Petra Saari

KYBERTURVALLISUUDEN OPETUSSISÄLTÖ PERUSKOULUSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Saari, Petra
Kyberturvallisuuden opetussisältö peruskoulussa
Jyväskylä: Jyväskylän yliopisto, 2024, 47 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Nykyisin kyberturvallisuuden osaamisesta puhutaan usein kansalaistaitona. Kouluissa ei kuitenkaan toistaiseksi tarjota erillistä kyberturvallisuuden opetusta, mutta joitakin kyberturvallisuuteen liitettäviä aiheita opetetaan opetussuunnitelman mukaan ns. laaja-alaisena oppimisena, integroituna osaksi muiden aineiden opetusta.

Tämän pro gradu tutkielman tarkoitus on selvittää mitä kyberturvallisuudesta tulisi opettaa peruskoulun tasolla, jotta Suomen kyberturvallisuusstrategian asettama tavoite kansallisen kyberturvallisuuden osaamisen varmistamisesta täyttyisi. Tavoitteena on alan kirjallisuuteen pohjautuen ja tutkimusta varten teetetyn kyselytutkimuksen avulla selvittää, minkälaisia kyberturvallisuuden osaamisen tarpeita voidaan peruskoulun tasolla tunnistaa ja millaisilla opetuksen sisällöillä voidaan vastata tunnistettuihin tarpeisiin.

Tutkimuksessa käytetty kyselytutkimus on suunnattu kartoittamaan juuri tietotekniikan opettajien käsityksiä tulevaisuudessa opetettavista aiheista, sillä mikäli kyberturvallisuudesta muodostettaisiin oma oppiaineensa, vastuu aineen opetuksesta siirtyisi luontevasti juuri tietotekniikan opettajille. Tietotekniikan opettajilla oletetaan lisäksi olevan tarvittava pohjaymmärrys vastata tutkimuksen kyselylomakkeessa esitettyihin kysymyksiin.

Tutkimuksen johtopäätöksinä voidaan todeta, että kyberturvallisuuden opetuksen sisältöjen yksityiskohtainen määrittäminen on haastavaa aiheen ja siihen liittyvien ilmiöiden alati muuttuvan luonteen vuoksi. Kyberuhat kehittyvät nopeasti ja tieto uhkien tunnistamisesta sekä torjumisesta vanhenee usein samaa tahtia. Tärkeintä olisikin opettaa lapsille ja nuorille kyberturvallisuuden jatkuvan oppimisen tärkeys ja keinot, kuinka sitä toteuttaa. Kyberturvallisuuteen liittyen esimerkiksi internetin hyvät käytöstavat, sekä medialukutaito, ovat aiheita, jotka eivät yhtä lailla kärsi aiheen jatkuvasta muutoksesta ja toimivatkin ns. kyberturvallisuuden- ja sen opetuksen kivijalkoina.

Asiasanat: kyberturvallisuus, perusopetus, kyberturvallisuuden opetus, kansalaisen kyberturvallisuustaidot

ABSTRACT

Saari, Petra
The teaching content of cyber security in primary school
Jyväskylä: University of Jyväskylä, 2024, 47 pp.
Cyber Security, Master's Thesis
Supervisor(s): Lehto, Martti

Nowadays, cyber security competence is often referred to as a civic skill. For the time being, schools do not yet offer separate cyber security education, but some topics related to cyber security are taught according to the curriculum in so called broad-based learning, where the teaching of the subject is integrated into other subjects.

The purpose of this master's thesis is to find out what should be taught about cyber security at the primary school, in order to meet the goal of ensuring national cyber security competence set by Finland's National Cyber Security Strategy. The aim is to find out, based on the literature review and questionnaire conducted for the study, what kind of cyber security competence needs can be identified at the primary school level and what kind of teaching content can be used to meet the identified needs.

The questionnaire used in the research is used to identify the perceptions of information technology teachers about the topics to be taught in the future, because if cyber security were to be formed as its own subject, the responsibility for teaching the subject would naturally be transferred to information technology teachers. IT teachers are also assumed to have the necessary basic understanding to answer the questions presented in the study's questionnaire.

As the conclusions of the research, it can be stated that the detailed defining of the contents of cyber security education is challenging due to the ever-changing nature of the subject and related phenomena. Cyber threats develop quickly and knowledge about identifying threats and countering them often becomes outdated at the same pace. This is why it would be important to teach children and young people the importance of continuous learning about cyber security and the means of how to implement it. In relation to cyber security, for example good manners on the internet, and media literacy, are topics that are not so strongly affected by the constant change of the topic and act as so-called cornerstones for cyber security and its teaching.

Keywords: Cyber security, basic education, cyber security education, cyber security competence

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Viime vuosikymmenten aikana, teknologian kehittymisen myötä internetistä on tullut jo lähes erottamaton osa meidän jokaisen arkea. Vaikka tällä kehityksellä onkin ollut paljon hyötyä mm. yhteiskunnan eri toimintojen, kommunikoinnin ja arjen sujuvoittamisen näkökulmasta, on se myös luonut uudenlaisia haasteita mm. tiedon ja teknologiasta riippuvaisten toimintojen turvaamiseksi. Kehityksen myötä internetistä on muodostunut myös rikollisuudelle merkittävä toimintaympäristö (Amankwa, 2021). Nykyään yhä suurempi osa poliisin tietoon tulleista rikoksista onkin tehty internetin välityksellä (Sisäministeriö, ei pvm.). Viime vuosien aikana mm. uudenlaisten teknologioiden käyttöönoton myötä erilaisten verkon välitteisten rikosten kirjo on laajentunut ja tapausten määrä kasvanut merkittävästi. Yksilön riskiä joutua kyberrikollisuuden uhriksi, voitaisiin kuitenkin vähentää kouluttamalla ihmisiä mm. lisäämällä ymmärrystä internetin käytön riskeistä ja luomalla ohjeistuksia siitä, kuinka toimia verkossa turvallisesti. (Amankwa, 2021)

Kansallisen kyberturvallisuusosaamisen tarpeeseen on havahduttu myös Suomessa. Suomen kyberturvallisuusstrategia (Turvallisuuskomitea, 2019) listaa yhtenä strategisena linjauksena kyberturvallisuuden osaamisen kehittämisen, jonka tavoitteena on varmistaa kansallisen kyberturvallisuuden osaaminen tunnistamalla osaamisen tarve, sekä vahvistamalla koulutusta ja alan tutkimusta. Strategiassa jokainen yksilö nähdään kyberturvallisuuden kannalta tärkeänä toimijana, joka voi arjessaan omalla toiminnallaan vaikuttaa sekä omaan, että muiden kyberturvallisuuteen. (Turvallisuusneuvos, 2019) Tavoitteena onkin varmistaa, että jokaisella olisi riittävät taidot toimia turvallisesti digitaalisessa ympäristössä. Myös Suomen kyberturvallisuuden kehittämisohjelmassa nostetaan tavoitteeksi huippuluokan osaaminen osana vahvan suomalaisen kyberturvallisuusekosysteemin luomista, sekä esitetään mm. kyberturvallisuuden opintojen sisällyttämistä osaksi peruskoulun opetussuunnitelmaa (Paananen, 2021).

Covid-19 pandemia sai aikaan nopean muutoksen opetuksen digitalisoitumisessa, kun hallitus 16. maaliskuuta 2020 linjasi koulujen sulkemisesta ja lähiopetuksen keskeyttämisestä koronaviruksen leviämisen estämiseksi. Lähiopetuksen sijaan, perusopetus tuli järjestää vaihtoehtoisella tavalla, kuten

etäopetuksena, hyödyntäen mm. digitaalisia oppimisympäristöjä ja -ratkaisuja. Pandemia edellytti uusien teknologioiden käyttöönottoa nopealla aikataululla, mikä osaltaan kasvatti hyökkäyksille altista kybertoimintaympäristön pinta-alaa. Erilaisten netin välityksellä tehtyjen huijausten ja haittaohjelmahyökkäysten määrän onkin raportoitu kasvaneen huomattavasti pandemian alun myötä. (Valtionneuvosto.fi, 2020) (Lallie, ym., 2021)

Kyberturvallisuuden näkökulmasta etenkin lapset ovat haavoittuvassa asemassa. Lapset aloittavat internetin käytön yhä nuorempina, usein ilman vanhemman valvontaa ja hyödyntäessään samoja verkkopalveluita kuin aikuiset, lasten riskit altistua erilaisille kyberuhkille kasvaa (Panhans ym., 2022), (Annansingh, Veli, 2016). Internetin turvallisen käytön oppimisen tulisikin alkaa samanaikaisesti itse käytön aloittamisen kanssa, sekä kulkea käsi kädessä niin lapsen, kuin käytössä olevien teknologioiden kehityksen kanssa. Ottamalla kyberturvallisuus osaksi perusopetusta, lapsille voitaisiin tarjota tietoja ja taitoja, joidenka avulla suojata itseään heihin yleisimmin kohdistuvilta kyberuhkilta.

Kyberturvallisuuden opetuksen sisällyttäminen osaksi perusopetusta voisi tukea osaltaan myös koulujen kykyä suojautua kyberhyökkäyksiltä. Koulujen tietokannat sisältävät paljon arkaluontoista dataa, kuten esimerkiksi henkilöiden koko nimiä, osoitteita, sähköpostiosoitteita, puhelinnumeroita, sosiaaliturvatunnuksia, mikä tekee kouluista kyberrikollisille houkuttelevia kohteita (Richardson, ym., 2020). Kouluja eivät nykyisin uhkaa myöskään vain ulkopuoliset toimijat, vaan osa kouluun kohdistuvista kyberhyökkäyksistä on koulun oppilaiden tekemiä. Oppilaiden tekemien hyökkäysten tavoitteena on usein esimerkiksi arvosanojen muuttaminen tai pelkkä kiusanteko. (Lallie et. al. 2023) Kyberturvallisuuden opettamisella voidaan myös vastata osaltaan tulevaisuuden tarpeeseen, sillä jatkuvan teknologisoitumisen myötä kyberturvallisuuden osaamista tullaan todennäköisesti tarvitsemaan kaikilla aloilla, lähes kaikissa työtehtävissä sekä yhä lisääntyvissä määrin yksilön jokapäiväisessä arjessa. Opetuksen tärkeyttä korostaa osaltaan myös se, että nykyisin yli 95 % kybertapahtumista aiheutuvat ihmisen virheellisen toiminnan (human error) seurauksena (Richardson, ym., 2020).

1.1 Tutkimuksen tavoitteet ja tutkimuskysymys

Itse pääaineen vaihtajana aineenopettajuudesta kyberturvallisuuteen olen opintojen aikana oppinut huomaamaan, kuinka paljon kyberturvallisuuteen liittyviä asioita kohtaan tavallisessa arjessa opintojen ja työn ulkopuolella. Kyseessä on kuitenkin asioita, joita todennäköisesti lähes kaikki kohtaavat arjessaan, riippumatta siitä ovatko he saaneet jonkinlaista koulutusta kyberturvallisuudesta vai ei. Opinnoissani olen törmännyt myös useisiin kyberturvallisuuden strategioihin ja raportteihin, joissa mainitaan kansalaisten kyberturvallisuuden osaaminen ja sen merkitys yhteiskunnan kokonaisturvallisuuden näkökulmasta. Kiinnostukseni niin pedagogiikkaa, kuin kyberturvallisuuttakin kohtaan herätti luonnollisesti kysymyksen siitä, mitä kyberturvallisuudesta opetetaan kouluissa, josta

juontui lopulta kysymys, mitä kyberturvallisuudesta tulisi opettaa? Tämän tutkimuksen tavoitteena onkin selvittää millaisia sisältöjä kyberturvallisuudesta tulisi sisällyttää osaksi perusopetusta, ja näin ollen pyrkiä vastaamaan seuraavaan tutkimuskysymykseen:

Mitä kyberturvallisuudesta tulisi opettaa peruskoulussa, jotta Suomen kyberturvallisuusstrategian tavoite kansalaisen arkiosaamisesta täyttyisi?

Tutkimus keskittyy kyberturvallisuuden opetukseen peruskoulussa, joka on oppivelvollisuuslain (1214/2020) myötä kaikille yhteinen, lain edellyttämä koulutuksen vaihe. Opetuksen toteutus peruskoulussa takaisi kyberturvallisuuteen liittyvien taitojen ja -tietojen saavutettavuuden, antaen eväät näiden kehittämiseen myös jatkossa, mikä näin ollen voisi parhaimmillaan vahvistaa kokonaisvaltaisesti ja tasavertaisesti kansalaisten kyberosaamista pitkällä aikavälillä.

Tässä tutkimuksessa keskitytään löytämään konkreettisia ehdotuksia siitä, mitä asioita kyberturvallisuudesta tulee opettaa juuri peruskoulutasolla. Tätä varten aihetta tarkastellaan opettamisen tarpeen tunnistamisen, opetuksen nykytilan ja lasten sekä nuorten tämänhetkisen osaamisen näkökulmasta, jotta kyetään mm. tunnistamaan millaisissa taidoissa on kenties puutteita, millaisille taidoille olisi tarvetta ja miksi, sekä millaisia muutoksia, tai lisäyksiä nykyiseen opetukseen tulisi tehdä, jotta opetuksella voitaisiin vastata mahdollisesti tunnistettuihin osaamisen puutokseen ja yleisimpiin kansalaisia koskettaviin kyberturvallisuuden haasteisiin. Tutkimuksella pyritään siis luomaan edellä mainittujen pohdintojen pohjalta ehdotuksia tulevaisuudessa opetettavista teemoista ja teemojen tarkemmista sisällöistä.

1.2 Aikaisempaa tutkimusta

Aikaisemmat tutkimukset kyberturvallisuuden opetukseen liittyen käsittelevät usein aihetta alan ammattilaisten koulutuksesta tai yritysten ja organisaatioiden varautumisen näkökulmasta, jättäen kansalaisen osaamisen tarkastelun ulkopuolelle. Tutkimukset aiheen opetuksesta peruskoulun tasolla ovat pääsääntöisesti liittyneet kyberturvallisuuden opetuksen tarpeen tunnistamiseen ja opetuksen nykytilan tarkasteluun, mutta varsinaisista kyberturvallisuuden opetuksen tulevista sisällöistä ei toistaiseksi ole tehty runsaasti tutkimusta, mutta aihetta käsittelevät mm. Nykäsen pro gradu –tutkielma ” *Kyberturvallisuuden/tietoturvallisuuden opetus peruskoulussa*.” (2023), sekä Kaipaisen ja Pyysingin opinnäytetyö *”Kyberturvallisuus suomalaisessa peruskoulussa*” (2022).

