125	359
Törkeä petos yhteensä	1138	1969
Lievä petos 36:3§	6264	14118
Kaikki petokset ja petosyritykset yhteensä	17475	36431

Viiden vuoden keskiarvoon nähden yhteenlasketut rikosilmoitusmäärät ovat muuttuneet 35 prosenttia ja kymmenen vuoden keskiarvoon nähden liki 50 prosenttia. (Tilastokeskus, 2021b)

5.3 Suomen kansalliset kyberturvallisuusohjelmat

Tällä hetkellä Suomessa käytössä oleva kyberturvallisuuden kehittämisohjelma on suunniteltu vuosille 2021–2030. Kehittämisohjelma on konkreettinen toimenpide, jolla Suomen kyberturvallisuusstrategiaa toteutetaan. Strategia on tehty yhteistyössä elinkeinoelämän, yrityksien, valtionhallinnon, järjestöjen sekä koulutussektorin kanssa. Kehittämisohjelmassa määritellään kyberturvallisuuteen liittyviä tavoitteita sekä tärkeimpiä painopisteitä. (Paananen, 2021a, ss. 8–9)

Kehittämisohjelmassa 2021–2030 todetaan, että kansalaisten on tunnistettava riskit, joita erilaisiin laitteisiin sekä digitaalisen yhteiskunnan palveluihin liittyy. Samalla ohjelmassa korostetaan kolmannen sektorin toimijoiden roolia kansalaisten taitojen kehittämisessä.

(Paananen, 2021a, ss. 11–12) Opinnäytetyömme kannalta olennaista on myös se, että kehittämisohjelmassa mainitaan, että kyberturvallisuuden sisällyttämistä perusopetuksen opetussuunnitelmiin harkitaan. Samalla todeten, että perusopetuksessa tulisi olla pyrkimys varmistaa nuorten riittävä taidot ja ymmärrys kyberturvallisuudesta ja kyberympäristöjen uhista. Tästä vastaa opetus- ja kulttuuriministeriö. (Paananen, 2021a, ss. 13)

Ihannekuvassa kansalaisella olisi tarvittavat tiedot ja taidot, jolla hän pystyy toimimaan turvallisesti digitaalisessa yhteiskunnassa. Tämän voidaan katsoa olevan merkittävä asia niin yksilön kohdalla kuin yhteiskunnankin näkökulmasta. (Paananen, 2021a, s. 33)

5.4 Suomen kyberturvallisuus osana Euroopan unionia

Suomella on aiemmassa kappaleessa esitelty oma kyberturvallisuusstrategiansa, joka limittyy yhteen EU:n laajuisen strategian kanssa. (Paananen, 2021a, s. 7) Suomen kansainvälisen yhteistyön pohjana ovat yhteiset sopimukset, oikeusvaltioperiaatteet, läpinäkyvyys sekä ihmisoikeuksien kunnioittaminen. Euroopan unionin lisäksi Suomi tekee yhteistyötä muun muassa YK:n ja ETYJ:n kautta. (Turvallisuuskomitea, 2019, s. 5)

Euroopan komissio on todennut, että vahva kyberresilienssi vaatii yhteistä lähestymistä ja sitä varten on luotava rakenteita sekä EU:lle itselleen, että sen jäsenmaille. Euroopan Unioni myös kohdistaa aktiivisesti rahoitusta kyberturvallisuuden sekä kyberturvallisuusalan kehitykseen. (Lehto ym, 2019, s. 15) Euroopan komissio kehittää jäsenmaiden kanssa myös koulutusjärjestelmiä. Komissio on määritellyt tärkeimpiä osaamisalueita, joita jäsenmaiden koulutuslaitosten tulisi edistää. Yksi kahdeksasta kompetenssista on digitaalinen kompetenssi, joka kuvastaa yksilön kykyä käyttää tieto- ja viestintäteknologiaa monipuolisesti niin opiskelussa, työelämässä sekä vapaa-ajallaan. Tätä kautta myös suomalaisessa peruskoulussa tehtävän opetuksen tulee tukea digitaalisen kompetenssin kehittymistä. (Holmström & Korkka, 2019, ss. 9–10)

6 Aiemmat tutkimukset

Kyberturvallisuuden oppiaineen puolesta ovat puhuneet Suomessa muun muassa Tom Packalen sekä Jarno Limnell. Heidän näkemyksensä mukaan opetuksen olisi hyvä alkaa jo ensimmäisellä luokalla ja siihen voisi sisältyä kyberajokortin saaminen todistukseksi osaamisesta. (MTV Uutiset, 2014) Varsinaista tutkimusta nyt tutkittavasta aihealueesta löytyi kuitenkin melko vähän.

Vuonna 2014 toteutettiin Sitran Uusi turvallisuus -foorumin kokeilu, jossa hahmoteltiin kyberturvallisuuden koulutuspakettia lukioikäisille. Tämän toteuttivat yhteistyössä Espoon yhteislyseon lukio ja Kaitaan lukio sekä Aalto-yliopisto, Espoon kaupunki ja Poliisi. (Sitra, 2014) Kokeilussa todettiin, että olennaisia kyberturvallisuuteen liittyviä taitoja ovat luotettavuuden arviointi, omien tietojen luovuttamisen turvallisuuden ja pysyvyyden pohtiminen sekä laitteiden päivittämiseen liittyvät taidot ja salasanojen turvallinen käyttö. Kokeilussa myös todettiin, että näiden taitojen opettaminen ei vielä ole systemaattista. Lisäksi todettiin, että nuorille suunnattuja materiaaleja on saatavilla liian vähän. (Karjalainen, 2014) Myös Aalto-yliopiston järjestämässä paneelikeskustelussa 2015 kybertoimintaympäristön turvallisuudesta ja yksityisyydestä useat asiantuntijat totesivat yhteisesti, että kansalaistaitojen opetus myös tämän osa-alueen kannalta olisi tärkeää. Keskustelussa todettiin myös, että kybermaailmasta tulee myös tehdä tarpeeksi ja laadukasta tutkimusta. (Aalto-yliopisto, 2015) Kyberturvallisuuden perusteiden opetusta on myös pilotoitu kurssimuotoisena ammatillisiin oppilaitoksiin Suomessa. (STUL, 2018)

Digiajan peruskoulu -selvityksessä on todettu, että digitalisaatiota on otettu paremmin huomioon opetuksen suunnittelussa ja, että opettajien digitaidot kehittyvät, kun kokemusta karttuu. Mutta pääosin vaikuttaa siltä, että digitaitojen hallinta painottuu nuorempiin opettajiin. Selvityksessä on myös todettu tarve taata lapsille ja nuorille tasavertaiset mahdollisuudet kartuttaa digiosaamista osana suomalaista peruskoulua. (Tanhua-Piiroinen ym., 2019)

Digitaidot ovat keskeisiä myös siirryttäessä työelämään. Turun yliopiston Koulutussosiologian tutkimuskeskuksessa (RUSE) tehdyn selvityksessä 2018 havaittiin, että

toisella asteella opiskelijoiden digitaidoissa on merkittäviä eroavaisuuksia. Huomiota selvityksessä herätti myös se, että naisvaltaisilla aloilla digiosaaminen on heikompaa sukupuoleen katsomatta. Lisäksi lukiolaisilla arvioitiin olevan paremmat taidot kuin ammattikoululaisilla. Selvityksessä arvioitiin, että erot syntyvät jo peruskoulun aikana ja tästä syystä perusopetuksessa tehtävä digitaitojen opetuksen merkitys korostuu. (Turun yliopisto, 2018) Edellä mainitun selvityksen ja muiden tutkimuksin perusteella myös Yleisradio perusti vuonna 2019 Digitreenit- kokonaisuuden kaikkien saataville. Kokonaisuus tähtää matalan kynnyksen digitaitojen opettamiseen. Yhtenä aihekokonaisuutena tietoturvallisuus. (Alijoki, 2019, ss. 51–55)

Malesialaisessa tutkimuksessa 2020 todettiin, että kyberturvallisuuden taitojen opetukseen pitäisi panostaa mahdollisimman aikaisessa vaiheessa, jotta isommilta uhilta vältyttäisiin. Lapset tarvitsevat taitoja, joita käyttää silloin kun he joutuvat vaaraan esimerkiksi rikollisuuden kohteeksi tai huijausyrityksen uhriksi. Käytännön opetuksessa voisi käyttää esimerkiksi piirrettyjä, esseiden kirjoittamista, ryhmätoimintaa sekä erilaisia kyberturvallisuusviikon aktiviteetteja. (Rahman ym., 2020, ss. 379–380)

Tutkimuksessa, johon osallistui lukion oppilaita, heidän vanhempiansa sekä opettajia yhdeksästä Euroopan maasta todetaan, että kyberturvallisuuden opetusmetodien tulisi olla innovatiivisia ja vuorovaikutuksellisia. Tähtäimenä koulutuksessa tulisi olla pitkäkestoiset taidot sekä tietoisuus kyberturvallisuuden eri ilmiöistä. (Blažic, 2022)

Hollantilaisessa tutkimuksessa tutkittiin peruskoulussa ja lukiossa olevien nuorten käyttäytymistä kyberturvallisuuden näkökulmasta. Tutkimuksessa todettiin, että nuoret harvoin jakavat vanhemmilleen tietoa siitä, jos kokevat jotain kummallista netissä. He myös harvoin kiinnittävät huomiota esimerkiksi profiilien yksityisyysasetuksiin. Yleisesti tutkimuksessa todettiin, että opetus on jäljessä siitä, mitä tosiasiallisesti maailmassa tapahtuu ja, että tietoisuuden lisääminen olisi olennaista muun muassa sen takia, että lapset ja nuoret ovat verkossa alttiita verkkorikollisuudelle. (Witsenboer ym., 2022)

Samaan aikaan tämän opinnäytetyön valmistumisprosessin aikana Aalto-Yliopiston tutkijat ovat kehittämässä kansalaisten kyberturvallisuuden koulutuspakettikokonaisuutta EU-

maihin, vuonna 2022 alkaneen kolmen vuoden rahoituksen turvin. Kansalaistaitojen opettamisen merkitys on siis tunnistettu ja erittäin ajankohtainen. (Liikenne- ja viestintäministeriö, 2022)

Lisäksi juuri opinnäytetyömme valmistumisen kynnyksellä syksyllä 2022 julkaistiin Jyväskylän yliopiston kyberturvallisuuden professori Martti Lehdon johtaman hankkeen loppuraportti, jossa selvityksen kohteena oli kybertuvallisuuden koulutusohjelman muutostarpeiden selvitys. Loppuraportissa oli avattu sekä selvitetty laajalti kyberturvallisuuden opetuksen järjestämistä eri opetusasteilla, yrityksissä, valtion toimesta sekä kolmannella sektorilla. Tutkimuksen osana selvitettiin myös tilannekuva peruskoulussa tapahtuvasta opetuksesta. (Lehto, 2022, s. 5)

Selvityksessä todetaan, että nykyisellään suomalaisessa peruskoulussa TVT-taitojen tavoitteet eri oppiaineissa eivät ole kovin selkeitä ja materiaalit ovat puutteellisia. Materiaaleista todettiin myös, että ne ovat lähinnä vapaasti käytettävissä eivät niinkään opetukseen velvoittavia. Huomiota selvityksessä kiinnitettiin myös siihen, että opetus voi vaihdella niin koulu- kuin paikkakuntakohtaisesti. Selvityksessä todettiin myös tarve lisätutkimukselle opetuksen tarpeellisuudesta. Varsinaisesta opetuksesta selvityksessä kävi ilmi se, että opetuskäytännöt digitaalisesta turvallisuudesta vaihtelevat ja osa opettajista ei käy aihealuetta ollenkaan lävitse. (Lehto, 2022, s.29)

Professori Lehdon johdolla tehdyn selvityksen mukaan tarve ja tärkeys digitaalisen turvallisuuden sisällyttämiseksi perusopetukseen tunnistetaan. Selvityksen lopputuloksena esiteltiin kolme mallia, joiden avulla tulevaisuuden opetusta voitaisiin järjestää ja lisätä peruskoulussa tapahtuvassa opetuksessa. Tiivistettynä kolme vaihtoehtoista mallia olisivat seuraavat: Lisätään digitaalinen turvallisuus omaksi osa-alueeksi opetukseen, vahvistetaan digitaalisen turvallisuuden näkyvämpi rooli osana tieto- ja viestintäteknologista osaamisaluetta (TVT) ja erillisen digitaalisen turvallisuuden osa-alueen lisääminen pakolliseksi osaksi tieto- ja viestintäteknologista opetusta. (Lehto, 2022, ss. 7- 8)

7 Tutkimuksen näkökulmat

Opinnäytetyömme ensimmäisen osan keskeisenä tavoitteena on kartoittaa, miten kyberturvallisen toimimisen opetus toteutuu nykytilassa ja reflektoida tutkimuksesta saatuja tietoja käytössä olevan opetussuunnitelman ohjeistuksiin. Opinnäytetyön toisessa osassa perehdymme siihen, mitä teemoja kyberturvallisuudesta ja millä keinoin kyberturvallisuutta voitaisiin opettaa peruskouluikäisille. Asiantuntijoiden kyselyvastausten avulla kootaan yhteen näkemyksiä siitä, mitä teemoja opetuksessa tulisi käsitellä ja miten opetus käytännössä voisi toteutua. Opinnäytetyössä ei tulla keskittymään pedagogiseen toteutukseen.

Opinnäytetyön tilaajana toimii Opetushallitus. Opetushallitus on Suomessa toimiva kehittämisvirasto, joka keskittyy opetuksellisiin asioihin sekä kehittämistoimintaan. Opetushallituksessa esimerkiksi laaditaan varhaiskasvatuksen, perusopetuksen ja lukion opetussuunnitelmien perusteet. Opetushallitus tekee myös säädöksiin, määräyksiin, ohjeistuksiin sekä suosituksiin liittyvää työtä. Opetushallitukselle on myös keskitetty koulutukseen liittyvien tietojärjestelmien sekä rekisterien hallinta. (Opetushallitus, 2022b)

8 Tutkimuksen toteutus

Opinnäytetyö on selkeästi tutkimuspainotteinen opinnäytetyö. Työn tutkimuksellinen osuus koostuu kahdesta tutkimusosiosta, joista molemmat toteutetaan kyselytutkimuksena tutkimuslomakkeella. Tutkimus rajattiin koskemaan suomalaisessa peruskoulussa 1.-9. luokalla tapahtuvaa opetusta, joka perustuu kyberturvallisuutta ja tietoturvaa koskeviin kokonaisuuksiin opetussuunnitelmien perusteissa. Tutkimuksessa selvitetään opetuksen nykytilaa peilattuna tämänhetkisiin opetussuunnitelmien perusteisiin sekä pyritään löytämään suuntaviivoja siihen, mitä osia kyberturvallisuudesta olisi olennaista opettaa suomalaisessa peruskoulussa. Opetusta selvittävän osuuden kyselytutkimus suunnataan peruskoulussa opetustyötä tekeville ja teemasisältöjä selvittävä kysely kyberturvallisuuden ammattilaisille.

Tutkimuksen rajaaminen peruskouluikäisiin lapsiin ja nuoriin mahdollistaa sen, että kyberturvallisuuden perusteita pystytään tarkastelemaan riittävän alkeista lähtien. Peruskoulu on merkittävä suomalainen instituutio, jota on olennaista tarkastella opinnäytetyön teeman näkökulmasta. Opinnäytetyön aihe mahdollistaa myös jatkotutkimuksen (esimerkiksi opettajakoulutuksen jatkotutkimukset) sekä tutkimuksen laajentamisen koskemaan myös varhaiskasvatusta sekä aikuisikäistä väestöä (esimerkiksi kyberturvallisuuden ajokortti). Opinnäytetyö voi parhaimmillaan toimia pohja-aineistona, kun peruskoulun opetussuunnitelmien perusteita uudistetaan seuraavan kerran.

8.1 Tutkimuskysymykset ja tutkimuksen tarkoitus

Pyrimme opinnäytetyössämme vastaamaan seuraaviin tutkimuskysymyksiin:

- Millainen on kyberturvallisuuden opetuksen tila tällä hetkellä ja miten perusopetuksen opetussuunnitelmien perusteiden mukainen ohjeistus toteutuu suomalaisessa peruskoulussa?
- Mitä osia kyberturvallisuuden aihepiiristä olisi olennaista opettaa suomalaisessa peruskoulussa kyberturvallisuuden ammattilaisten näkökulmasta ja miten kyberturvallisuuden opetusta voitaisiin suositella edistettävän tulevina vuosina?

Tutkimuksen tarkoituksena on koota yhteen opetusalan sekä kyberturvallisuusalan ammattilaisten näkemykset kyberturvallisuuden opetuksen tämänhetkisestä tilasta ja toteutumisesta sekä selvittää, mihin teemoihin olisi tarkoituksenmukaista keskittyä tulevaisuudessa, jotta peruskoulutuksessa voidaan tarjota lapsille ja nuorille riittävät taidot niin kyberympäristössä toimimiseksi, kuin myös jatkokoulutusta sekä työelämää varten. Tutkimuksen avulla tuotetaan tietoa kyberturvallisuuden opetuksen nykytilasta sekä kuvaa mahdollisesta tulevaisuuden opetuksesta sekä sen sisällöistä.

