Valetiedon tunnistaminen

Marika Peuraniemi

Julkaisuvuosi Laurea

Laurea-ammattikorkeakoulu

Valetiedon tunnistaminen

Marika Peuraniemi
Turvallisuusjohtamisen YAMK
Opinnäytetyö
Marraskuu 2023

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusjohtaminen

Liiketalouden (YAMK)

Marika Peuraniemi

Valetiedon tunnistaminen

Vuosi 2023 Sivumäärä 57

Opinnäytetyön tarkoituksena on tutustua valetietoon ja auttaa tunnistamaan valetieto erilaisista medioista. Valetieto on tämän hetken kuuma puheenaihe hybridivaikuttamisen johdosta. Tutkimusstrategiaksi valittiin tutkimuksellinen kehittämistoiminta. Teoreettisessa viitekehyksessä käytettiin luotettavien tahojen laatimia julkisia julkaisuja.

Opinnäytetyön tarkoituksena on lisätä ymmärrystä ja tietoisuutta valetiedosta toisen asteen opiskelijoissa. Opinnäytetyönä tehtyä opetusmateriaalia voidaan hyödyntää myös kohdeorganisaation henkilöstön tietoisuuden lisäämisessä. Tavoitteena on esitellä valetiedon laajuutta ja monimuotoisuutta teoksen lukijalle ja opetusmateriaalia opiskelevalle. Ymmärtämisen lisäksi tärkeintä on, että tietoon tutustumisen jälkeen osaa suhtautua siihen kriittisesti. Opinnäytetyön tulokset ovat Tampereen seudun ammattiopiston saatavilla.

Valetieto on tällä hetkellä kuuma aihe ja materiaalia on saatavilla runsaasti. Verkossa on saatavilla erittäin laadukkaita opintomateriaaleja oppimiseen eri ikäryhmille. Valetieto on erittäin mielenkiintoinen ja monitahoinen aihe, jonka tunnistamiseen on suunnattu ja suunnataan paljon koulutusta ja ohjausta. Opinnäytetyönä laadittu opintomateriaali vahvistaa kohdeorganisaationi valmiuksia valetiedon suhteen ja aihetta on käsitelty monipuolisesti sekä konkreettisin esimerkein.

Teoreettisen osuuden lisäksi valmistui verkkoon opetusmateriaalia kohdeorganisaatioon, sekä artikkeli aiheesta. Kaikki aiheesta tehdyt asiat nähdään aiheen, valetiedon tunnistamisen osalta tietoisuuden lisäämisenä kohdeorganisaatiossa ja ovat siksi tärkeä osa kokonaisuutta. Artikkeli on avuksi kohdeorganisaatiossa tiedottamisessa, sillä kohdeorganisaatiossa on useita toimipisteitä toiminta-alueella Pirkanmaalla.

Opinnäytetyöprosessin aikana syntyneet tuotokset ovat kaikki saatavilla ja ajan tasalla kohdeorganisaatiossa. Valetiedon tunnistaminen ja mediatietoisuuden lisääminen on tärkeää, kun ollaan siirtymässä työelämään ja työnantajan tietojärjestelmän käyttäjäksi.

Asiasanat: valeuutinen, misinformaatio, disinformaatio, hybridivaikuttaminen, kyberturvallisuus

Laurea University of Applied Sciences

Degree Programme in Security Management

Master of Business Administration

Marika Peuraniemi

Identifying False Information

Year 2023 Pages 57

Abstract

The purpose of the thesis is to familiarise people with fake news and to help them identify fake news from different types of media. Fake news is the hot topic of the moment in the field of hybrid influencing. The research strategy chosen was research and development. The theoretical framework was based on public publications by reputable sources.

The aim of the thesis is to increase understanding and awareness of misinformation among upper secondary school students. The educational material produced in this thesis can also be used to raise awareness among the staff of the target organisation. The aim is to introduce the scope and diversity of misinformation to the reader and the student of the educational material. In addition to understanding, the most important thing is to be able to take a critical approach to the information once it has been presented. The results of the thesis are available at to Tampere Vocational College.

False information is currently a hot topic and there is a wealth of material available. Very high quality learning materials for different age groups are available online. False information is a very interesting and complex topic, and a lot of training and guidance has been and is being directed towards its identification. The learning material developed for this thesis strengthens the capacity of the target organisation to deal with disinformation and the topic is covered in a comprehensive way and with concrete examples.

In addition to the theoretical part, online teaching material for the target organisation and an article on the topic were produced. All the work done on the topic is seen as awareness raising in the target organisation on the subject of identifying false information and is therefore an important part of the overall project. The article is helpful in the target organisation for information dissemination, as the target organisation has several branches in the area of operation in Pirkanmaa.

The outputs generated during the thesis process are all available and up-to-date within the organisation. Identifying misinformation and raising media awareness is important when making the transition to working life and becoming a user of the employer's information system.

Keywords: fake news, misinformation, disinformation, hybrid influencing, cybersecurity

Sisällys

1 Johdanto

Valeuutiset eivät ole uusi ilmiö, Yhdysvaltojen presidentinvaaleissa 2016 valeuutiset herättivät paljon huomiota ja niistä huolestuttiin. Huoli ei niinkään johtunut demokratian toteutumisesta tai vaalien merkityksestä, vaan siitä että se oli niin valtavan laajaa. Sosiaalinen media on mahdollistanut viestinnän osalta uusia toimintoja, joita ovat mm. nopea leviäminen, helppo saatavuus, kohdeyleisön laajuus ja kontrollin puutteen. (Grinberg, Joseph, Friedland, Swire-Thompson & Lazer 2016). Yhdysvaltojen presidentin vaalien lisäksi toinen valeuutisten aalto oli COVID-19-kriisin aikana (Eurooppa-neuvosto 2023).

Koronapandemian aikana Euroopan Unioni (EU) aloitti keräämään ja julkaisemaan avoimesti oikeaa tietoa ja taistella näin valetietoa (dis- ja misinformaatiota) vastaan. Pian tämän jäljessä monet kansainväliset ja kansalliset luotettavat tahot alkoivat EU:n ohjeistuksen ja esimerkin avulla toimimaan samoin (Eurooppa-neuvosto 2023). Kansallisesti perustettiin tahoja, joissa uutisten oikeellisuuden voi tarkistaa, Suomessa mm. Faktabaari. Suomessa toimii Julkisen sanan neuvosto, joka valvoo toimittajien julkaisuja ja jokainen voi tehdä kantelun havaitessaan valeuutisen tai hyvän tavan vastaista uutisointia. (Julkisen sanan neuvosto 2023).

Valetiedon englanninkielestä tuotetut määritelmät tarkoittavat Tepa -termipankin mukaan seuraavaa, disinformaatio tarkoittaa väärää tietoa, jota jaetaan tietäen tiedon olevan väärää ja misinformaatio tarkoittaa tahattomasti jaettua väärää tietoa (Tepa-termipankki 2023a). Suomen kielessä ei väärän tiedon erilaisia variaatioita voi yhdellä sanalla sanoa, sen vuoksi terminä dis- ja misinformaatio ovat käyttökelpoisia kuvaten eri tavalla väärää tietoa ja sen levittämistä.

Opinnäytetyössä on pyritty keskittymään valeuutisiin (mis- ja disinformaatio) ja mm. näennäistiede, salaliittoteoriat tms. on pyritty rajaamaan työstä pois. Opinnäytetyö kuvaa valetietoa IMMUNE 2 INFODEMIC-hankkeen sisältöjen suhteen ja hankkeen aiheiden pohjalta on laadittu kohdeorganisaatioon turvallisuusalan perustutkintoon paikallinen tutkinnon osa. Paikallinen tutkinnon osa tarkoittaa opintokokonaisuutta, jonka voi paikallisesti kohdeorganisaatiossa, Tampereen seudun ammattiopisto, Tredussa, opiskella ja sisällyttää perustutkintoonsa, mikäli opiskelija tutkinnon muodostuminen sen sallii. Kohdeorganisaatio on Suomen toiseksi suurin ammatillisen koulutuksen järjestäjä. Opinnäytetyössä valetietoa selvitettiin olemassa olon sekä seurausten kautta, sekä selvittiin missä valetietoa esiintyy tällä hetkellä eniten. Tämän vuoksi työssä on tietoa tietojenkalastelusta sekä hybridiuhista. Hybridivaikuttaminen tarkoittaa poliittisesti motivoitunut suunnitelmallista toimintaa, jolla pyritään saavuttamaan omia tavoitteita, erilaisia toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen (Tema-termipankki 2023b). Tietojenkalasteluhyökkäykset ovat usein

sähköpostitse tapahtuvia, joissa tyypillisesti pyritään huijaamalla saada käyttäjältä henkilökohtaisia tietoja. (Glamoslija 2023). Opinnäytetyössä on myös huomioitu valetietoon liittyviä tulevaisuuden näkymiä, sekä tekoälyn vaikutuksia.