1.2.1 Opetuksen tarve

Kyberturvallisuuden opetuksen tärkeyttä koulussa käsittelee tutkimus, jossa opetuksen tarvetta perustellaan mm. juuri lapsiin ja nuoriin kohdistuvilla kyberuhilla, kuten kyberkiusaaminen, nettihuijaukset ja netin välityksellä

toteutettava seksuaalinen hyväksikäyttö (Rahman, ym., 2020). Tutkimuksessa opetuksen sisällyttämistä kouluihin perusteltiin myös aikuisten vähäisellä kiinnostuksella kyberturvallisuutta koskevia seminaareja tai koulutusohjelmia kohtaan, minkä vuoksi kansalaisten kouluttaminen kyberturvallisuuteen liittyvistä aiheista olisikin olennaisen tärkeää sisällyttää kouluihin. Opetuksen kautta voitaisiinkin vaikuttaa myös yksilöiden mielipiteeseen kyberturvallisuuden tärkeydestä. (Rahman, ym., 2020)

Opetuksen tarvetta voidaan perustella myös lasten tämänhetkisillä, sekä tulevaisuudessa tarvittavilla tietotekniikan taidoilla. Luokanopettajien käsityksiä tieto- ja viestintäteknologian mahdollisuuksista tulevaisuuden taitojen kehittämisessä kartoittava tutkimus (Suuronen, Eskola, 2023) tunnistaa lasten luontaisen teknologian käytön haasteita tieto- ja viestintäteknologisten taitojen näkökulmasta. Vaikka lasten teknologian ja erilaisten älylaitteiden käytön voidaan katsoa olevan sujuvaa, ei se kuitenkaan automaattisesti tarkoita, että heillä olisi tarvittavia tietoja ja taitoja tulevaisuuden kannalta tärkeistä tieto- ja viestintäteknologian perustaidoista, kuten esimerkiksi tietoturvasta. Lasten tietotekniikan käytön todetaan myös olevan hyvin yksipuoleista. Oppilaiden joutuessa hyödyntämään teknologiaa normaalista totutun viihdekäytön sijaan työvälineenä, paljastuu tietoteknisten taitojen vähyys ja kuinka oppilaiden tieto- ja viestintäteknologiset käyttövalmiustaidot eivät ole sillä tasolla, mitä voisi olettaa. Tutkimuksen mukaan opettajat tunnistavat digiosaamisen merkityksen lasten ja nuorten tulevaisuudessa. Teknologiset taidot nähtiin niin välineenä tulevaisuuden kannalta tärkeiden taitojen kehittämiselle kuin itse yhtenä opeteltavista taidoista. (Suuronen, Eskola, 2023)

Lisäksi eri maiden kyberturvallisuusstrategioita tarkasteleva tutkimus osoittaa strategioissa tunnistetun tarpeen kyberturvallisuuden osaamiselle osana kansallisen kyberuhkien sietämisen kyvyn, eli kyberresilienssin vahvistamista. (AlDaajeh, ym., 2022)

1.2.2 Opetuksen nykytila

Opetuksen nykytilasta on raportoitu laajasti mm. Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportissa. Hankkeen asettama tutkimuskysymys oli "Millaisia toimenpiteitä tarvitaan Suomen kyberturvallisuusosaamisen määrällisen ja laadullisen tilanteen parantamiseksi?". Tutkimuskysymykseen vastatakseen hankkeessa laadittiin tilannekuva opetuksen nykytilasta eri koulutusasteilla, sekä selvitys tarvittavista toimenpiteistä, jotta opetusohjelma voisi vastata tavoitteisiin, joita on esitetty EU:n kyberturvallisuusstrategiassa (2020), EU:n digitaalista kehitystä edistävissä ohjelmissa, Suomen kyberturvallisuusstrategiassa (2019) ja sen kehittämisohjelmassa (2021) sekä EU:n ja Suomen osaamisen kehittämisen ohjelmissa. (Lehto, 2022)

Edellä mainittuun hankkeeseen liittyen tehty pro gradu -tutkielma "Kyberturvallisuuden/tietoturvallisuuden opetus peruskoulussa" (Nykänen, 2023), pyrkii kirjallisuuskatsauksen ja opettajille suunnatun kyselytutkimuksen avulla tarkemmin selvittämään opetuksen nykytilaa Suomen peruskouluissa. Tutkielman mukaan tieto- ja viestintäteknologian aiheiden opetukselle ei ole opettajien

näkökulmasta annettu tarpeeksi selkeitä ohjeita, ja opetuksen tavoitteiden kuvaukset jäävät laveiksi. Tämän takia opetuksen sisältö sekä taso vaihtelee paikkakunta-, koulu- ja opettajakohtaisesti. Myös tutkimuksen kyselyyn saatujen vastausten perusteella, osa opettajista ei sisällytä kyberturvallisuuteen liittyviä tieto- ja viestintäteknologian aiheita opetukseensa lainkaan. Kuitenkin alakouluopettajat sisällyttävät aiheita opetukseensa yläkouluopettajia enemmän. (Nykänen, 2023)

Tutkielmassa tehtyjen johtopäätösten perusteella kyberturvallisuus tulisi sisällyttää aikaisempaa tehokkaammin osaksi perusopetusta. Tutkielma ehdottaakin kahta kehityssuuntaa, joilla opetusta voitaisiin lisätä ja kehittää. Ensimmäinen kehityssuunnitelma ehdottaa kyberturvallisuuden sisällyttämistä osaksi jo olemassa olevaa tieto- ja viestintäteknologian osa-aluetta. Toisen kehityssuunnitelman mukaan kyberturvallisuus tulisi muodostaa kokonaan omaksi laaja-alaisen oppimisen osa-alueekseen. Lisäksi tutkimus ehdottaa yleisten tietoturvaohjeiden laatimista opetushenkilöstölle, että itse opetuksesta saataisiin kyberturvallista. (Nykänen, 2023)

1.2.3 Kyberturvallisuusopetuksen tulevat sisällöt

Yksi keskeinen aihetta käsitellyt tutkimus on opetushallituksen toimeksiantona annettu, Hämeen ammattikorkeakoulussa teetetty opinnäytetyö kyberturvallisuudesta suomalaisessa peruskoulussa (Kaipainen, Pyysing, 2022). Opinnäytetyössä selvitettiin opetuksen nykytilaa ja kartoitettiin kyberturvallisuusalan asiantuntijoiden näkemyksiä siitä, millaisia asioita kyberturvallisuudesta olisi peruskoulun tasolla olennaista opettaa.

Opinnäytetyötä varten teetettiin kaksi kyselytutkimusta, joista ensimmäinen suunnattiin peruskoulun opettajille, liittyen opetuksen nykytilaan, ja toinen kyberturvallisuuden asiantuntijoille, liittyen heidän näkemyksiinsä kyberturvallisuusopetuksen tulevaisuudesta ja opetettavista aiheista. Opettajilta saamien vastausten perusteella kyberturvallisuuden opetus peruskoulussa on nykyisellään hajanaista ja järjestäytymätöntä. Lisäksi tarvetta olisi opettajien lisäkoulutukselle ja konkreettisille ohjeille, joilla voitaisiin tukea opetusta. Asiantuntijoille suunnatun kyselyn perusteella, kyberturvallisuuden opetus koetaan tärkeäksi ja yksilön osaaminen sekä toiminta kybertoimintaympäristössä nähdään vaikuttavan osaltaan myös yhteiskunnan kokonaisturvallisuuden, -luottamuksen ja -resilienssin tasoon. (Kaipainen, Pyysing, 2022)

Opinnäytetyön mukaan kyberturvallisuustaitoja voidaan pitää nykypäivän kansalaistaitona, mitä tulisi opettaa jo peruskoulutasolla. Opettajien sekä kyberturvallisuuden ammattilaisten näkemykset opetuksen nykytilasta ja tulevaisuuden näkemyksistä olivat tutkimuksen mukaan melko yhteneväiset. Jotta kyberturvallisuutta voitaisiin opettaa tarvittavalla tavalla, edellyttäisi se opettajien osaamisen ja resurssien lisäämistä, sekä opetettavien aiheiden tarkentamista peruskoulun opetussuunnitelmassa. Tutkimuksen kyselyn vastauksista käy ilmi, että vaikka lasten ja nuorten oletetaan yleisesti olevan taitavia teknologian käyttäjiä, sen käyttöön liittyviä riskejä moni ei tule kuitenkaan huomioineeksi.

Peruskoulutasolla opetuksen tulisi olla vielä varsin yleistasoista ja oppilaan ikätason huomioivaa. Kyberturvallisuudesta tulisi tutkimuksen mukaan opettaa perustaitoja, joita kyberturvallisuuden ammattilaisten mukaan ovat medialukutaito, uhkien tunnistaminen, internetin hyvät käytöstavat, laitteiden turvallinen käyttö, sekä perustason turvallisuuskäytännöt, kuten turvalliset salasanat, uhkilta suojautuminen ja ymmärrys oman toiminnan vaikutuksista kybertoimintaympäristössä. (Kaipainen, Pyysing, 2022)

Opetuksen toteutuksen osalta kyberturvallisuuden ammattilaisten mukaan opetuksen toteutuksessa voitaisiin hyödyntää esimerkiksi viranomaisia, yhdistyksiä, kolmatta sektoria ja vapaaehtoisia. Ehdotuksia tehtiin myös osaaja- ja materiaalipankeista, joita voitaisiin varsin nopeallakin aikataululla toteuttaa perusopetuksen tueksi. Koulun ja kyberturvallisuuden ammattilaisten välinen yhteistyö voisi keskittyä myös pienempiin kokonaisuuksiin, kuten esimerkiksi, yksittäisiin luentoihin, kursseihin, kampanjoihin, teemapäiviin, kilpailuihin sekä erilaisiin tapahtumiin. (Kaipainen, Pyysing, 2022)

1.3 Tutkimuksen rakenne

Tutkimuksen ensimmäisessä luvussa on käsitelty tutkimuksen tavoitteita, sekä lyhyesti esitelty aiheesta tehtyä aikaisempaa tutkimusta. Tutkimuksen toisessa luvussa käydään läpi tutkimuksen kannalta keskeisiä käsitteitä ja niiden määritelmiä. Kolmas luku keskittyy tutkimuksen toteutukseen, jossa esitellään tarkemmin käytettyjä tutkimusmenetelmiä, esitellään tutkimusta varten teetetty kyselylomake, sekä kuinka kysely on toteutettu, minkä lisäksi kappaleen lopussa käydään läpi, kuinka tutkimusta varten kerättyä aineistoa on analysoitu. Neljännessä luvussa käydään läpi aiheeseen liittyvää aikaisempaa tutkimusta, julkaisuja ja kirjallisuutta kirjallisuuskatsauksen muodossa. Viidennessä luvussa esitellään saadut tutkimustulokset. Kuudes luku koostuu tulosten yhteenvedosta sekä johtopäätöksistä. Viimeisessä luvussa käydään läpi pohdintaa itse tutkimuksesta, tutkimukseen liittyvistä mahdollisista haasteista sekä ehdotuksia mahdollisista jatkotutkimusaiheista.

2 KESKEISTEN KÄSITTEIDEN MÄÄRITELMÄT

Kyberturvallisuudesta puhuttaessa käytetään usein termejä, joilla ei ole Suomessa vielä vakiintunutta määritelmää ja erilaisissa aiheeseen liittyvissä käsitteissä on päällekkäisyyksiä. Tässä kappaleessa esitellään tutkimuksen kannalta keskeisiä käsitteitä, jotka nousevat esille itse tutkimuksessa tai kuvatessa tutkimusta pohjustavaa tausta-aineistoa, ja avataan lukijalle alan peruskäsitteistöä sekä aiheesta yhteiskunnan tasolla meneillään olevaa keskustelua. Tarkoituksena on lisäksi selventää lukijalle, mihin käytetyillä käsitteillä viitataan juuri tämän tutkimuksen viitekehyksessä.

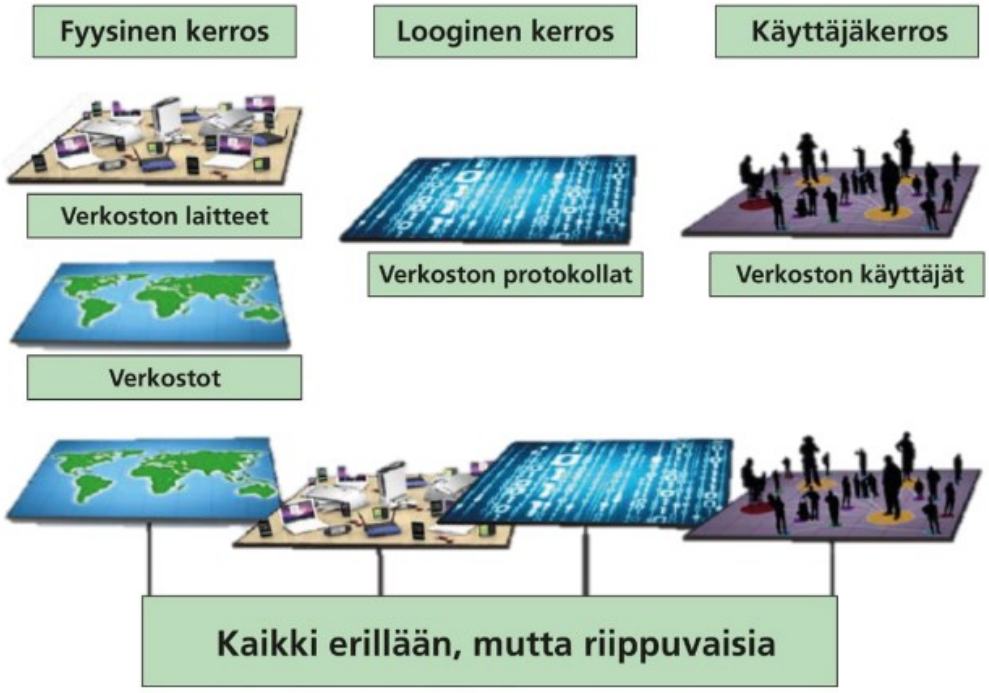
Itse kyberistä puhutaan nykyisin jokseenkin luontevasti jo iltapäivälehtienkin otsikoissa, vaikka sanan merkitys ei yleisesti ottaen välttämättä ole kaikille kovinkaan tuttu. Kyber -sanan alkuperä juontaa juurensa kreikan kielen sanasta "kybereo", joka voidaan suomen kielessä kääntää joko "ohjata", "opastaa" tai "hallita". Sanaa käytetään yleisimmin yhdyssanan etuliitteenä ja merkitykseltään viittaa yleensä digitaalisessa muodossa olevan informaation käsittelyyn. (Sanastokeskus, 2018, s. 21)

2.1 Kybertoimintaympäristö

Kybertoimintaympäristöllä, tai kyberympäristöllä, tarkoitetaan ihmisen luomaa toimintaympäristöä, joka muodostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä (Sanastokeskus, 2018, s.21), (Ulkoministeriö, ei pvm.).

Kybertoimintaympäristöä ja sen rakennetta paremmin ymmärtääkseen aihetta voidaan tarkastella jakamalla ympäristö kolmeen eri kerrokseen: fyysiseen, loogiseen ja käyttäjäkerrokseen (KUVIO 1). Fyysisellä kerroksella viitataan nimensä mukaisesti kybertoimintaympäristön olemassaolon mahdollistaviin fyysisiin laitteisiin, kuten kaapeleihin, tietokoneisiin, niistä muodostuviin verkostoihin sekä niiden fyysiseen että maantieteelliseen sijaintiin. Loogisella kerroksella viitataan taas ympäristön vähemmän näkyvään osaan, kuten ohjelmakoodiin ja

laitteiden välisiin yhteyksiin. Käyttäjäkerroksen luo taas ihmiset ja heidän toimintansa kybertoimintaympäristössä. (Laari, ym., 2019)



KUVIO 1 Kybertoimintaympäristön kerrokset (Laari, ym., 2019).

Kybertoimintaympäristön ominaisuuksia ja luonnetta voidaan kuvata sen lainalaisuuksista muodostetun ATTAT-kaavan avulla (aika, tila, tunnistamattomuus, asymmetrisyys ja tehokkuus). Toimintaympäristössä tapahtumat eivät ole ajasta riippuvaisia, sillä tapahtumat ovat usein reaaliaikaista ja hyvin valmisteltu toiminta on mahdollista toteuttaa välittömästi, vaikka toiselta puolelta maailmaa. Ajan lainalaisuuteen liittyykin läheisesti tilan merkitys. Kybermaailma ei nimittäin ole tilasta tai paikasta riippuvainen, sillä mikäli käytössä on vain tarvittavat yhteydet, voidaan kyberympäristössä toimia fyysisestä sijainnista riippumatta. Ympäristö tarjoaa myös runsaasti mahdollisuuksia toimia anonyymisti, ja kyberympäristössä toimivan tahon tunnistamattomuus onkin rikollisten näkökulmasta otollinen ominaisuus, kun taas lainvalvonnalle se on haaste. Kybertoimintaympäristö mahdollistaa myös toiminnan asymmetrisyyden, jossa toimintaan käytetyt resurssit ovat suhteessa merkittävästi siitä aiheutuvia vaikutuksia pienemmät. Vaikutuksiltaan mittava toiminta ei kybertoimintaympäristössä välttämättä vaadi suurta määrää ihmisiä ja laitteita, vaan jo pienellä määrällä asiantuntevia ja osaavia henkilöitä on mahdollista saada paljon aikaan. Tehokkuudella kybertoimintaympäristössä viitataan ympäristön mahdollistamaan tilanteeseen, jossa voidaan tehdä useita eri asioita samanaikaisesti ja nopeasti, niin hyvässä kuin pahassa. (Limnéll, ym., 2014)

Nykypäivän yhteiskunnan kannalta elintärkeät toiminnot, kuten teollisuus, vesi- ja energiahuolto-, pankkijärjestelmä-, terveydenhuolto sekä liikenne ovat

kaikki jollain tavoin riippuvaisia kyberympäristöstä. Kyberympäristö on kuitenkin haavoittuvainen, ja siihen kohdistuu kasvavissa määrin erilaisia kyberuhkia. (Ulkoministeriö, ei pvm.)