8.2 Kvantitatiivinen tutkimus

Kvantitatiivisessa eli määrällisessä tutkimuksessa hyödynnetään erilaisia mittareita ja mittaustekniikoita, joilla aineiston muoto ja tulosten esitystapa on numeerinen. Määrällisen

tutkimuksen analysointi tapahtuu tilastollisin menetelmin ja vastaajien määrä on yleensä suuri. Määrällisellä tutkimuksella pyritään tutkittavan ilmiön selittämiseen sekä tulevaisuuden suuntien hahmottamiseen. Tutkimuksen luotettavuutta sekä yleistettävyyttä tukee riittävän laaja aineisto. (Vilpas, N.d, s. 1) Kvantitatiivisessa tutkimuksessa pyritään havainnollistamaa käsiteltävää ilmiötä numeerisesti. Samalla voidaan käyttää erilaisia luokittelumenetelmiä ja hahmottaa syy-seuraus -suhteita. (JYU, 2015)

Yhdistelemme opinnäytetyössä molempia edellä mainittuja suuntauksia. Opinnäytetyömme numeerinen osuus koostuu kysymyksistä, joissa vastaajalla oli käytössään asteikko tai ennalta määritellyt vastausvaihtoehdot. Näissä kohdissa pystymme muun muassa prosenttimääräisesti tuomaan ilmi vastaajien tai vastaajaryhmien vastausten tuloksia sekä vastausten yhteneväisyyksiä sekä eroja.

Opinnäytetyömme sisältää myös kvalitatiivisen eli laadullisen tutkimuksen elementtejä. Laadullisessa tutkimuksessa ollaan yleensä jollain tavalla kiinnostuneita vastaajan subjektiivisista näkemyksistä ja kokemuksista eli henkilökohtaisesta kokemusmaailmasta. Näin ollen vastaajien vastausten käsittelyssä ja tulkinnassa korostuvat heidän eri asioille antamat merkitykset ja painoarvot. Laadullisista aineistoista voi olla haastavampaa poimia yleistyksiä, syy-seuraus -suhteita tai muuta selkeää, koska ihmisten yksilölliset vastaukset eivät noudata yhtenäistä kaavaa tai rakennetta. (Kallinen & Kinnunen, n.d.)

8.3 Tutkimusmenetelmät ja kohderyhmä

Kyselylomake on perinteinen tapa kerätä tutkimusaineistoa. Nykyisin lomakkeet toimitetaan usein sähköisenä vastaajille paperisten sijaan. Sähköisen kyselyn etu on se, että tieto on suoraan tutkijan hyödynnettävissä. (Valli, 2015, s.101) Kysymysten muotoiluun on tärkeä keskittyä, koska ne luovat perustan sille, että kyselytutkimus onnistuu ja, jotta tutkimustuloksiin ei tulisi kysymyksien asettelusta johtuvia virheellisyyksiä. Jos samasta aiheesta ei ole aiemmin tehty tutkimuksia, tutkimuksen tekijä voi joutua käyttämään aikaa myös sen pohdintaan, miten aihealueen käsitteet ja aiheet muutetaan mittareiksi eli kysymyksiksi. Kyselytutkimukset sisältävät yleensä useanlaisia kysymyksiä: taustakysymyksiä, helppoja kysymyksiä, laajoja kysymyksiä ja jäähdyttelykysymyksiä. Myös lomakkeen kieliasu

tulee olla harkittu. (Valli, 2015, ss. 92-96) Toteutus on poikittaistutkimus eli vastauksia kerätään tietyllä ajan hetkellä useammalta vastaajalta (Valli, 2015, s. 129)

Tutkimuslomakkeen kysymyksissä mittausasteikkoina käytimme Likertin viisiportaista asteikkoa, Intensiivisyysasteikkoa sekä avoimia kysymyksiä. (Valli, 2015, ss. 106-107, 112, 114). Näiden tekniikoiden yhdistelemisellä saadaan aikaan numeerisesti kuvattavaa dataa vastauksista, mutta annetaan myös vastaajille mahdollisuus vapaasti sanallisesti kommentoida tutkimuksen kohteena olevia asioita. Käytännössä verkkolomake toteutettiin Webropol-työkalun avulla, jonka saamme ammattikorkeakoulun kautta käyttöön. (HAMK, N.d.; Valli & Aaltola, 2018, ss. 122–123) Vastaajat vastasivat kyselyihin itsenäisesti omalla laitteellaan ilman tutkimuksen tekijän paikallaoloa. Kyselyt olivat kaikille avoimia verkkokyselyitä. Kyselyitä mainostettiin sosiaalisessa mediassa esimerkiksi Facebookissa, Instagramissa sekä ammattilaisten verkostoitumispalvelu LinkedIn:ssa. Opinnäytetyön tekijöiden lisäksi kyselyitä lähtivät jakamaan edelleen useat yhdistykset, organisaatiot ja yksityiset henkilöt.

Osa tutkimuskysymyksistä toteutettiin puolistrukturoidusti. Puolistrukturoitujen kysymysten kohdalla ei ole valmiita vastausvaihtoehtoja, vaan vastaajat saivat vapaasti vastata haluamallaan tavalla avoimiin tekstikenttiin. Avoimien tekstikenttien käytön tavoite ei ole löytää tilastollisesti yleistettäviä kokonaisuuksia, vaan kartoittaa vastaajien näkemyksiä tutkimuksen kohteena olevista ilmiöistä. (Tuomi & Sarajärvi, 2018, s. 98)

Lomakkeet pyrittiin tekemään tarpeeksi kevyiksi, jotta vastaajat eivät kokisi vastaamista liian raskaaksi. Arvioimme, että kyselyiden täyttö kestäisi maksimissaan noin 20 minuuttia. Pyrimme herättämään luottamusta sekä mielenkiintoa mainitsemalla kyselyiden ensimmäisellä sivulla kokonaisuuden, johon kysely liittyy, ammattikorkeakoulumme nimen sekä opinnäytetyön tekijöiden sekä työn ohjaajan yhteystiedot. Ulkoasuksi valitsimme melko minimalistisen teeman ja hillityt värit. Koimme, että tällä tavoin kyselyä tehtäessä vastaajan huomio keskittyisi olennaiseen ja kysely olisi kokonaisuutena selkeä. Selkeyteen pyrimme myös sillä, että jaottelimme kyselyn pienempiin osiin sivun vaihtojen, ohjeistuksen sekä pääteemojen luomisen avulla.

8.4 Tutkimuksen rajaukset ja aineiston keruu

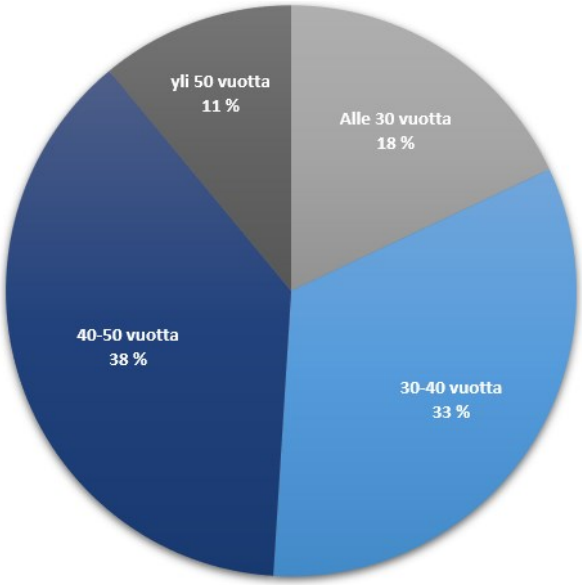
Opettajille kohdennetussa tutkimuksessa oli alun perin tarkoitus toteuttaa koko maan laajuinen kysely kaikille perusopetuksen opettajille. Kuitenkin osoittautui, että koko maan laajuinen tutkimus on eri kaupunkien osalta vaihtelevan tutkimuslupamenettelyn vuoksi pitkäkestoinen, erittäin työläs ja opinnäytetyölaajuudessa mahdoton toteuttaa. Tästä syystä koko maan laajuisen peruskoulututkimuksen sijaan päädyttiin toteuttamaan tutkimus avoimella verkkokyselyllä, jota välitettiin vastaajille verkostojen ja sosiaalisen median kautta.

Avoin verkkokysely oli auki kaksi viikkoa. Kysely oli suunnattu suomalaisessa peruskoulussa opetustyötä tekeville henkilöille. Myös ammattilaisille suunnattu kyselytutkimus toteutettiin avoimella verkkokyselyllä samankaltaisiin syihin perustuen. Ammattilaisille suunnattu avoin verkkokysely niin ikään avoinna vastattavaksi kahden viikon ajan. Kysely oli suunnattu kyberturvallisuuden parissa työskenteleville henkilöille.

Avoimien kyselyiden epävarmuustekijänä ja osin rajauksen hankaluutta aiheuttavana tekijä voidaan pitää sitä, että emme voi täysin varmistua vastanneiden henkilöiden taustoista. Periaatteessa julkisessa levityksessä olleisiin verkkokyselylomakkeisiin on voinut vastata kuka vain. Pidämme kuitenkin melko pienenä riskinä sitä, että kukaan kyselyn kohderyhmän ulkopuolelta olisi vastannut useamman sivun kyselyyn esittäytyen taustaltaan toisenlaisena henkilönä kuin oikeasti on.

Ammattilaisten kyselyyn vastasi kyselyn aukioloaikana 149 henkilöä. Heistä 18 prosenttia oli alle 30-vuotiaita, 33 prosenttia 30–40-vuotiaita, 38 prosenttia 40-50 vuotiaita ja 11 prosenttia yli 50 -vuotiaita. Suurimmalla osalla 46 % vastaajista oli 3–10 vuotta kokemusta kyberturvallisuuden parissa työskentelystä (Kuva 5).

Kuva 5. Ikäjakauma



Selvästi suurin osa 77 % vastaajista oli Etelä-Suomen alueelta. Vastaajia saatiin myös muilta alueilta: Länsi-Suomi ja Ahvenanmaa, Itä-Suomi, Oulun seutu sekä Pohjois-Suomi. Suurin osa, 78 % vastaajista, työskentelee yli 250 henkiä työllistävissä organisaatioissa.

Opettajien kyselyyn vastaukset saatiin 9 henkilöltä. Suurin osa vastaajista oli iältään yli 40-vuotiaita (56 prosenttia). Vastaajista 6 oli aineenopettajia ja 3 luokan opettajia. Enemmistöllä vastaajista (55 prosenttia) opetuskokemusta oli 10 vuotta, loput vastanneista ilmoittivat työkokemuksensa pituudeksi 3-6 vuotta. Vastaajista 22 prosenttia työskenteli 200-400 oppilaan koulussa, 33 prosenttia 400-700 oppilaan koulussa ja 45 prosenttia yli 700 oppilaan koulussa. Vastaajista kolmasosa kertoi tekevänsä opetusta alakoulussa ja kaksi kolmasosaa yläkoulussa. Maantieteellisesti eniten vastaajia oli Etelä-Suomen alueelta (67 %), loput vastaukset jakautuivat suhteellisen tasan muun Suomen kesken.

8.5 Analysointi

Kerättyä tietoa pyritään opinnäytetyössä havainnollistamaan kaavioin ja kuvioin sekä mahdollisilla sitaateilla. Pyrimme myös hahmottamaan molemmissa tutkimuksissa havaittuja ilmiöitä, jotka kuvaavat kyberturvallisuuden opetuksen nykytilaa sekä hahmotelmia tärkeistä opetettavista teemoista.

Valitsimme analysointiin menetelmät, joiden avulla aineistosta nostetaan esiin toistuvimmat teemat sekä muut huomion arvoiset asiat, jotka vastaavat asettamiimme tutkimuskysymyksiin. (Eskola & Suoranta, 1998, ss. 87-90) Aineistosta pyritään koodauksen ja teemoittelun avulla hahmottamaan toistuvuutta ja samankaltaisuuksia. Yhtenäisistä havainnoista pyritään muodostamaan kategorioita, jotka kuvaavat merkityksiä, joita vastaajat kirjoituksissaan luovat. Tarvittaessa nostamme myös vastauksista sitaatteja, jotka kuvaavat vastaajan ydinsanomaa. Tyypittelyn avulla havaituista teemoista saadaan vielä tarkempi kuva etsimällä yhteneväisyyksiä ja lopulta muodostamalla yleistetty näkemys. (Eskola & Suoranta, 1998, ss. 170-172, 175-181; Tuomi & Sarajärvi, 2018, ss. 105-107) Kokonaisuudessaan sisällön analysoinnilla pyritään muodostamaan yhtenäistä kuvaa tutkittavasta aineistosta ja myöhemmin luotettavia johtopäätöksiä käsiteltävistä aiheista. Tarkoitus on liikkua empiirisestä aineistosta käsitteelliseen selostukseen tutkittavasta ilmiöstä. (Tuomi & Sarajärvi, 2018, ss. 122-127).

Strukturoinnin avulla määrittelimme tutkittavasta teemasta kysymyksiä kyselylomakkeisiin. Näiden kysymysten vastausvaihtoehdot olimme ennalta määritelleet. Vastausvaihtoehtoja oli usein miten viisi ja jokaiselle vaihtoehdolle annettiin numeerinen vastine. Moni käyttämistämme asteikoista mukaili Likertin sekä Osgoodin asteikkoa. (Vilkka, 2007, ss. 15, 46 -47) Aineiston käsittelyvaiheessa hyödynsimme käytössämme ollutta kyselytyökalua, jonka avulla saimme valmiiksi numeerisista muuttujista laskettuja arvoja ja graafeja.

Ensimmäisestä tutkimuksesta saatujen vastauksien avulla pyrittiin muodostamaan vastauksista yhteenveto, joka kuvaisi opetuksen tilaa ylipäätään Suomessa. Toisessa tutkimuksessa samankaltaista yhteenvetoa pyrittiin tuottamaan kyberalan ammattilaisten näkemyksistä kyberturvallisuuden osa-alueiden opetuksesta sekä opetuksen tulevaisuudesta.

8.6 Eettisyys ja luotettavuus

Tutkimusta tehdessä tulee aina noudattaa hyvää tieteellistä käytäntöä. Hyvän tieteellisen käytännön noudattamisesta ovat vastuussa työn tekijät itse. Hyvä käytäntö edellyttää, että kaikki tutkimuksen tekemisen vaihteet suoritetaan huolellisesti ja tarkasti. Huomiota on

myös syytä kiinnittää tutkimus- ja arviointimenetelmiin sekä siihen, että toteutuksessa tehdyt valinnat ovat eettisesti kestäviä. Lähteisiin tulee viitata noudattaen huolellisesti valittua viittaustapaa. (Tutkimuseettinen neuvottelukunta, 2022)

Kyselytutkimusten toimitustapa heikentää tutkimusten luotettavuutta siltä osin, että vastaajan ammatillisesta taustasta ei voida täysin varmistua. Kyselytutkimuksessa esitettyjen kysymysten laajuuden sekä kyselyyn kuluvan ajan vuoksi voidaan kuitenkin olettaa, että vastaaja kuuluu kohderyhmään tai hänellä vähintäänkin on näkemystä kyselyn aiheeseen.

9 Tulokset

Kyselytutkimusten julkaisu toteutettiin yhtenäisesti niin, että jakelussa hyödynnettiin ammattiryhmän verkostoja, sosiaalista mediaa sekä ammattilaisverkostopalvelu LinkedIn:a. Kyselytutkimuskutsu sisälsi tiivistetysti tiedon tutkimuksen kohderyhmästä, taustasta ja tavoitteesta, minkä lisäksi saatetekstin yhteyteen sisällytettiin kyselytutkimuksen linkki.

Seuraavaksi esitellään kyselytutkimusten tulokset: ensin opettajille suunnatun (kyberturvallisuuden opetuksen nykytila) kyselytutkimuksen tutkimuksen tulokset, minkä jälkeen kyberturvallisuuden ammattilaisille suunnatussa kyselytutkimuksessa (kyberturvallisuuden opetuksen teemat ja tulevaisuus) esiin nousseet asiat.

9.1 Kyberturvallisuuden opetuksen nykytila

Opettajille kohdennetun kyselytutkimuksen kutsu julkaistiin kymmenessä sosiaalisen median opettajaryhmässä sekä ammattilaisverkostopalvelu LinkedIn:ssa. Opettajille suunnatun kyselyn toimittamisessa vastaajille havaittiin, että verkostojen kautta välitettävän kyselytutkimuksen haasteena on riittävän laajan vastaajajoukon tavoittaminen sekä mahdollisesti myös vastaajien innostaminen kyselyyn vastaamiseen.

Puolessa välissä opettajien kyselytutkimuksen toteutusta (viikko julkaisusta), oli havaittavissa kyselytutkimuksen tavoittavuuden haasteet, minkä perusteella kyselytutkimusta pyrittiin tuomaan esille tehokkaammin sisältöpalveluiden (Instagram, Facebook) sekä

Opetushallituksen verkostojen avulla. Lisäksi julkaistiin muistutuksenomaiset uudet julkaisut kaikkiin alkuperäisiin sosiaalisen median kanaviin, minkä lisäksi alkuperäisiä julkaisuja nostettiin uudelleen esille.

Opettajille suunnattuun kyselyyn saatiin yhteensä yhdeksän vastausta. Pienen vastausmäärän vuoksi kattavasti yleistettäviä trendejä ei voida määritellä. Vastauksista voidaan kuitenkin hahmottaa selkeät teemat, jotka näiden yhdeksän vastaajan vastauksissa ilmenevät. Kyselytutkimuksen avoimiin kysymyksiin annettuja vastauksia käsitellään yleisellä tasolla vastaajien yksityisyyden suojaamiseksi.

Opettajien kyselylomakkeen vastauksissa on havaittavissa osaamiseen näkökulmasta katsottuna kahta ääripäätä sekä osaamisen keskitasoa edustavia vastaajia. Kyselyyn vastanneista kolme työskentelee luokanopettajina (1.-9. -luokilla). Vastaajista kuusi työskentelee aineenopettajina, ja heistä kolme opettaa myös tieto- ja viestintätekniikkaa.