IMMUNE 2 INFODEMIC eli jäljempänä I2I-hankkeen tavoitteena on immunisoida kansalaiset infodemiaa vastaan. Hankkeen tavoitteena on antaa mahdollisuus tehdä tietoon perustuvia päätöksiä, sekä varustaa kansalaiset välineillä, joilla voi tiedon oikeellisuuden varmistaa. Haasteena I2I-hankkeessa nähdään, että dis- ja misinformaatiolla, valeuutisilla tai muunlaisella häirinnällä vaikutetaan vakavasti demokraattiseen osallistumiseen ja sitoutumiseen sekä infodemian leviäminen. (IMMUNE 2 INFODEMIC 2023).

Opinnäytetyö syntyi paikallisen tutkinnon osan laatimisen tueksi. Paikallinen tutkinnon osa on koulutuksen järjestäjän oma paikalliseen tarpeeseen laadittu opintokokonaisuus (Opetushallitus 2023a). Paikallisesti eli tässä tilanteessa Tampereen seudun ammattiopisto Tredussa, sitä käytetään siis joko kohdeorganisaation toimialueen työelämän tarpeeseen tai muuhun alueellisti tarpeelliseksi nähtyyn tarpeeseen, tämä voi olla esimerkiksi koulutuksen järjestäjän yhdessä työelämän kanssa tehty ennakointi tai jonkin puuttuvan osaamisen tuominen tarjontaan. Tredun perustutkintoa opiskeleva opiskelija voi paikallisia tutkinnon osia sisällyttää omiin opintoihinsa oman perustutkinnon muodostumisen mukaisesti. Jokaisessa perustutkinnossa on määritelty miten opiskelija voi tutkinnon muodostaa. Tutkinnossa on ammatillisia tutkinnon osia, jotka on jaoteltu pakollisiin ja valinnaisiin tutkinnon osiin. Valinnaisiin tutkinnon osiin opiskelija voi henkilökohtaisen kehittämissuunnitelman mukaisesti tehdä yksilöllisiä valintoja opintojen koostamiseksi (Opetushallitus 2023a).

Paikallisen tutkinnon osan opintomateriaalin, sekä opinnäytetyön lisäksi on aiheesta kirjoitettu artikkeli Osaava Tredun julkaisuihin (Liite 2). Osaava Tredu on kohdeorganisaation henkilöstön osaamista keräävä ja jakava sivusto, missä esitellään sen sisällä olevaa osaamista, mutta myös tarjotaan apua erilaisten ohjeiden muodossa. Artikkeli kertoo nimenomaan Valetiedon tunnistamisen paikallisen tutkinnon osan valmistumisesta, sekä sen sisällöstä. Valetiedon tunnistamista on käsitelty I2I- hankkeen aiheiden, sekä muiden valetietoon liittyvien ajankohtaisten aiheiden kautta. Valitut aiheet ovat sosiaalinen media, painettu media, kriittinen infrastruktuuri, EU vaalit 2019 sekä kyberhyökkäykset. Valeuutinen käsitteenä käsittää tässä työssä, disinformaation, misinformaation, malinformation, sekä hybridivaikuttamiseen liittyviä aiheita. Tepa-termipankin mukaan malinformaatio tarkoittaa oikeaa tietoa jaetaan tietoista haittaa tai vahinkoa aiheuttaen (Tepa-termipankki 2023a). Tietojenkalastelu perustuu valetiedon käyttämiseen, jolla pyritään saamaan haltuun käyttäjätunnuksia ja/tai taloudellista hyötyä.

Valetiedon tunnistaminen tutkinnon osan tavoitteena on laatia ajantasainen ja mielenkiintoinen opintokokonaisuus toisen asteen opiskelijoille valetiedosta. Tutkinnon osa pyrkii luomaan

ymmärrystä siitä, että kaikki luettu niin verkossa, kuin painetussa mediassa, ei välttämättä ole totta ja että valheellista tietoa voi olla tarkoituksella liikkeellä, mutta sen jakamista pitäisi välttää. Tavoitteita tutkinnon osan suorittajan osaamisesta ymmärrys valetiedon olemassa olosta, sekä kriittisen medialukutaidon kehittyminen kertyneen osaamisen ansiosta. Tavoitteena lisäksi on että, opiskelijalle kehittyy jatkossa taitoa löytää luotettavia tiedon lähteitä, sekä ymmärrys että, epäselvässä tilanteessa on mahdollista tarkistaa tiedon oikeellisuus luotettavista faktantarkastusta tarjoavista palveluista internetissä. Harjaantuminen etsimään mahdollisen valeuutisen tunnusmerkkejä ja tekemään sen perusteella päätelmiä tiedon oikeellisuudesta. Kohderyhmä, joka käytännössä on toisen asteen perustutkintoa suorittavat opiskelijat 16-18-vuotiaat, on ajatellen, että perustutkintoa suorittavat ovat sosiaalisen median eri palveluiden suuria kuluttajia. Tämän lisäksi he ovat työuran alussa, jolloin oppilaitoksessa saatuja taitoja ja tietoja viedään työelämään ja osaaminen voidaan käyttää hyödyksi käytännön työtehtävissä, sekä saada juuri hankittu osaaminen työyhteisön käyttöön. Paikallisen tutkinnon osan taso on asetettu toisen I2I-hankkeen kohderyhmän 18-25-vuotiaiden tasolle, sillä pääosin paikallista tutkinnon osaa suoritetaan viimeisenä lukuvuonna, opiskelijoiden ollessa silloin 18-vuotta. Kohdeorganisaatiota ajatellen paikallinen tutkinnon osa on siten käyttökelpoinen sekä nuorten opiskelijoiden, että aikuisten opiskelijoiden osalta, lisäten sen käytettävyyttä.

Työ hyödyttää kohdeorganisaation Tampereen seudun ammattiopiston, Tredun, ammatillisen perustutkinnon opiskelijoita. Tredu on Suomen toisiksi suurin ammatillinen oppilaitos. Tredussa voit opiskella yli 60 tutkintoa 14 eri toimipisteessä Pirkanmaalla. Opiskelijoita Tredussa on noin 16 000 vuosittain. Perustutkinnon lisäksi Tredu tarjoaa ammattitutkintoja, erikoisammattitutkintoja, maahanmuuttajakoulutusta, kansainvälisiä polkuja ja -opintoja, tutkintokoulutukseen valmentavaa koulutusta, yrityksille ja työelämälle suunnattuja koulutuksia, tutkinnon osia (Tampereen seudun ammattiopisto 2023a).

1.1 Työn tavoitteet

Päätavoite on ollut tutustua valetietoon käsitteenä, ymmärtää että tiedossa, niin painetussa kuin verkossa olevassa, on mahdollisuus siihen, että se on valheellista; tahallisesti tai tahattomasti tuotettua. Tavoitteena on, että osaaminen valetiedon havaitsemisen, ennakoinnin ja seurausten osalta kasvaa. Tavoitteen saavuttamiseksi on laadittu paikallinen tutkinnon osa valetiedon tunnistamisesta Tredulle osaksi turvallisuusalan perustutkintoa.

Tutkinnon osan tavoitteena on toisen asteen opiskelijoiden ymmärryksen kasvattaminen valetiedon osalta paremmaksi. Verkossa tapahtuva opiskelu on nopea ja joustava tapa levittää tietoa laajemmin, verrattuna perinteiseen luokkamuotoiseen opetukseen. Tampereen seudun ammattiopistossa, Tredussa on käytössä verkko-oppimisalusta Moodle verkossa tapahtuvaan opiskeluun, jonka vuoksi se oli työhön luonnollinen valinta (Tampereen seudun

ammattiopisto, 2023b). Moodle voidaan asentaa mihin tahansa tietokoneeseen tai sitä voidaan käyttää joustavasti internetselaimen kautta (Moodle 2023). Verkko-oppimisalustalle voidaan luoda monipuolisia opetuskokonaisuuksia. Tavoitteena on kehittää opiskelijan kriittistä ajattelua ja osaamista luotettavien lähteiden käyttämisessä. Helsingin seudun kauppakamarin tekemän kyselytutkimuksen mukaan suurimpia esteitä kyberturvallisuuden toteuttamisessa on yrityksen henkilöstön tietotaidon ylläpitäminen kyberturvallisuuden suhteen, sekä piittaamattomuus (Vesterinen & Korslow 2022). Tutkinnon osa siis vastaa valetiedosta tietoiseksi tulemisesta, sekä pyrkii vaikuttamaan siihen, että opiskelija kokee valetiedon osalta saamansa osaamisen olevan tärkeä osa ammattitaitoaan ja merkityksellisenä osana työnantajan turvallisuustyötä.