2.2 Kyberuhat

Yleisesti kyberuhka määritellään olevan "mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon" (Sanastokeskus, 2018, s.24). Kyberuhat voivat kohdistua yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin tai kansalaisiin. Kyberuhkat voivat olla peräisin maan rajojen sisä- tai ulkopuolelta ja ne voivat kohdistua kohteisiin joko suoraan tai välillisesti. (Sanastokeskus, 2018) Kyberuhkia ovat esimerkiksi erilaiset verkonvälitteisesti toteutetut huijaukset, jossa kohdetta manipuloimalla pyritään saamaan joko tietoja ja/tai rahaa, monenlaiset haittaohjelmat, verkkosivuja kaatavat palvelunestohyökkäykset sekä datan varastamiseen, vuotamiseen tai manipuloimiseen pyrkivä vihamielinen toiminta.

Kyberuhkia aiheuttavat mm. sisäpiiriläiset, kybervandaalit kuten hakkerit ja haktivistit, kybervakoilijat, kyberterroristit sekä kyberrikolliset (Lehto, Limnéll, 2017). Kyberuhkien aiheuttajat luokitellaan usein toiminnan, ja sen takana olevan motiivin perusteella. (Taulukko 1.)

TAULUKKO 1 Kyberuhkien aiheuttajat (Turvallisuuskomitea, 2019), (Laari, 2019)

Termi	**Määritelmä**
Sisäpiiriläiset	Henkilö, jolla on, tai on ollut, luvallinen pääsyoikeus organisaation järjestelmiin, ja näitä väärin käyttämällä aiheuttaa haittaa edustamalleen organisaatiolle. Toiminnan motiivina voi olla esimerkiksi kosto, ideologia tai rahallinen hyöty.
Kybervandaalit: Hakkerit ja haktivistit	*Hakkerit:* Henkilö, joka tietoisesti tunkeutuu tai vaikuttaa tietoverkkoon, tietojärjestelmiin tai näiden sisältämään tietoon, hyödyntäen ohjelmaa, palvelua tai muuta resurssia toiminnassaan. Hakkereiden toiminnan motiivina on usein huomion hakeminen ja oman osaamisen esittely. *Haktivistit*: Muodostuu sanoista hakkeri + aktivisti. Hyödyntävät kybertoimintaympäristöä oman aatteen tai tavoitteen edistämiseksi. Voivat hyödyntää toiminnan toteuttamisessa myös rikollisia keinoja.
Kybervakoilijat	Esimerkiksi valtioihin, organisaatioihin tai yrityksiin kohdistuva vakoilu, jossa tiedon saamiseksi hyödynnetään tietoverkkoja, niihin liitettyjä laitteita ja ohjelmistoja.
Kyberterroristit	Toteuttavat terroristista toimintaa, jossa kybertoimintaympäristöä hyväksi käyttäen hyökätään esimerkiksi

	kansalaisia, kriittistä infrastruktuuria tai muita yhteiskunnan kannalta elintärkeitä toimintoja vastaa. Tavoitteena voidaan katsoa perinteisen terrorismin tapaan olevan pelon ilmapiirin ja yhteiskunnallisen epävarmuuden luominen.
Kyberrikolliset	Tekevät rikoksia joko viestintäverkkoja ja tietojärjestelmiä hyödyntäen, tai niihin kohdistuen. Toiminnan motiivina usein rahallinen hyöty.

Erilaisten kyberuhkien ja -hyökkäysten torjumisesta haastavaa tekee kuitenkin teknologian nopea kehitys, joka tahattomasti luo samalla uusia tapoja hyväksikäyttää teknologiaa vihamieliseen toiminnan toteuttamiseen kybertoimintaympäristössä. Nykyisin keskusteluun onkin noussut huoli mm. tekoälyn roolista kyberhyökkäysten kehittämisessä. Tekoälyn voidaankin todeta nopeuttavan uusien kyberhyökkäysten luomista automatisoimalla aikaisemmin manuaalisesti toteutettuja työvaiheita, tehden hyökkäyksistä myös aikaisempaa tehokkaampia ja laajempia. (Aksela, ym., 2022)

Euroopan parlamentin mukaan digitalisaation ja covid-19 pandemian myötä kyberuhkien määrä on ollut kasvussa sekä uusia uhkia on syntynyt. Euroopan unionin kyberturvallisuusvirasto ENISA:n tekemän selvityksen mukaan, vuosien 2021–2022 välisenä aikana "suuri yleisö" oli kyberturvallisuusuhille alttiimpien sektorien listalla kolmantena. ENISA:n vuoden 2022 uhkaympäristöä koskevan raportin mukaan, eräinä yleisimpinä kyberturvallisuusuhkina vuonna 2022, ja sen jälkeen, voidaan pitää yksittäiseen käyttäjään kohdistuvat uhat, kuten käyttäjän manipulointi inhimillisiä virheitä hyväksikäyttämällä, sekä disinformaatio. (Euroopan parlamentti, 2022)

2.3 Kyberturvallisuus

Kyberturvallisuutta voidaan tarkastella yhtenä kansallisen turvallisuuden osa-alueena, minkä keskeisenä tavoitteena on sähköisen ja verkotetun yhteiskunnan turvallisuus (Sisäministeriö, ei pvm.). Kyberturvallisuus voidaan nähdä myös eräänlaisena tavoitetilana, missä kybertoimintaympäristön toiminta on turvattu ja siihen voidaan luottaa (Laari et. al. 2019). Kyberturvallisuus edellyttää toimenpiteitä, joilla kyetään ennakoivasti hallitsemaan, ja joissain tilanteissa jopa sietämään erilaisia kyberuhkia sekä niiden vaikutuksia. Kyberturvallisuuden toteutumisen kannalta keskeisimpiä tekijöitä on tietoturva, minkä lisäksi tulisi pyrkiä toteuttamaan erilaisia toimenpiteitä, joilla voidaan turvata kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. (Sanastokeskus, 2018, s. 22)

2.4 Tietoturvallisuus

Tietoturvallisuus, tai lyhyemmin sanottuna tietoturva, usein määritellään järjestelyinä, joilla pyritään varmistamaan tiedon saatavuus (tieto on hyödynnettävissä haluttuna aikana), eheys (tieto ei ole joko vahingossa tai tahallisen toiminnan seurauksena muuttunut) ja luottamuksellisuus (tieto ei päädy sivullisille, keille tieto ei kuulu). Esimerkkejä tietoturvan järjestelyistä ovat muun muassa kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu myös esimerkiksi tietoaineistojen, laitteistojen ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvalla, tai tietoturvallisuudella voidaankin tarkoittaa myös tilannetta, jossa tietoturvariskit ovat hallinnassa. (Sanastokeskus, 2018, s.15) Tietoturvallisuutta käytetään monesti myös kyberturvallisuuden synonyyminä. Terminä se ei kuitenkaan ole kyberturvallisuuden kanssa ristiriidassa, sillä sen voidaan katsoa olevan yksi keskeinen osa Kyberturvallisuuden kokonaisuutta. (Laari et. al. 2019).

2.5 Digiturvallisuus

Digiturvallisuus, tai lyhyemmin digiturva, voidaan nähdä ns. kattoterminä sen viidelle keskeiselle toteutusalueelle, joita ovat johtaminen ja riskienhallinta, jatkuvuudenhallinta, kyberturvallisuus, tietosuoja ja tietoturvallisuus. Digiturvalla ja toteutusalueilla pyritään varmistamaan digitaalisen toimintaympäristön luotettavuus, turvallisuus sekä saatavuus. Termin määritelmän mukaan digitaalisella toimintaympäristöllä tarkoitetaan kaikkia sellaisia tietojärjestelmiä, joissa tietoa käsitellään eri tavoin ohjelmistoilla, laitteilla tai verkossa, mutta se voidaan käsittää samana kuin kybertoimintaympäristö. Digiturvallisuuden edellytyksenä on, että osataan varautua digitaaliseen toimintaympäristöön kohdistuviin uhkiin sekä pystytään kestämään siihen kohdistuvia erilaisia häiriötilanteita ja palautumaan häiriötilanteista mahdollisimman tehokkaasti. Siinä missä teknologia on tullut osaksi meidän kaikkien jokapäiväistä arkea, on teknologian muodostaman digitaalisen toimintaympäristön turvallisuus myös yhtä laajasti jokaisen arjessa läsnä. Digiturvallisuutta ei tulekaan nähdä sijoittuvan pelkästään digitaaliseen maailmaan, sillä kuten kyberturvallisuudella on merkitys kybertoimintaympäristöstä riippuvaisiin fyysisen maailman toimintoihin, myös digiturvallisuus ulottuu digitaalisen maailman ulkopuolelle. Digiturvallisuus onkin lähes huomaamaton osa meidän arkeamme ja näkyvämpää onkin usein sen puute, jolloin viestiminen, asiointi ja muu arjen toiminta digitaalisessa maailmassa häiriintyy. (Digi- ja väestötietovirasto, ei pvm.)

2.6 Kyberturvallisuustaidot

Englannin kielessä termi ”cyber security skills” viittaa useimmiten teknisiin taitoihin, joita kyberalan ammattilaisilla tulisi olla. Suomessa kyberturvallisuustaitoja ei kuitenkaan mielletä pelkästään tietoteknisiksi taidoiksi ja kyberturvallisuustaidoista puhutaankin nykyisin jopa kansalaistaitoina, joita kaikkien tulisi osata (Kyberturvallisuuskeskus, 2021) (Rajamäki, 2021).

Kyberturvallisuustaidoille ei toistaiseksi ole kuitenkaan luotu virallista määritelmää, mutta tässä tutkimuksessa termillä viitataan niihin tietoihin ja taitoihin, joita hyödyntämällä yksilö osaa tunnistaa erilaisia internetiin liittyviä, joko yksilöön tai tietoon kohdistuvia turvallisuusriskejä, sekä suojautua erilaisista kyberuhkilta ja tietää kuinka toimia, joutuessaan kyberuhan kohteeksi. Kyberturvallisuuden takaavien perustaitojen tulisikin nykypäivän digitalisoituneessa maailmassa nähdä lukemisen, laskemisen ja kirjoittamisen kaltaisina kansalaistaitoina (Limnéll, ym., 2014). Peruskouluihin mahdollisesti tulevaisuudessa sisällytettävä kyberturvallisuuden opetus koostuisikin paljolti juuri kyberturvallisuustaitojen oppimisesta ja niiden kehittämisestä.

Oli sitten kyse alan ammattilaisten tai tavan kansalaisten osaamisesta, molemmille yhteistä on erilaisten kyberuhkien jatkuvan kehityksen takia tarve myös kyberturvallisuustaitojen kehittämiselle. Yksilön kyberturvallisuustaitoja tuleekin siis jatkuvasti ylläpitää ja päivittää, jotta kyberuhkilta kyetään suojautumaan niin nyt, kuin tulevaisuudessakin.

3 TUTKIMUKSEN TOTEUTUS

Tässä kappaleessa esitellään, kuinka tutkimus on toteutettu. Ensimmäinen alaluku esittelee yleisesti tutkimuksessa käytettyjä tutkimusmenetelmiä, ja perustelee, miksi juuri kyseiset menetelmät valittiin tämän tutkimuksen tekemiseen. Toinen alaluku kuvailee tarkemmin aineiston keruussa käytettyä materiaalia, sekä itse aineiston keruun prosessia. Kolmannessa alaluvussa kuvaillaan vielä, kuinka kerättyä aineistoa on analysoitu tutkimuksen tarpeisiin.

3.1 Tutkimusmenetelmät

Tutkielman aineisto koostuu alan kirjallisuudesta ja aiheeseen liittyvistä aikaisemmista tutkimuksista sekä tätä tutkielmaa varten teetetyn kyselytutkimuksen vastausten analysoinnista. Tutkimusmenetelminä tutkimuksessa käytetään kirjallisuuskatsausta, jonka myötä osoitetaan tutkijan oma perehtyneisyys aiheeseen. Kirjallisuuskatsauksen tavoitteena on myös valottaa lukijalle aiheen taustaa, nykytilaa ja esitellään aiheesta tehtyä muuta tutkimuksia, jotta lukijalle voisi muodostua tarvittava ymmärrys aiheesta.

Kirjallisuuskatsauksen lisäksi tutkimusmenetelmäksi valikoitui kyselytutkimus, jonka myötä pyritään keräämään kokonaan uutta tietoa tutkittavaan aiheeseen liittyen. Aineistonkeruumenetelmäksi valittiin netissä tehtävä kyselytutkimus, sillä se on nopea ja helppo toteuttaa, eikä vastausten saaminen ole ajasta tai paikasta riippuvainen. Verkonvälitteisesti kerätyt vastaukset on myös helppo analysoida sähköisesti. Tässä tutkimuksessa käytetyllä kyselytutkimuksella pyritään kartoittamaan peruskoulussa työskentelevien tietotekniikan opettajien käsityksiä peruskoulutasoisen kyberturvallisuusopetuksen sisällöistä, mahdollisista osaamisen tarpeista peruskouluikäisillä, ja opettajien oman osaamisen tasosta sekä mahdollisesta lisäkoulutuksen tarpeesta. Kyselyn kohderyhmän rajaus perustuu ajatukseen, että mikäli kyberturvallisuudesta tulisi tulevaisuudessa oma oppiaineensa, lankeaisi opetuksen vastuu mitä todennäköisimmin kyseiselle ryhmälle. Vastaajien valinnassa hyödynnettiin niin sanottua eliittiotantaa,

missä informanteiksi valitaan sellaisia henkilöitä, keiltä uskotaan saatavan parhaiten tietoa tutkimuksen kohteena olevasta ilmiöstä (Tuomi ja Sarajärvi, 2018). Kyselyn vastaajien rajaamista vain tietotekniikan aineenopettajiin voidaankin perustella juuri kohderyhmän riittävällä pohjatiedolla aiheesta, mikä itsessään mahdollistaa tutkimuksen näkökulmasta mielekkäiden kysymysten esittämisen.

3.2 Kyselylomake ja kyselyn toteutus

Tutkimusta varten teetettiin sähköinen Webropol -kyselylomake (kts. liite 1), jonka avulla pyrittiin kartoittamaan tietotekniikan opettajien näkemyksiä kyberturvallisuuden opettamisen tarpeista peruskoulutasolla. Lomaketta edelsi saateviesti, jossa kuvattiin tutkimuksen agenda, sekä pyydettiin vastaamaan lomakkeeseen, mikäli kuului kyselyn kohderyhmään. Itse lomakkeen alussa on teksti, jolla pyritään selventämään vastaajalle, mitä kyselyssä käytetyillä termeillä "tietosuoja" ja "tietoturva" tarkoitetaan. Tällä pyrittiin heti kyselyn alussa minimoimaan vastaajien mahdollisesti erilaiset käsitykset kyseisistä termeistä, mikä olisi osaltaan voinut vääristää annettuja vastauksia ja niiden vertailtavuutta.

Lomake koostuu yhteensä seitsemästä kysymyksestä, ja vastaajan vastauksen mukaan, yhdestä jatkokysymyksestä. Lomakkeessa hyödynnettiin useita eri kysymystyyppejä, joita yhdistelemällä pyrittiin saamaan monimuotoista dataa analysoitavaksi. Kysymyksiin vastattiin anonyymisti ja kysymykset oli valittu niin, ettei vastauksista voitu päätellä vastaajaa yksilöiviä tietoja, kuten ikää, sukupuolta, kotipaikkakuntaa tai työpaikkaa. Tämä oli kyselylomaketta muodostettaessa tehty tietoinen valinta, jolla haluttiin madaltaa kyselyyn vastaamisen kynnystä.