9.1.1 Opettajien valmiudet kyberturvallisuuden opetukseen

Kyselyyn vastanneista opettajista suurin osa kokee tuntevansa kyberturvallisuuden peruskäsitteistöä melko hyvin. Kyselytutkimuksessa opettajia pyydettiin arvioimaan omaa osaamistaan kyberturvallisuuden käsitteistä asteikolla 1-5:

1 = En tiedä mitä käsite tarkoittaa
2= Tiedän mihin aihe-alueeseen käsite liittyy
3 = En osaa sanoa
4 = Osaan melko tarkasti kuvata käsitteen
5 = Osaan kattavasti kuvata mitä käsite tarkoittaa.

Peruskäsitteistön osaamista koskevassa kysymyksessä opettajat arvioivat osaamistaan 11 eri termin kautta. Termit kuvasivat kyberturvallisuuden eri osaamisalueita. Opettajien arvioimat termit vaihtelivat yleisesti tunnetuista vähemmän tunnettuihin enimmäkseen kyberalan ammattilaisten käyttämiin termeihin. Parhaiten tunnistettuja termejä olivat tietoturvallisuus (4,4), kaksivaiheinen tunnistautuminen (4,3), haittaohjelma (4,1), identiteettivarkaus (4,7) ja

informaatiovaikuttaminen (4,3). Vieraimmiksi koetut termit olivat CIA-malli (1,4), kriittinen infrastruktuuri (2,8) ja kyberresilienssi (2,2). Suluissa olevat luvut kuvaavat vastausten keskiarvoja yllä esiteltyyn asteikkoon perustuen.

Opettajia pyydettiin myös arvioimaan opettajan opinnoissa saamiaan valmiuksia kyberturvallisuuteen liittyvistä kokonaisuuksista asteikolla 0-10 (en ole saanut lainkaan tietoa – olen saanut kattavasti tietoa). Vastausten keskiarvo oli 2,8, mediaani 1, minimiarvo 0 ja maksimiarvo 8. Kyselytutkimuksen avoimissa vastauksissa oli havaittavissa selkeästi, että suurin osa vastaajista ei ole saanut minkäänlaista täydennyskoulutusta kyberturvallisuuden osaamisalalta, eikä opettajan opinnoissa ole käsitelty aihepiiriä juurikaan. Mikäli opetusta on ollut, se on ollut pintapuolista. Yksi vastaaja kertoi käyneensä työnantajan tarjoaman verkkokurssin liittyen tietosuojaan ja GDPR:n. Kaksi vastaajaa nosti esiin omatoimisen opiskelun. Täydennyskoulutuksen tapaan myös opettajan opinnoissa saadut tiedot ovat rajautuneet aiheen käsittelyyn pintapuolisesti. Sen lisäksi useammassa vastauksessa tuotiin esille, että opetuksessa on käsitelty tietoturvaa opettajan työn tekemisen näkökulmasta. TVT-opettajina (tieto- ja viestintätekniikka) työskentelevä vastaaja kertoi seuraavansa aihepiiriä itsenäisesti.

Opettajilta pyydettiin numeerista arvioita omista valmiuksistaan opettaa kyberturvallisuus- ja tietoturva-aiheita. Arviointi asteikkona käytettiin numeerista asteikkoa 0–10 (en koe omaavani valmiuksia kyberturvallisuuden opetukseen – koen omaavani kattavat valmiudet). Vastausten keskiarvo oli 5,4, mediaani 5,5, minimiarvo 0 ja maksimiarvo 9.

Kuvatessaan omaa osaamistaan sanallisesti avoimessa kentässä, vastaajat nostavat esiin pysyttelevänsä ajan tasalla muun muassa seuraamalla itsenäisesti ajankohtaisia uutisia, artikkeleja sekä aihepiiriin liittyviä sivustoja. Osa vastaajista kertoi myös tekevänsä yhteistyötä kollegojensa kanssa. Useampi vastaaja kertoi ylläpitävänsä perustaitoja käyttämällä arjessaan tietokonetta tai muita omia tietoteknisiä laitteita. Muutamissa vastauksissa nousee esille arvio hyvästä osaamistasosta tietoturva-asioissa. Toisaalta osa vastaajista toteaa, ettei perustason laitteiden käyttötaidoista huolimatta ymmärrä riittävästi niihin liittyviä turvallisuusasioita. Avoimien vastausten perusteella varsinainen tietotekninen sekä kyberturvallisuuden teemoihin suuntautuva osaaminen opettajilla perustuu

mahdolliseen pohjakoulutukseen (tieto- ja viestintätekniikan opettajat), omaan teknologiakiinnostukseen, sosiaalisen median käyttöön, mediaseurantaan ja aiheeseen liittyviin artikkeleihin.

Opettajilta kysyttiin, miten heidän opetusvalmiuksiaan kyberturvallisuuden osalta voitaisiin kehittää tai parantaa. Avoimen kentän vastauksissa nousi esiin täydennyskoulutuksen tarve. Lisäksi esimerkiksi erityisesti työnantajan tarjoaman koulutuksen puute nousi esiin kahdessa vastauksessa. Aiheen sisällyttäminen opettajaopintoihin sekä valmiiden materiaalien (tehtäväpaketit ja videomateriaali) saatavuuden tarve mainittiin vastauksissa. Yksi vastaaja toivoi hyvin selkeää ja oppilaiden kanssa käsiteltäväksi soveltuvaa oppimateriaalia, jotta opettajan itsensä ei tarvitsisi laatia materiaaleja.

Edellä mainittujen lisäksi avoimessa kentässä yksi vastaaja nosti esiin tietotekniikan opetuksen aineopetuksen tilan: opetusta haluttaisiin tarjota kaikille eikä ainoastaan valinnaisaineena sen valinneille. Vastauksissaan opettajat kokivat, että materiaalia opetuksen tueksi on tällä hetkellä saatavilla lähinnä internet-sivustoilta ja itse hakukoneiden avulla etsien. Yksi vastaaja totesi, että tietotekniikan opettajilla on monipuolisia materiaaleja mutta opetukselle ei anneta resursseja.

Opettajien osaamista kartoittaessa heitä pyydettiin myös arvioita siitä, miten hyvin he tuntevat internetin välityksellä tapahtuvat rikokset asteikolla 0-10 (huonosti – kiitettävästi). Vastausten keskiarvo oli 6,1, mediaani 5,0, minimiarvo 2 ja maksimiarvo 9. Kun opettajat arvioivat kykyään kuvailla yleisimpiä rikoksia asteikolla 0-10 (en tunne rikoksien pääpiirteitä lainkaan – pystyn kattavasti kuvailemaan yleisimpiä rikoksia ja niiden ilmenemismuotoja), vastausten keskiarvoksi saatiin 7,1, mediaaniksi 8,0, miniarvon ollessa 2 ja maksimiarvon 10.

9.1.2 Opetus ja opetuksen sisällöt

Kyselytutkimuksessa pyrittiin selvittämään myös, missä määrin opettajat tunnistavat peruskoulun opetussuunnitelmien perusteiden (2014) sisältöä kyberturvallisuuden aihealueeseen liittyen. Opettajat vastasivat tähän numeerisella arviolla sekä asteikolla 0-10

(en ole tietoinen – olen perehtynyt kattavasti näihin osa-alueisiin). Vastausten keskiarvo oli 6,7, mediaani 8,0, minimiarvo 1 ja maksimiarvo 10.

Tutkimuksen opetussisältöihin liittyvässä osiossa vastaajille esitettyjä kysymyksiä taustoitettiin kertomalla, että vuoden 2014 perusopetuksen opetussuunnitelmien perusteissa tietoturvaan liittyvä opetus on sidottu osaksi laaja-alaista osaamista ja, että aihealueet sisältyvät osaksi muiden aineiden opetusta. Opetettavista teemoista mainittiin vastaajille vastuullinen ja turvallinen toiminta, eettisesti kestävä tieto- ja viestintäteknologian käyttö, tietoturvariskeiltä suojautuminen, tietosuoja ja tekijänoikeudet.

Avoimen kentän vastauksissa opettajat kertoivat, että edellä mainitut teemat näkyivät heidän opetuksessaan lähinnä yksittäisinä opetustunteina tai kursseina. Yksi vastaajista mainitsi myös, että opiskelulaitteiden käyttöönoton yhteydessä käsitellään turvallisuuteen liittyviä asioita. Suurin osa vastaajista toteaa teemojen nousevan esiin TVT-taitojen opetuksen yhteydessä, minkä lisäksi asioita käsitellään erilaisten teemaviikkojen ja projektien yhteydessä. Avoimen kentän kohdalla opettaja pyydettiin myös kuvailemaan mikäli taustoituksessa mainitut teemat eivät nouse opetuksessa esiin ja heitä pyydettiin pohtimaan, mistä se voisi johtua. Opettajien vastausten perusteella syynä teemojen käsittelemättömyydelle ovat riittämätön täydennyskoulutus, ajan puute sekä epäselvyydet siitä, missä oppiaineissa teemoja tulisi käydä läpi.

Haastavina asioina kyberturvallisuuden opetuksen näkökulmasta useat opettajat kokivat taitojen riittämättömyyden ja ajanpuutteen. Sanallisista vastauksista ilmenee, että teknologiaa käytetään opetuksen apuvälineenä opetettavan aineen sisältöihin liittyen, mutta opetuksessa ei keskitytä varsinaisesti itse teknologiaan tai sen turvalliseen käyttöön. Vastaajat kertoivat myös, ettei aiheen tärkeyttä välttämättä ymmärretä ja, että opetusmateriaalien valikointi tuntuu haastavalta huolimatta saatavilla olevasta materiaalin määrästä. Yksi vastaajista toi esille, etteivät aineenopettajat kunnolla hallitse aihetta, koska tietotekniikkaa ei enää opeteta omana aineenaan.

Myös se, ettei asioiden perusteellinen läpikäyminen nykyresursseilla muiden oppiaineiden aihesisältöjen ohella ole mahdollista, mainittiin vastauksissa. Kysyttäessä onnistumisen

kokemuksista kyberturvallisuuden teemojen opetukseen liittyen, puolet vastaajista kertoi, ettei heille tule mieleen mitään onnistumisen kokemuksia. Osa mainitsi aihealueiden käsittelyn seurauksena oppilaiden havainneen esimerkiksi käyttämiensä salasanojen heikkouksia sekä havainnoineensa paremmin käyttämiensä sosiaalisen median alustojen soveltuvuutta omalle ikäryhmällensä.

Osaamiseen liittyen kyselylomakkeessa kysyttiin myös, minkälaista tukea tai koulutusta peruskoulun opettajat toivovat tulevaisuudessa kyberturvallisuuden teemojen opetukseen liittyen. Vastauksista korostuu lisäkoulutuksen tarve, lapsille soveltuvien materiaalien tarve sekä konkreettiset ohjeistukset. Yksi vastaajista nosti esiin, että valtakunnallisesti tasalaatuinen opetus voitaisiin taata tietotekniikan aineenopettajien vetämien pakollisten TVT-kurssien muodossa. Kyselyn vastaajat kokivat, että kyberturvallisuuden perusteiden opetuksen tulisi olla peruskoulun, huoltajien sekä mahdollisesti esimerkiksi alan osaajien vastuulla. Erityisesti peruskoulun rooli vastuun ottajana korostui vastauksissa.

9.1.3 Opetuksen merkityksellisyys

Opettajilta kysyttiin, minkälaisen vaikutuksen he kokevat peruskoulun kyberturvallisuus teemojen opetuksella olevan lasten ja nuorten kykyyn tunnistaa mahdollisia uhkia ja rikoksia verkkomaailmassa. Tähän kysymykseen opettajat antoivat numeerisen arvioin asteikolla 0-10 (opetuksella ei voida välttää uhriksi joutumista – opetuksella on ratkaiseva rooli uhkien tunnistamisessa). Vastausten keskiarvo oli 8,3, mediaani 9,0, minimiarvo 6 ja maksimiarvo 10. Numeerisella arviolla opettajat vastasivat myös kysymykseen siitä, miten tärkeäksi he kokevat kyberturvallisuuden opetuksen peruskoulussa. Vastausasteikko oli 0-10 välillä (ei lainkaan tärkeää – erittäin tärkeää). Vastausten keskiarvo oli 8,4, mediaani 10,0, minimiarvo 5 ja maksimiarvo 10. Avoimen kentän vastausten perusteella kyberturvallisuuden opetus koettiin tärkeäksi, koska siihen liittyvät aiheet ovat olennainen osa nykymaailmaa ja, koska turvallisuus rakentuu yksittäisten käyttäjien toimien pohjalta.

Uhkien tunnistamiseen liittyen kysyttiin, kuinka oleellisena opettajat pitävät sitä, että myös huoltajille jaettaisiin tietoa ja ohjeistuksia liittyen kriittiseen medialukutaitoon, turvataitoihin, nettikiusaamiseen, uhkien havaitsemiseen sekä havaittujen rikosten

ilmiantamiseen. Numeeriset arvioit tähän kysymykseen annettiin asteikolla 0-10 (ei lainkaan tärkeää – erittäin tärkeää). Vastausten keskiarvo oli 8,9, mediaani 9,0, minimiarvo 6 ja maksimiarvo 10.

Pyydettäessä arvioimaan peruskouluikäisten kyberturvallisuuden perustaitoja yleisesti tällä hetkellä, opettajat vastasivat asteikolla 0-10 (riittämättömät taidot – hyvin kattavat taidot). Vastausten keskiarvo oli 3,8, mediaani 4,0, minimiarvo 0 ja maksimiarvo 6. Arvioitaessa samalla asteikolla suomalaisten työikäisten vastaavia taitoja, keskiarvoksi muodostui 4,6, mediaaniksi 4,5, minimiarvoksi 1 ja maksimiarvoksi 7.

9.2 Kyberturvallisuuden opetuksen teemat ja tulevaisuus

Kyberturvallisuuden parissa työskenteleville ammattilaisille suunnatun kyselytutkimuksen kutsu julkaistiin ammattilaisverkostopalvelu LinkedIn:ssa. Kyberturvallisuuden ammattilaiset kokivat kyselytutkimuksen tärkeäksi ja moni heistä jakoi kyselytutkimuksen linkkiä edelleen omiin verkostoihinsa. Lisäksi viikko kyselyn avaamisesta julkaistiin muistutus LinkedIn:ssa sekä kyberturvallisuuteen keskittyvässä Facebook-ryhmässä. Kyselytutkimus tavoitti kyberturvallisuuden ammattilaiset suhteellisen hyvin, kun otetaan huomioon, että tutkimuskutsu toimitettiin pääasiassa LinkedIn:n välityksellä.

9.2.1 Tietoisuus kyberturvallisuuden opetuksesta peruskoulussa

Ammattilaiset eivät kyselyn perusteella olleet kovin tietoisia siitä, että opetussuunnitelmien perusteissa (2014) on mainintoja kyberturvallisuuden opetukseen liittyen. Vastaajista yli puolet (56 % vastaajista, eli 83 vastaajaa) kertoi, ettei tiennyt, että kyberturvallisuuden opetusta sisältyy millään tavalla suomalaiseen peruskouluun. 40 % vastaajista kertoi kuulleensa, että joitakin osa-alueita opetetaan ja loput 4 % kertoi perehtyneensä opetussuunnitelmien perusteisiin sekä mainintoihin kyberturvallisuudesta.

Edelliseen kysymykseen liittyen vastaajia pyydettiin kuvailemaan vapaassa tekstikentässä tietojaan kyberturvallisuuteen liittyvän peruskouluopetuksen sisällöstä. Avoimessa kentässä vastaajat kertoivat, että ovat kuulleet perusopetuksessa opetettavan lähinnä tietotekniikan

perustaitoja sekä asioita medianlukutaidosta, lähdekritiikistä, turvallisesta netin käyttämisestä, sosiaalisesta mediasta ja salasanoista. Muutamia havaintoja nousi esiin myös siitä, että aihepiiriä on kuultu tuotavan esille lähinnä ”pelottelun” kautta. Useat ammattilaiset kertoivat, että ovat kuulleet opetuksesta lähinnä omaan lähipiiriinsä kuuluvien peruskoulua käyvien henkilöiden kautta. Kuitenkin suurin osa vastaajista totesi, ettei ole kuulut mitä peruskoulussa aihepiiristä opetetaan.