I2I-hankkeen mukainen ikäryhmä on 18-25 vuotiaat, jotka toimivat tutkimuksen mukaan impulsiivisesti ja harkitsematta jakaen informaatiota ja he luottavat verkossa julkaistuun tietoon (Williams, Hindis & Joinson 2018). Valmistunut paikallinen tutkinnon osa on Tredun perustutkinnon opiskelijoille toisella asteella erittäin sopiva huomioiden tutkinnon osan suorittavien ikä. Verkko-oppimisalusta Moodleen valmistunut viiden (5) osaamispisteen tutkinnon osa valeuutisten tunnistamisesta tuo heille tarvittavaa osaamista tulevaisuutta ajatellen. Osaamispiste tarkoittaa tutkinnon osan laajuutta. Materiaalin avulla voi valetiedon ilmiön monimuotoisuudesta ja -tahoisuudesta tulla tietoiseksi ja kehittyä ymmärrystä valetiedon olemassa olosta ja sen seurauksista.

Paikallinen tutkinnon osa valmistui pääosin kesällä 2023. Valmistumisen jälkeen tutkinnon osasta on pyydetty palautetta, palautteiden mukaiset korjaukset ja muokkaukset tapahtuivat syksyllä 2023 ja lopulliseen muotoonsa tutkinnon osa valmistui vuoden 2023 joulukuun lopussa. Kohdeorganisaatiossa paikallisen tutkinnon osan perusteena on aina työelämän tarve ko. osaamiselle tai jokin muu perusteltu tarve, joka voi olla mm. ennakointi ja/tai alueellinen tarve osaamiselle. Uusi paikallinen tutkinnon osa ei myös saa olla samanlainen kuin jo jokin olemassa oleva, joten ensin tulee aina selvittää, onko aiheen mukainen tutkinnon osa jo olemassa. Selvityksen jälkeen, ja kun perusteet uudelle tutkinnon osalle on selvitetty, tulee laatia uuden paikallisen tutkinnon osan laajuus, ammattitaitovaatimukset, sekä ammattitaidon osoittamistavat. Arvioinnin kriteerit ovat ammatillisen koulutuksen osalta yhdenmukaistuneet, joten ne ovat kaikissa uudistetuissa tutkinnon osissa samanlaiset, myös tässä paikallisessa tutkinnon osassa (Opetushallitus 2023b). Ammatillisen koulutuksen johtotiimi hyväksyy esitetyt uudet paikalliset tutkinnon osat, mikäli se on perusteltu ja siihen on laadittu kohdeorganisaation laatukriteereiden mukaisesti yllä mainitut ammattitaitovaatimukset ja muut tarkemmat kuvaukset. Hyväksynnän jälkeen paikallista tutkinnon osaa on mahdollista opiskelijoiden suorittaa kohdeorganisaatiossa. Valetiedon tunnistaminen paikallinen tutkinnon osa hyväksyttiin kohdeorganisaation ammatillisen koulutuksen johtotiimin 6.9.2023 kokouksessa.

Työn tavoitteena on herättää valetietoon liittyvää tietoisuutta omassa työyhteisössä mahdollisimman laajasti. Tämän johdosta, tutkinnon osan lisäksi on kirjoitettu artikkeli Valetiedon tunnistamisesta. Artikkeli julkaistiin Osaava Tredun sivustolla 06.11.2023. Osaava Tredu on sivusto, mihin kerätään osaamista Tredun sisältä, sekä ohjeita erilaisten ohjelmien tai välineiden käyttöön esim. Teamsin käyttöön ja vinkkejä esim. Teamsin uusista ominaisuuksista. Osaava Tredun suurin julkaisija on e-oppimisen eli verkko-oppimisen parissa työskentelevällä ryhmällä, josta puhutaan kohdeorganisaatiossa nimellä eTredu. Osaava Tredussa on artikkeleita erilaisesta osaamisesta eri puolilta Tredun toimipisteissä tapahtuvasta toiminnasta. Artikkeli on liitteenä työn lopussa.

Aikataulullisesti opinnäytetyötyöskentely alkoi heti opintojen käynnistymisen jälkeen keväällä 2023 aiheanalyysin laatimisella, jonka jälkeen varsinainen työskentely opinnäytetyön parissa alkoi. Varsinaisella työskentelyllä tarkoitetaan paikallisen tutkinnon osan esittelyä kohdeorganisaation ammatillisen koulutuksen johtotiimille (syksy 2023), sekä sen tekemistä Moodleen (kesä 2023). Opinnäytetyö valmistui vuoden 2023 joulukuun lopussa.

1.2 Määritelmiä

Tutkimuksessa käytettävät käsitteet liittyvät valetietoon ja valetiedolla vaikuttamisen keinoihin. Käsitteet on selitetty aakkosittain, seuraavin poikkeuksin: Huoltovarmuuskeskuksen informaatioturvallisuuteen liittyvät käsitteet ovat omana kokonaisuutena sekä tietojenkalastelun käsitteet ovat omana kokonaisuutenaan:

Disinformaatio – väärää tietoa tuotetaan ja jaetaan siten, että ollaan tietoisia sen tuomasta haitasta tai vahingosta (Tepa-termipankki 2023a).

Hybridivaikuttaminen – poliittisesti motivoitunut suunnitelmallinen toiminta, jolla pyritään saavuttamaan omia tavoitteita, erilaisia toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen (Tema-termipankki 2023b).

I2I-hanke – IMMUNE 2 INFODEMIC kansainvälinen hanke, jonka tavoitteena on herkistää ja lisätä tietoisuutta EU kansalaisissa dis- ja misinformaation osalta (IMMUNE 2 INFODEMIC 2023).

Infodemia - Infodemialla tarkoitetaan liikaa tietoa, mukaan lukien väärää tai harhaanjohtavaa tietoa digitaalisissa ja fyysisissä ympäristöissä (WHO 2023).

Informaatiovaikuttaminen – vaikutetaan järjestelmällisesti yleiseen mielipiteeseen, ihmisen käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn (VNK) On yksi osa hybridivaikuttamista (Valtioneuvoston kanslia 2019).

Malinformaatio – oikeaa tietoa jaetaan tietoista haittaa tai vahinkoa aiheuttaen (Tepa-termipankki 2023a).

Misinformaatio – väärää tietoa jaetaan tahattomasti (Tepa-termipankki 2023a).

Moodle – verkko-oppimisympäristö, jonka avulla luodaan verkkokursseja ja web-sivuja. Moodle voidaan asentaa mille tahansa tietokoneelle ja sitä voidaan käyttää internetselaimella. (Moodle 2023).

Huoltovarmuuskeskuksen informaatioturvallisuuteen liittyvät käsitteet on listattu alla omaksi kokonaisuudekseen:

Informaatioturvallisuus - Tila, jossa informaatioympäristön uhkat ja riskit ovat hallittavissa (Kangasniemi 2022).

Informaatiovaikuttaminen - Kohteelle haitallinen toiminta, jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla pyritään vaikuttamaan kohteen käsityksiin tai toimintaan (Kangasniemi 2022).

Informaatiovaikuttamiselta suojautuminen - Jatkuva, ennaltaehkäisevä toiminta, jolla heikennetään informaatiovaikuttamisen vaikutuksia (Kangasniemi 2022).

Informaatio-operaatio - Suunnitelmallinen sarja toimintoja, joilla tuetaan ja koordinoidaan informaatiovaikuttamiseen pyrkiviä toimenpiteitä määritetyn tavoitteen saavuttamiseksi (Kangasniemi 2022).

Tietoturva yritys F-Secure avaa kohdennetun tietojenkalastelun termejä seuraavalla tavalla:

Kohdennettu tietojenkalastelu eli spear phishing. Phishing-viestejä lähetetään usein satunnaisesti isolle joukolle ihmisiä. Kun kyseessä on tarkempi, kohdennettu tietojen-kalastelu, puhutaan ilmiöstä nimeltään spear phishing. Spear phishing -huijauksen kohteena voi olla yksityishenkilöiden lisäksi organisaatioita sekä niiden johtohenkilöitä. Kun kyseessä on kohdettaan varten räätälöity, kohdennettu tietojen-kalastelu, voi huijausta olla paljon vaikeampi tunnistaa kuin tavan-omaisessa tietojen-kalastelussa. (F-Secure 2023a).

Tekstiviestihuijaus eli smishing hyödyntää joko teksti- tai pikaviestipalveluita kalastelun välineenä. Verkkorikolliset voivat myös ujuttaa olemassa oleviin viestiketjuihin omia, haitallisia viestejään. Tällöin voi olla vaikea tunnistaa esimerkiksi postin tai lähettipalvelun viestin perään ilmestynyttä huijausviestiä. Myös smishing-viestit sisältävät sähköpostien tapaan linkkejä, jotka ohjaavat huijaussivustoille. (F-Secure 2023a).