Ensimmäisessä kysymyksessä "Missä tärkeysjärjestyksessä seuraavia kyberturvallisuuteen liittyviä tietoja/taitoja tulisi mielestäsi peruskoulussa opettaa?", vastaajia pyydettiin laittamaan lomakkeella valmiiksi annetut aiheet mieleiseensä järjestykseen välillä 1 (tärkeä) – 9 (vähiten tärkeä). Kyselyyn valitut aiheet valikoituivat alustavan kirjallisuuskatsauksen pohjalta tunnistetuista kyberturvallisuusosaamisen tiedoista/taidoista. Toinen kysymys "Tuleeko mieleesi jotain muita aiheita, jota kyberturvallisuudesta tulisi opettaa?" oli avoin tekstilaatikko, johon pystyi halutessaan kirjoittamaan aihe-ehdotuksia. Lomakkeen kolmas kysymys "Millä vuosiluokilla kyberturvallisuuden aiheita tulisi mielestäsi opettaa?" vastaaja pystyi esitetyssä matriisikuviossa valitsemaan millä vuosiluokilla (1–9) kyselyssä valmiiksi annettuja aiheita tulisi opettaa. Saman aiheen pystyi halutessaan valitsemaan opetettavaksi useammalla vuosiluokalla. Neljännessä kysymyksessä "Millaiseksi arvioit peruskoulun päättävien osaamisen seuraavissa tiedoissa/taidoissa?" vastaaja pystyi antamaan listattujen aiheiden osalta arvosanan 1 (välttävä) – 6 (erinomainen) tai tarvittaessa 0 (ei osaamista). Viidennessä kysymyksessä "Millaiseksi koet omat kyberturvallisuuden opettamisen taidot?" vastaaja pystyi antamaan itselleen sanallisen arvosanan kuusiportaisella asteikolla välillä välttävä – erinomainen. Kuudenteen kysymykseen "Koetko tarvitsevasi lisäkoulutusta kyberturvallisuuden opetukseen liittyen?"

vastausvaihtoehto oli yksiselitteinen kyllä tai ei. Mikäli vastaaja valitsi vaihtoehdon ”kyllä”, aukesi hänelle alakysymys ”Millaista koulutusta koet tarvitsevasi?” jossa oli mahdollista kuvata tarvitsemaansa koulutusta avoimessa tekstilaatikossa. Lomakkeen seitsemäs ja viimeinen kysymys oli vapaaehtoinen avoin kysymys ”Heräsikö sinulla ajatuksia/ideoita kyberturvallisuuden opetukseen liittyen? Sana on vapaa!”, jossa kysymyksen muotoilulla pyrittiin rohkaisemaan vastaajia jakamaan ajatuksiaan aiheeseen liittyen.

Linkki kyselylomakkeeseen jaettiin ensimmäisen kerran “Tietotekniikka ja teknologia opetuksessa” -Facebook ryhmään loppukeväästä 2023. Keväällä lomakkeeseen ei tullut vastauksia, minkä vuoksi lomake lähetettiin samaiseen Facebook -ryhmään uudelleen syksyllä 2023. Tällöin saatiin yhteensä 7 vastausta. Lomakkeen kysymysten kvantitatiivisen luonteen takia lomakkeeseen haluttiin vielä lisää vastauksia, mitä varten päätettiin lähestyä suoraan kouluja kyselylomakkeella. Tätä edelsi lyhytmuotoinen selvitys eri kaupunkien vaihtelevista tutkimuslupamenettelyistä. Kuopion kaupungilta reagoitiin nopeasti tutkimusluvan hakemiseen liittyvissä kysymyksissä, jolloin ensimmäinen koko kaupungin kouluille lähetettävä kutsu kyselylomakkeeseen vastaamiseen voitiin lähettää. Lomake lähetettiin sähköpostitse 34 kuopiolaiselle peruskoululle tammikuussa 2024. Kuun loppupuolella kouluille lähetettiin vielä muistutusviesti.

Koska kouluille lähetetyt viestit eivät juurikaan tuoneet lisävastauksia, ja tutkimuslupien kaupunkikohtaisesti vaihteleva hakuprosessi sekä yhteydenottaminen kaikkiin alueen kouluihin osoittautui saatuihin vastausmääriin nähden varsin työlääksi, ei kaupunkikohtaisia kutsuja enää lähetetty. Mutta koska vastausmäärää haluttiin kasvattaa, lähetettiin kyselylomake vielä suoraan muutamalle jyväskyläläiselle tieto- ja viestintäteknologian opettajalle, joiden yhteystiedot löytyivät julkisista lähteistä. Gradun valmistumisen aikataulun takia vastausten keruu päätettiin maaliskuun alussa ja kerätty aineisto tallennettiin Jyväskylän yliopiston MS O365 OneDrive pilvipalveluun.

3.3 Aineiston analysointi

Kyselylomakkeeseen vastasi loppujen lopuksi 10 vastaajaa. Saatujen vastausten vähäisen määrän takia vastausten analysoinnissa pyritään tilastollisen kuvailun kautta parhaan mukaan esittämään lukijalle kyselyn kautta saatuja vastauksia, niiden merkityksiä ja peilaamaan niitä kirjallisuuskatsauksessa esille nousseihin havaintoihin aiheesta. Vastausten esittämisen tueksi työssä esitetyt kuviot on toteutettu vastauksista koostetuista Excel-taulukoista muodostettujen kaavioiden avulla.

4 KIRJALLISUUSKATSAUS

Kyberturvallisuuden opetuksesta peruskoulun tasolla on tehty eri näkökulmista joitakin tutkimuksia etenkin viime vuosina. Tutkimuksissa käsitellään pääsääntöisesti joko kyberturvallisuuden opetuksen tarpeen tunnistamista, opetuksen nykytilan kartoitusta ja tuoreimmissa tutkimuksissa myös opetuksen tulevaisuuden suuntaviivoja. Kirjallisuuskatsaukseen on valittu niin englanniksi, kuin suomeksi tehtyjä tutkimuksia, raportteja sekä julkaisuja, joita haettiin useampaa hakusanaa hyödyntäen, hakusanojen kehittyessä aikaisempien hakutulosten myötä. Kirjallisuuskatsauksessa tarkastellaan lisäksi yhteiskunnallista uutisointia, jotta saataisiin muodostettua mahdollisimman laajakatseinen kokonaiskuva aiheeseen liittyen.

4.1 Kyberturvallisuuden opetuksen tarve

”Kyberturvallisuuden osaaminen ei ole vain erillinen ammatillinen osaamisalue vaan se kattaa kyvykkyyksiä kansalaistaidoista aina kansainväliseen professioon saakka.” (Lehto, Kähkönen, 2015)

Vaikka esimerkiksi kybertoimintaympäristön teknisen turvallisuuden ammattiosaamisen kehittäminen onkin ympäristön turvallisuuden näkökulmasta erittäin keskeinen osa-alue, se ei kuitenkaan yksinään ole riittävä, sillä myös yksittäiset kansalaiset hyödyntävät digitaalisia palveluja päivittäin. Raportti digitaalisen turvallisuuden kasvun tiekartan valmistelutyöstä nostaakin yhtenä teemakohtaisena visiona tilan, jossa Suomi on vuoteen 2030 mennessä digitaalisen turvallisuuden koulutuksen ja oppimisen mallimaa (KUVIO 2.). Tämän toteutuminen edellyttää, että tuolloin Suomessa asuvista ihmisistä lähes kaikki osaisivat toimia turvallisesti ja vastuullisesti digitaalisessa ympäristössä. Kyberturvallisuudesta puhutaankin nykyisin juuri kansalaistaitona. Kansalaistaito ei kuitenkaan synny itsestään, vaan edellyttää kaikille kansalaisille saatavilla olevaa koulutusta ja kansalaisten sitoutumista asian oppimiseen, sekä opittujen taitojen kehittämiseen. Tätä varten onkin tehty ehdotus digitaalisen turvallisuuden kansalaisportaalista, josta kansalainen voi löytää ajantasaista materiaalia osaamisensa kehittämiseksi. Monien eri maiden kansallisissa strategioissa digiturvallisuuden koulutus onkin nähty tärkeänä, ja siihen liittyen on asetettu yksityiskohtaisia tavoitteita. Strategioissa on mainittu koulutuksen merkitys kaikilla koulutusasteilla, ja mm. Alankomaissa on tehty päätös sisällyttää kyberturvallisuuden opetus lähivuosien aikana osaksi perusopetusta. (Karjaluoto ym., 2019)

KUVIO 2 Tiekartan kokonaisvisio ja siihen liittyvät teemakohtaiset visiot. Kasvua digitaalisesta turvallisuudesta: Tiekartta 2019–2030. (Karjaluoto ym., 2019).

Opetuksen sisällyttäminen osaksi perusopetusta on osaltaan aiheellista, sillä lapset altistuvat internetille nykyisin yhä aikaisempaa enemmän sekä aikaisempaa nuorempina. Suomessa lapset saavat ensimmäisen älypuhelimensa tyypillisimmin 7-vuotiaana, mutta jo reilulla kolmasosalla 6-vuotiaista on käytössään oma älypuhelin (IRO Research, 2019). Vuonna 2003 Suomessa 37 % alle 11-vuotiaista lapsista käytti internetiä viikoittain, kun vuonna 2009 vastaava luku oli 88,9 % (Oinas-Kukkonen, Kurki, 2009). Nykyisin puhekielessä puhutaan diginatiivista sukupolvesta, mikä viittaa ajatukseen sukupolvesta, joka on jo varhaisesta iästä asti ollut tekemisissä tietotekniikan kanssa, ja joilla olisi näin ollen luonnollisesti paremmat tietojenkäsittelytaidot aikaisempiin sukupolviin verrattuna. Todellisuudessa nuorten tietotekninen tietämys, sekä -taidot ovat puutteelliset, sillä osaaminen ei synny itsestään. (Falck, 2016)

Opetuksen tarpeen perustelu ei kuitenkaan rajoitu pelkästään lasten ja nuorten tietoteknisiin taitoihin, vaan myös internettiin liittyviin riskeihin. Internettiin liittyen lapsiin kohdistuvia uhkia ovat mm. nettikiusaaminen, ikäryhmälle sopimattoman materiaalin näkeminen, seksuaalinen hyväksikäyttö, lapsen henkilökohtaisen datan väärinkäyttö, internettiin yhteydessä olevien laitteiden tietoturvariksit sekä digitaalinen addiktio. Uhkilla voi toteutuessaan olla vaikutuksia talouteen, yleiseen turvallisuuteen, mutta myös yleiseen terveyteen lapsen fyysisen ja psyykkisen hyvinvoinnin näkökulmasta. (Panhans et. al., 2022)

11-vuotiaiden internetin käyttökokemuksia kartoittavassa tutkimuksessa ilmeni, että arviolta 19,7 % - 29,9 % lapsista oli internetiä käyttäessään kohdannut pelottavaa, tai järkyttävää materiaalia (Oinas-Kukkonen, Kurki, 2009). Tuoreempana esimerkkinä tapauksesta mainitsee MTV uutisten haastattelema nuorisolääketieteen dosentti Silja Kosonen, jonka mukaan suomalaiset lapset olivat ensimmäisten joukossa näkemässä suodattamatonta materiaalia lokakuussa 2023 alkaneesta Gazan sodasta (MTV, 2024). Ikäiselleen sopimattoman materiaalin näkemisellä voi olla negatiivisia vaikutuksia mm. lapsen käyttäytymiseen ja

mielenterveyteen. Esimerkiksi sosiaalisen median, ja siellä nähdyn materiaalin on tutkittu aiheuttavan osalle käyttäjistä mm. ahdistusta, masennusta ja itsetunto-ongelmia (Palatsi, Tuononen, 2020). Väkivaltaiselle materiaalille altistumisen on taas tutkittu lisäävän lasten impulsiivista väkivaltaista käyttäytymistä ja vähentävän empatiakykyä (Toikkanen, 2009).

Netissä nähtävä materiaali ei kuitenkaan ole ainoa lasten ja nuorten terveyttä ja turvallisuutta uhkaava tekijä. Yhdysvalloissa New Yorkin poliisin tekemä selvitys paljasti, että lähes 80 % seksuaalisista hyväksikäytöistä voitiin liittää internetin välityksellä luotuihin virtuaalisiin ystävyyssuhteisiin. Selvityksessä kävi myös ilmi, että kyseisenlaisten rikosten uhrit olivat pääasiassa teini-ikäisiä, mikä osaltaan osoittaa tarvetta opettaa kyberturvallisuustaitoja lapsille jo varhaisessa vaiheessa, ennen teini-ikää. (Amankwa, 2021)

Vaikka teknologian kehitys on osaltaan lisännyt lasten riskiä joutua verkkorikoksen uhriksi, on se samanaikaisesti madaltanut kynnystä kyseisten rikosten tekemiseen. Nuorten tekemien verkkorikosten määrä korostuu tilastoissa, ja tietoverkkorikoksiin syyllistyvät ensikertalaiset ovat aikaisempaa nuorempia. Suomessa jopa 7-vuotiaita on syyllistynyt kyberrikoksiin. Vuonna
2021 Poliisin rekisteröimistä kyberrikoksista jopa 30 % oli alaikäisten tekemiä. Verkkorikosten tekemisen taustalla uskotaan olevan mm. tietämättömyys ja puutteellinen ymmärrys siitä, kuinka verkossa tulee toimia. Nuorten kyberrikoskierteen kerrotaankin usein alkavan lievistä teoista, joita nuori ei välttämättä edes itse tunnista rikoksiksi. Myös mielikuva verkossa toimimisen anonymiteetistä osaltaan madaltaa tietoisestikin tehtyjen rikosten toteuttamisen kynnystä. (Somerkallio, Latomaa, 2023) (Lehtinen, Somerkallio, 2022)

Kyberturvallisuuden opettamisella voidaan auttaa lapsia tunnistamaan ja ehkäisemään erilaisia, heihin arjessa kohdistuvia kyberuhkia. Opettamalla lapsia navigoimaan internetissä ja käyttämään nettiä turvallisesti, voidaan vähentää lasten riskiä joutua kyberrikoksen uhriksi. Tämän lisäksi itse alaikäisten tekemiä kyberrikoksia voitaisiin ehkäistä lisäämällä lasten ymmärrystä siitä, mikä on rikollista toimintaa ja millaisia rikosoikeudellisia seuraamuksia kyseisestä toiminnasta voi koitua. Euroopan unionin lainvalvontavirasto Europolin teettämässä, nuorten kyberrikollisuutta käsittelevässä tutkimuksessa, sen lisäksi että lapsia ja nuoria valistettaisiin kyberrikosten vakavuudesta ja seuraamuksista, etenkin kybertaidoiltaan lahjakkaita nuoria tulisi opettaa ja ohjata siihen, kuinka näitä taitoja voidaan käyttää positiivisessa mielessä, rikosten toteuttamisen sijaan. (Aiken et. al. 2022)

Kyberturvallisuuden osaamiseen liittyvät taidot ovatkin ns. tulevaisuuden taitoja. Nykyhetkellä tulevaisuus näyttäytyy vahvasti teknologian varaan rakentuvalta, ja sen voidaan katsoa vaativan nykyistä laajempia teknologian käytön-, luovan hyödyntämisen-, kriittisen ajattelun- ja tiedonhallinnan taitoja. (Suuronen, Eskola, 2023)

4.2 Opetuksen nykytila peruskoulussa

Nykyisessä opetussuunnitelmassa kyberturvallisuudella ei ole omaa oppiainekokonaisuutta. Opetussuunnitelmassa on kuitenkin nimetty yhtenä laaja-alaisen osaamisen osa-alueena tieto- ja viestintäteknologia, mikä tarkoittaa, että osa-alueen osaamistavoitteita on tarkoitus sisällyttää eri oppiaineissa aineen vuosiluokkakohtaisiin tavoitteisiin. Opetussuunnitelmassa tieto- ja viestintäteknologian oppiainekuvaus osana laaja-alaista osaamista nimetään neljä pääaluetta, joilla osaamista kehitetään:

1) Oppilaita ohjataan ymmärtämään tieto- ja viestintäteknologian käyttö- ja toimintaperiaatteita ja keskeisiä käsitteitä sekä kehittämään käytännön tvt-taitojaan omien tuotosten laadinnassa.
2) Oppilaita opastetaan käyttämään tieto- ja viestintäteknologiaa vastuullisesti, turvallisesti ja ergonomisesti.
3) Oppilaita opetetaan käyttämään tieto- ja viestintäteknologiaa tiedonhallinnassa sekä tutkivassa ja luovassa työskentelyssä.
4) Oppilaat saavat kokemuksia ja harjoittelevat tvt:n käyttämistä vuorovaikutuksessa ja verkostoitumisessa.