Kyberturvallisuuden parissa työskentelevien näkemysten mukaan peruskoulun kyberturvallisuusopetuksen tulisi olla yleistasoista ja helposti ymmärrettävää, alkaen täysin perusteista ja tähdäten siihen, että oppilas kykenee hahmottamaan suuren kuvan. Sanallisissa vastauksissa nousi esiin myös eri ikäisten ja kehitystasojen huomioiminen sekä keskittyminen niihin teknologioihin ja medioihin, joita oppilaat käyttävät. Referenssinä voidaan käyttää esimerkiksi yritysten omille työntekijöilleen suuntaamia tietoturvakoulutuksia, joissa käsitellään esimerkiksi salasanoja tai tietojenkalastelua. Peruskoulu opetuksen ikätasoisuuden huomioon ottavaa opetusta pohdittiin vastauksissa esimerkiksi seuraavasti:

> *”Peruskouluaika on pitkä aika lapsen kehityksessä, joten eri asioita pitää opettaa useaan eri otteeseen eri ikävaiheissa sen hetkiseen lapsen kontekstiin sopivilla tavoilla.”*

> *”Teknologioita tulisi opettaa sen mukaan, mitä oppilaat käyttävät. Eli ehkä aloittaa älypuhelimista, kun niihin lapset usein ensin törmäävät ja sitten laajentaa siitä eteenpäin. Myös sovelluksista pitäisi olla ajantasalla eli käyttää esimerkkeinä sellaisia sovelluksia joita lapset juuri siinä iässä käyttävät.”*

Perustaitoina vastaajat pitivät medialukutaitoa sekä lähdekriittisyyttä, joihin liittyen mainittiin esimerkiksi huijausten ja tietojenkalastelun havaitseminen, valeuutisten sekä psykologisen vaikuttamisen tunnistaminen. Vastauksissa nostettiin esille, että perustaitoihin voisi kuulua myös yleisimpien uhkien tunnistaminen tai tunnusmerkkien havaitseminen (esimerkiksi haittaohjelmat, petokset, huijaussivut, grooming, mustamaalaus). Toisena perustaitoteemana esille nostettiin sosiaalisen median taidot sekä verkossa tapahtuva

kommunikointi. Vastaajat mainitsivat esimerkiksi netiketin (netti-etiketti), somekäyttäytymisen opettelun sekä oman toiminnan vaikutusten arvioinnin. Salasanojen osalta useat vastaajat kokivat tärkeäksi opettaa vahvojen salasanojen perusteita, salasanojenhallintaa sekä monivaiheisen tunnistautumisen merkitystä. Edellä kuvattuja nostettiin vastauksissa esiin muun muassa seuraavasti:

> *”Pohjana tulisi olla perusteet IT-taidoista: kybertaidot ovat usein hukassa jos ei osaa käyttää tietokoneita ja älylaitteita. Tulee osata käyttää yleisimpiä käyttöjärjestelmiä (ei vain Androidia tai iOSia). Tähän päälle sitten medialukutaitoa ja opetusta internetissä olevasta pahuudesta.”*

> *”Sellaista, että koululaiset oppivat perusasiat kuten esim. salasanojen (salasanalauseet) oikeanlaisen käytön, ohjelmistojen ja laitteiden ajan tasalla pitämisen ja muun suojaamisen, kriittisen suhtautumisen mobiililaitteiden sovelluksiin (esim. ei ylimääräisiä sovelluksia ja ylimääräisiä käyttöoikeuksia sovelluksille), välttämään haitallisten viestien ja linkkien vaaroja.”*

> *”Maailma on jatkuvasti menossa enemmän ja enemmän verkkoon, nuoret käyttävät sujuvasti TikTokia ja muita sovelluksia, mutta he eivät samalla tavalla ymmärrä kuinka kybermaailma pohjimmiltaan toimii ja massan mukana tulevat trendit hukuttavat helposti alleen varovaisuuden. Jos nuorilla olisi valmiina perustiedot kyberturvallisuuden osalta, heillä olisi paremmat valmiudet havaita mahdolliset väärinkäytökset, huijaukset ja ongelmalliset tilanteet, sekä välttää niitä. ”*

Vastauksissa nousi esiin myös turvallisen nettikäyttäytymisen perustaidot, jotka koostuvat vastauksien perusteella esimerkiksi yksityisyyden suojan perusymmärryksestä, hyvien tietoturvakäytäntöjen tuntemisesta, itsensä sekä omien tilien ja laitteiden suojaamisen ymmärtämisestä. Yksi vastaajista nosti esiin, että varsinaisen teknologian käytön lisäksi tulisi huomioida myös teknologiaan liittyvät eri ilmenemisen tasot, kuten kognitiivinen, sosiaalinen tai yhteiskunnallinen taso.

Edistyneempinä taitoina vastaajat mainitsivat muun muassa ohjelmoinnin, hakkeroinnin ja kyberturvallisuuden ymmärtämisen osana isompia kokonaisuuksia kuten politiikkaa ja historiaa tai maanpuolustusta. Nämä koettiin voitavan jättää hieman vähemmälle huomiolle, kun opetuksen fokus suuntautuisi perusasioiden ymmärtämiseen ja opettamiseen. Opetuksen käytännön toteutuksista esiin nostettiin esimerkiksi harrastekerhot, pelillistäminen, teemaviikot, nanolearning, tehtävät, työpajat sekä e-kurssit.

9.2.2 Kansalaistaitojen merkitys

Kyselyssä kyberalan ammattilaisille tiedusteltiin, kuinka tärkeänä he pitävät jokaisen suomalaisen kansalaistaitoja kyberturvallisuudesta. Vastaukset annettiin numeerisesti asteikolla 0-10 (ei lainkaan tarpeellista – erittäin tarpeellista). Vastausten keskiarvo oli 9,2, mediaani 10,0, minimiarvo 4 ja maksimiarvo 10. Tähän kysymykseen pyydettiin avoimessa kentässä tarkentamaan, mitä nämä kyberturvallisuuden kansalaistaidot voisivat tarkoittaa.

Kyselytutkimuksessa tiedusteltiin kyselyn alkuosassa, mitä perustaitoja kyberturvallisuudesta tulisi opettaa peruskoulussa. Kansalaistaitoon liittyvissä vastauksissa nousevat peruskouluopetukseen liittyvää kysymystä vahvemmin ja laajemmin esille kyberturvallisuuden ilmiöt, uhkakentän ymmärrys ja oman vastuun korostuminen osana kokonaisuutta. Kansalaistaitokysymyksessä korostui peruskouluosaamiseen nähden enemmän se, että yksilö kykenee hahmottamaan oman toimintansa ja vastuunsa osana kokonaisuutta (yhteisöä, yhteiskuntaa). Lisäksi myös kansalaistaitoaiheeseen liittyen mainittiin omien tietojen luovuttamisen ja esille laittamisen merkityksen ymmärtäminen sekä oman selustan suojaaminen. Vastauksissa pohdittiin kansalaistaitoja muun muassa näin:

> *”Mielestäni olisi tärkeää poistaa mystisyyttä kyberturvallisuudesta ja arkipäiväistää toimenpiteet, joilla kansalaiset voivat suojata omia tietojaan. Mitä tahansa halutaan kansalaisten tekevän paremmin, sen pitäisi olla ensisijaisesti sellaisessa muodossa, ettei se aiheuta syyllisyyttä tai pelottele liikaa.”*

> *”Perusymmärrys verkon vaaroista, tietokoneen haittaohjelmista ja tietokoneen suojaamisesta, turvallinen käyttäytyminen internetissä, kalasteluviestien tunnistaminen, salasanakäytännöt + kaksivaiheinen tunnistautuminen jne. Ei mitään teknistä, vaan kansankielellä parhaita käytäntöjä tietokoneen ja internetin käyttöön.”*

Yhteiskunnallisella tasolla vastauksissa korostui kokonaisvaltainen ymmärrys tietoturvan laajuudesta ja siitä, mitä kaikkea se arkielämässä koskettaa. Muutamissa vastauksissa mainittiin myös, että kansalaistaidoissa oleellista on yhteisöllinen asenne: jokainen on mukana ja jokaista tarvitaan, osana kokonaisuutta. Yksi vastaaja mainitsi yhteiskunnan kestävyyden, turvallisuuden, luottamuksen ja resilienssin merkityksen pohdittaessa kyberturvallisuus osaamista kansalaistaitojen näkökulmasta. Edellä kuvattuja näkökulmia vastauksissa nostettiin esiin esimerkiksi näin:

> *”Ymmärrys siitä että kyberturva EI OLE vain tietoverkkojen suojaamista vaan osa yhteiskunnallista kestävyyttä. Jokainen suomalainen osana yhteiskuntaa on velvollinen vaalimaan kansallisia arvoja, jotka koskevat myös digitalisoituvaa yhteiskuntaa. Oletus ei saisi olla, että koulutamme kyberturvan ammattilaisia vaan "jokamiestaidot" olisivat sellaiset, jotka tukevat yhtenäisiä tavoitteita, vapautta, tasa-arvoa ja luottamusta.”*

> *”Ymmärretään, miten tietoturva on osa kaikkea elämää, esimerkiksi kodin älylaitteiden merkitys tietoturvalle tulisi olla kaikkien tiedossa. Tärkeää olisi ymmärtää, miksi tietoturva on tärkeää yksilön kannalta, sekä mikä on yksilön merkitys yhteiskunnan kyberturvallisuudessa. Olisi myös hyvä opettaa, mitä konkreettisia tekoja ihminen voi tehdä oman turvallisuutensa eteen.”*

Pääosin kansalaistaitoja käsittelevän kysymyksen avoimen kentän vastaukset noudattelevat kuitenkin niitä teemoja, joita vastaajat nostivat esiin myös kyselylomakkeen alussa peruskoulun opetusta koskevien teemojen yhteydessä.

9.2.3 Opetettavat teemat

Ammattilaisille suunnatussa kyselylomakkeessa haluttiin myös selvittää tarkempia kyberturvallisuuden kokonaisuuteen liittyviä teemoja, joita tulisi opettaa peruskoulussa. Kyselyssä pyydettiin ammattilaisia arvioimaan eri teemojen opetuksen tärkeyttä numeerisesti asteikolla 1-5:

1 = Ei lainkaan tärkeää
2= Vain vähän tärkeää
3 = En osaa sanoa
4 = Jokseenkin tärkeää
5 = Erittäin tärkeää.

Tällä numeerisella asteikoilla ammattilaiset arvioivat 13 eri teemaa, jotka vaihtelivat yleistason teemoista syvällisempiin yksittäisiä asioita koskeviin teemoihin. Tärkeimpinä teemoina opetuksen kannalta pidettiin seuraavia:

- hyvät käytöstavat ja turvallinen toiminta internetissä (4,7)
- laitteiden turvallinen käyttö (4,6)
- kaksivaiheinen tunnistautuminen ja muut turvallisuutta lisäävien toimenpiteiden tuntemus (4,6)
- tietoturvariskeiltä suojautuminen (4,4)
- yleisimpien verkkorikosten tunnusmerkkien tunnistaminen (4,2)
- kyberturvallisuuden peruskäsitteiden tunteminen (4,0)
- ohjaus eettisesti kestävään tieto- ja viestintäteknologian käyttöön (3,8).

13 kyselyssä olleesta käsitteestä vähiten oleellisiksi arvioitiin Suomen kyberturvallisuuden strategia ja muut kansalliset ohjelmat (2,3), CIA-malli (2,5), GDPR-lainsäädännön tunteminen (3,0), kybermaailman lainalaisuuksien tunteminen (3,3) ja tietotekniikan teknisten toimintaedellytysten tunteminen (3,3).

Ammattilaisten kyselyssä tiedusteltiin, miten tärkeänä he pitävät opettajien osaamista internetin välityksellä tapahtuvista rikoksista ja niiden piirteistä. Kysymykseen vastattiin

asteikolla 1-10 (ei tarvitse tuntea rikoksien pääpiirteitä lainkaan – tulee pystyä kuvailemaan kattavasti yleisimpiä rikoksia ja niiden ilmenemismuotoja). Vastausten keskiarvo oli 7,8, mediaani 8,0, minimiarvo 3 ja maksimiarvo 10. Arvioitaessa asteikolla 0-10 (opetuksella ei voida välttää uhriksi joutumista – opetuksella voidaan välttää uhriksi joutuminen) sitä, kuinka suuri vaikutus peruskouluopetuksella kyberturvallisuuden ammattilaisten näkemyksen mukaan olisi lasten ja nuorten kykyyn tunnistaa mahdollisia uhkia ja rikoksia verkkomaailmassa, luvut olivat: keskiarvo 8,4, mediaani 9,0, minimiarvo 2 ja maksimiarvo 10.

Numeeristen arvioiden perusteella myös oppilaiden huoltajille jaettavan tiedon ja ohjeistusten merkitys on suuri. Kysymyksessä annettiin esimerkkeinä jaettavasta tiedosta ja ohjeistuksista seuraavat teemat: kriittinen medialukutaito, turvataidot, nettikiusaaminen, uhkien havaitseminen sekä havaittujen rikosten ilmiantaminen. Ammattilaiset antoivat vastaukset asteikolla 0-10 (ei lainkaan tärkeää – erittäin tärkeää), keskiarvo oli 8,9, mediaani 10,0, minimiarvo 5,0 ja maksimiarvo 10.

Numeerisesti arvioituna kyberturvallisuuden opetus peruskoulussa kokonaisuudessaan nähtiin asteikolla 0–10 (ei lainkaan tärkeää – erittäin tärkeää) erittäin tärkeänä. Vastausten keskiarvo oli 9,0, mediaani 10,0, miniarvo 5 ja maksimiarvo 10. Ammattilaiset arvioivat myös opetuksen aloittamisajankohdan tärkeyttä ensimmäisestä vuosiluokasta alkaen asteikolla 0–10 (Ei lainkaan tärkeää – erittäin tärkeää). Vastausten keskiarvo oli 7,3, mediaani 8,0, minimiarvo 0 ja maksimiarvo 10.

9.2.4 Opetuksen järjestäminen

Kyselyssä selvitettiin, voisiko kyberturvallisuuden ammattilaisten mielestä kyberturvallisuuden opetuksesta olla vastuussa joku tai jotkin tahot, kuin suomalainen peruskoulu. Pääasiassa avoimen tekstikentän vastauksissa todettiin peruskoulun olevan ainoa väylä, jota kautta opetus voidaan järjestää, jotta kaikille saadaan samantasoiset taidot. Kyberturvallisuuden katsottiin monessa vastauksessa olevan yleissivistystä ja perustaito. Ammattilaisvastauksissa esille nousi peruskoulun avainrooli tavoitettaessa koko ikäluokkaa. Vastuullisena ammattilaiset pitivät peruskoulua, mutta useat vastaajat toivat esiin, ettei opetuksesta tarvitsisi olla vastuussa yksittäisten opettajien. Vastaajat näkivät, että

peruskoulun opetuksen tukena voitaisiin hyödyntää mm. viranomaisia, yksityistä ja kolmatta sektoria ja vapaaehtoistoimijoita. Vastuullisuutta pohdittiin vastauksissa muun muassa seuraavasti:

> *"…Toimiminen digitaalisessa ympäristössä on vaadittu kansalaistaito ja peruskoulu on ainoa paikka mikä tavoittaa kaikki nuoret. Perusasian ymmärryksen saatavuus ei saa jäädä kiinnostuksesta kiinni."*
>
> *"Kyllä peruskoulun pitää pystyä tuottamaan kulloisenkin suomalaisen yhteiskunnan kaipaamia kelvollisia kansalaisia. Ei tätä tule sälyttää kenenkään muun vastuulle. Suomessa peruskoulutus on aika hyvin resursoitu, joten siltä pitää odottaa tuloksia myös tällä saralla."*
>
> *" Peruskoulu on ainoa paikka, joka tavoittaa lähes koko ikäluokan. Näin oleellista kansalaistaitoa ei voida jättää minkään muun tahon opetettavaksi."*

Ammattilaisilta kysyttiin myös tarkemmin heidän arviotaan siitä, mitkä eri tahot voisivat tehdä yhteistyötä perusopetuksen järjestäjien kanssa kyberturvallisuuden opetuksen toteutukseen liittyen. Vastauksissa nousivat esiin seuraavat toimijat / tahot:

- yksittäiset vapaaehtoiset (ammattilaiset)
- järjestöt (Tietoturva ry, Disobey, CitySec:t, Women4Cyber, Partio, Kirkko, MPK, MLL, harrastusseurat, kyberVPK)
- yritykset (tietoturvayritykset, pankit, yritysten kyberturvallisuusosastot, Yle, teleoperaattorit)
- viranomaiset (Traficom/kyberturvallisuuskeskus, Poliisi, Puolustusvoimat, KRP, SuPo, DVV, Opetushallitus, ministeriöt)
- julkinen sektori (nuorisotoimi, kirjastot, kansalaisopistot)
- korkeamman tason oppilaitokset (lehtorit, yliopistot, korkeakoulut).

Alla esitetyssä kuvassa esitetään ammattilaisten ehdottamat tahot peruskoulun yhteistyökumppaineiksi (Kuva 6).

Kuva 6. Ehdotetut yhteistyötahot.

Muutamassa vastauksessa pohdittiin sitä, onko perustaitojen opetukseen kannattavaa ottaa mukaan kaupallisia toimijoita. Pohdintaa esiintyi vastauksissa myös rajallisista resursseista. Eräs vastaajista pohti yhteistyötä rajallisten resurssien valitessa seuraavasti:

> *”Ensisijassa varmaan ekonomistien kanssa kannattaisi miettiä opetuksen vaihtoehtokustannuksia ja resurssien rajallisuutta ja sitten yhteistyössä kyberturvallisuuden tutkimuspuolen kanssa (yliopistot ja amkit) miettiä keinovalikoima joka rajallisten resurssien kanssa antaisi parhaan vasteen. ”*

Yleisesti yhteistyön tekeminen nähtiin positiivisena asiana ja vastauksissa uskottiin, että usean eri toimijan yhteistyöllä kyberturvallisuuden opetus ja perusopetuksen järjestäjien tukeminen onnistuisi.

Jatkokysymyksenä edelliseen, pyydettiin kuvailemaan konkreettisia yhteistyömahdollisuuksia perusopetuksen järjestäjien kanssa. Vastauksista nousi vahvasti esiin, että yhteistyötä voitaisiin tehdä esimerkiksi opetusmateriaalien tuottamisessa sekä opetussisältöjen suunnittelussa. Esille nousivat myös muun muassa eri tahojen yhteistyössä tehdyt luennot, kurssit, kampanjat, teemapäivät, kilpailut sekä tapahtumat. Edellä

mainittujen lisäksi useissa vastauksissa nousi esiin, että ammattilaiset voisivat osallistua perusopetuksen opettajien kouluttamiseen sekä tarjota materiaaleja opettajille heidän omien taitojensa kehittämiseksi.