Huijaus-puhelut eli vishing. Henkilökohtaisia tietoja, kuten pankki- ja henkilötunnuksia, voidaan urkkia myös puhelimitse. Tämä vishing-nimellä kulkeva ilmiö viittaa huijauspuheluihin. Nimi tulee sanoista voice ja phishing. Kuten muut kalastelun muodot, vishing-puheluiden soittajat voivat esiintyä pankin tai muun luotettavan tahon nimissä. Yleisiä ovat myös yritysten

tai kohteen työnantajan IT-tuen nimissä tehtävät huijauspuhelut. Näiden tarkoituksena on saada huijauksen uhri asentamaan etä-hallinta-ohjelma tieto-koneelleen. (F-Secure 2023a).

Määritelmiä käytetään erilaisissa medioissa, usein oletetaan näiden olevan lukijalle tuttua. Aiheeseen liittyvien määritelmät ovat kuitenkin melko uusia, joten ne kaipaavat sen vuoksi työssä selitteitä.

2 Tutkimusmenetelmät ja toteutus

Perustutkimuksessa ei tiedon etsintään liity erityistä käyttötarkoitusta, vaan sen tarkoituksena on edistää tietämystä. Perustutkimuksessa tuotettua tietoa uusien tai parannettujen menetelmien osalta käytetään ja sovelletaan kehitystyön tukena. (Toikko & Rantanen 2009).

Tutkimusmenetelmäksi valikoitui yleisellä tasolla laadullinen toimintatutkimus ja teoriapohjainen sisältöanalyysi. Laadullisen tutkimuksen ominaispiirteitä on löydettävissä useita, näitä ovat mm. keskittyminen toimintaan, tutkija aineiston tulkitsijana, sekä joustavuus. Hyviä aineistoja on aiheesta olemassa paljon ja tämän vuoksi työssä on käytetty lähteitä paljon. Opinnäytetyössä on myös pyritty käyttämään ajantasaisia aineistoja. Ajantasaisuus aineistojen valinnassa tarkoittaa kymmenen (10) vuoden sisällä julkaistuja aineistoja, pääosin aineisto kuitenkin on tätä ajantasaisempaa, johtuen aiheesta. Poikkeuksia aineiston ajantasaisuuden osalta on mm. poikkeuksellisen laadukas tai aikaa kestävä tutkimus tai julkaisu, johon on viitattu uudemmissa julkaisuissa. Aineiston valinnassa on pyritty käyttämään alkuperäisiä aineistoja, joten jos uudessa aineistossa on käytetty lähteenä vanhempaa aineistoa, on tähän työhön valittu aineiston alkuperäinen lähde. Laadullisen tutkimuksen kohteena on usein jokin yhteiskunnallisesti ajankohtainen kysymys, valetieto on yhteiskunnallisesti ajankohtainen aihe. Laadullinen tutkimus on usein aineistovetoista. (Kallinen & Kinnunen 2021). Laadullinen tutkimus on tyypillisesti kokonaisvaltaista tiedon hankintaa. Laadullisen tutkimuksen piirteisiin kuuluu tutkimussuunnitelman muotoutuminen samalla, kun tutkimus etenee ja sitä voidaan muuttaa olosuhteiden mukaisesti. (Hirsijärvi, Remes & Sajavaara 1997; 164).

Aineistoa tutkimukseen kerättiin alkuvaiheessa ProQuest Centralin kautta, joka on laaja monitieteellinen yhteistietokanta. Hakusanoina käytettiin ”disinformation” ja ”misinformation”. Löydettyihin artikkelien ja tutkimustuloksien osalta pyrittiin aina alkuperäiseen tiedon tuottajaan, sekä mahdollisimman ajankohtaiseen. Toisessa vaiheessa hakusanat olivat ”disinformation” AND ”cybersecurity” sekä ”misinformation” AND ”cybersecurity”. Kolmannessa vaiheessa aineistoa kerättiin hakusanoilla ”hybrid influence”, sekä ”critical infrastructure”. Näiden osalta oli loogista tehdä haku myös ”hybrid influence” AND ”cybersecurity” sekä, ”critical infrastructure” AND ”cybersecurity”. Tutkimuksen laajentuessa käytin hakusanoina myös ”phishing” ja ”cybersecurity”, sekä ” artificial intelligence”, jotta aiheen ajankohtaiset

artikkelit tuli tutkittua laajemmin. Hakusanojen tuli esiintyä valittujen aineistojen otsikossa tai abstraktissa. Sisältöanalyysin analyysirungon muodostumisen vaiheessa valittiin aineistoa ajantasaisuuden varmistamiseksi tietokannassa mainittujen luotettaviksi havaittujen yritysten ja julkishallinnon toimijoiden internetjulkaisuista. Aineiston ajankohtaisuuden, joka tässä työssä tarkoittaa pääosin alle kymmenen (10) vuotta sitten julkaistua materiaalia. Tutkimuksessa on käytetty mahdollisuuksien mukaan aina alkuperäisiä lähteitä, jos se on saatavilla. Alkuperäisten lähteiden vuoksi ajankohtaisuus on kymmenen (10) vuotta. Yhteiskunnallinen merkittävyys oli osana valitun aineiston kriteereitä. Yhteiskunnallinen merkittävyys aineiston kriteerinä tarkoittaa sitä, että se on huomioitu luotettavissa medioissa ja tutkimuksissa. Yhteiskunnallinen merkittävyys on tässä työssä tarkoittanut myös sitä, että aihe itsessään on yhteiskunnallisesti merkittävä aihe. Yhteiskunnallinen merkittävyys huomioidaan valitsemalla luotettavien tahojen yhteisesti tehtyjä ohjeistuksia, säädöksiä, virallisten kanavien esimerkiksi Eurooppa neuvosto, Kyberturvallisuuskeskus, Huoltovarmuuskeskus jne. lähteiksi.

2.1 Toimintatutkimus

Työelämätutkimuksessa erilaisissa kehittämis- ja muutoshankkeissa käytetään usein toimintatutkimusta. Toimintatutkimukselle tyypillistä on käytäntöön suuntautuminen. Toimintatutkimusotteen vaatimuksena on osallisuus ja osallisuuden vahvistaminen yhteiskunnan eri alueilla. Toimintatutkimuksen Lewinin hahmoittelema perusmalli on spiraalimainen, joka lähtee liikkeelle ongelman havaitsemisesta. Ongelman pohjalta laaditaan tutkimussuunnitelma, jota toteutetaan reflektoiden. Tehtyä suunnitelmaa havainnoidaan ja arvioidaan. Havaintojen ja arvioinnin pohjalta uudistetaan laadittua suunnitelmaa ja tarvittaessa täsmennetään. Prosessi jatkuu niin kauan, kunnes suunnitelmassa olevat tavoitteet saavutetaan tai todetaan niiden olevan saavuttamattomissa. (Kallinen & Kinnunen 2021). Toimintatutkimuksen prosessin ja periaatteiden toteutus on tehty jatkuvan havainnoinnin ja reflektoinnin sekä arvioinnin kautta, näiden apuna on pyydetty palautetta kohdeorganisaatiossa. Palautteita on havainnoitu ja arvioitu sekä reflektoitu ja niiden pohjalta on tehty tarpeellisia parannuksia ja muutoksia. Tutkinnon osan muutokset näyttäytyvät opiskelijalla siten, että ne ovat konkreettisempia, tutkinnon osaan suorittavalle opiskelijalle selkeämpiä, johdonmukaisempana kokonaisuutena näyttäytyviä muutoksia, sekä myös sisällön ja osaamispistemäärän parempana vastaavuutena. Osallisuutta ja sen vahvistamista on tapahtunut palautteiden pyytämisen ja käsittelyn aikana. Toimintatutkimuksen vaatimus osallisuudesta ja osallisuuden vahvistamisesta toteutuu myös työn aiheen myötä, opiskelija tulee tietoisemmaksi ja pystyy omalta osalta osallistua valetiedon havaitsemiseen ja poistamiseen ilmoittamalla siitä eteenpäin, sekä jakamatta jättämisellä, jolloin valetieto ei leviä.

Aineistojen ja menetelmien monipuolisuus kuvaa toimintatutkimusta. Monipuolisuuden johdosta toimintatutkimuksesta on tapana puhua aineisto- ja menetelmätriangulaationa. Triangulaatiolla tarkoitetaan erilaisten menetelmien, tutkijoiden, tietolähteiden tai teorioiden

yhdistämistä tutkimuksessa. Aineistoa ja tietoa voidaan kerätä laajasti niin laadullisesti ja määrällisesti. Aineistot voivat olla osallistuvaa havainnointia, haastatteluita, dokumentteja. Oleellista toimintatutkimuksen tutkimusprosessissa on jatkuva havainnointi ja arviointi. (Kallinen ym. 2021). Jatkuva havainnointi ja arviointi työssä näkyy tehtyinä muutoksina, joita on tehty saatujen palautteiden ansiosta, reflektoinnin jälkeen. Muutoksia on saadun palautteen ansiosta tehty tähän kirjalliseen opinnäytetyöhön, sekä tutkinnon osaan Moodlessa. Palaute on aiheuttanut reflektiota kumpaakin kokonaisuutta kohtaan ja uusien havaintojen tekemistä, joiden jälkeen työt ovat täydentyneet parannuksin ja tarpeellisin muutoksin.