(Perusopetuksen opetussuunnitelman perusteet, 2014)

Laaja-alaisen osaamisen yleistavoitteet tieto- ja viestintäteknologian osalta on peruskoulun opetussuunnitelmassa esitelty karkeasti jaetuilla vuosiluokkakohtaisilla kuvauksilla. Vuosiluokkien 1–2 opetuksessa pyritään hyödyntämään oppilaiden esiopetuksessa sekä koulun ulkopuolella kertyneitä tietoja sekä taitoja tieto- ja viestintäteknologiasta. Ensimmäisillä vuosiluokilla leikkiin perustuva työskentely on vielä keskeisessä roolissa ja opetuksessa keskitytään paljolti perustietojen ja -taitojen opetteluun sekä mm. laitteiden käyttöön ja merkitykseen arjessa ja lähiympäristössä. Käytännön taitojen ja oman tuottamisen osalta opetellaan laitteiden sekä palveluiden käytön lisäksi niiden keskeisiä käyttö- ja toimintaperiaatteita. Pienten lasten opetuksessa pyritään hyödyntämään myös pelillistämistä, sekä oppilaiden omien tvt-kokemuksien jakamista toisilleen oppimisen välineinä. Oppilaiden omien kokemusten lisäksi heidän kanssaan pyritään keskustelemaan tvt:n turvallisista käyttötavoista ja hyvistä käytöstavoista sekä kiinnittämään huomiota mm. terveellisiin työasentoihin. Opetuksessa oppilaita opastetaan perinteisimpien hakupalveluiden käyttöön erilaisten tiedonhankintatehtävien kautta niin yhdessä kuin yksin ja hyödyntämään tieto- ja viestintäteknologiaa erilaisissa vuorovaikutustilanteissa.

Vuosiluokkien 3–6 vuosiluokkakohtaisissa tavoitteissa tieto ja viestintäteknologiaa pyritään jo monipuolisesti hyödyntämään eri oppiaineissa ja erilaisissa koulutöissä. Tarkoituksena on vahvistaa yhteisöllistä oppimista mm. kannustamalla toteuttamaan ideoitaan tvt:n avulla niin yksin kuin yhdessä muiden kanssa. Tavoitteena on myös tarjota oppilaille mahdollisuuksia etsiä, kokeilla ja käyttää erilaisia työtapoja sekä -välineitä jotta jokainen voisi löytää parhaiten

omaan oppimiseen ja työskentelyyn soveltuvia työkaluja. Vuosiluokilla tutkitaan lisäksi tieto- ja viestintäteknologian vaikutuksia arjessa ja pyritään kehittämään omia käytännön taitoja. Käytännön taidoista mainitaan laitteiden, ohjelmistojen ja palveluiden käyttö, tekstin tuottaminen, kuvan, äänen, videon ja animaation tekemistä. Lisäksi mainitaan ohjelmoinnin kokeilu, jonka avulla oppilaat luovat ymmärrystä siitä, miten teknologian toiminta on riippuvainen ihmisen tekemistä ratkaisuista. Tieto- ja viestintäteknologian vastuullisen ja turvallisen käytön osalta keskitytään vielä hyviin käytöstapoihin, ergonomiseen työskentelyyn ja tutustutaan tekijänoikeuksien perusperiaatteisiin. 3–6 luokkalaisten tavoitteissa mainitaan ensimmäisen kerran myös lähdekritiikin kehittäminen useampaa lähdettä hyödyntävän tiedonhankinnan ja itse kerätyn tiedon kriittisen arvioinnin myötä. Vuorovaikuttamisen ja verkostoitumisen osalta oppilaita ohjataan mm. ottamaan vastuuta omasta viestinnästään ja tarkastelemaan sekä arvioimaan tieto- ja viestintäteknologiaa vaikuttamisen keinona.

Peruskoulun viimeisillä vuosiluokilla 7–9 tavoitteena on, että oppilaat integroivat tieto- ja viestintäteknologian käytön luontevaksi osaksi oppimista. Aikaisemmin opittuja taitoja sekä tietoja pyritään syventämään ja hyödyntämään myös koulun ulkopuolella opittuja tvt-taitoja eri oppiaineiden opiskelussa. Tarkoituksena on muodostaa käsitys siitä, kuinka tieto- ja viestintäteknologiaa voidaan lisäksi hyödyntää myöhemmissä opinnoissa, työelämässä ja yhteiskunnallisessa toiminnassa sekä vaikuttamisessa. Ohjelmointia pyritään harjoittelemaan aikaisempaa enemmän eri oppiaineissa. Peruskoulun viimeisten vuosiluokkien tavoitteissa mainitaan myös ensimmäisen kerran kyberturvallisuuden kannalta keskeisiä aiheita, kuten kuinka suojautua tietoturvariskeiltä, kuinka välttyä tiedon häviämiseltä ja mitä tarkoitetaan tietosuojalla, sekä millaisia seurauksia lainvastaisesta toiminnasta voi olla. Lisäksi opitaan hahmottamaan tvt:n merkitystä, sen tarjoamia mahdollisuuksia ja riskejä globaalissa maailmassa. Myös aikaisempien vuosien tavoitteissa mainitut ergonomia, tiedonhankinta, lähdekriittisyys ja tieto- ja viestintäteknologian hyödyntäminen vuorovaikutustilanteissa toistuvat 7–9 luokkalaisten tavoitteissa, hieman aiempaa laajemmin ja ikäryhmän huomioiden kuvattuna.

Opetussuunnitelman voidaankin nähdä laaja-alaisen osaamisen osalta kuvaavan varsin kattavan kirjon peruskoulussa opittavia tieto- ja viestintäteknologian taitoja, joita tulisi sisällyttää osaksi eri oppiaineita. Opetussuunnitelmassa lisäksi määritellään laaja-alaisen osaamisen aiheet oppiainekohtaisesti. On kuitenkin huomioitava, että opetussuunnitelmaa noudattavan opetuksen sisällöstä ja toteutuksesta vastaa lopulta opetuksen järjestäjä, mikä mahdollistaa alueellisten erojen synnyn tieto- ja viestintäteknologian opettamisen sekä osaamisen tasossa (Lehto, 2022). Myös paikalliset opetussuunnitelmat, joilla pyritään varmistamaan alueellisen koulutuksen tasa-arvo ja laatu, huomioimalla oppilaiden tarpeet sekä paikalliset erityispiirteet, voivat osaltaan tahattomasti synnyttää alueellisia eroja opetuksen järjestämisessä. Erot oppimisen mahdollisuuksissa, koulun resursseissa, opettajien omissa digitaidoissa ja kuinka mielellään he sisällyttävät tieto- ja viestintäteknologiaa opetukseensa asettaa oppilaat epätasa-arvoiseen asemaan, jonka vaikutukset voivat yltää pitkälle tulevaisuuteen (Suuronen,

Eskola, 2023). Ala-asteella luokan opettajan on lisäksi luultavasti helpompi suunnitella tieto- ja viestintäteknologiaan liittyvien aiheiden tasaista sisällyttämistä luontevasti osaksi lukuvuoden aikana käytävää opetusta. Ala-asteellakin opetuksen yhtenäistämisen haasteena on kuitenkin se, että opettajat eivät välttämättä opeta samoja luokkaryhmiä peräkkäisinä vuosina. Opetuksen vastuunjaot voivat olla epäselviä myös ala- ja yläasteen kesken. Opettajat saattavat vain olettaa, että mitä ei ala-asteella ole ehditty käydä läpi, niin kyllä joku sen yläasteella opettaa. Viimeistään yläasteella eri oppiaineille on usein omat aineenopettajansa, mikä voi entisestään lisätä opetuksen vastuunjaon haasteita. (Tuovinen, 2022)

Suomessa opettajille teetetyn, kyberturvallisuuden opetusta käsittelevän kyselyn mukaan valtaosa opettajista ei kuitenkaan näe tarpeelliseksi eriyttää kyberturvallisuutta omaksi oppiaineekseen ja kokevat että tieto- ja viestintäteknologian tavoitteen toteutuvat opetuksessa. Kyselyyn vastanneet opettajat suhtautuivat melko positiivisesti omiin kykyihinsä sisällyttää kyberturvallisuutta osaksi opetustaan. Kyselyn vastausten perusteella voidaan kuitenkin todeta, että yläkoulun opettajat kokevat muita vähemmän vuosiluokkakohtaisten tavoitteiden toteutuvat opetuksessa ja ovat myös enemmän sitä mieltä, että kyberturvallisuuden opetus olisi järkevämpää eriyttää omaksi oppiaineekseen. (Lehto, 2022) Vaikka valtaosa opettajista kokee tieto- ja viestintäteknologian tavoitteiden toteutuvan opetuksessaan, oppilaiden osaamista käsittelevät tutkimukset osoittavat mm. opettajien tietoteknisten laitteiden käytön olevan lapsiin verrattuna heikompaa, mutta lasten ja nuorten tietoteknisten taitojen ja tietoturvan hallinnan kuitenkin olevan puutteellisia (Falck, 2016) (Kosonen, 2019).

Kyberturvallisuus on aiheena laaja kokonaisuus, johon opetussuunnitelma ei tarjoa yksityiskohtaisempaa ohjeistusta (Kaipainen, Pyysing, 2022). Tarvetta olisi saada konkreettisia esimerkkejä tieto- ja viestintäteknologian hyödyntämisestä opetuksessa niin, että opetussuunnitelmassa asetetut tavoitteet toteutuisivat (Luukka, 2018). Opetussuunnitelmassa ei mm. kuvata, kuinka tieto- ja viestintäteknologian eri osa-alueita tulisi eri oppiaineissa käsitellä. Tämänhetkiset opetuksen materiaalit ja työkalut ovat enemmänkin tukea tarjoavia ohjenuoria kuin velvoitteita, mikä jättää opetuksen järjestäjälle vastuun valita käyttääkö materiaaleja, vai ei (Lehto, 2022).

Tietoturvataitojen opettamista peruskoulussa käsittelevä opinnäytetyössä selvitettiin myös opettajien tietoturvataitojen oppimista ja aiheesta saamaansa koulutusta. Tutkimuksessa Kymenlaakson peruskoulujen opettajat vastasivat kyselylomakkeeseen, jossa kysyttiin tietoteknisen- ja tietoturvaosaamisen tasoa, kuinka opettajat ovat oppineet eri tietoturvataitoja, kuinka näitä taitoja on koulutettu, millä tasolla he kokevat eri tietoturvataitojen osaamisensa olevan ja kuinka hyvin he kokevat pystyvänsä käsittelemään eri teemoja oppilaiden kanssa. Tutkimuksessa käy ilmi, että suurin osa kyselyyn vastanneista opettajista on opiskellut tietoturvataitoja itsenäisesti. Koulutusta koskevien vastausten laajan hajonnan perusteella voitiin tietoturvataitojen koulutuksessa ja koulutuksen tarjonnassa olevan eroja. Opetuksen taso arvioitiin tyydyttävälle, tai melko hyvälle tasolle. Opetuksen tasosta ei kuitenkaan voida tehdä luotettavia havaintoja, ennen kuin päästään todentamaan oppimisen tasoa. (Tuovinen, 2022).

Tieto- ja kyberturvallisuuden opetukseen voidaan katsoa liittyvän monia haasteita, jotka tulisi ottaa huomioon tulevaisuuden opetusta suunnitellessa. Nykyisen muotoisen opetuksen vastuunjaon, opetussuunnitelman suurpiirteisten ohjeiden ja yhtenäisen opetusmateriaalin puuttumisen lisäksi opetukseen liittyvinä haasteina voidaan tunnistaa mm. kyberuhkien kasvava määrä sekä niiden laajeneva kirjo, mikä edellyttää opettajilta ajantasaista tietoa ja osaamista senhetkisistä kyberuhkista (Amankwa, 2021).

4.3 Opetuksen tulevia suuntaviivoja

Kyberalan ammattilaisten mukaan, peruskouluissa tulisi opettaa kyberturvallisuuden perustaitoja, joita voidaan katsoa olevan medialukutaito, uhkien tunnistaminen, internetissä toimimisen hyvät käytöstavat, laitteiden sekä salasanojen turvallinen käyttö, kyky suojautua yleisimmiltä uhkilta ja oman toiminnan vaikutuksen tunteminen. Opetuksen tulisi kuitenkin olla yleistasoista, helposti ymmärrettävää ja oppilaan ikätasoon suhteutettua. (Kaipainen, Pyysing, 2022)

Kyberturvallisuuden opetuksen kehittämistä varten on myös esitetty kolme eri toimintamallia. Ensimmäinen toimintamalli voitaisiin toteuttaa nykyisen opetussuunnitelman perusteella lisäämällä digitaalinen turvallisuus kokonaan omaksi laaja-alaisen osaamisen osa-alueekseen. Tätä perustellaan mm. digitaalisen turvallisuuden merkityksen kasvulla yhteiskunnan kaikilla sektoreilla, myös koulumaailmassa. Opetuksen sisällyttäminen muiden laaja-alaisen osaamisen osa-alueiden tavoin jokaiseen oppiaineeseen vaatisi osaltaan lisäresursseja peruskouluihin ja koko opettajiston lisäkoulutusta. Toinen toimintamalli esittää digitaalisen turvallisuuden sisällyttämistä osaksi nykyistä tieto- ja viestintäteknologian osa-aluetta. Tämä toimintamallin edellyttäisi kaikista vähiten muutoksia nykyisen muotoiseen opetukseen ja olisi näin ollen helpoiten toteutettavissa. Kolmannen toimintamallin tavoitteena olisi sisällyttää digitaalinen turvallisuus osaksi laajennettua tieto- ja viestintäteknologian opetusta ja sitä voitaisiin toteuttaa vahvistamalla oppiaineen pakollisuutta peruskoulussa. Nykyisellään valinnaisten TVT-opintojen tarjonta on paljolti riippuvainen koulukohtaisista painotuksista ja halusta tarjota kyseisiä opintoja valinnaisaine -tarjonnassaan. (Lehto, 2022)

Kyberturvallisuuden opetussisältöjä suunnitellessa haasteeksi kuitenkin muodostuu mm. aiheen monimutkaisuus, teknisyys, suomenkielisten termien puute, sekä alan nopeat muutokset. Opetusta suunnitellessa tulisikin ottaa huomioon, että opetuksen sisältö ja opetuksessa käytettävä kieli on opetettavan ikäryhmän ymmärryksen ja osaamisen tason mukaista. Myös opetusmateriaalin ja -menetelmien tulisi kehittyä samaa tahtia alan muutosten kanssa, jotta oppiminen olisi mielekästä ja saatu osaaminen olisi ajantasaista ja siitä olisi aidosti hyötyä oppilaan arjessa. (Karjaluoto, ym., 2019)

Opetus- ja kulttuuriministeriö käynnisti syksyllä 2020 Uudet lukutaidot -kehittämisohjelman, jonka tavoitteena on ”vahvistaa lasten ja nuorten medialukutaitoa, tieto- ja viestintäteknologista (tvt) osaamista sekä ohjelmointiosaamista

varhaiskasvatuksessa sekä esi- ja perusopetuksessa.” (Opetus- ja kulttuuriministeriö, ei pvm.). Kehittämisohjelman tarkoituksena on, että ”opetuksen ja varhaiskasvatuksen järjestäjät päivittävät digistrategioitaan ja -suunnitelmiaan sekä opetussuunnitelmiaan vastaamaan kansallista digitaalisen osaamisen viitekehystä. Osaamisen yksityiskohtaisella määrittelyllä edistetään lasten ja nuorten yhdenvertaisia mahdollisuuksia saavuttaa opiskelussa, työelämässä ja yhteiskunnallisessa osallistumisessa tarvittava digitaalinen osaaminen. Oppijalla on oikeus digitaalisen osaamiseen.” (Opetushallitus, ei pvm.).