Yritysten osalta esiin nostettiin osallistuminen opetuksen toteuttamiseen esimerkiksi yritysvierailujen, tietoiskujen ja sisällöntuotannon kautta. Yhtenä ehdotuksena annettiin, että kyberturvallisuuden parissa työskentelevien työnantajat voisivat tarjota mahdollisuuden palkalliseen aikaan, jolloin ammattilaiset voisivat talkootöinä vierailla kouluissa luennoimassa tai osallistumassa opetukseen. Vastaajat kuvasivat näitä asioita esimerkiksi näin:

> *” Olisi tietysti hyvä, että tulevat työnantajat (yksityinen ja julkinen sektori) voisivat osallistua talkootöihin, koska tämä opetus vastaa myös tulevaisuuden tarpeisiin. On tuki sitten projektien tai materiaalien rahoitusta tai ammattilaisten ajankäytön mahdollistamista vapaaehtoistyöhön.”*

> *” Me, kyberturvallisuuden ammatillaiset probono hengessä mukana, palkallinen päivä + luento koululaisille”*

Muutama vastaaja ehdotti, että kyberturva-ammattilaiset, yritykset ja muut toimijat voisivat yhdessä osallistua suomalaisen verkoston kokoamiseen. Verkostoon ilmoittautuneita vapaaehtoisia koulut pystyisivät kutsumaan vieraileviksi luennoitsijoiksi. Vastaavanlainen tietoturvakummipankki on erään vastaajan mukaan ollut aiemmin jo olemassa. Yhteistyötä ja koordinointia eräät vastaajat hahmottelivat vastauksissaan seuraavasti:

> *”Lisäksi tietoturvayritykset, MPK, Tietoturva Ry, kyber-VPK jne voisivat kerätä vapaaehtoisten verkoston ympäri suomea tarjoamaan koulutusta ja tukea paikallisille peruskouluille.”*

> *”Kuitenkaan ei ole välttämätöntä, että opetuksesta vastaavat yksin luokanopettajat. Myös alan asiantuntijoita voisi hyödyntää opetuksessa jollain tavalla. Vähintä mitä voidaan tehdä on luoda kattava materiaali ja*

koulutuspaketti opettajille. Tämän avulla saataisiin oikeat opit kaikille opettajille.”

Ammattilaiset vastasivat myös kysymykseen siitä, millä tavoin peruskoulun opettajia voitaisiin tukea tai auttaa opetuksen sisällön tai toteutuksen suunnittelussa. Vastauksissa korostuivat erityisesti eri tahojen yhteistyössä tuottamat materiaalit, myös valmiit materiaalipaketit, opetuksen tueksi. Muutama vastaaja mainitsi ammattilaisten itsensä, sekä yhteistyötahojen osallistumisen opetuksen suunnitteluun, tuottamalla esimerkiksi valmiita opetuskokonaisuuksia tai oppiaineisiin sisällytettävien kyberturvallisuusasioiden valmiita tehtäviä ja opetusvinkkejä.

Vastauksissa nostettiin usein esiin, että opettajien kouluttaminen ja perehdyttäminen kyberturvallisuuden aihepiiriin on tärkeää. Ehdotuksina opettajaa tukevista menetelmistä nostettiin esiin muun muassa säännöllisesti päivitettävä wiki-sivu, opettajan opas kyberturvallisuuden opettamiseksi, täydennyskoulutukset ja valmennukset, infotilaisuudet sekä peruskoulun yhteistyö ammatillisten oppilaitosten ja korkeakoulujen kanssa.

Vastaajat listasivat myös valmiita julkisia materiaaleja, joita opettajat voisivat hyödyntää kyberturvallisuuden opetuksessa. Eniten mainintoja kertyi Kyberturvallisuuskeskuksen (Traficom) materiaaleille, joita ovat esimerkiksi Turvallisesti netissä -opas ja Kybersää. Vastauksissa useimmin mainittiin seuraavat tahot / materiaalit: Spoofy-mobiilipeli, DVV:n digiturvallisuusaineistot, Poliisi, Turvallisuuskomitean Kodin kyberopas, JYU:n kansalaisen kyberturvallisuus -kurssi, Maanpuolustuskoulutusyhdityksen (MPK ry) materiaalit ja kurssit sekä Vahti-ohjeet.

Varsinaisia materiaalilinkkejä kertyi useita kymmeniä, joista esimerkkeinä FiTech-kurssit sekä Mannerheimin lastensuojeluliiton verkkosivut oppaineen. Vastauksissa nousivat esiin myös Yhdistyneiden Kansakuntien kansallisen kyberturvallisuuskeskuksen materiaalit (NCSC GOV UK), joista Cybersprinters-peli ja CyberFirst-hanke materiaaleineen mainittiin. Vastauksista ilmeni myös, että materiaalin määrä ei välttämättä ole ongelma vaan se, että materiaalia on niin paljon mutta opettajilla on rajalliset mahdollisuudet haarukoida saatavilla olevasta materiaalista olennaisimmat asiat.

10 Johtopäätökset

Seuraavaksi esitellään tutkimuksen johtopäätökset. Ensin esittelemme opettajien suunnatun kyselyn johtopäätökset ja sen jälkeen ammattilaisille suunnatun kyselyn johtopäätökset.

10.1 Kyberturvallisuuden opetuksen nykytila

Opettajien kyselyn perusteella kyberturvallisuuden opetuksen nykytila peruskoulussa hahmottuu melko epäselvänä kokonaisuutena. Opetuksen sisältö sekä toteutuminen tuntuu saatujen vastausten perusteella olevan olennaisesti kiinni kulloinkin kyseessä olevasta opettajasta, hänen taidoistaan sekä näkemyksestään asian tärkeydestä. Kyselytutkimukseen vastanneet opettajat kuvaavat osaamisensa olevan melko hyvää, mutta tuovat selkeästi esille myös lisä- ja täydennyskoulutuksen tarpeen sekä aihepiirin käsittelyn puutteet opettajan peruskoulutuksen yhteydessä. Myös yleisimpien verkkorikoksien tunnusmerkit tuntuivat olevan opettajilla hallinnassa.

Opetusvalmiuksia koskevista vastauksista voi päätellä, että opettajat kokevat hieman epävarmuutta ja puutetta omissa valmiuksissaan opettaa kybertuvallisuuden teemoja. Tosin tämäkin varmasti vaihtelee opettajakohtaisesti ja riippuen siitä, mihin aineeseen opettaja on suuntautunut. Opettajien valmiudet ja niiden ylläpitäminen perustuu kyselyn vastausten perusteella yksittäisen opettajan omaan kiinnostukseen ja aktiivisuuteen. Jo olemassa olevien kyberturvallisuuden aihealueiden materiaalien hyödyntäminen on vastausten perusteella sen varassa, mitä yksittäinen opettaja ehtii ja sattuu löytämään internetin hakukoneita käyttämällä.

Peruskoulun opetussuunnitelmien perusteiden maininnat kyberturvallisuuden teemojen osalta ovat kyselyn perusteella opettajilla melko hyvin tiedossa. Opettajien opetuksessa kyberturvallisuuden teemat konkretisoituvat tällä hetkellä yksittäisinä opetustunteina, projekteina tai kurssikokonaisuuksina. Myös laitteiden käyttöönoton yhteydessä turvallisuuteen liittyviä asioita käydään läpi. Teemat eivät kuitenkaan välttämättä nouse opetuksessa lainkaan esille johtuen riittämättömästä koulutuksesta, ajan puutteesta sekä siitä, että on epäselvää, missä oppiaineissa teemoja tulisi käydä lävitse. Haasteena

opetuksen järjestämisessä on myös materiaalien valitsemisen vaikeus sekä se, etteivät opettajat hallitse aihealuetta. Huolestuttavasti kyselyssä nousi esiin myös se, ettei merkittävällä osalla opettajista ole onnistumisen kokemuksia kyberturvallisuuden aihealueiden opetuksesta.

Vastauksista hahmottuu kuva, että kyberturvallisuuden ilmiöiden käsitteleminen havainnollistavasti osana laaja-alaisen osaamisen kokonaisuutta ja integroituna nykyisiin oppiaineisiin saattaa olla nykyresursseilla haasteellista. Kyberturvallisuuteen liittyvien asioiden osoittaminen toteen (demoaminen) sekä kokeileminen eivät onnistu perinteisten aineiden yhteydessä luontevasti, ellei opettajalla ole osaamista aihealueeseen. Monessa koulussa on tarjolla valinnaista TVT-opetusta, johon ohjautuvat vain aihealueesta kiinnostuneet.

Niin opettajat kuin kyberturva-ammattilaisetkin kokivat suomalaisten peruskoululaisten ja aikuisväestön kyberturvallisuuteen liittyvässä yleisosaamisessa olevan kehitettävää. Selvityksen perusteella kyselytutkimukseen vastanneet opettajat kokevat lasten ja nuorten kyberturvaosaamisen olevan heikommalla tasolla, kuin mitä ammattilaiset ovat vastanneet. Aikuisväestön osalta kyberosaamista arvioivan kysymyksen vastaukset olivat kummassakin tutkimuksessa samansuuntaiset. Selkeä tarve kansalaistaitojen opetukselle on vastausten perusteella olemassa.

Kyselyyn vastanneet opettajat pitivät kyberturvallisuuden opetusta hyvänä keinona opettaa lapsille ja nuorille erilaisten uhkien ja rikosten tunnusmerkkejä verkkomaailmassa. Kyberturvallisuuden opetukseen liittyen opettajat pohtivat myös sitä, miten opetusta voitaisiin järjestää kaikille, koska tällä hetkellä se on vain osa laaja-alaista osaamista (TVT-taidot). Tähän ratkaisuna ehdotettiin kyberturvallisuuden osa-alueen liittämistä osaksi tieto- ja viestintätekniikan aineopetusta, jolloin opetuksesta vastaa tieto- ja viestintätekniikkaan opinnoissaan keskittynyt opettaja. Tämä mahdollistaisi tasalaatuisemman opetuksen. Haasteista huolimatta kyberturvallisuuden opetusta peruskoulussa pidettiin opettajien vastausten perusteella erittäin tärkeänä.

Lisäksi kyselyssä nousi esiin, että vaikka tietotekniikan opettajilla olisi osaamista ja materiaaleja, ei resursseja heidän järjestämään opetukseen ohjata riittävästi. Tulevaisuuden konkreettisina tukikeinoina opettajat näkevät lisäkoulutuksen järjestämisen, lapsille soveltuvien materiaalien tuottamisen ja konkreettiset ohjeistukset kyberturvallisuuden opettamiseen. Opettajien vastausten perusteella kyberturvallisuuden teemojen opetuksessa voivat olla avuksi myös lasten huoltajat sekä alan ammattilaiset.

10.2 Kyberturvallisuuden opetuksen teemat ja tulevaisuus

Kyberalan ammattilaiset eivät toteutetun kyselyn mukaan olleet kovinkaan perehtyneitä siihen, minkälaisia kokonaisuuksia kyberturvallisuuden aihepiiristä suomalaisen peruskoulun opetussuunnitelmien perusteet pitävät tällä hetkellä sisällään. Kyberturvallisuuden ammattilaisilla on kuitenkin melko yhteneväinen näkemys siitä, mitä taitoja peruskoulussa tulisi opettaa kyberturvallisuuteen liittyen opettaa.

Vastauksissaan ammattilaiset totesivat, että kokonaisuudessaan kyberturvallisuuden opetuksen tulisi olla yleistasoista, oppijan ikätason huomioivaa sekä helposti ymmärrettävää. Kyberturvallisuuden perustaitoina ammattilaisten vastauksien perusteella voidaan pitää medialukutaitoa, uhkien tunnistamista, hyviä käytöstapoja internetissä, laitteiden turvallista käyttöä sekä perustason turvallisuuskäytäntöjen tunteminen kuten turvalliset salasanat, suojautuminen yleisimmiltä uhilta ja oman toiminnan vaikutusten tunteminen.

Ammattilaiset näkevät, että kyberturvallisuus on vahvasti kansalaistaito, jota jokaisen suomalaisen tulisi hallita perustasolla. Kansalaistaidoissa ammattilaiset näkevät merkittävänä osa-alueena sen, että yksittäinen kansalainen hahmottaa oman kybermaailmassa tapahtuvan toiminnan vaikutuksensa ja paikkansa osana laajempaa kokonaisuutta, kuten suomalaista yhteiskuntaa. Ammattilaisten vastauksista nousee esille myös tausta-ajatus, jonka mukaan yksilöiden toiminta vaikuttaa loppujen lopuksi myös yhteiskunnan kokonaisturvallisuuden, -luottamuksen ja -resilienssin tasoon.

Kyselyn vastausten perusteella ammattilaiset katsovat kyberturvallisuuden opetuksen peruskoulussa olevan erittäin tärkeää. Pääasiassa ammattilaiset näkevät, että peruskoulun olisi hyvä ottaa vastuullinen rooli kyberturvallisuuden opetuksen osalta, koska peruskoulu tavoittaa kattavasti kaikki tiettyyn ikäluokkaan kuuluvat lapset ja nuoret. Myös ammattilaisten näkemys siitä, että nykymaailmassa kyberturvallisuus on yleissivistystä ja perustaito, tukee näkemystä peruskoulusta vastuutahona. Myös lasten huoltajien rooli tiedon välittäjänä ja opettajina on merkittävä kyberturvallisuuden teemojen osalta.

Ammattilaiset eivät kuitenkaan koe, että opetuksen tulisi olla yksittäisten opettajien vastuulla, vaan opetuksen tukena voitaisiin hyödyntää mm. viranomaisia, yhdistyksiä, kolmatta sektoria tai vapaaehtoistoimijoita. Konkreettisesti yhteistyötä voisi syntyä esimerkiksi opetusmateriaalien tuottamisessa sekä opetussisältöjen suunnittelussa. Yhteistyö voisi myös keskittyä pienempiin kokonaisuuksiin kuten luennot, kurssit, kampanjat, teemapäivät, kilpailut sekä erilaiset tapahtumat. Myös ideoita verkostosta, jonka kautta voitaisiin koordinoidusti tehdä yhteistyötä, nousi kyselyssä esille.

11 Pohdinta

Tutkimukseen vastanneilla kyberturvallisuuden ammattilaisilla sekä peruskoulun opettajilla on melko yhteneväiset näkemykset kyberturvallisuuden opetuksen nykytilasta sekä tulevaisuuden näkymistä. Opettajien vastauksista käy ilmi, että yleisesti oletetaan lasten ja nuorten hallitsevan nettietiketin sekä osaavan käyttää sujuvasti tietoteknisiä laitteita, koska he kuuluvat nykysukupolveen. Laitteiden, internetin ja erilaisten sovellusten käyttöön liittyy kuitenkin paljon riskejä, joita moni lapsi ja nuori ei tule huomioineeksi, ennen kuin riskit ovat realisoituneet. Internet ja sen myötä muun muassa sosiaalinen media on erottamaton osa lasten ja nuorten arkea, ja internetiin liittyvien vaaran paikkojen olisi erittäin tärkeää. Tutkimuksen perusteella näiden riskien toteutumista voitaisiin vähentää opettamalla kyberturvataitoja.

Opinnäytetyössä pyrittiin vastaamaan kahteen tutkimuskysymykseen, joista yhtenä: *”Mitä osia kyberturvallisuuden aihepiiristä olisi olennaista opettaa suomalaisessa peruskoulussa kyberturvallisuuden ammattilaisten näkökulmasta?”*. Tutkimuskysymykseen liittyen saatiin

kattavasti vastauksia kyberturvallisuuden ammattilaisille kohdennetusta kyselytutkimuksesta. Kyselytutkimuksen pohjalta kyberturvallisuuden perusosaamista pidetään tärkeänä taitona, jonka opettaminen peruskoulussa mahdollistaisi tasalaatuisemman osaamisen valtakunnallisella tasolla. Kyberturvallisuuden peruskouluopetuksen lisäämisellä voidaan edesauttaa kyberturvallisen toimimisen kehittymistä peruskansalaistaidoksi. Kyberturvallisuus ja siihen liittyvät taidot ovat ajankohtaisia ja erittäin merkittäviä suomalaisen yhteiskunnan kestävyyden, turvallisuuden, luottamuksen ja palautumiskyvyn näkökulmasta.

Toisena tutkimuskysymyksenä oli *”Millainen on kyberturvallisuuden opetuksen tila tällä hetkellä ja miten perusopetuksen opetussuunnitelmien perusteiden mukainen ohjeistus toteutuu suomalaisessa peruskoulussa ja miten kyberturvallisuuden opetusta voitaisiin suositella edistettävän tulevina vuosina?”.* Opettajille suunnatun tutkimuksen osalta haasteita tuotti tutkimuslupamenettelyiden monimutkaisuus. Opettajien vastauksista oli saatavissa jonkin verran pohjatietoa tutkimuskysymykseen vastaamiseksi mutta se ei ole yleistettävissä vähäisen vastausmäärän vuoksi. On mahdollista, että vastausmäärä jäi pieneksi osittain siitä syystä, että kyselytutkimuksen jakelussa ei tutkimuslupamenettelyn tavoin voitu hyödyntää perusopetuksen sisäisiä jakeluväyliä. Nykytilan selvitykseen liittyen on tästä syystä havaittavissa jatkotutkimuksen tarve. Jatkotutkimuksessa tulee myös arvioida, miten mahdollisimman moni opettaja saataisiin vastaamaan kyselyyn, esimerkiksi mahdollistamalla aika kyselyyn vastaamiseksi.