2.2 Teoriapohjainen sisältöanalyysi

Dokumenttien ja aineistojen systemaattinen ja objektiivinen analysointi voidaan tehdä sisällönananlyysillä. Sisällönanalyysi on perusanalyysimenetelmä. Tutkittavasta ilmiöstä pyritään saamaan tiivistetty ja yleinen muoto. (Tuomi & Sarajärvi 2009; 91-103).

Päätösten tekeminen, aineiston litterointi tai luokittelu, teemoittelu tai tyypittely ovat sisällön analyysin vaiheita. Tutkija tekee päätöksen mikä aineistossa kiinnostaa. Litteroinnissa tutkija merkitsee aineistosta kiinnostusta vastaavat asiat. Aineiston luokittelussa määritellään luokat ja lasketaan aineiston esiintyvyys. Teemoittelussa painottuu teemoista kerrotut asiat. (Tuomi ym. 2009; 91-93).

Sisältönanalyysin ensimmäinen vaihe on analyysirungon muodostaminen. Analyysirunko voi olla väljä tai strukturoitu. Väljään analyysirunkoon voidaan poimia runkoon kuuluvat ja kuulumattomat asiat. Ulkopuolelle jäävistä asioista muodostetaan uusia luokkia analyysirungon ulkopuolelle. Strukturoidussa rungossa kerätään vain analyysirunkoon sopivia asioita. Strukturoidussa rungossa voidaan siten testata aikaisempaa teoriaa tai käsitejärjestelmää uudessa kontekstissa. (Tuomi ym. 2009; 113). Opinnäytetyössä on käytetty väljää analyysirunkoa, jossa analyysi toteutetaan osittain aineistolähtöisen eli induktiivisen sisällönanalyysin kaltaisesti. Aineistolähtöisessä sisältöanalyysissa luokitusrakenne syntyy aineistojen perusteella ja aineistorunkoon voi poimia aineistoa nimensä mukaisesti väljästi. Aineistolähtöisessä analyysissa alaluokat ja pääluokkien muodostamisen jälkeen tuloksia tulkitaan ja kirjoitetaan raportti tuloksista. Aineistolähtöinen analyysirunko etenee aineiston ehdoilla. (Salin 2020). Aineistolähtöisessä sisältöanalyysissa oleellista on aineiston ryhmittely. Yhdistävä kategoria kaikelle on valetieto, yläkategorioina sosiaalinen media, painettu media, kriittinen infrastruktuuri, EU vaalit 2019, sekä kyberhyökkäykset. Näiden yläkategorioiden yhteisiä alakategorioita on muun muassa tietojenkalastelu, tekoäly, pedagogiikka sekä tulevaisuuden haasteet, sekä niiden liittyminen yhdistävään kategoriaan valetietoon ja sen tunnistamiseen.

2.3 Tutkimuskysymykset

Tutkimuskysymykset rakentuivat työn tavoitteen mukaisesti. Tavoitteena paikallisen tutkinnon osan laatiminen valetiedon tunnistamiseksi. Opiskelua varten tarvitaan jonkinlainen lähtötaso, joka tässä tutkinnon osassa on tiedon merkitys ja miksi tieto ylipäätään on tärkeää. (Kallinen & Kinnunen 2021). Tämän jälkeen aloitetaan tunnistamaan valetiedon tuntomerkkejä, jonka jälkeen osaamista voidaan aiheen parissa laajentaa seurauksien ja merkittävyyden tutkimiseen. Tutkinnon osan suorittamisen tavoitteena on, että opiskelija aiheeseen perehtymisen jälkeen tietää, että on olemassa valheellista tietoa erilaisissa medioissa, tämän lisäksi hänen tulisi osata tunnistaa valetiedon lähteitä, sekä ymmärtää minkälaisia seurauksia valetiedosta voi olla.

Tutkimuskysymykset ovat:

1. Mitä valetieto on?
2. Missä valetietoa voi esiintyä ja mitä siitä seurata?
3. Miten valetiedon voi oppia tunnistamaan?

Tutkimuskysymyksiin pyritään vastaamaan määrittelemällä tutkimuksen kannalta oleelliset hakusanat, saaden näin ajankohtaista ja aiheeseen liittyvää aineistoa nimenomaan aiheena olevan valetiedon osalta. Valetiedon ollessa nyt kuuma puheenaihe on aiheesta kirjoitettu erittäin paljon, tutkimuksessa hyödynnettävää materiaalia on siis erittäin laajasti saatavilla, tämä näkyy työssä lähteiden runsautena. Toimintatutkimuksen ominaispiirteiden mukaisesti aineistoa on myös pyritty hyödyntämään mahdollisimman monipuolisesti. Aineistoa on käytetty laajasti niin laadullisesti, kuin määrällisesti. Laajan aineiston tarkoitus on ollut kokonaiskuvan luominen, mutta kuitenkin rajaamiseen aiheeseen, valetietoon. Pyrkimys on, että aineisto vahvistaa opetusmateriaalin taustalla olevaa tutkimuksellista tietopohjaa ja lisää aiheesta tietoa tarpeeksi laajasti, sekä perustelee tutkimuksen näkökulmasta aiheen ajankohtaisuuden sekä tärkeyden. Kyberturvallisuudesta yleisesti ja valetiedosta erikseen tai osana kyberturvallisuutta, on ohjeistusta ja oppaita erilaisten toimijoiden osalta mm. Kyberturvallisuuskeskus ja Kuntaliitto ovat kiinnostaneet monia opiskelijoita opinnäytetyön aiheena, sekä myös yritykset ohjeistavat ja tarjoavat osaltaan palveluksiaan. Valetiedon tunnistamisesta on tutkittu tämän hetken tiedon osalta ja pyritty saamaan aineistoltaan kattavaksi. Opetusmateriaalin osalta pyritty luomaan mielekäs ja kohderyhmälle soveltuva kokonaisuus.

Tutkimusprosessi on alkanut tutkimuskysymysten asetannan jälkeen tutkimuskirjallisuuteen ja julkaisuihin perehtymisellä. Tavoitteen määrittelyn jälkeen seuraavaksi analysoitiin hankittua tietoa ja aloitettiin laatimaan tutkinnon osaa. Aineistosta on nostettu esiin käytännön esimerkkejä, oikeita valetietoa käyttäviä huijauksia. Valetiedon tunnistamisen lisäksi on tutkittu tietoa seurauksista, joka luo merkityksellisyyttä aihetta kohtaan. Vaikuttavuutta ja aiheen

merkittävyyttä luo esimerkiksi työssä mainitut yrityksien mittavat tappiot, sekä konkurssi valetiedon johdosta. Valetiedon tunnistaminen tutkinnon osa on suunnattu ikäryhmälle (18-25 vuotiaat), joka jakaa eniten valetietoa eteenpäin mm. sosiaalisen median välinein. Tavoitteena on ollut tietämyksen lisääminen, joka on tieteellisen tutkimuksen tavoite. Tutkimus ja kehittäminen risteävät työssä. Toimintatutkimuksessa käytännön ongelmat ja kysymykset ohjaavat osaltaan tietotuotantoa. (Toikko ym. 2019).

Tutkinnon osan sisällöistä sekä hyödynnettävyydestä on pyydetty kohdeorganisaation edustajien kommentteja ja kehitysehdotuksia, jotka ovat olleet avuksi analysoinnissa. Palautteiden ja kehittämisehdotuksien jälkeen tutkinnon osan sisällöt ovat saaneet lopullisen muotonsa. Työ on siis hyvin konkreettinen kehittämistoimi, joka vastaa erinomaisesti kohdeorganisaation tarpeeseen. Tutkimuksen suuntaa antoi myös I2I-hankkeen tavoitteet ja aiheet. Teemat I2I-hankkeesta muodostivat tutkinnon osan osiot, sekä niiden sisällä olevat ajankohtaiset pulmat, joita ratkaisemalla opiskelija suorittaa tutkinnon osan. (IMMUNE 2 INFODEMIC 2023). Tutkimusetiikan osalta käytetään hyvää tieteellistä käytäntöä (Kallinen ym. 2021).