Marraskuussa 2022, Opetushallitus julkaisi kasvatuksen ja koulutuksen turvallisuussivustolleen, kyberturvallisuuden osion, jossa esitetään kyberturvallisuusosaamisen edistämistä varhaiskasvatuksesta toiselle asteelle (Opetushallitus, 2022). Turvallisuussivuston tavoitteena on ”antaa käytännön ohjeita turvallisuussuunnitteluun ja -johtamiseen varhaiskasvatuksen, opetuksen ja koulutuksen järjestäjille ja tuottajille, päiväkodin johtajille ja rehtoreille sekä päiväkotirakennusten ja koulujen omistajille ja ylläpitäjille.”. Kyberturvallisuuden opetukseen peruskoulussa sivusto esittelee laaja-alaisen oppimisen tavoin kyberturvallisuuden osaamisen tavoitteet vuosiluokille 1–2, 3–6, ja 7–9.

Kyberturvallisuuden tulevan opetuksen tavoista, työkaluista tai oppimismateriaaleista ei kuitenkaan ole peruskoulun osalta esitetty tarkempia kuvauksia. Kansalaisten osaamisen kehittämiseksi on esitetty netissä avoimesti saatavilla olevaa kansalaisportaalia, joka toimisi kansalaisille suunnattuna digitaalisen osaamisen tietopankkina, sisältäen tietoa digitaalisesta turvallisuudesta, ajankohtaisista tutkimuksista sekä opetuspaketteja (Karjaluoto, ym., 2019). Opetuksen toteutukseen liittyen on tehty ehdotuksia yhteistyöstä esimerkiksi koulujen ja viranomaisten välillä (Kaipainen, Pyysing, 2022). Yritysten ja organisaatioiden kyberturvallisuusosaamisen parantamisessa hyödynnetäänkin esimerkiksi viranomaispalveluna tuotettuja kyberharjoituksia. Kyberharjoituksessa simuloidaan kyberuhkia tai -häiriöitä luomalla kuvitteellinen tilanne, jossa voidaan testata uhkien sekä häiriöiden vaikutuksia organisaation toimintaan. Harjoitusten tavoitteena on parantaa organisaation valmiuksia toimia ja reagoida vakaviin kybertapahtumiin, sekä pienentää kyberhyökkäysten vaikutuksia ja nopeuttaa niistä toipumista. Kyberharjoituksen etuina ovat mm. parantunut kyky havainnoida organisaatiota uhkaavia vakavia tietoturvaloukkauksia, sekä parantuneet valmiudet reagoida kyberuhkiin ja niistä nopeasti toipumiseen. Kyberharjoitus voi auttaa myös tunnistamaan mahdolliset puutteet ja heikkouden osaamisessa, toimintamalleissa ja resursseissa. (Kyberturvallisuuskeskus, 2023) (Uusikartano, 2023). Selvityksiä kyberharjoitusten soveltamisesta kouluihin lasten ja nuorten kyberturvallisuustaitojen kehittämiseksi, ei kuitenkaan toistaiseksi ole tehty.

4.4 Yhteenveto

Kyberturvallisuuden opetuksen tarve voidaan nähdä olevan hyvin perusteltavissa jo yhteiskunnan digitalisoitumisella, mutta virallisemmin myös kansainvälisesti eri valtioiden strategioissa sekä tiekartoissa tunnistetulla osaamisen

tarpeella. Opetuksen tarvetta juuri peruskoulussa voidaan taas perustella lasten ja nuorten aikaisempaa varhaisemmassa iässä alkaneella ja lisääntyneellä teknologian käytöllä, tietoteknisten taitojen vajaavaisuudella, erilaisten kyberuhkien lisääntyvällä määrällä, sekä nuorten osalta lisääntyneellä kyberrikollisuudella niin uhrin kuin tekijän näkökulmasta.

Opetuksen nykytilaa selvitellessä havaitaan joitakin itse opetukseen, opetuksen sisältöön ja opetussuunnitelmaan liittyviä haasteita, jotka osaltaan voivat selittää lasten ja nuorten taitojen puutteellisuutta. Vaikka opetussuunnitelma mainitseekin mm. laitteiden turvallisen käytön osana 1–2 luokkalaisten tieto- ja viestintäteknologian laaja-alaisen osaamisen tavoitteita, vasta yläasteikäisten vuosiluokkakohtaisissa tavoitteissa puhutaan konkreettisemmista kyberturvallisuuteen liittyvistä aiheista, kuten tietoturvariskeistä ja tiedon suojaamisesta. Tiedon tuottamista ja jakamista opetellaan kuitenkin jo peruskoulun varhaisemmassa vaiheessa. Lisäksi tarjolla oleva opetuksen määrä ja taso vaihtelee alueittain, eikä käytössä ole käytännössä lainkaan, saati yhtenäistä, opetusmateriaalia. Myös nykyisin opetuksesta vastaavien opettajien oma osaaminen ja saama koulutus aiheeseen liittyen on vaihtelevaa.

Itse kyberturvallisuuden opetuksesta, tai opetuksen sisällöistä on toistaiseksi vielä vähän tehty selvitystä, mutta aihetta käsittelevät tutkimukset tukevat osaltaan ajatusta kyberturvallisuuden opetuksen aloittamisesta jo peruskoulutasolla ainakin jossain muodossa, olkoon se sitten omana oppiaineenaan, tai erilaisin toteutusvaihtoehdoin osana muuta opetusta. Kyberturvallisuudesta nähdään olennaisena opettaa ainakin medialukutaitoa, kyberuhkien tunnistamista, internetissä toimimisen hyviä käytöstapoja, laitteiden sekä salasanojen turvallista käyttöä, kykyä suojautua yleisimmiltä uhilta, sekä omasta toiminnasta aiheutuvien vaikutusten tunnistamista.

Myös joitakin alustavia ehdotuksia opetuksen suhteen on tehty. Kyberopetuksen toteuttamiseksi peruskoulussa on esitetty vaihtoehtoja, jotka vaihtelevat yksinkertaisesta aiheen lisäämisestä osaksi nykymuotoista opetusta, aiheen omaksi oppiaineekseen eriyttävästä suunnitelmasta, mikä luultavasti edellyttäisi jo suurempia muutoksia peruskouluopetuksen toteuttamiseen.

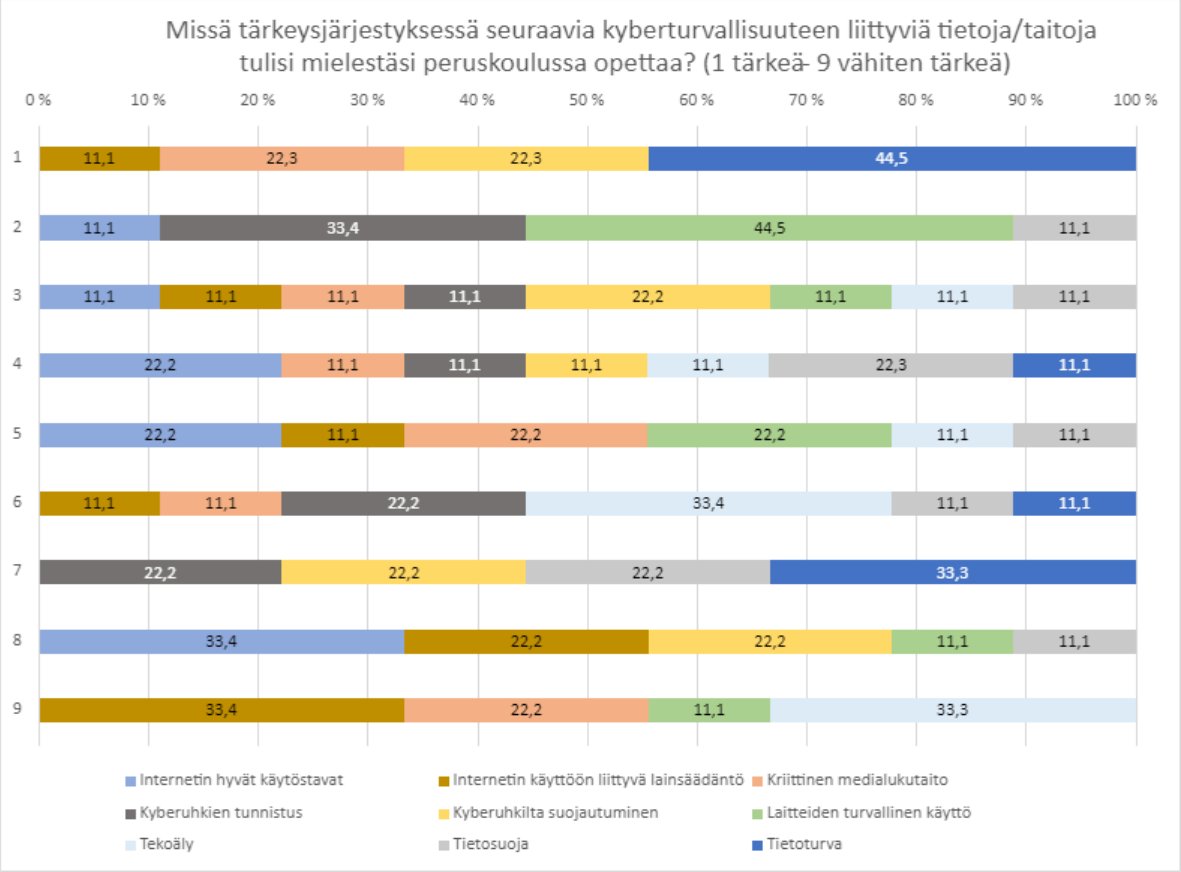
5 TUTKIMUSTULOKSET

Tämän kappaleen alaluvuissa 5.1–5.7 käsitellään tutkimuksen kyselylomakkeella kerättyjä vastauksia kysymyskohtaisesti osin kuvaamalla yksittäisten vastausten sisältöä, mutta myös vastauksista saatavaa kokonaiskuvaa. Viimeisessä alaluvussa 5.8 arvioidaan tutkimuksen, aineiston keräämiseen käytetyn kyselyn ja siitä saatujen vastausten luotettavuutta.

5.1 Opetettavien aiheiden tärkeysjärjestys kyberopetuksessa

Kysymys: Missä tärkeysjärjestyksessä seuraavia kyberturvallisuuteen liittyviä tietoja/taitoja tulisi mielestäsi peruskoulussa opettaa?

Vastaajien tuli kysymyksessä asettaa valmiiksi annetut vaihtoehdot mieleiseensä järjestykseen 1 tärkeä – 9 vähiten tärkeä. Annetusta vaihtoehdoista tärkeimmäksi opetettavaksi aiheeksi kyberturvallisuuteen liittyen nousi tietoturva (44,5 %) (KUVIO 3). Toiseksi tärkeimpänä aiheena koettiin laitteiden turvallinen käyttö (44,5 %). Tärkeydessään asteikon keskivaiheilla vastaukset jakautuivat jo aikaisempaa tasaisemmin. Tietoturva, joka nousi osalle vastaajista tärkeimpänä opetettavana aiheena, oli 33,3 % vastaajista vähemmän tärkeä aihe, sijoittuen kolmanneksi viimeiseksi tärkeysjärjestyksessä. Myös internetin hyvät käytöstavat, jonka yli puolet vastaajista oli asettanut tärkeysjärjestyksessä asteikon tärkeämmälle puolelle, oli 33,4 % mielestä toisiksi vähiten tärkeä aihe opetettavaksi peruskoulussa. Vähiten tärkeäksi mielletyt aiheet olivat internetin käyttöön liittyvä lainsäädäntö (33,4 %), sekä tekoäly (33,3 %). Osa vastaajista asetti myös kriittisen medialukutaidon (22,2 %), sekä laitteiden turvallisen käytön (11,1 %) vähiten tärkeiden aiheiden joukkoon.



KUVIO 3 Opettajien näkemys kyberturvallisuuteen liittyvien tietojen/taitojen opetuksen tärkeydestä.

5.2 Muita kyberturvallisuudesta opetettavia aiheita

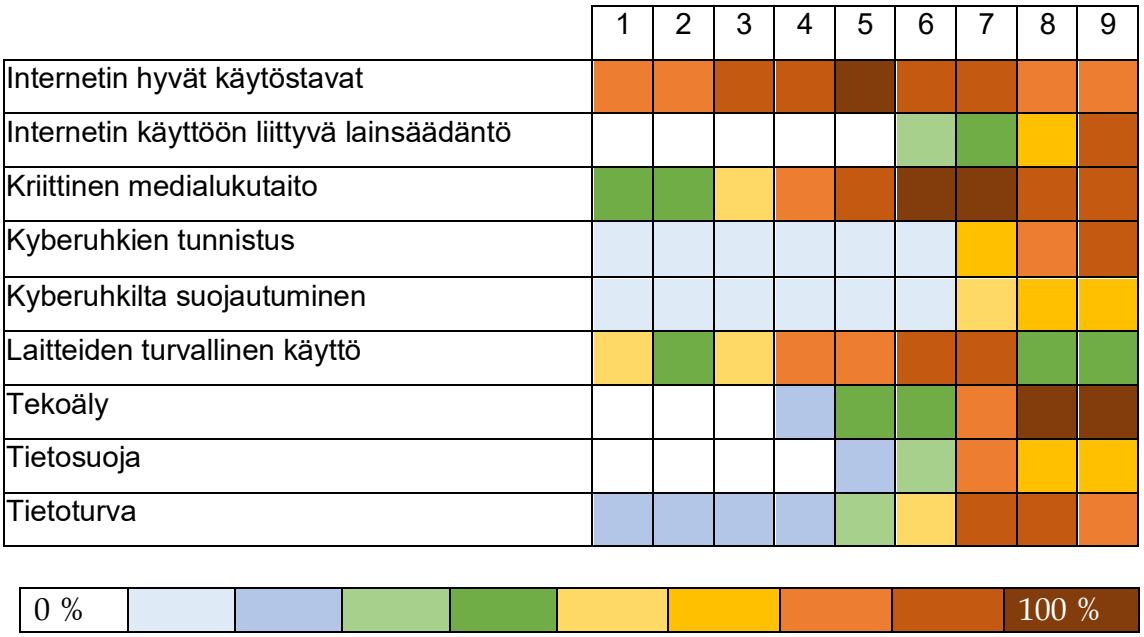
Kysymys: Tuleeko mieleesi jotain muita aiheita, joita mielestäsi peruskoulussa tulisi opettaa kyberturvallisuuteen liittyen?

Vapaaehtoiseen avoimeen kysymykseen tulleissa vastauksissa nostettiin kyberturvallisuuden osalta ilmiön nopeat muutokset ja sen vuoksi jatkuvan oppimisen tarve. Vastausten perusteella olisi tärkeää saada oppilaat myös itse ymmärtämään jatkuvan oppimisen tärkeys niin teknologian käytön, kuin turvallisuudenkin kannalta. Lisäksi arjen tietoturvariskit, kuten kodin lähiverkko ja älylaitteiden aliverkot sekä digitaalinen jalanjälki nostettiin yhtenä tarpeellisena opetuksen aiheena. Hieman kyberturvallisuuden ulkopuolelta esille tulleita aiheita olivat mm. Linux -käyttöjärjestelmän käyttö: ”Häpeällistä, että ollaan Suomessa ja esim Linux ei juuri millään tavalla näy.”, sekä huoli Googlen ”ylivallasta” koulumaailmassa, viitaten mitä ilmeisimmin tiedonhaussa käytettäviin hakukoneisiin.

5.3 Aiheiden opetus vuosiluokkakohtaisesti

Kysymys: Millä vuosiluokilla kyberturvallisuuden aiheita tulisi mielestäsi opettaa?