Kyberturvallisuuden ammattilaisille kohdennetun tutkimuksen vastauksissa ehdotettiin, että esimerkiksi osaaja- ja materiaalipankit olisivat nopeastikin perustettavissa perusopetuksen tueksi. Osaajapankin kautta koulut voisivat esimerkiksi kutsua vapaaehtoisiksi puhujiksi ilmoittautuneita kyberturvallisuuden ammattilaisia vierailijoiksi kouluille, kertomaan kyberturvallisuuteen liittyvistä aiheita. Materiaalipankkiin ammattilaiset voisivat koota opettajille heidän opetuksessaan hyödynnettäväksi esimerkiksi valmiita tehtäviä ja hyväksi havaittuja materiaalipaketteja tai -lähteitä.

Tutkimuksen pohjalta seuraavaksi konkreettiseksi toimenpiteeksi voidaan nähdä vähintään kyberturvallisuuden aikaisempaa vahvempi sisällyttäminen perusopetuksen

opetussuunnitelmien perusteisiin. Laaja-alaisen osaamisen alle kirjattuja osa-alueita olisi hyvä myös tarkentaa niiltä osin, kuin viitataan kyberturvallisuuteen ja kyberturvataitoihin.

Aikaisemmissa kappaleissa käsiteltiin kyselytutkimuksen perusteella tärkeimpinä perustaitoina pidettyjä taitoja, kuten medialukutaitoa, uhkien tunnistamista sekä turvallisuuskäytäntöjen tuntemista. Viittaukset näihin taitoihin soveltuvissa kohdissa perusopetuksen opetussuunnitelmien perusteissa, saattaisivat parantaa niiden viemistä käytäntöön. Tieto- ja viestintätekniikan aineopettajilla on koulutuksensa perusteella muiden aineiden opettajia ja luokanopettajia vahvemmat valmiudet opettaa kyberturvataitoja. Mahdollisuuksia tieto- ja viestintätekniikan aineopetuksen tuomisesta pakolliseksi oppiaineeksi olisi syytä selvittää tarkemmin – missä voisi olla mahdollisuus jatkotutkimukselle.

Perusopetuksen kautta voitaisiin myös toimittaa keskitetysti peruskouluikäisten huoltajille yleistietopaketti kyberturvataitoihin liittyen. Konkreettinen paperimateriaali saa digitalisoituneessa ympäristössä suuremman huomion, kuin viestinä toimitettu liite tai materiaalilinkki. Materiaali voitaisiin julkaista fyysisen oppaan lisäksi myös digitaalisena. Oppaan tarkoituksena olisi tarjota huoltajille tietoa kyberturvallisuuden perusasioista, kyberympäristöön liittyvistä uhista sekä kyberturvataitojen merkityksestä. Huoltajat voisivat oppaan perusteella arvioida keskustelutarpeen lapsen tai nuoren kanssa ja tarvittaessa käydä perusasioita läpi myös kotona. Opas lisäisi myös huoltajien tietoa aiheesta.

Opinnäytetyön tutkimusosuudessa vastaan tulleista haasteista huolimatta opinnäytetyö valmistui aikataulusuunnitelman puitteissa. Opinnäytetyöprosessi oli erittäin mielenkiintoinen ja antoisa. Opinnäytetyön aihe on ajankohtainen ja herätti kiinnostusta kyberturvallisuuden ammattilaisten keskuudessa kyselytutkimusvaiheessa. Opinnäytetön aiheeseen liittyen oli mielenkiintoista käydä keskusteluja muiden aihepiiristä kiinnostuneiden kanssa.

Lähteet

Aalto-yliopisto (11.2.2015). *Kyberturvallisuus nostatti vilkkaan keskustelun Otaniemessä.* https://www.aalto.fi/fi/uutiset/kyberturvallisuus-nostatti-vilkkaan-keskustelun-otaniemessa

Alijoki, V. (2019). *Digitaidot kansalaistaitoina 2019.* DIGITALISAATIO JA NUORISOTYÖ. VERKE & ENTK. www.verke.org/uploads/2021/01/37b0da65-digitalisaatio-ja-nuorisotyo-verke.pdf

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security, 12*, 233-249. https://10.4236/jis.2021.124013

Anthony, S., Guðmundsdóttir, A., Hylander, A., Kuokkanen, M., Sbertoli, G., Skoglöf, M., Størset, H. & Valgeirsdóttir, H. (2019). *Aikuisten digitaaliset perustaidot Pohjoismaissa*. *Haasteista mahdollisuuksiksi?.* Nordic Network for adult learning - Pohjoismainen aikuiskoulutusverkosto. https://tyottomat.fi/wp-content/uploads/2021/03/nvl_aikuisten_digitaaliset_perustaidot_0170920.pdf

Blaži˘c, J. (2022). Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability 2022, 14, 4763*. https://doi.org/10.3390/su14084763

Dutton, W. H. (2017). Fostering a cyber security mindset. University, East Lansing, United States. *Internet Policy Review*, 6(1). https://policyreview.info/articles/analysis/fostering-cyber-security-mindset

Eskola, J & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen.* Vastapaino.

Fortinet (2022). *What is the CIA Triad?* Cyberglossary. Resources. https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions

HAMK (N.d.) It-palvelut. *Kyselyiden tekeminen Webropol*. https://www.hamk.fi/it-palvelut/kyselyiden-tekeminen-webropol/

Holmström, L. & Korkka, D. (2019). *DIGI HALTUUN! Luokanopettajaopiskelijoiden asenne tieto viestintäteknologiasta sekä digitaalinen kompetenssi.* Turun yliopisto. https://www.utupub.fi/bitstream/handle/10024/147775/Opiskelija1Holmstrom_Laura_Opiskelija2Korkka_Daria_opinnayte.pdf?sequence=1&isAllowed=y

JYU, (2015). Menetelmäpolkuja humanisteille. *Määrällinen tutkimus.* Haettu 17.9.2022. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus

Kallinen, T. & Kinnunen, T. (n.d.). *Laadullisen tutkimuksen verkkokäsikirja.* Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullisen-tutkimuksen-ominaispiirteet/

Karjalainen, S. (23.4.2014). *Lukiolaiset kyberturvallisuuden äärellä.* Sitra. https://www.sitra.fi/blogit/lukiolaiset-kyberturvallisuuden-aarella/

Kyberturvallisuuskeskus (2022a). *Kyberturvallisuuden perussanasto.* https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-perussanasto

Lehto, M., Tyrvänen,P., Pöyhönen, J. & Talja,R. (2019*). Kyberturvallisuus Suomessa 2019-2029.* Strategiasarja. Allied ICT Finland. Jyväskylän yliopisto. https://www.alliedict.fi/wp-content/uploads/2021/06/3.Kyberturvallisuus_Suomessa_2019-2029.pdf

Leino,K., Rikala, J., Puhakka,E., Niilo-Rämä, M., Sirén,M. & Fagerlund, J. (2019). *Digiloikasta digitaitoihin.* Kansainvälinen monilukutaidon ja ohjelmoinnillisen ajattelun tutkimus (ICILS 2018). Koulutuksen tutkimuslaitos. https://jyx.jyu.fi/bitstream/handle/123456789/66250/1/978-951-39-7937-9.pdf

Lehto, M. (2022). *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti*. Informaatioteknologian tiedekunnan julkaisuja No. 93/2022. JYU. https://jyx.jyu.fi/bitstream/handle/123456789/82709/Kyberturvallisuuden%20koulutusohjelman%20muutostarpeiden%20tutkimus%20v4.pdf?sequence=1&isAllowed=y

Liikenne- ja viestintäministeriö (8.2.2022). *Suomi kehittää kyberturvallisuuden kansalaistaitoja koko Euroopan unionin alueelle.* https://www.lvm.fi/-/suomi-kehittaa-kyberturvallisuuden-kansalaistaitoja-koko-euroopan-unionin-alueelle-1656643

Limnéll, J. (2014). *Kyber rantautui Suomeen.* Aalto-yliopiston julkaisusarja TIEDE + TEKNOLOGIA 12/2014. Unigrafia Oy. https://aaltodoc.aalto.fi/bitstream/handle/123456789/14606/isbn9789526060224.pdf?sequence=1&isAllowed=y

Limnéll, J. (28.2.2022). *Kyberturva-asiantuntijoiden koulutuksessa tarve yritysten ja korkeakoulujen väliselle yhteistyölle.* Sivistystyönantajat. https://www.sivista.fi/blogi/kyberturva-asiantuntijoiden-koulutuksessa-tarve-yritysten-ja-korkeakoulujen-valiselle-yhteistyolle/

Limnéll, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus*. Docendo.

Luukka, A. (2018). *Opetussuunnitelman ohjeista käytännön työhön : kehittämistutkimus Perusopetuksen opetussuunnitelman perusteissa (2014) olevien tieto- ja viestintäteknologisten tavoitteiden saavuttamiseksi.* [Pro gradu-tutkielma. Tampereen yliopisto]. https://trepo.tuni.fi/handle/10024/103598

Lönnqvist, I. & Moilanen, P. (2017). *Kyberin taskutieto – keskeisin kybermaailmasta jokaiselle.* Jyväskylän yliopisto & Maanpuolustuskoulutusyhdistys. https://jyx.jyu.fi/bitstream/handle/123456789/53510/978-951-39-7009-3.pdf?sequence=1&isAllowed=y

Mattila, j., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J. & Tervo, E. (2020). *Digibarometri 2020: Kyberturvan tilannekuva Suomessa.* Taloustieto Oy. https://www.etla.fi/wp-content/uploads/digibarometri_2020.pdf

Merilehto, H. (2019). *Kyberturvallisuuden oppimisympäristö ammatilliseen koulutukseen.* [Opinnäytetyö, Metropolia Ammattikorkeakoulu.] https://www.theseus.fi/bitstream/handle/10024/166607/Päättötyö_valmis.pdf?sequence=2

Moilanen, P. (01.10.2015). *Arjen kyberturvallisuus on uusi tutkimushaaste.* Jyväskylän yliopisto. https://www.jyu.fi/blogit/tiedeblogi/moilanen_p

MTV Uutiset (2014). *Asiantuntijat: Kyberturvallisuus ekaluokan oppiaineeksi.* https://www.mtvuutiset.fi/artikkeli/asiantuntijat-kyberturvallisuus-ekaluokan-oppiaineeksi/3104692

Opetushallitus (2016). *Perusopetuksen opetussuunnitelman perusteet 2014.* Määräykset ja ohjeet 2014:96. Next Print Oy. https://www.oph.fi/sites/default/files/documents/perusopetuksen_opetussuunnitelman_perusteet_2014.pdf

Opetushallitus (2022a). Koulutus- ja tutkinnot. Perusopetus. *Perusopetuksen opetussuunnitelmien perusteet.* https://www.oph.fi/fi/koulutus-ja-tutkinnot/perusopetuksen-opetussuunnitelman-perusteet

Opetushallitus (2022b). Opetushallituksen tehtävät. *Mitä opetushallitus tekee?* https://www.oph.fi/fi/tietoa-meista/opetushallituksen-tehtavat

Paananen, R. (2021a). *Kyberturvallisuuden kehittämisohjelma.* Liikenne- ja viestintäministeriön julkaisuja 2021:7. Valtioneuvosto. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163219/LVM_2021_7.pdf

Paananen, R. (10.6.2021b). *Kyberturvallisuutta on kehitettävä jatkuvasti.* Impulssi. Blogit. https://impulssilvm.fi/2021/06/10/kyberturvallisuutta-on-kehitettava-jatkuvasti/

Pitkänen, E & Saarenmaa, K. (17.12.2021). *Mobiiliteknologia mullisti lasten arjen – nettiin ei mennä, vaan siellä ollaan.* Tieto&trendit. https://www.stat.fi/tietotrendit/artikkelit/2021/mobiiliteknologia-mullisti-lasten-arjen-nettiin-ei-menna-vaan-siella-ollaan/

Rahman N.A. A, Sairi I. H., Zizi A. N. A. M. & Khalid F. (2020).The Importance of Cybersecurity Education in School. Universiti Kebangsaan Malaysia. *International Journal of Information and Education Technology, Vol. 10, No. 5, May 2020.* www.ijiet.org/vol10/1393-JR419.pdf

Riku (2019a). Rikosuhripäivystys. *Nettirikokset*. https://www.riku.fi/rikoksen-uhrina/lapsi-ja-nuori-rikoksen-uhrina/nettirikokset/

Riku (2019b). Rikosuhripäivystys. *Grooming on uhka lasten turvallisuudelle.* https://www.riku.fi/rikosuhripaivystys/riku-lehti/riku-lehti-3-2019/grooming-on-uhka-lasten-turvallisuudelle/

Riku (2019c). Rikosuhripäivystys. *Petokset*. https://www.riku.fi/erilaisia-rikoksia/petokset/

Tietosuojavaltuutetun toimisto (2022a). *Usein kysyttyä EU:n tietosuoja-asetuksesta.* https://tietosuoja.fi/gdpr

Salasuo, M. (2020). *Harrastamisen äärellä.* Lasten ja nuorten vapaa-aikatutkimus 2020. Opetus- ja kulttuuriministeriö, Valtion nuorisoneuvosto, Nuorisotutkimusseura ja tekijät. https://tietoanuorista.fi/wp-content/uploads/2021/05/lasten-ja-nuorten-vapaa-aikatutkimus-2020-web.pdf

Salokoski, T & Mustonen, A. (2007). *Median vaikutukset lapsiin ja nuoriin — katsaus tutkimuksiin sekä kansainvälisiin mediakasvatuksen ja - säätelyn käytäntöihin.* https://mediakasvatus.fi/wp-content/uploads/2018/06/ISBN978-952-99964-2-1.pdf

Sandroos, L. (2021). *Kyberturvallisuus kuuluu kaikille: viestinnälliset kehykset yksityishenkilöille suunnatussa tietoturvaviestinnässä* [pro gradu -tutkielma, Jyväskylän yliopisto]. https://jyx.jyu.fi/handle/123456789/76351#

Silfverberg, K & El-Khoury, A-K. (8.1.2016). *Koululaisten tietoturvaopetus jää uudessakin opetussuunnitelmassa vajaaksi.* Helsingin Sanomat. https://www.hs.fi/kaupunki/art-2000002878639.html

Sisäministeriö (2017). *Tietoverkkorikollisuuden torjuntaa koskeva selvitys.* Sisäministeriön julkaisu 14/2017. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1

Sitra (2014). *Uuden turvallisuuden kokeilut.* Sitra. https://www.sitra.fi/hankkeet/uuden-turvallisuuden-kokeilut/

STUL (5.10.2018). Sähkö- ja teleurakoitsijaliitto. *Kyberturvallisuuden perusteet -kurssi ammatillisten oppilaitosten käyttöön.* Haettu 22.06.2022. https://www.stul.fi/kyberturvallisuuden-perusteet-kurssi-ammatillisten-oppilaitosten-kayttoon/

Säntti, J. (2020) Joukkoviestinnästä digiaikaan : Tieto- ja viestintätekniikka suomalaisen perusopetuksen opetussuunnitelmien perusteissa 1970-2014. *Kasvatus & Aika. 14(3),* 60-79. https://doi.org/10.33350/ka.82657

Tanhua-Piiroinen, E., Kaarakainen, S-S., Kaarakainen, M-T., Viteli, J., Syvänen, A. & Kivinen, A. (2019). *Digiajan peruskoulu.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 6/2019. Valtioneuvoston kanslia. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161383/6-2019-Digiajan%20peruskoulu_.pdf

Tietosuojavaltuutetun toimisto (2022b). *Tietosuoja.* https://tietosuoja.fi/tietosuoja

Tilastokeskus (18.2.2021a). *Peruskoulujen määrä jatkoi laskuaan, eniten lakkautuksia Pohjois-Pohjanmaalla.* Tilastot. https://tilastokeskus.fi/til/kjarj/2020/kjarj_2020_2021-02-18_tie_001_fi.html

Tilastokeskus (2021b). *Rikos- ja pakkokeinotilasto.* Suomen virallinen tilasto (SVT). Haettu 28.6.2022. https://pxweb2.stat.fi/PxWeb/pxweb/fi/StatFin/StatFin__rpk/statfin_rpk_pxt_13gw.px/table/tableViewLayout1/

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällön analyysi.* Kustannusosakeyhtiö Tammi.

Turun yliopisto (9.10.2018). *Erot nuorten digitaidoissa syntyvät jo peruskoulussa.* https://www.utu.fi/fi/ajankohtaista/uutinen/erot-nuorten-digitaidoissa-syntyvat-jo-peruskoulussa

Turvallisuuskomitea (2018). *Kyberturvallisuuden sanasto.* Ordlista om cybersäkerhet. Vocabulary of Cyber Security. Sanastokeskus TSK ry. Huoltovarmuuskeskus. Haettu 14.06.2022. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Turvallisuuskomitea (2019). *Suomen kyberturvallisuusstrategia 2019.* Valtioneuvoston periaatepäätös. Turvallisuuskomitea. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Tutkimuseettinen neuvottelukunta (2022). *Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa.* Haettu 15.06.2022. https://tenk.fi/fi/ohjeet-ja-aineistot/HTK-ohje-2012

Valli, R. (2018). *Ikkunoita tutkimusmetodeihin 1.* Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. PS-kustannus.

Valli, R. & Aaltola, J. (2018). *Ikkunoita tutkimusmetodeihin 2.* Näkökulmia aloittavalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. PS-kustannus.