3 Tulokset

Merkittävimpänä tuloksena kohdeorganisaation tiedon lisääntyminen valetiedon osalta. Artikkelin ansiosta tietoa on valetiedosta levitetty myös laajemmin, kuin mitä normaalisti uuden paikallisen tutkinnon osan valmistumisen jälkeen levitetään. Valetieto on kiinnostanut kohdeorganisaation henkilöstöä aiheen ajankohtaisuuden ansiosta. Valetiedon tunnistamisesta laadittua materiaalia on tarkoitus käyttää turvallisuusalan perustutkinnon paikallisena tutkinnon osana sinällään, mikäli opiskelija sen koko laajuudessaan haluaa omiin opintoihinsa sisällyttää. Valetiedon tunnistaminen turvallisuusalan paikallinen tutkinnon osa hyväksyttiin virallisesti Tampereen seudun ammattiopisto Tredun paikalliseksi tutkinnon osaksi 6.9.2023. Liitteenä (liite 1) tutkinnon osan ammattitaitovaatimukset, arviointi ja ammattitaidon osoittamistavat. Hyväksymistä edelsi selvitystyö aiheen sopivuudesta työelämän tarpeita ajatellen, sekä olemassa olevien ammatillisten tutkinnon osien läpi käyminen, jolla selvitettiin, onko ko. aihetta käsitelty missään muussa ammatillisessa perustutkinnossa, jolloin uuden tutkinnon osan laatiminen ei olisi ollut perusteltua. Paikallisen tutkinnon osan hyväksynnän jälkeen Moodleen valmistui ammattitaitovaatimuksia vastaavaa materiaalia, sekä ammattitaitovaatimuksien osoittamistapaa vastaava näyttötehtävä. Tavoitteena on kuitenkin käyttää Moodlessa olevaa materiaalia opetuksessa myös yleisesti hyödyksi ja opiskelijalle tuoda tietämystä ja osaamista valetiedon osalta. Aihe koetaan turvallisuusalan perustutkinnon opiskelijoiden osaamisen kannalta niin oleelliseksi. Kohdeorganisaation opetushenkilöstöä on laajemmin tutustunut valetiedon tunnistamisen tutkinnon osaan ja tutkinnon osan sisältöä on useat kertoneet käyttävänsä jatkossa osittain osana omaa opetustyötään.

Tredun turvallisuusalan opettajien tiimi piti aihetta niin oleellisena turvallisuusalan perustutkinnon opiskelijoiden opintoja, että vaikka opiskelija ei valitse koko tutkinnon osaa omiin opintoihin sellaisenaan, tullaan laadittua materiaalia käyttämään opetuksessa myös muiden ammatillisten tutkinnon osien aikana. Turvallisuusalan perustutkinnon on tutkinnon osissa ammattitaitovaatimuksissa maininta tieto- ja kyberturvallisuuden huomioiminen, jolloin valetiedon tunnistamiseen laadittu materiaali soveltuu näiden tutkinnon osien opetuksen osaksi (Eperusteet 2023). Laaditun tutkinnon osan materiaalia käytetään myös muiden perustutkinnon opiskelijoiden opinnoissa mm. liiketalouden osalta. Äidinkielen opettajien aineryhmässä on aiheesta myös kiinnostunut ja heillä on vaihtelevasti valetieto ollut osana opetusta. Materiaalin laadinnan jälkeen on keskusteluun tullut, pitäisikö tämä aiheena olla osa jokaisen perustutkinnon opiskelijan tutkintoa äidinkielen opetuksen kautta.

Tärkeimpänä tuloksena kohdeorganisaatiossa voi siis nostaa aiheesta nousseen keskustelun. Valetieto ja sen liittyminen ajankohtaisiin tapahtumiin on nostanut kiinnostusta entisestään valmistuneeseen tutkinnon osaan. Kohdeorganisaation ollessa suuri ja laajalle Pirkanmaan alueelle levittynyt, on kuitenkin vielä tiedotuksessa työtä, artikkelin julkaisu auttoi hyvin alkuun.

3.1 Valetiedon tunnistaminen, paikallinen tutkinnon osa

Valetiedon tunnistaminen on viiden (5) osaamispisteen paikallinen tutkinnon osa, joka tarkoittaa sitä, että se on kohdeorganisaation, Tampereen seudun ammattiopisto, Tredun perustutkinnon opiskelijoiden mahdollista omiin ammatillisiin opintoihinsa sisällyttää, mikäli tutkinnon muodostaminen sen sallii (Opetushallitus 2023a). Laajuudeltaan tutkinnon osa ei ole kovin suuri, yleisesti ammatilliset tutkinnon osat ovat viidentoista (15) osaamispisteen tai sitä suurempia. Paikallinen tutkinnon osa voi olla 5-15 osaamispisteen laajuinen. (Eperusteet 2023). Tutkinnon osa toteutettiin verkkototeutuksena, Tredussa verkko-oppimisalusta Moodle käytössä (Tampereen seudun ammattiopisto 2023b). Tämän vuoksi kohdeorganisaatiossa Moodlen käyttö ja siihen tutkinnon osan laatiminen on perusteltua myös siksi, että tällöin opiskelijan ei enää tarvitse oppia uutta verkko-oppimisalustaa, vaan alustan toimivuus ja käytettävyys on tuttua.

Tutkinnon osa on mahdollista suorittaa paikallisesti myös muissa Tredun ammatillisissa perustutkinnoissa, jolloin sen tulee olla selkeä, hyvin ohjeistettu ja omasta ammatillisesta perustutkinnosta huolimatta aiheen käsittely tulee olla mahdollista jokaisen perustutkinnon suorittajalta. Tutkinnon osan alussa pitää olla siis hyvä johdanto, joka auttaa orientoitumaan aiheeseen ja saamaan osallistujat samankaltaiselle lähtötasolle (Marstio 2020). Tutkinnon osaan valituissa teemoissa on vuorovaikutuksen ja kokemusten jakamisen vuoksi keskustelualue aiheen materiaaleista, sekä opiskelijoilla on mahdollisuus jakaa aiheista omia kokemuksiaan. Keskusteluista saadaan myös lisätietoa opiskelijoilta opintojaksosta kokemusten jakamisen

myötä. Jokaiseen teemaan liittyy ajankohtainen aiheeseen liittyvä ongelma tai huijaus, minkä opiskelija ratkaisee. Ongelma on sellainen, mikä on voinut opiskelijan omissa verkkopalveluissa jo esiintyä, näin kokemuksien jakaminen aiheesta onnistuu. Mikäli ongelmaa ei vielä opiskelijan omissa verkkopalveluissa ole vielä esiintynyt, käyvät ne hyvin ennalta ehkäisevästä tiedosta, jolloin opiskelija osaa varautua paremmin jatkossa.

Perustutkinnossa osaaminen näytetään näytöllä ja työelämälähtöisesti, joten tutkinnon osassa on työelämään sijoittuva näyttötehtävä, jossa tutkinnon osassa saatuja oppeja siirretään työelämän käyttöön (Opetushallitus 2023a). Näyttötehtävässä on tarkoitus viedä valetietoon liittyvää tietoisuutta työelämälle ja laatia ohjeistusta valetiedon tunnistamisen suhteen omaan työpaikkaan. Ihannetilanteessa tutkinnon osa suoritettaisiin kootusti ryhmän kera, jolloin yhteiset keskustelut tuottavat mahdollisesti merkittävää lisäarvoa tutkinnon osan suorittamisessa. Ihannetilanteessa myös jokainen uusi teema aloitettaisiin opettajan pitämällä lyhyehköllä noin tunnin alustuksella, jossa alustetaan aihe ja opiskelijoiden on mahdollista esittää ko. teemaan liittyviä kysymyksiä, tai mikäli on aiemmista teemoista jäänyt jotain epäselvää. Opinnot tulee kuitenkin aina olla mahdollista suorittaa myös omaan tahtiin, oman henkilökohtaisen suunnitelman mukaisesti (Marstio 2020). Realistisesti todeten opintojakso todennäköisimmin tulee olemaan yksilöiden omaan tahtiin suorittama, jolloin vuorovaikutteisuutta samaan aikaan aloittavan ryhmän osalta ei ole. Opiskelijoiden keskustelupalstalle jakamien kokemusten kautta tutkinnon osa luo kokemusten ja ajatusten vaihtoa. Opettajan ja opiskelijan välistä vuorovaikutusta myös vähemmän, kuin ihannetilanteessa, kuitenkin opettajan tuki ja apu on kohdeorganisaation verkko-opinnoissa aina oltava saatavilla. Opettajan tuen vuoksi verkko-opinnoissa tulee olla yleinen kysymysalue, jossa opiskelija voi esittää kysymyksiä tai pulmia opintojaksoon ja sen etenemiseen liittyen, näitä hallinnoi ja niihin vastaa opettaja, mutta toki myös kurssin muilla opiskelijoilla on mahdollista omia kokemuksiaan ja tietojaan tuoda esiin. Lisäksi tutkinnon osan suorittajalla tulee olla tieto, kuka opettaja hallinnoi kyseessä olevaa tutkinnon osaa ja keneltä siihen liittyvistä asioista voi kysyä. Info osiossa on perinteisesti arviointiin liittyvää aineistoa, jotta opiskelija pystyy sitä seuraamalla pohtimaan omia tavoitteitaan arvosanan osalta (Marstio 2020). Info osiosta löytyy myös osaamisen arvioinnin suunnitelma, missä kerrotaan mm. arvosanan oikaisemiseen liittyvistä asioista, mikäli opiskelija kokee tälle tarvetta. Opettajalla on kuitenkin päävastuu tiedottaa tutkinnon osaan liittyvistä käytänteistä alusta loppuun, joten henkilökohtaista ohjausta tulee olla tarjolla koko kurssin suoritusajan tarpeen mukaan, oli toteutustapa sitten minkälainen tahansa.