Internetin hyvät käytöstavat koettiin aiheeksi, jota suurin osa vastaajista opettaisi kaikilla peruskoulun luokilla (KUVIO 4). Internetin käyttöön liittyvä lainsäädäntöä ei vastausten perusteella tulisi opettaa kuin aikaisintaan kuudennella luokalla, painottuen peruskoulun viimeisille luokille. Kriittistä medialukutaitoa ehdotettiin opetettavaksi kaikilla vuosiluokilla, vastausten kuitenkin painottuessa ylemmille vuosiluokille. Kyberuhkien tunnistusta ei juurikaan ehdotettu käsiteltäväksi ala-asteella, mutta moni vastaajista koki, että aihetta tulisi opettaa yläasteella. Kyberuhkilta suojautuminen mukaili kyberuhkien tunnistuksen vastauksia. Aihe nähdään oleellisemmaksi opettaa mieluummin ylä- kuin ala-asteella. Laitteiden turvallista käyttöä taas suosittiin opetettavaksi kaikilla vuosiluokilla, kuitenkin painottuen 4–7 luokkiin. Tekoäly ja tietosuoja oli lainsäädännön lailla aiheita, joita ei ehdoteta opetettavaksi ala-asteella, varsinkaan ensimmäisillä vuosiluokilla. Tekoälyä ehdotetaan opetettavaksi aikaisintaan neljänneltä luokalta lähtien. Lähes kaikki vastaajista olivat kuitenkin sitä mieltä, että aihetta tulisi opettaa yläasteella. Tietosuojaa ehdotettiin opetettavaksi aikaisintaan viidennellä vuosiluokalla ja sitä ei aiheena koettu aivan yhtä tärkeäksi, kuin tekoälyä. Tietoturvaa ehdotettiin taas opetettavaksi jokaisella vuosiluokalla, vastausten opetuksen painottuen kuitenkin jälleen yläasteen puolelle.



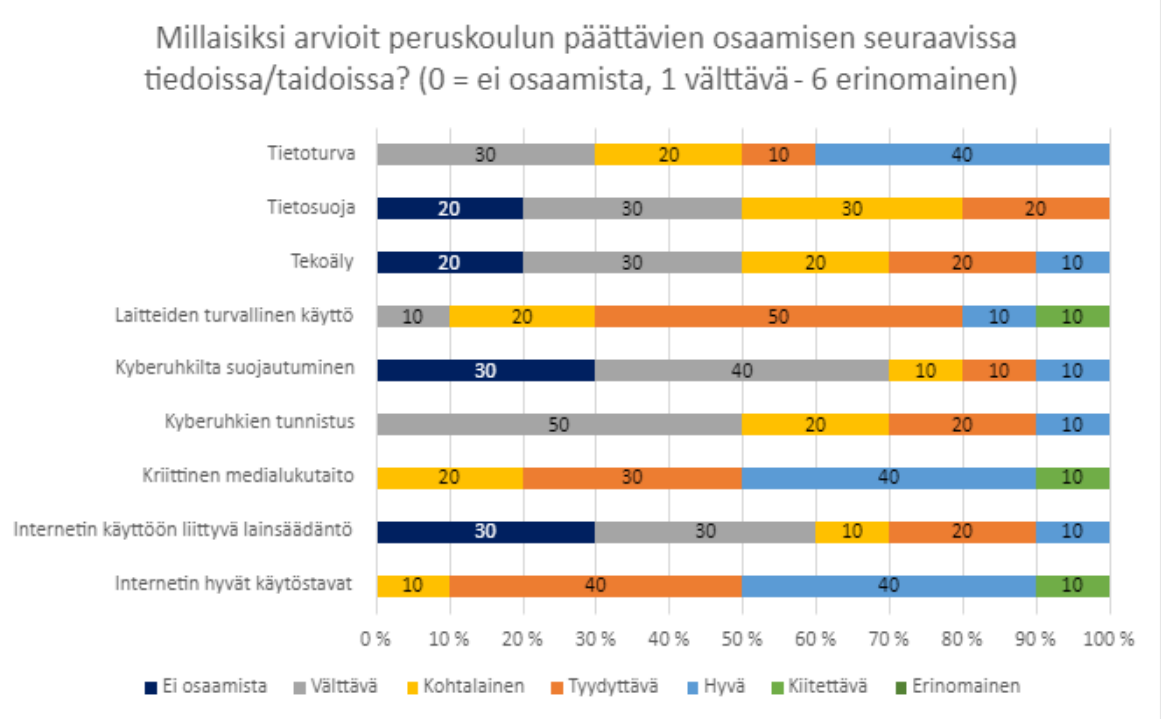
KUVIO 4 Opettajien näkemys siitä, millä vuosiluokilla eri kyberturvallisuuteen liittyviä aiheita tulisi opettaa.

5.4 Nykyisin peruskoulunsa päättävien osaaminen kyberturvallisuuteen liittyvissä tiedoissa/taidoissa

Kysymys: Millaisiksi arvioit peruskoulunsa päättävien osaamisen seuraavissa tiedoissa/taidoissa?

Vaikka osa kyselyssä listatuista kyberturvallisuuteen liittyvistä tiedoista ja taidoista mainitaankin jo nykyisessä opetussuunnitelmassa osana laaja-alaista oppimista, arvioivat opettajat peruskoulunsa päättävien taidot olevan suurimmalta osin osaamisen asteikon huonommassa päässä (ei osaamista, tai välttävä – tyydyttävä osaaminen) (KUVIO 5).

Aiheet, joista peruskoulunsa päättävillä ei osan vastaajien mielestä ollut lainkaan osaamista, olivat tietosuoja, tekoäly, kyberuhkilta suojautuminen ja internetin käyttöön liittyvä lainsäädäntö. Kuitenkin opetussuunnitelmassa 7.–9. luokkalaisten laaja-alaisen osaamisen kuvauksessa ”*Vastuulliseen toimintaan ohjataan pohtimalla, mitä esimerkiksi käsitteet tietosuoja ja tekijänoikeus tarkoittavat, ja mitä seurauksia vastuuttomasta ja lainvastaisesta toiminnasta voi olla.*” (Opetushallitus, 2014). Osaamisen puute esimerkiksi tekoälyyn liittyen on osaltaan ymmärrettävää, sillä tekoäly on tullut nykyisessä muodossaan vasta varsin hiljattain osaksi kansalaisen arjessa käytettäviä työkaluja, eikä vielä ole selkeitä suuntaviivoja siitä, kuinka tekoälyä tulisi hyödyntää koulussa ja miten aihetta tulisi käsitellä opetuksessa.



KUVIO 5 Opettajien arvio peruskoulun päättävien osaamisesta kyberturvallisuuteen liittyvissä tiedoissa/taidoissa.

5.5 Opettajien arvio omista kyberturvallisuuden opettamisen taidoista

Kysymys: Millaisiksi itse koet omat kyberturvallisuuden opettamisen taidot?

Kyselyn viidennessä kysymyksessä vastaajia pyydettiin sanallisen arvosanan valitsemalla itsearvioimaan omia kyberturvallisuuden opettamisen taitojansa (KUVIO 6). Vastauksien pohjalta tehtävä positiivinen havainto on, että yksikään vastaajista ei arvioinut taitojaan asteikon huonoimmilla arvosanoilla joko kohtalaiseksi tai välttäväksi ja enemmistö vastaajista arvioikin taitonsa ansaitsevan vähintään hyvän arvosanan. Parhaimman arvosanan, erinomainen, itselleen antoi 10 % vastaajista. Taitonsa kiitettäväksi arvioi 50 % ja hyväksi 30 % vastanneista. Tyydyttäväksi taitonsa oli arvioinut 10 % kyselyyn vastanneista.

KUVIO 6 Opettajien itsearvio omista kyberturvallisuuden opettamisen taidoistaan.

5.6 Opettajien kokema lisäkoulutuksen tarve

Kysymys: Koetko tarvitsevasi lisäkoulutusta kyberturvallisuuden opetukseen liittyen?

Kysymys oli yksinkertainen kyllä/ei -kysymys, johon vastaamalla "kyllä" aukesi avoin alakysymys, jossa vastaajaa pyydettiin kertomaan tarkemmin, millaista koulutusta hän kokee tarvitsevansa. Vastaajista vain 20 % ei kokenut tarvitsevansa lisäkoulutusta kyberturvallisuuteen liittyen (KUVIO 7). Loput 80 %

kokivat kuitenkin tarvitsevansa lisäkoulutusta. Tulos koetusta lisäkoulutuksen tarpeesta on sikäli mielenkiintoinen, että valtaosa vastaajista kokee tarvitsevansa lisäkoulutusta aiheesta, vaikka edellisen kysymyksen vastausten perusteella suurin osa kuitenkin kokee kyberturvallisuuden opettamisen taitonsa olevan vähintään kiitettävällä tasolla.

Kysyttäessä millaista koulutusta vastaaja kokee tarvitsevansa, monessa vastauksessa nousi esille kyberturvallisuuteen liittyvät ajankohtaiset asiat, kuten uudistuva lainsäädäntö ja kyberturvallisuuden haasteet. Toisena teemana nousi tekoäly, siihen liittyvät turvallisuusuhkat sekä miten ja mitä aiheesta tulisi opettaa eri ikäisille oppilaille. Toiveena oli myös saada koulutusta kyberuhkista ja niiden torjumisesta, sekä kyberturvallisuuden peruskoulutusta, sillä osalle vastaajista aihe itsessään ei ollut kovin tuttu. Vastauksissa mainittiin lisäksi tarve tietotekniikan opettajien tekniseen opettamiseen, mistä esimerkkinä annettiin demotöiden käyttö, kuten kemian opetuksessa.

KUVIO 7 Opettajien kokemukset lisäkoulutuksen tarpeesta.

5.7 Aiheesta heränneet ajatukset ja ideat

Kysymys: Heräsikö sinulla ajatuksia/ideoita kyberturvallisuuden opetukseen liittyen? Sana vapaa!

Kyselylomakkeen lopussa olevaan avoimeen kysymykseen vastaaminen oli vapaaehtoista, mutta kuitenkin suurin osa vastaajista oli halukas jakamaan ajatuksiaan aiheeseen liittyen. Opetuksen nykymuotoinen toteutus sai osakseen kritiikkiä siitä, kuinka tietotekniikan opettajien opetettavaksi katsottavat aiheet

integroidaan paperilla osaksi muiden oppiaineiden opetusta, jolloin aiheesta vastaa opettaja, jolta usein puuttuu tekninen pohjakoulutus. Vastauksista ilmeni myös osin turhautuneisuutta resurssien jaosta kouluissa. Tieto- ja viestintäteknologian opetus on ajettu lähes kokonaan alas ja valinnaisia kursseja ei kouluissa koeta tarpeelliseksi järjestää, sillä aiheen nykyinen integraatio osaksi muuta opetusta nähdään olevan riittävää. Pohdintaa herätti myös opetuksen ja oppimisen valvonnan puute, koska oppiaineeseen integroidusta aiheesta ei ole erillistä opetusmateriaalia, eikä oppimista testata erikseen kokeilla. Eräs vastaaja kertoikin hyödyntävänsä opetuksen tukena Turvallisuuskomitean Kodin kyberopas -julkaisua, ja toivoi että vastaavanlaista materiaalia olisi myös nuorille suunnattuna. Vaikka useimmista vastauksista voitiin tulkita positiivisia asenteita kyberturvallisuutta kohtaan sekä ymmärrys kyberturvallisuuden opetuksen tärkeydestä, nousi eräässä vastauksessa esille myös vastahakoisuus uusien oppimiskokonaisuuksia tuomiseksi kouluun, sillä osaa aiheista, kuten medialukutaitoa, on opetettu kouluissa jo pitkään.

5.8 Tulosten luotettavuus

Lomakkeeseen saatujen vastausten vähäisen määrän takia vastauksista saatavat tutkimustulokset eivät ole yleistettävissä, eikä niiden pohjalta voida tehdä syvällisempiä jatkopäätelmiä. Koska lomakkeella ei myöskään kerätty vastaajan henkilötietoja, vaan vastauksen pystyi antamaan täysin anonyymisti, ei etenkään netissä vapaasti jaetun linkin kautta kyselyyn vastanneiden todellisesta henkilöllisyydestä ja roolista tietotekniikan aineenopettajana voida olla varmoja.

Itse kyselyn luotettavuutta saatujen tulosten näkökulmasta voidaan kyseenalaistaa kysymysten asettelulla. Se, että useassa kysymyksessä vaihtoehdot oli annettu valmiiksi, saattoi osaltaan sulkea kyselyn ulkopuolelle joitakin aiheita/vastausvaihtoehtoja, joita olisi kenties ollut hyvä käsitellä tässä tutkimuksessa.

6 JOHTOPÄÄTÖKSET

Tutkimuksen perusteella kyberturvallisuuden opettamiselle jo peruskoulutasolla on tunnistettu tarve. Lapset nimittäin aloittavat internetin käytön yhä nuorempina ja viettävät siellä myös aikaisempaa enemmän aikaa. Internetissä lapset altistuvat erilaisille kyberuhkille, joiden määrän ja kirjon on tutkittu jatkuvasti lisääntyvän. Internet tarjoaa myös edellytykset ja matalan kynnyksen lapsille toteuttaa kyberrikoksia.

Jotta Suomessa kansalaisten kyberturvataidot voitaisiin saada strategioissa asetettujen tavoitteiden mukaiselle tasolle, tulee nykyisen muotoiseen opetukseen tehdä vähintäänkin sisällöllisiä muutoksia ja tarkennuksia. Tämän hetken opetussuunnitelma ei opettajien mukaan tarjoa riittäviä ohjeita kyberturvallisuuteen liitettävien tieto- ja viestintäteknologian teemojen opettamiseen, minkä takia on mahdollista, että opetuksen sisältö ja taso vaihtelee suuresti eri koulujen ja jopa opettajien välillä. Tieto- ja viestintäteknologian opetus on nykyisellään sisällytetty osaksi muita oppiaineita, jolloin aihetta usein opettavat sellaiset, keillä ei välttämättä ole minkäänlaista koulutusta aiheesta. Aiheesta ei myöskään ole olemassa omaa oppimateriaalia opetuksen tueksi, mikä tekee aiheen opettamisesta entistäkin haastavampaa. Oli opetuksen toteutus mikä tahansa, muutoksia tarvitaan myös opettajien koulutuksen osalta. Nykyisin opettajan tehtävissä oleville tulisi pyrkiä tarjoamaan helposti saavutettavaa koulutusta aiheeseen liittyen. Opettajien osaamisen haasteisiin olisi hyvä puuttua jo kenties opettajakoulutukseen kohdistuvilla muutoksilla.

Kyberturvallisuudesta tulisi peruskoulutasolla opettaa aiheita, jotka palvelevat oppilaiden osaamistarpeita. Lapset ovat monesti aikuisia taitavampia eri teknisten laitteiden käytössä, mutta mm. lasten tietoturvataidoissa voidaan tunnistaa olevan puutteita. Lasten kyberturvallisuuden osaamisen puutteen voidaan nähdä lisäävän lapsen riskiä joutua kyberuhan uhriksi. Tietämättömyys internetin hyvistä käytöstavoista voi osaltaan johtaa tilanteisiin, jossa kyberuhkien aiheuttaja on lapsi itse. Tärkeää olisi tunnistaa, kuinka lapset ja nuoret käyttävät tietoteknisiä laitteita, sovelluksia ja internetiä myös koulun ulkopuolella. Tähän perustuen voitaisiin tehdä arvioita siitä, minkälaisia kyberuhkia lapset todennäköisimmin kohtaavat arjessa ja opetuksella pyrkiä vastaamaan juuri näihin uhkiin.

Kyberturvallisuudesta opetettavia yksityiskohtaisia aiheita päätettäessä haasteeksi muodostuu kuitenkin itse kyberturvallisuuden ja siihen liittyvien ilmiöiden sekä teknologian nopeat muutokset. Yhden, kenties opetushetkellä ajankohtaisen kyberuhan yksityiskohtainen tunnistaminen ja siltä suojautuminen voi jo vuoden päästä olla vanhentunutta tietoa, joka ei enää pidä paikkaansa, eikä näin ollen täysin suojaa käyttäjää uhkalta. Yleisellä tasolla voidaan kuitenkin tunnistaa aiheita, jotka eivät yhtä lailla kärsi teknologian kehityksestä aiheutuvasta muutoksesta ja toimivat enemmänkin aiheen oppimisen perustana. Näitä ovat mm. Internetin hyvät käytöstavat, kriittinen medialukutaito sekä laitteiden tietoturvallinen käyttö. Samoja aiheita on lisäksi hyvä käydä läpi useammalla eri

vuosiluokalla, huomioiden oppilaiden iän ja ymmärryksen tason opetuksen sisältöä laatiessa.