Varmuuden vuoksi (N.d.). *Kyber-esite.* Huoltovarmuuskeskuksen verkkolehti. https://www.varmuudenvuoksi.fi/filebank/a/1416224994/ebe6ce40e87e4d1972490571a63ad0de/439-Kyber_esite_WEB.pdf

Vehkoo, J. (8.2.2021). *Valheenpaljastaja: Kahdeksan asiaa, jotka jokaisen pitäisi ymmärtää misinformaatiosta.* Yle. https://yle.fi/aihe/artikkeli/2021/02/08/valheenpaljastaja-kahdeksan-asiaa-jotka-jokaisen-pitaisi-ymmartaa

Vilkka H. (2007). *Tutki ja mittaa.* Määrällisen tutkimuksen perusteet. Tampereen yliopisto. http://hanna.vilkka.fi/wp-content/uploads/2014/02/Tutki-ja-mittaa.pdf

Vilpas, P. (N.d.) *Kvantitatiivinen tutkimus.* Metropolia ammattikorkeakoulu. Haettu 27.07.2022. https://users.metropolia.fi/~pervil/kvantsu/Moniste.pdf

Witsenboer, J., Sjitsma, K & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education. *Computers & Education. Volume 186*, September 2022, 104536. https://doi.org/10.1016/j.compedu.2022.104536

Liite 1: Aineistonkäsittelysuunnitelma

Opinnäytetyöhön koottava aineisto koostuu sähköisellä kyselylomakkeella kerätystä aineistosta, jossa henkilöön liittyviä tietoja kerätään mahdollisimman vähän, vain sen verran, kuin on välttämätöntä aineiston taustatietojen kannalta.

Sähköinen kyselylomake toteutetaan Webpropol-työkalulla, jonka käyttöoikeuden omistaa HAMK ja jonka opiskelijat saavat käyttöönsä. Aineisto koostuu kyselylinkin vastaanottajien vastauksista kyselylomakkeissa ja ne ovat muodoltaan numeraalisia, tekstimuotoisia tai koostuvat ennalta määritellyistä valitusta vaihtoehdosta.

Sähköisen kyselyn materiaaleja säilytetään Webpropol työkalussa. Tietosuojailmoitus Webpropol-työkalusta on saatavilla HAMKin verkkosivustolta. Myöhemmässä vaiheessa tietoja tullaan siirtämään osaksi myöhemmin julkaistavaa opinnäytetyötä sekä käsittelemään mahdollisissa muissa työkaluissa, joilla määrällisiä tuloksia analysoidaan ja muutetaan visuaaliseen muotoon opinnäytetyön tekijöiden toimesta (esimerkiksi MS Office Excel). Tekstimuotoinen aineisto analysoidaan sekä käsitellään tekstinkäsittelyohjelmassa (MS Office Word), ja siirretään lopulliseen opinnäytetyöhön.

Molempia aineistoja käsittelevät vain opinnäytetyön tekijät sekä tarvittaessa tarkasteluun osallistuu korkeakoulun määräämä opinnäytetyön ohjaaja. Opinnäytetyön aineiston ja tulokset sekä aineiston omistus- ja käyttöoikeudet omistavat opinnäytetyötä tekevät opiskelijat.

Opinnäytetyössä tullaan viittamaan myös erilaisiin lähteisiin. Lähteisiin viitataan HAMKin lähdeviittausohjeen mukaisesti ja lainsäädäntöä noudattaen.

Varsinaista opinnäytetyötä sekä sen liitteitä säilytetään OneDrive-alustalla opinnäytetyöntekijöiden ammattikorkeakoulusta saamilla tunnuksilla. Molemmilla opinnäytetyöntekijöillä on näillä tunnuksilla käytössään kaksivaiheinen tunnistautuminen (MFA). Myös OneDrive-alustalle on pääsy ainoastaan opinnäytetyöntekijöillä sekä tarvittaessa ohjaavalla opettajalla.

Opinnäytetyöhön kerättyä aineistoa ei annetta jatkokäyttöön. Opinnäytetyön tekijöiden tulee säilyttää aineistoa yhden (1) vuoden ajan opinnäytetyön hyväksymispäivästä, jotta tulokset voidaan tarvittaessa varmistaa. Aineisto tuhotaan noudattaen HAMKin ohjeita, kun opinnäytetyöprosessi sekä yhden vuoden vähimmäissäilytysaika on umpeutunut.

Liite 2: Perusopetuksen opettajille suunnattu kysely

HÄMEEN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Kyberturvallisuuden opetuksen nykytilan selvitys

Hei,

Tämä kysely on osa Opetushallituksen toimeksiantamaa opinnäytetyötä, joka liittyy Hämeen ammattikorkeakoulun tieto- ja viestintätekniikan insinöörin tutkintoon.

Opinnäytetyön tavoitteena on opetusalan ammattilaisille kohdennetulla kyselytutkimuksella selvittää kyberturvallisuuden opetuksen nykytila sekä kyberturvallisuuden ammattilaisille suunnatulla kyselytutkimuksella kartoittaa, mitä kyberturvallisuuden aihepiirejä perusopetuksessa olisi perusteltua käsitellä, jotta peruskouluikäisten ymmärrystä kyberturvallisuudesta sekä aihepiiriin liittyvistä turvataidoista voitaisiin kehittää.

Tämä kysely on suunnattu peruskoulussa opetusta tekevälle henkilökunnalle. Kyselyyn vastaamiseen kuluu aikaa noin 20 minuuttia.

Vastaukset käsitellään ilman nimiä ja tunnistetietoja.

Ystävällisin terveisin

Sari Kaipainen
Sari.Kaipainen@student.hamk.fi

ja

Miiro Pyysing
Miiro.Pyysing@student.hamk.fi

Opinnäytetyön ohjaaja
Ismo Turve
ismo.turve@hamk.fi

Tämä kysely on jaettu viiteen osaan:

- Taustatiedot
- Kyberturvallisuuden opetus
- Kybermaailman uhat

- Kyberturvallisuuden tulevaisuus
- Vapaa sana

Lähes jokainen osio sisältää lyhyen intron, joka johdattaa sinut kysymyksien aihepiiriin.

Pääset etenemään kyselyssä osio kerrallaan ja kysely päättyy, kun olet lähettänyt vastauksesi "Lähetä" painikkeella.

Aloita kyselyyn vastaaminen painamalla "Seuraava"-painiketta!

Osio 1: Taustatiedot

1. Ikäsi

- ◯ Alle 30 vuotta
- ◯ 30-40 vuotta
- ◯ 40-50 vuotta
- ◯ Yli 50 vuotta

2. Perusopetuksen työkokemus vuosina

- ◯ 0-1 vuotta
- ◯ 1-3 vuotta
- ◯ 3-6 vuotta
- ◯ 6-10 vuotta
- ◯ 10-20 vuotta
- ◯ Yli 20 vuotta

3. Mikä vaihtoehto kuvaa parhaiten työtehtäviäsi opettajana?

- [ ] Luokanopettaja
- [ ] Aineenopettaja, oppiaine? _____
- [ ] Muu, mikä? _____

Osio 1: Taustatiedot

4. Peruskoulun sijainti

- ◯ Etelä-Suomen lääni
- ◯ Itä-Suomen lääni
- ◯ Länsi-Suomen lääni ja Ahvenanmaa
- ◯ Oulun lääni
- ◯ Pohjois-Suomen lääni

5. Koulun koko

- ◯ Alle 50 oppilasta
- ◯ 50-200 oppilasta
- ◯ 200-400 oppilasta
- ◯ 400-700 oppilasta
- ◯ Yli 700 oppilasta

6. Opetusaste

- [ ] Alakoulu
- [ ] Yläkoulu

Osio 2: Kyberturvallisuuden opetus

Tietokoneet, tabletit, älypuhelimet ja muut elektroniset laitteet ovat osa jokapäiväistä elämäämme. Laitteiden, erilaisten tekniikoiden ja yhteyksien kehitys on ollut huimaa viime vuosikymmeninä. Samalla on kehittynyt uusia riskejä, jotka koskettavat meistä jokaista ja vaikuttavat kaikkien turvallisuuteen. Tästä muodostuu kyberympäristö, joka tarkoittaa mahdollisuuksia - mutta myös vaaran paikkoja.

7. Miten koet osaavasi seuraavat käsitteet?

1 = En tiedä mitä käsite tarkoittaa
2= Tiedän mihin aihe-alueesseen käsite liittyy
3 = En osaa sanoa
4 = Osaan melko tarkasti kuvata käsitteen
5 = Osaan kattavasti kuvata mitä käsite tarkoittaa

	1	2	3	4	5
Kyberturvallisuus	◯	◯	◯	◯	◯
CIA-malli	◯	◯	◯	◯	◯
Tietoturvallisuus	◯	◯	◯	◯	◯
Kyberresilienssi	◯	◯	◯	◯	◯
Haittaohjelma	◯	◯	◯	◯	◯
Identiteettivarkaus	◯	◯	◯	◯	◯
Grooming	◯	◯	◯	◯	◯
Haavoittuvuus	◯	◯	◯	◯	◯
Kriittinen infrastruktuuri	◯	◯	◯	◯	◯
Kaksivaiheinen tunnistautuminen	◯	◯	◯	◯	◯
Informaatiovaikuttaminen	◯	◯	◯	◯	◯

Osio 2: Kyberturvallisuuden opetus

Kyberturvallisuus sanana kuvaa useita toimenpiteitä, joita toteutetaan, jotta voidaan hallita erilaisia riskejä ja uhkia, joita toimintaympäristöön liittyy. Olennaista on ehkäistä kyberuhkia ja niiden vaikutuksia yksilöön ja yhteiskuntaan. Erilaiset haitalliset tapahtumat tai teot, jolla voi olla

vaikutusta kyberympäristön toimintaan ovat kyberuhkia.

Turvallisuuskomitea. (2018). ss. 22, 25. Kyberturvallisuuden sanasto. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

8. Missä määrin olet saanut opettajan opinnoissasi tietoa kyberturvallisuuteen liittyvistä kokonaisuuksista?

9. Missä määrin olet osallistunut mahdolliseen kyberturvallisuuden osaamiseen liittyvään täydennyskoulutukseen?

10. Minkälaista opetus kyberturvallisuuteen liittyvistä aiheista opettajan opinnoissasi tai täydennyskoulutuksessa on ollut?

Osio 2: Kyberturvallisuuden opetus

11. Kuinka hyvät valmiudet koet omaavasi kyberturvallisuus-/tietoturva-aiheiden opetukseen?

12. Kuvaile osaamistasi muutamalla lauseella

Osio 2: Kyberturvallisuuden opetus

13. Miten kyberturvallisuuden opetusvalmiuksiasi voisi kehittää tai parantaa?

14. Mitä kautta voit saada materiaalia tai koulutusta, jolla parantaa valmiuksiasi kyberturvallisuuden opettamiseen?

Osio 2: Kyberturvallisuuden opetus

Perusopetuksen opetussuunnitelmien perusteissa (2014) todetaan, että perusopetuksen on tarkoitus ohjata oppijaa toimimaan myös teknologisoituneessa arjessa ja että oppilaat tarvitsevat perustiedot teknologiasta sekä sen kehityksestä ja vaikutuksesta heidän omaan elämäänsä. Huomiota suunnataan erityisesti järkevien teknologisten ratkaisujen tekemisen oppimiseen sekä

toimintaperiaatteiden, eettisyyden ja vastuullisuuden ymmärtämiseen.

Opetushallitus. (2016). s. 22. Perusopetuksen opetussuunnitelman perusteet 2014. https://www.oph.fi/sites/default/files/documents /perusopetuksen_opetussuunnitelman_perusteet_2014.pdf

15. Oletko tietoinen, että kyberturvallisuuden aihealueesta on jo nyt mainintoja perusopetuksen opetussuunnitelmien perusteissa (2014)?

Osio 2: Kyberturvallisuuden opetus

Vuoden 2014 perusopetuksen opetussuunnitelmien perusteissa tietoturvaan liittyvä opetus on sidottu osaksi laaja-alaista osaamista. Tämä tarkoittaa, että se ei ole itsenäinen oppiaine vaan sen aihealueet sisällytetään muuhun opetukseen ja opetettaviin aineisiin.

Esille nostetaan muun muassa vastuullinen ja turvallinen toiminta, johon kuuluvat muun muassa hyvät käytöstavat ja laitteiden turvalliset käyttötavat. Ohjeistuksen mukaan oppilaita tulee myös ohjata turvalliseen ja eettisesti kestävään tieto- ja viestintäteknologian käyttöön. Sekä siihen miten suojaudutaan mahdollisilta tietoturvariskeiltä ja vältytään tiedon häviämiseltä. Vastuulliseen toimintaan ohjataan pohtimalla, mitä esimerkiksi käsitteet tietosuoja ja tekijänoikeus tarkoittavat, ja mitä seurauksia vastuuttomasta ja lainvastaisesta toiminnasta voi olla.

Opetushallitus. (2016). s. 284. Perusopetuksen opetussuunnitelman perusteet 2014. https://www.oph.fi/sites/default/files/documents /perusopetuksen_opetussuunnitelman_perusteet_2014.pdf

Silfverberg, K & El-Khoury, A-K. (2016). Koululaisten tietoturvaopetus jää uudessakin opetussuunnitelmassa vajaaksi. https://www.hs.fi/kaupunki/art-2000002878639.html

16. Miten kyberturvallisuuden yllä mainitut teemat näkyvät omassa opetuksessasi?

_____

_____

17. Mikäli kyseiset teemat eivät ole tuttuja omassa opetuksessasi, niin mistä arvelet sen johtuvan?

_____
_____
_____
_____
_____

Osio 2: Kyberturvallisuuden opetus

Opettajilla on merkittävä rooli tieto- ja viestintätekniikan opetuskäytännöissä. Loppujen lopuksi heistä on myös paljon kiinni, miten oppilaiden mielissä mahdollistuu tieto- ja viestintätekniikan ja sitä kautta myös kyberturvallisuuteen liittyvät merkityksien tunnistaminen ja, miten opetustilanteissa oivalletut asiat konkretisoituvat.

Perusopetuksen opetussuunnitelmien perusteet luovat puitteet tämän toteutumiselle. Kyberturvallisuus on laaja kokonaisuus, johon opetussuunnitelmien perusteista ei kuitenkaan löydy seikkakohtaista ohjeistusta. Kyberturvallisuuden opetukseen liittyvien olennaisten asioiden karsiminen suurista kokonaisuuksista voi olla haasteellista.

Säntti , J. (2020). Joukkoviestinnästä digiaikaan : Tieto- ja viestintätekniikka suomalaisen perusopetuksen opetussuunnitelmien perusteissa 1970-2014. Kasvatus & Aika, 3/14 , Nro 3, 60-79.

Merilehto, H. (2019). Kyberturvallisuuden oppimisympäristö ammatilliseen koulutukseen. [Opinnäytetyö, Metropolia Ammattikorkeakoulu]. https://www.theseus.fi/bitstream/handle/10024/166607/Päättötyö_valmis.pdf?sequence=2

18. Mitkä asiat koet haastaviksi ajatellen kyberturvallisuuden teemojen opetusta?

_____
_____
_____
_____
_____

19. Kuinka luontevaksi koet sen, että kyberturvallisuuden teemoja sisällytettäisiin opettamiisi oppiaineisiin?

Osio 2: Kyberturvallisuuden opetus

20. Millaisia onnistumisen kokemuksia sinulla on kyberturvallisuuden teemojen opetuksesta?

_____
_____
_____
_____
_____

21. Minkälaista tukea tai koulutusta toivot tulevaisuudessa kyberturvallisuuden teemojen opetukseen?

_____
_____
_____
_____
_____

Osio 3: Kybermaailman uhat

Internetin välityksellä tapahtuvia rikoksia ovat esimerkiksi kunnianloukkaus, laiton uhkaus, yksityiselämää loukkaavan tiedon levittäminen, erinäiset huijaukset ja petokset sekä seksuaalirikokset. Tilastokeskuksen julkaisemasta rikos- ja pakkokeinotilastosta selviää, että lapsiin kohdistuneista seksuaalirikoksista kirjattujen rikosilmoitusten määrissä on havaittavissa kasvava trendi.

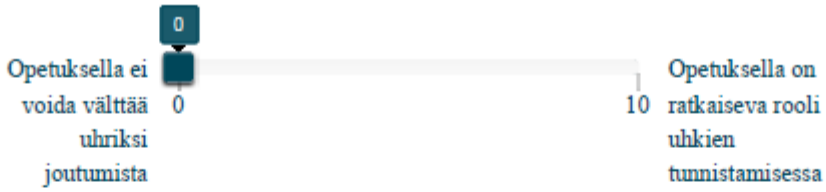
Rikosuhripäivystys. (28.6.2022). Lapsi ja nuori nettirikoksen uhrina. Nettirikokset. https://www.riku.fi/rikoksen-uhrina/lapsi-ja-nuori-rikoksen-uhrina/nettirikokset/

22. Kuinka hyvin koet tuntevasi internetin välityksellä tapahtuvat rikokset?

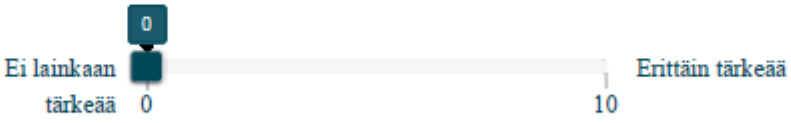
23. Kuinka helposti pystyt kuvailemaan yleisimpiä internetissä tapahtuvia rikoksia?

Osio 3: Kybermaailman uhat

24. Minkälaisen vaikutuksen ajattelet peruskoulun opetuksella olevan siihen, että lapset ja nuoret tunnistaisivat mahdollisia uhkia ja rikoksia verkkomaailmassa?