3.2 Palaute

Kohdeorganisaatiolta pyydettiin palautetta valmistuneesta tutkinnon osasta. Palautteita saatiin turvallisuusalan ja liiketalouden perustutkintoa opettavilta opettajilta, sekä äidinkieltä opettavalta opettajalta. Palaute kerättiin ns. avoimesti, eli pyydettiin kertomaan omin sanoin tutkinnon osan hyödynnettävyydestä aloilla tai ainetta opetettaessa.

Turvallisuusalan perustutkintoa opettavat yhdeksän (9) opettajaa näkivät hyödynnettävyyden olevan iso, koska tutkinnon osa antaa laajan ja selkeän käsityksen valetiedosta. Käytettävyys nähdään hyvänä ja tehtävät toimivina. Tutkinnon osaa pidettiin myös ajankohtaisena. Kehittämisehdotuksia tuli joitakin mm. ikkunoiden avautuminen samaan ikkunaan yhden tehtävän osalta. Kehittämisehdotukset huomioidaan ja korjaataan.

Palautetta pyydettiin myös liiketalouden perustutkinnon, sekä aikuiskoulutusta liiketalouden osalta opettavilta kahdelta (2) lehtorilta ja tiimivastaavalta. Liiketalouden tutkinnon uudistuksessa kyberturvallisuuden merkitystä jatkossa korostetaan, eikä valmista materiaalia liiketalouden alalla vielä ole. Valmiiden ammatillisten ja paikallisten tutkinnon osien hyödynnettävyyttä pyritään siis tutkimaan. Liiketalouden palautteessa todettiin, että asiasisältö on heille tärkeä ja kurssipohjaa tullaan hyödyntämään liiketalouden opetuksessa soveltaen. Liiketalouden palautteessa tuli useita erinomaisia kehittämisehdotuksia mukaan mm. käsitteiden ja määrittelyiden parempi avaaminen. Tutkinnon osassa on myös joitakin englanninkielisille sivuille vieviä linkkejä, joiden käyttö koettiin haastavana liiketoiminnan opetuksessa.

Äidinkielen lehtorin palautteessa korostui valetiedon ymmärtämisen merkitys nykyajassa, sekä sen tärkeys myös yhteisten aineiden opetuksessa, jolloin saavutettaisiin suurempi määrä opiskelijoita kohdeorganisaatiossa. Palautteen antanut äidinkielen lehtori totesi omassa opetuksessaan käyttävän noin kaksi (2) tuntia valetiedon käsittelyyn jo tällä hetkellä, sillä kokee aiheen erittäin tärkeäksi ja ajankohtaiseksi. Palautteessa todettiin, että opettajat eivät varmasti kaikki kohdeorganisaatiossa opeta nykyisellään valetiedosta ja sen tunnistamisesta äidinkielen opetuksessa. Palautteen antanut lehtori totesi vievänsä aiheen äidinkielen aineryhmään, tiedustellen kollegoiden mielipidettä aiheen tuomisesta äidinkielen opetuksen osaksi jollakin laajuudella.

Laurea ammattikorkeakoulun opiskelijat tutustuivat myös tutkinnon osaan ja palautekommentteja tuli kolme (3). Heiltä saatujen palautteiden perusteella tutkinnon osan tehtäviä hieman helpotettiin ja yksinkertaistettiin, sopivammaksi kohdeyleisölle. Jokaisessa kommentissa oltiin sitä mieltä, että tutkinnon osan sisältö oli hyvä ja että siitä oli kommentin antaneille opiskelijoille itselleenkin hyötyä. Laurea ammattikorkeakoulun opiskelijoiden palautteissa pääosin opintokokonaisuus sai positiivista palautetta, mutta toisaalta mukana oli kommentti, että linkkejä oli liikaa, sekä että opintojakso sopii 25-30-vuotiaille opiskelijoille. Palautteen mukaisesti sisältöjä suunnataan alkuperäiselle kohdeyleisölle sopivammaksi. Alkuperäinen kohdeyleisö on ollut tutkinnon osaa laatiessa 18-25-vuotiaat opiskelijat. Palautteen mukaisesti osio EU vaalit 2019 muuttuu ajankohtaisia ilmiöitä tai muun opiskelijan mieleen jääneen aiheen käsittelyksi valetiedon osalta. Opiskelijan tulee oma valintaisessa osiossa siis tuoda hänelle valetiedon osalta uusi tai mieleen jäänyt ilmiö esiin. Ajankohtainen ilmiö tässä ajassa voisi olla esim. Itärajan tilanne, jonka nähdään olevan hybridivaikuttamista, jossa valheellisella ja/tai väärällä tiedolla on saatu maahanmuuttajia siirrettyä rajalle pyrkimään Suomen

puolelle. Ajankohtaisena opiskelijan omana aiheena voisi olla myös jokin tietojenkalasteluhuijaus, jossa valheellisella tiedolla pyritään saamaan käyttäjältä käyttäjätunnuksia ja salasanoja. Tutkinnon osa tulee kestämään tämän johdosta aikaa, kun opiskelijan oman mielenkiinnon tai työelämän tarpeen mukainen lisäys tulee huomioitua. Keskustelualueet jokaisen osion kohdalla tuovat lisää mahdollisuuksia sille, että aihe pysyy ajankohtaisena ja tuoreena. Tutkinnon osan päivitystä tulee tehdä vuosittain vastaamaan ajankohtaisia valetietoon liittyviä aiheita ja huijauksia. Palautteiden aikana jatkuvaa parantamista kehittämisehdotuksien osalta tapahtui koko ajan tutkinnon osan Moodlessa. Lopullinen versio tutkinnon osasta on vuoden 2023 loppuun mennessä käytettävissä.

Alun perin tutkinnon osa syntyi I2I-hankkeen teemoista, joista osa on tämän päivän toisen asteen ammatillista koulutusta käyvälle opiskelijalle hieman haastavia (esim. EU vaalit 2019) ja näitä teemoja on helpotettu kohdeyleisölle sopivammiksi. Tutkinnon osa opiskellaan kokonaisuudessa verkossa, jolloin aiheiden tulee olla ajankohtaisia ja nuoria kiinnostavia, tämä varmistaa sen, että tutkinnon osa tulee suoritettua loppuun varmemmin. Tehtävänannot mitoitettiin siten, että työmäärän on vastaa osaamispistemäärää (viisi). Opiskelijat todennäköisesti suorittavat tutkinnon osaa omaan tahtiin, jolloin keskustelualueet eivät toimi vuorovaikutteisesti, kuten alkuperäinen ajatus oli. Keskustelualueet kuitenkin jäävät aiheisiin, jotta saadaan kerättyä kyseisen osion ajankohtaisia teemoja ylös. Näillä toimenpiteillä pyritään saamaan paremmin aikaa kestävä verkossa oleva opintokokonaisuus. Tutkinnon osa on jo tällaisenaan käyttökelpoinen, mutta tutkinnon osaa todellisuudessa tekevien opiskelijoiden mielipidettä vielä toivotaan sen kehittämisessä eteenpäin.

Pedagogisesti käytännön toteutus on hyvin joustava verkkototeutus. Opiskelijoiden tutkinnon osassa olevat tehtävät ovat aitoja huijauksia, joita on voinut tai voi tulla henkilökohtaisessa elämässä tai työelämässä vastaan. Tehtävät tuovat siis valetiedon osalta konkreettisia käytännön esimerkkejä tutkinnon suorittajalle. Näyttötehtävä on erittäin työelämälähtöinen, se tuo valmistuessaan yritykseen koottua tietoa valetiedon osalta. Näyttötehtävälle on valmis täytettävä pohja, vähimmäisvaatimukset eli arvioinnin 1 taso tulee saavutettua kysymyksiin vastaamalla. Arvosanaa nostaa se, miten perusteellisesti on aihetta käsitellyt. Turvallisuusalan perustutkinnon kirjallisissa näytöissä on ollut käytössä valmiita pohjia, joita opiskelija voi halutessaan käyttää. Opiskelija voi myös tehdä näyttötehtävän omalla tavallaan halutessaan, tutkinnon osan arvioinnin kriteeristö määrittelee osaamisen tason. Ammattitaitovaatimuksissa kirjattu opiskelijan osaamisen monipuolinen esittäminen osaamista arvioitaessa nostaa arvosanaa. Arvioinnin kriteeristöä on ammatillisessa koulutuksessa uudistettu ja se on uudistetuissa tutkinnoissa kaikille sama (Opetushallitus 2023b).