Kyberturvallisuuteen liittyen on toki hyvä opetella myös sillä hetkellä ajankohtaisia aiheita ja käytänteitä, jotta lapset ja nuoret pystyisivät suojautumaan sen hetken kyberuhkilta. Tärkeintä olisi kuitenkin painottaa opetuksessa omien tietojen ja taitojen jatkuvan kehittämisen merkitystä. Oppilaille tulisi pystyä tarjoamaan opetuksessa tarvittava pohjatieto ja työkalut, joita hyödyntämällä he voisivat itsenäisesti kehittää omaa osaamistaan aiheesta, jotta heillä säilyisi kyky suojata itseään kyberturvallisuuden alati muuttuvassa maailmassa myös tulevaisuudessa.

Alustavia ehdotuksia opetuksen kehittämiseen ja toteutukseen liittyen on jo tehty. On ehdotettu, että kyberturvallisuus tulisi sisällyttää osaksi nykyistä tieto- ja viestintäteknologian laaja-alaisen osaamisen kokonaisuutta, tai että kyberturvallisuudesta tulisi muodostaa täysin oma laaja-alaisen osaamisen kokonaisuus. Lisäksi on esitetty vaihtoehtoa, jossa tieto- ja viestintäteknologia eriytettäisiin täysin omaksi pakolliseksi oppiaineekseen, sisältäen myös kyberturvallisuuden opetuksen. Vaihtoehdoista ensimmäinen vaatii vähiten muutoksia nykyiseen opetukseen ja onkin näin ollen opetuksen mahdollinen kehityssuunta. Toistaiseksi opetuksen muutoksen suhteen ei kuitenkaan ole tehty virallisia, kouluja ja opetushenkilöstöä velvoittavia päätöksiä.

7 POHDINTA JA JATKOTUTKIMUSAIHEITA

Tutkimuksen tavoitteena oli löytää konkreettisia ehdotuksia siitä, mitä kyberturvallisuudesta tulisi juuri peruskoulussa opettaa. Tutkimuksen alussa ajatuksena oli tutkimustuloksiin pohjautuen kyetä muodostamaan jonkinlainen valmis lista, joka kuvaisi tärkeimmät kyberturvallisuudesta peruskoulutasolla opetettavat aiheet. Tutkimuksessa kyselylomakkeella kerättyjen vastausten vähyys, mutta etenkin oma kirjallisuuskatsausta laatiessa muodostunut käsitys kyberturvallisuuden luonteeseen kansalaisen näkökulmasta osoittivat, että opetettavien aiheiden yksityiskohtainen kuvaus ei olisi järkevää.

Tutkimuksen osalta haasteita aiheutti useiden muiden opettajille tai kouluille suunnatuiden tutkimuskyselyiden tavoin suunnitellun kohderyhmän tavoittaminen. Koska tietotekniikka ei ole omana oppiaineena pakollinen osa perusopetusta, ei kaikissa kouluissa ole kyseisen aineen opettajaa, ja joissakin kouluissa vastaavaa roolia hoitaa tvt-vastaavaksi nimetty opettaja, jolla ei välttämättä ole sen enempää koulutusta aiheesta kuin muillakaan opettajilla. Kyselylomakkeen lähettäminen sähköpostitse koulun rehtorille tai koulun omaan yhteiskäyttöiseen sähköpostiin on mahdollisesti johtanut siihen, että viesti ei lopulta tavoittanut lomakkeen kohderyhmään kuuluvia. Vaikka kyselyyn ei ollut saatu tutkimuksen teon näkökulmasta järkevää määrää vastauksia, oli vastausten kerääminen keskeytettävä työn valmistumiseen liittyvien aikataulullisten paineiden vuoksi. Tämän pro gradun haasteena oli myös tutkimuksen toteuttaminen kokoaikaisen työn ohessa.

Tutkimus itsessään ei tarjonnut valmiita vastauksia tutkimuksen alussa esitettyyn tutkimuskysymykseen, mutta auttoi osaltaan tunnistamaan aiheeseen liittyviä haasteita ja siitä tehtävän lisätutkimuksen tarvetta. Mahdollisia aiheita jatkotutkimukselle olisi esimerkiksi selvittää, millaisia kyberuhkia lapset todennäköisimmin kohtaavat omassa arjessaan, kuinka lapset osaavat soveltaa tietoturvataitoja käytännössä ja millaisilla opetuskeinoilla saadaan parhaita oppimistuloksia kyberturvallisuuteen liittyen. Näihin kysymyksiin vastaamalla voitaisiin selvittää lasten todellista osaamisen tasoa sekä tarvetta ja sitä kautta tehdä päätelmiä siitä, millaisten asioiden opettaminen parhaiten palvelee lasten osaamisen kehittämistä. Jälkimmäiseen jatkotutkimusehdotukseen liittyen, olisi mielenkiintoista esimerkiksi testata koululaisille räätälöityä kyberharjoitusta ja tutkia sen käytännön toteutusta ja onnistumista opetusmetodina, sekä vaikutuksia oppimistuloksiin.

LÄHTEET

Aiken, M., Davidson, J., & Amann, P. (2016). Youth pathways into cybercrime.

Aksela, M., Marchal, S., Patel, A., Rosenstedt, L., WithSecure, (2022). Tekoälyn mahdollistamat kyberhyökkäykset. (*Traficomin tutkimuksia ja selvityksiä 30/2022*).

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754.

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, *12*(4), 233–249.

Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet: a study of Devon, UK. *Interactive technology and smart education*, 13(2), 147–165.

Euroopan parlamentti: Kyberturvallisuus: Nykyiset ja tulevat uhat. (2022) [Viitattu: 25.11.2023] https://www.europarl.europa.eu/topics/fi/article/20220120STO21428/kyberturvallisuus-nykyiset-ja-tulevat-uhat

Falck, K. (2016). Diginatiiveja vai ei?: tietotekninen osaaminen yläkoulun 7-luokkalaisten keskuudessa. https://jyx.jyu.fi/bitstream/handle/123456789/52337/URN%3aNBN%3afi%3ajyu-201612145094.pdf?sequence=1&isAllowed=y

IRO Research (2019). Lapset ja älypuhelinten käyttö.

Kaipainen, S., & Pyysing, M. (2022). Kyberturvallisuus suomalaisessa perusopetuksessa: suomalaisessa peruskoulussa tapahtuvan kyberturvallisuuden opetuksen nykytila ja opetussuunnitelmien perusteiden tulevaisuuden suuntaviivat.

Karjaluoto, A., Parts, Ü., Lehtinen, R., & Frantti, T. (2019). Kasvua digitaalisesta turvallisuudesta: Tiekartta 2019–2030.

Kosonen K., (2019). Viides ja kuudesluokkalaisten oppilaiden tietotekniikka-osaaminen ja käyttö.

Kyberturvallisuuskeskus, (2021). Tietoturva Nyt! Jumpataan kyberturvallisuuden perustaidot kuntoon - Tule mukaan! Artikkeli Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskuksen verkkosivuilla. [Viitattu: 6.4.2024]. ttps://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/jumpataan-kyberturvallisuuden-perustaidot-kuntoon-tule-mukaan

Kyberturvallisuuskeskus, (2023). Harjoitustoiminta. Artikkeli Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskuksen verkkosivuilla. [Viitattu: 2.5.2024]. ttps://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/harjoitustoiminta

Laari, T., Flyktman, J., Härmä, K., Timonen, J., & Tuovinen, J. (2019). # kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle. *Julkaisusarja 3: Työpapereita nro 12*.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.

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

Lehtinen, Somerkallio (2022). Hauskaksi tarkoitettu jekku voi olla kyberrikos, Poliisi. [Viitattu: 22.11.2023]. https://poliisi.fi/blogi/-/blogs/hauskaksi-tarkoitettu-jekku-voi-olla-kyberrikos

Lehto, M., & Kähkönen, A. (2015). Kyberturvallisuuden kansallinen osaaminen. *Informaatioteknologian tiedekunnan julkaisuja*, (20/2015).

Lehto, M., & Limnéll, J. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.

Lehto, M. (2022). Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus–hankkeen loppuraportti. *Informaatioteknologian tiedekunnan julkaisuja*, (93).

Nykänen, A. (2023). Kyberturvallisuuden/tietoturvallisuuden opetus peruskoulussa.
https://jyx.jyu.fi/bitstream/handle/123456789/86525/URN%3aNBN%3afi%3ajyu-202304242639.pdf?sequence=1&isAllowed=y

Oinas-Kukkonen, H., & Kurki, H. (2009). Internet through the eyes of 11-year-old children: First-hand experiences from the technological environment children live in. *Human Technology*, *5*(2), 146–162.

Opetushallitus, Digitaalisen osaamisen kuvaukset. (ei pvm.). [Viitattu: 6.5.2024]. https://eperusteet.opintopolku.fi/#/fi/digiosaaminen/8706410/tekstikappale/8709071

Opetushallitus, Kyberturvallisuusosaamisen edistäminen varhaiskasvatuksesta toiselle asteelle. (2022) https://www.oph.fi/fi/kyberturvallisuus

Opetushallitus, Perusopetuksen opetussuunnitelman perusteet 2014.

https://eperusteet.opintopolku.fi/#/fi/perusopetus/419550/tekstikappale/428611

Opetus- ja kulttuuriministeriö: Uudet lukutaidot – kehittämisohjelma. [Viitattu: 25.4.2024] https://okm.fi/uudet-lukutaidot

Opetus- ja kulttuuriministeriö: Kasvatuksen ja koulutuksen digitalisaation linjaukset 2027. (2023), Opetus- ja kulttuuriministeriön julkaisuja: 2023:17. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164853/OKM_2023_17.pdf?sequence=1&isAllowed=y

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

Palatsi, K., & Tuononen, I. (2020). Sosiaalisen median vaikutukset nuorten mielenterveyteen ja itsetuntoon: Kysely yhdeksäsluokkalaisille.

Panhans, D., Hoteit, I., Yousuf, S., Breward, T., Alfaadel, A. M., AlShaalan, B. H. (2022). Why children are unsafe in cyberspace. BCG, Global Cybersecurity Forum.

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Savola, R., Salonen, J., ... & Remes, J. (2016). Kyberosaaminen Suomessa–Nykytila ja tiekartta tulevaisuuteen.

Perusopetuslaki 2020. (30.12.2020/1214). [Viitattu: 23.11.2022]. https://www.finlex.fi/fi/laki/ajantasa/2020/20201214

Rahman, N., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382.

Rajamäki, M. (2021). Kyberturvallisuustaidot ovat kansalaistaitoja – kehota sinäkin työntekijöitäsi käyttämään tunti työaikaa kyberturvallisuuteen viikolla 43. Elinkeinoelämän keskusliitto. [Viitattu: 6.4.2024]. https://ek.fi/ajankohtaista/uutiset/kyberturvallisuustaidot-ovat-kansalaistaitoja-kehota-sinakin-tyontekijoitasi-kayttamaan-tunti-tyoaikaansa-kyberturvallisuuteen-viikolla-43/

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23-39.

Sanastokeskus (2018). *Kyberturvallisuuden sanasto.* Turvallisuuskomitean toimeksianto.

Sisäministeriö, Kyberturvallisuus osana kansallista turvallisuutta. [Viitattu 24.11.2022]. https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

Sisäministeriö, Kyberrikollisuus ylittää rajat tietoverkoissa. [Viitattu 28.11.2022]. https://intermin.fi/poliisiasiat/kyberrikollisuus

Suuronen, E., & Eskola, L. (2023). Luokanopettajien käsityksiä tieto- ja viestintäteknologian mahdollisuuksista tulevaisuuden taitojen kehittämisessä.

Somerkallio, Latomaa (2023). Vastuullisesti verkossa, Poliisi. [Viitattu 22.11.2023]. https://poliisi.fi/blogi/-/blogs/vastuullisesti-verkossa

Turvallisuuskomitea (2019). *Suomen kyberturvallisuusstrategia 2019.* Valtioneuvoston periaatepäätös. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Tuomi, J., & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos.). Kustannusosakeyhtiö Tammi.

Tuovinen, J. (2022). Tietoturvataitojen opettaminen peruskoulussa. *Kaakkois-Suomen ammattikorkeakoulu.*

Toikkanen, U., (2009). Väkivaltapelit lisäävät lasten impulsiivista väkivaltaista käyttäytymistä. Lääkärilehti, 16.12.2009.

Ulkoministeriö, Kyberturvallisuus ja kybertoimintaympäristö. [Viitattu 29.11.2022]. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

Uusikartano, M. (2023). Kyberharjoitus osana organisaation jatkuvasti kehittyvää kyberturvahallintaa.

LIITE 1: KYSELYLOMAKE S. 45–47

Kyberturvallisuuden opetus peruskoulussa

Luethan tämän ennen kyselyyn vastaamista!

Kyselyssä seuraavilla termeillä tarkoitetaan:
Tietosuoja = kansalaisen perusoikeus, jonka tarkoituksena on osoittaa milloin ja millä edellytyksillä tietoja voidaan käsitellä (Esim. EU-alueen yhteinen GDPR-laki).
Tietoturva = yksi tietosuojan toteuttamisen keino, jonka tarkoituksen on suojata tietoaineistoja ja tietojärjestelmiä esim. teknisillä toimenpiteillä.

Missä tärkeysjärjestyksessä seuraavia kyberturvallisuuteen liittyviä tietoja/taitoja tulisi mielestäsi peruskoulussa opettaa? (1 tärkeä - 9 vähiten tärkeä)

Internetin hyvät käytöstavat	Valitse
Internetin käyttöön liittyvä lainsäädäntö	Valitse
Kriittinen medialukutaito	Valitse
Kyberuhkien tunnistus	Valitse
Kyberuhkilta suojautuminen	Valitse
Laitteiden turvallinen käyttö	Valitse
Tekoäly	Valitse
Tietosuoja	Valitse
Tietoturva	Valitse

Tuleeko mieleesi jotain muita aiheita, joita mielestäsi peruskoulussa tulisi opettaa kyberturvallisuuteen liittyen?

Millä vuosiluokilla kyberturvallisuuteen liittyviä aiheita tulisi mielestäsi opettaa?

	1	2	3	4	5	6	7	8	9
Internetin hyvät käytöstavat	☐	☐	☐	☐	☐	☐	☐	☐	☐
Internetin käyttöön liittyvä lainsäädäntö	☐	☐	☐	☐	☐	☐	☐	☐	☐
Kriittinen medialukutaito	☐	☐	☐	☐	☐	☐	☐	☐	☐
Kyberuhkien tunnistus	☐	☐	☐	☐	☐	☐	☐	☐	☐
Kyberuhkilta suojautuminen	☐	☐	☐	☐	☐	☐	☐	☐	☐
Laitteiden turvallinen käyttö	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tekoäly	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tietosuoja	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tietoturva	☐	☐	☐	☐	☐	☐	☐	☐	☐
Muu:	☐	☐	☐	☐	☐	☐	☐	☐	☐

Millaiseksi arvioit peruskoulun päättävien osaamisen seuraavissa tiedoissa/taidoissa (0 = ei osaamista, 1 välttävä - 6 erinomainen) *

	0	1	2	3	4	5	6
Internetin hyvät käytöstavat	○	○	○	○	○	○	○
Internetin käyttöön liittyvä lainsäädäntö	○	○	○	○	○	○	○
Kriittinen medialukutaito	○	○	○	○	○	○	○
Kyberuhkien tunnistus	○	○	○	○	○	○	○
Kyberuhkilta suojautuminen	○	○	○	○	○	○	○
Laitteiden turvallinen käyttö	○	○	○	○	○	○	○
Tekoäly	○	○	○	○	○	○	○
Tietosuoja	○	○	○	○	○	○	○
Tietoturva	○	○	○	○	○	○	○

Millaiseksi itse koet omat kyberturvallisuuden opettamisen taidot *

- ◯ Erinomainen
- ◯ Kiitettävä
- ◯ Hyvä
- ◯ Tyydyttävä
- ◯ Kohtalainen
- ◯ Välttävä

Koetko tarvitsevasi lisäkoulutusta kyberturvallisuuden opetukseen liittyen? *

- ◉ Kyllä
- ◯ En

Millaista koulutusta koet tarvitsevasi?

Heräsikö sinulla ajatuksia/ideoita kyberturvallisuuden opetukseen liittyen? Sana on vapaa!

Lähetä