25. Kuinka oleellisena pidät sitä, että myös oppilaiden huoltajille jaettaisiin tietoa sekä ohjeistuksia liittyen kriittiseen medialukutaitoon, turvataitoihin, nettikiusaamiseen, uhkien havaitsemiseen sekä havaittujen rikosten ilmiantamiseen?



Osio 4: Kyberturvallisuuden opetuksen tulevaisuus

26. Kuinka tärkeänä näet kyberturvallisuuden opetuksen peruskoulussa?

27. Minkä takia koet tai et koe, että kyberturvallisuuden opetus on tärkeää?

_____
_____
_____
_____
_____

28. Kuinka tarpeellista mielestäsi olisi aloittaa kyberturvallisuuden perusteiden opetus ensimmäisestä vuosiluokasta (keskimäärin 7-vuotiaat) lähtien?

Osio 4: Kyberturvallisuuden opetuksen tulevaisuus

Kun teknologiset ratkaisut yleistyvät ja yksityishenkilöt pääsevät yhä laajemmin kiinni verkottuneeseen maailmaan sekä tuottamaan sisältöä, voidaan samalla nähdä jokaisen henkilön vastuun laajenevan. Toistaiseksi on melko vähän tutkimusta siitä, minkälaisessa arvossa ihmiset näkevät kyberturvallisuustaidot ja miten tärkeänä he pitävät kyberturvallisuus osaamisen kehittämistä.

Dutton, W. H. (2017). Fostering a cyber security mindset. Internet Policy Review, 6(1). https://policyreview.info/articles/analysis/fostering-cyber-security-mindset

29. Miten riittävät kyberturvallisuuden perustaidot koet suomalaisilla peruskouluikäisillä olevan keskimäärin tällä hetkellä?

30. Miten riittävät kyberturvallisuuden perustaidot koet suomalaisilla työikäisillä olevan keskimäärin tällä hetkellä?

31. Voisiko kyberturvallisuuden perusteiden opetuksesta olla vastuussa jotkin muut tahot kuin peruskoulu? Mitkä?

Osio 5: Vapaa sana

32. Jäikö mieleesi vielä jotain muuta sanottavaa? Tähän voit halutessasi kirjoittaa vapaasti ajatuksia.

Liite 3: Kyberturvallisuuden ammattilaisille suunnattu kysely

HAMK
HÄMEEN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Kysely ammattilaisille kyberturvallisuuden opetuksesta suomalaisessa peruskoulussa

Hei,

Tämä kysely on osa Opetushallituksen toimeksiantamaa opinnäytetyötä, joka liittyy Hämeen ammattikorkeakoulun tieto- ja viestintätekniikan insinöörin tutkintoon.

Opinnäytetyön tavoitteena on opetusalan ammattilaisille kohdennetulla kyselytutkimuksella selvittää kyberturvallisuuden opetuksen nykytila sekä kyberturvallisuuden ammattilaisille suunnatulla kyselytutkimuksella kartoittaa, mitä kyberturvallisuuden aihepiirejä perusopetuksessa olisi perusteltua käsitellä, jotta peruskouluikäisten ymmärrystä kyberturvallisuudesta sekä aihepiiriin liittyvistä turvataidoista voitaisiin kehittää.

Tämä kysely on suunnattu kyberturvallisuuden parissa työskenteleville henkilöille. Kyselyyn vastaamiseen kuluu aikaa noin 20 minuuttia.

Vastaukset käsitellään ilman nimiä ja tunnistetietoja.

Ystävällisin terveisin

Sari Kaipainen
Sari.Kaipainen@student.hamk.fi

ja

Miiro Pyysing
Miiro.Pyysing@student.hamk.fi

Opinnäytetyön ohjaaja
Ismo Turve
ismo.turve@hamk.fi

Tämä kysely on jaettu viiteen osaan:

- Taustatiedot

- Kyberturvallisuuden opetus
- Kybermaailman uhat
- Kyberturvallisuuden opetuksen tulevaisuus
- Vapaa-sana

Lähes jokainen osio sisältää lyhyen intron, joka johdattaa sinut kysymyksien aihepiiriin.

Pääset etenemään kyselyssä osio kerrallaan ja kysely päättyy, kun olet lähettänyt vastauksesi "Lähetä" painikkeella.

Aloita kyselyyn vastaaminen painamalla "Seuraava"-painiketta!

Osio 1: Taustatiedot

1. Ikä

- ◯ Alle 30
- ◯ 30-40
- ◯ 40-50
- ◯ Yli 50

2. Kyberturvallisuusalan työkokemus vuosina

- ◯ 0-1 vuotta
- ◯ 1-3 vuotta
- ◯ 3-6 vuotta
- ◯ 6-10 vuotta
- ◯ 10-20 vuotta
- ◯ yli 20 vuotta

Osio 1: Taustatiedot

3. Yrityksen sijainti

- ◯ Etelä-Suomen lääni
- ◯ Länsi-Suomen lääni ja Ahvenanmaa
- ◯ Itä-Suomen lääni
- ◯ Oulun lääni
- ◯ Pohjois-Suomen lääni

4. Organisaation koko

- ◯ Alle 10 työntekijää
- ◯ 11-50 työntekijää
- ◯ 51-250 työntekijää
- ◯ Yli 250 työntekijää

Osio 2: Kyberturvallisuuden opetus

Suomessa peruskoulujen opetus pohjautuu perusopetuksen opetussuunnitelmien perusteisiin, minkä pohjalta laaditaan paikalliset opetussuunnitelmat. Järjestelmällä pyritään varmistamaan koulutuksen tasalaatuisuus sekä edellytykset oppimiselle.

Opetushallitus. (2016). s. 9-13. Perusopetuksen opetussuunnitelman perusteet 2014. https://www.oph.fi/sites/default/files/documents /perusopetuksen_opetussuunnitelman_perusteet_2014.pdf

5. Tiesitkö, että perusopetuksen opetussuunnitelmien perusteissa (2014), joihin opetussuunnitelmat ja aineopetuksen sisällöt perustuvat, on mainintoja kyberturvallisuuteen liittyen?

- ◯ En tiennyt, että kyberturvallisuuden opetusta sisältyy millään tavalla suomalaiseen peruskouluun
- ◯ Olen kuullut, että joitakin osa-alueita kyberturvallisuudesta opetetaan peruskoulussa
- ◯ Olen perehtynyt perusopetuksen opetussuunnitelmien perusteissa oleviin mainintoihin kyberturvallisuuden teemasta

Osio 2: Kyberturvallisuuden opetus

Perusopetuksen opetussuunnitelmien perusteissa (2014) todetaan, että perusopetuksen on tarkoitus ohjata oppijaa toimimaan myös teknologisoituneessa arjessa ja että oppilaat tarvitsevat perustiedot teknologiasta sekä sen kehityksestä ja vaikutuksesta heidän omaan elämäänsä. Huomiota suunnataan erityisesti järkevien teknologisten ratkaisujen tekemisen oppimiseen sekä toimintaperiaatteiden, eettisyyden ja vastuullisuuden ymmärtämiseen.

Opetushallitus. (2016). s. 22. Perusopetuksen opetussuunnitelman perusteet 2014. https://www.oph.fi/sites/default/files/documents /perusopetuksen_opetussuunnitelman_perusteet_2014.pdf

6. Oletko kuullut, että kyberturvallisuuden perustaitoja käsiteltäisiin perusopetuksessa? Mitä olet kuullut opetettavan?

_____
_____
_____
_____
_____

7. Minkälaista ja -tasoista kyberturvallisuuden perustaitojen opetusta mielestäsi peruskoulussa tulisi opettaa?

_____
_____
_____
_____
_____

Osio 2: Kyberturvallisuuden opetus

8. Miten tärkeänä asiana pidät jokaisen suomalaisen kansalaistaitoja kyberturvallisuuteen liittyen?

9. Mitä nämä kyberturvallisuuden kansalaistaidot voisivat tarkoittaa?

_____
_____
_____
_____
_____

Osio 2: Kyberturvallisuuden opetus

Vuoden 2014 perusopetuksen opetussuunnitelmien perusteissa tietoturvaan liittyvä opetus on sidottu osaksi laaja-alaista osaamista. Tämä tarkoittaa, että se ei ole itsenäinen oppiaine vaan sen aihealueet sisällytetään muuhun opetukseen ja opetettaviin aineisiin.

Esille nostetaan muun muassa vastuullinen ja turvallinen toiminta, johon kuuluvat muun muassa hyvät käytöstavat ja laitteiden turvalliset käyttötavat. Ohjeistuksen mukaan oppilaita tulee myös ohjata turvalliseen ja eettisesti kestävään tieto- ja viestintäteknologian käyttöön, sekä siihen miten suojaudutaan mahdollisilta tietoturvariskeiltä ja vältytään tiedon häviämiseltä. Vastuulliseen toimintaan ohjataan pohtimalla, mitä esimerkiksi käsitteet tietosuoja ja tekijänoikeus tarkoittavat, ja mitä seurauksia vastuuttomasta ja lainvastaisesta toiminnasta voi olla.

Opetushallitus. (2016). s. 284. Perusopetuksen opetussuunnitelman perusteet 2014. https://www.oph.fi/sites/default/files/documents /perusopetuksen_opetussuunnitelman_perusteet_2014.pdf

Silfverberg, K & El-Khoury, A-K. (2016). Koululaisten tietoturvaopetus jää uudessakin opetussuunnitelmassa vajaaksi. https://www.hs.fi/kaupunki/art-2000002878639.html

10. Kuinka tärkeänä pidät seuraavien teemojen opetusta suomalaisessa peruskoulussa?

1 = Ei lainkaan tärkeää
2= Vain vähän tärkeää
3 = En osaa sanoa
4 = Jokseenkin tärkeää
5 = Erittäin tärkeää

	1	2	3	4	5
Hyvät käytöstavat ja turvallinen toiminta internetissä	◯	◯	◯	◯	◯
Laitteiden turvallinen käyttö	◯	◯	◯	◯	◯

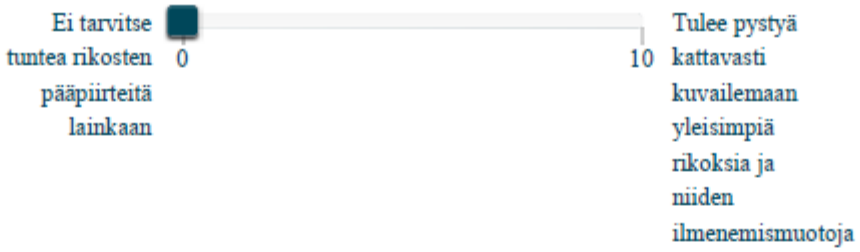
	1	2	3	4	5
Ohjaus eettisesti kestävään tieto- ja viestintäteknologian käyttöön	○	○	○	○	○
Tietoturvariskeiltä suojautuminen	○	○	○	○	○
GDPR-lainsäädännön tunteminen	○	○	○	○	○
Tekijänoikeudet	○	○	○	○	○
Tietotekniikan teknisten toiminta edellytysten tunteminen	○	○	○	○	○
Yleisimpien verkkorikosten tunnusmerkkien tunnistaminen	○	○	○	○	○
Kyberturvallisuuden peruskäsitteiden tunteminen	○	○	○	○	○
Kybermaailman lainalaisuuksien tunteminen	○	○	○	○	○
CIA-malli	○	○	○	○	○
Suomen kyberturvallisuuden strategia ja muut kansalliset ohjelmat	○	○	○	○	○
Kaksivaiheinen tunnistautuminen ja muiden turvallisuutta lisäävien toimenpiteiden tuntemus	○	○	○	○	○

Osio 3: Kybermaailman uhat

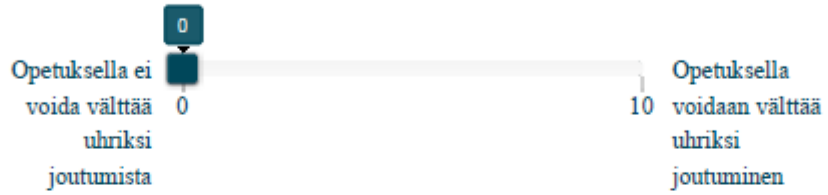
Internetin välityksellä tapahtuvia rikoksia ovat esimerkiksi kunnianloukkaus, laiton uhkaus, yksityiselämää loukkaavan tiedon levittäminen, erinäiset huijaukset ja petokset sekä seksuaalirikokset. Tilastokeskuksen julkaisemasta rikos- ja pakkokeinotilastosta selviää, että lapsiin kohdistuneista seksuaalirikoksista kirjattujen rikosilmoitusten määrissä on havaittavissa kasvava trendi.

Rikosuhripäivystys. (28.6.2022). Lapsi ja nuori nettirikoksen uhrina. Nettirikokset. https://www.riku.fi/rikoksen-uhrina/lapsi-ja-nuori-rikoksen-uhrina/nettirikokset/

11. Kuinka hyvin koet, että kyberturvallisuutta opettavien opettajien tulisi hallita internetin välityksellä tapahtuvat rikokset ja pystyä kuvailemaan yleisimpiä internetissä tapahtuvia rikoksia?



12. Minkälaisen vaikutuksen ajattelet peruskoulun opetuksella olevan siihen, että lapset ja nuoret tunnistaisivat mahdollisia uhkia ja rikoksia verkkomaailmassa?



13. Kuinka oleellisena pidät sitä, että myös oppilaiden huoltajille jaettaisiin tietoa sekä ohjeistuksia liittyen kriittiseen medialukutaitoon, turvataitoihin, nettikiusaamiseen, uhkien havaitsemiseen sekä havaittujen rikosten ilmiantamiseen?

Osio 4: Kyberturvallisuuden opetuksen tulevaisuus

Opettajilla on merkittävä rooli tieto- ja viestintätekniikan opetuskäytännöissä. Loppujen lopuksi heistä on myös paljon kiinni, miten oppilaiden mielissä mahdollistuu tieto- ja viestintätekniikan ja sitä kautta myös kyberturvallisuuteen liittyvät merkityksien tunnistaminen ja, miten opetustilanteissa oivalletut asiat konkretisoituvat.

Säntti , J. (2020). Joukkoviestinnästä digiaikaan : Tieto- ja viestintätekniikka suomalaisen perusopetuksen opetussuunnitelmien perusteissa 1970-2014. Kasvatus & Aika, 3/14 , Nro 3, 60-79.

14. Kuinka tärkeänä näet kyberturvallisuuden opetuksen peruskoulussa? Ja

miksi koet tai et koe sitä tärkeänä?

15. Kuinka tarpeellista mielestäsi olisi aloittaa kyberturvallisuuden perusteiden opetus ensimmäisestä vuosiluokasta (keskimäärin 7-vuotiaat) lähtien?

16. Voisiko kyberturvallisuuden perusteiden opetuksesta olla vastuussa jotkin muut tahot kuin peruskoulu? Mitkä?

_____
_____
_____
_____
_____

Osio 4: Kyberturvallisuuden opetuksen tulevaisuus

17. Voisivatko eri tahot tehdä yhteistyötä perusopetuksen järjestäjien kanssa kyberturvallisuuden perusopetukseen liittyen? Mitkä tahot?

_____
_____
_____
_____
_____

18. Minkälaista yhteistyötä eri tahot voisivat tehdä perusopetuksen järjestäjien kanssa kyberturvallisuuden opetukseen liittyen?

_____
_____
_____

Osio 4: Kyberturvallisuuden opetuksen tulevaisuus

Kun teknologiset ratkaisut yleistyvät ja yksityishenkilöt pääsevät yhä laajemmin kiinni verkottuneeseen maailmaan sekä tuottamaan sisältöä, voidaan samalla nähdä jokaisen henkilön vastuun laajenevan. Toistaiseksi on melko vähän tutkimusta siitä, minkälaisessa arvossa ihmiset näkevät kyberturvallisuustaidot ja miten tärkeänä he pitävät kyberturvallisuus osaamisen kehittämistä.

Dutton, W. H. (2017). Fostering a cyber security mindset. Internet Policy Review, 6(1). https://policyreview.info/articles/analysis/fostering-cyber-security-mindset

19. Miten riittävät kyberturvallisuuden perustaidot koet suomalaisilla peruskouluikäisillä olevan keskimäärin tällä hetkellä?

20. Miten riittävät kyberturvallisuuden perustaidot koet suomalaisilla työikäisillä olevan keskimäärin tällä hetkellä?

Osio 4: Kyberturvallisuuden opetuksen tulevaisuus

Perusopetuksen opetussuunnitelmien perusteet (2014) luovat puitteet tämän toteutumiselle. Kyberturvallisuus on laaja kokonaisuus, johon opetussuunnitelmien perusteista ei kuitenkaan löydy seikkakohtaista ohjeistusta. Opettajien voi olla vaikea hahmottaa sitä, mikä on missäkin yhteydessä olennaista.

Merilehto, H. (2019). Kyberturvallisuuden oppimisympäristö ammatilliseen koulutukseen. [Opinnäytetyö, Metropolia Ammattikorkeakoulu]. https://www.theseus.fi/bitstream/handle/10024/166607/Päättötyö_valmis.pdf?sequence=2

21. Millä tavoin peruskoulun opettajia voisi tukea tai auttaa opetuksen sisällön ja toteutuksen suunnittelussa?

_____
_____
_____
_____
_____

22. Mitä julkisia materiaaleja tiedät olevan, joita peruskoulun opettajat voisivat hyödyntää kyberturvallisuuden teemojen opetuksessa?

_____
_____
_____
_____
_____

Osio 5: Vapaa sana

23. Jäikö mieleesi vielä jotain muuta sanottavaa? Tähän voit halutessasi kirjoittaa vapaasti ajatuksia.

_____
_____
_____
_____
_____