3.3 Artikkeli

Artikkelin sisältö kertoo lyhyesti valetiedosta, sekä turvallisuusalan perustutkintoon valmistuneesta paikallisesta tutkinnon osasta. Artikkeli julkaistiin Osaava Tredun artikkelien joukossa, joiden tarkoitus on esitellä erilaista osaamista Tampereen seudun ammattiopistossa. Artikkeli toimi erittäin hyvin tuoden tutkinnon osan laajempaan tietoisuuteen kohdeorganisaatiossa. Artikkelin ansiosta valetiedosta on keskusteltu erilaisissa yhteyksissä (esimerkiksi eri alat ovat olleet aiheesta kiinnostuneita ja toivoneet pääsevänsä tutustumaan tutkinnon osaan ja sen materiaaleihin) ja sen tärkeys on huomioitu eri alojen opetuksessa. Kohdeorganisaation ollessa suuri ja useisiin Pirkanmaan kaupunkeihin toimipisteineen sijoittuva, on artikkeli yksi tavoista saada aihetta laajempaan tietoisuuteen.

Artikkeli on laadittu aiheen markkinointiajatuksena. Artikkelin kirjoitus on myös tapa tiedottaa valetiedosta ja sen merkityksestä ja tehdä lukijat tietoisiksi aiheesta. Artikkeli on enemmän informatiivinen kuin tutkimuksellinen. Artikkeli löytyy liitteenä (liite 2).

4 Valetieto

Valetietoa tarkastellessa tulee erottaa tahalliset ja tahattomat toimet. Voimme välittää valetietoa, koska luulemme siinä hetkessä sen olevan totta omissa sosiaalisen median välineissä, mutta valetietoa myös luodaan ja levitetään haittatarkoituksena. Usein perimmäinen syy on hyötyä jollakin tavalla, taloudellisesti tai luoden mainehaittaa (kosto, pahantahtoisuus). Tutkimuksen mukaan, väärän tiedon uhasta varoittaminen vähentää merkittävästi väärän tiedon vaikutusta. (Karanian, Rabb, Wulff & Race 2020).

Vehkoo on kirjoittanut omassa valheenpaljastaja blogissaan, että ongelman ydin on ihmisen psykologiassa, ei teknologiassa. Joukko psykologisia mekanismeja vaikuttavat meihin ja saavat uskomaan väärään tietoon. Kukaan ei ole näille vaikutuksille immuuni, mutta jos niille tulee tietoiseksi, voi niitä vastustaa. Vehkoon valheenpaljastaja blogista löytyy hänen keräämänsä lista olemassa olevista valemedioista, lista auttaa tiedostamaan, että on olemassa tahoja, jotka tuottavat pelkästään valheellista tietoa (Vehkoo, 2016b; Vehkoo 2019a).

Valetiedon osalta voidaan nähdä olevan hyvin eritasoisia julkaisijoita. Valetieto voi olla harmitonta ja hauskaa. Kuitenkin olemassa on erittäin vaarallisia valetiedon tuottajia, joiden ajatuksena on levittää omaa aatetta ja ideologiaa hinnalla millä hyvänsä eteenpäin, haluten aiheuttaa mahdollisimman paljon harmia ja vahinkoa. Richards on kuvannut visuaalisesti eritasoisia valetiedon tuottajia. Valetiedon tuottajat on jaoteltu Richardsin laatimassa kuvassa niihin mitkä ovat totta; niihin, joista herää kysymyksiä mutta ovat harmittomia; sekä väärää tietoa tuottavia, jotka ovat vaarallisia kaikille. Richardsin tuottaman mallin visuaalinen jaottelu konkretisoi ja kategorisoi valeuutisia selkeästi. Richardsin visuaalisesta mallista löytyy

paljon sellaisia ryhmiä, joiden toimista on uutisoitu myös meillä painetussa lehdissä, sekä muissa medioissa. Richardsin laatimassa mallissa on oleellista huomioida myös se, että valeuutisia ja niiden kautta vaikuttamista on hyvin eri tasoista. Valetiedon osalta on siis ymmärrettävä, että on olemassa ns. harmittomia valetietoa jakavia tahoja ja toisaalta myös mahdollisimman suureen vahinkoon pyrkiviä tahoja. Harmittomienkin valetiedon julkaisijoiden osalta voi tulla yritykselle haittaa, jos levittäjä on erittäin sinnikäs ja vakuuttava. Olemassa on kuitenkin myös erittäin vaarallisia yhteisöjä, joiden levittämät valetiedot voivat luoda pelkoa ja epätietoisuutta lukijassa ja joiden tarkoitus on nimenomaan luoda pelkoa ja epätietoisuutta niin laajasti kuin on mahdollista, jolloin julkaisijan toive olisi, että julkaistu valetieto leviäisi mahdollisimman laajalle. Mallissa on myös nimettynä näitä erilaisia tahoja nimeltä, jotka valetietoa systemaattisesti julkaisevat oman ideologiansa tarkoitusperiin sopivalla tavalla. Mallin avulla nähdään helposti, lähes yhdellä vilkaisulla, keitä tiedettyjä valeuutisten levittäjiä on maailman laajuisesti tiedossa, sekä tietoa heidän vaarallisuudestaan. (Richards 2023).

Valeuutiset voidaan jakaa eri kategorioihin. Kasperskyn mukaan jaottelu voisi olla seuraava: klikkiotsikot; oudot tarinat, vääristyneet kuvat tai sensaationtavoittelu, joka myy ja houkuttelee käyttäjiä avaamaan tarinan, usein näissä ei ole muuta hurjaa kuin otsikko. Propaganda; yleisön harhauttamiseksi, poliittisen agendan tai puolueellisen näkökulman mainostamiseksi on laadittu valheellisia tai vääristeltyjä tarinoita. Heikkolaatuinen journalismi; journalistin virheen tai väärien faktojen vuoksi muodostunut valeuutinen. Heikkolaatuisen journalismin ollessa kyseessä, usein journalisti korjaa virheen ja tiedottaa siitä myöhemmin. Harhaanjohtavat otsikot; sensaatiomaisella tai harhaanjohtavalla otsikolla houkutellaan lukijoita. Joskus juttu voi olla suurilta osin tottakin, mutta otsikkoa jakamalla saadaan johdatettua käyttäjiä harhaan. Huijareitten sisältö; huijauksen tai harhautuksen vuoksi valheelliset ja keksityt jutut, usein imitoivat uutislähteitä. Satiiri tai parodia; viihteenä julkaistu valeuutinen. Nämä eivät pyri huijaamaan, eikä niitä ole tarkoitettu otettavan tosissaan, vaan ne on laadittu huumorilla. (Kaspersky 2023a).

Tutkimuksen mukaan sosiaalinen media mahdollistaa valeuutisten nopean leviämisen. Sosiaalisessa mediassa valeuutiset itseasiassa leviävät paljon nopeammin kuin todelliset uutiset. Valeuutiset ovat tyypillisesti laadittu vetoamaan tunteisiin ja kiinnittämään huomiota, tämä selittää niiden nopean leviämisen. Valeuutiset voivat olla usein omituisia väitteitä ja tarinoita ja ne voivat lietsovat vihaa ja pelkoa. Sosiaalisen median botit massatuottavat ja levittävät artikkeleita verkossa ottamatta huomioon niiden lähteiden luotettavuutta. Botit voivat luoda verkossa valetilejä, jotka saavat seuraajia, tunnustusta ja auktoriteetteja ja näistä osa on voitu ohjelmoida levittämään virheellistä tietoa. Internetin käyttäjissä on myös ns. trolleja, jotka tarkoituksella yrittävät aloittaa riitoja tai suututtaa ihmisiä ja osaltaan myös levittävät valeuutisia. Trolleille voidaan myös maksaa tästä toiminnasta. Poliittiseen päätöksentekoon pyrkiviä vakiintuneista trolliryhmistä käytetään termejä ”trollifarmi” tai ”trollitehdas”. Valeuutiset voivat myös sisältää syvävääreennöksiä. Syvävääreennökset ovat digitaalisella

ohjelmistolla, koneoppimisella ja kasvojen vaihdolla luotuja valevideoita. Kuvia yhdistelemällä luodaan uutta kuvamateriaalia, jotka esittävät tapahtumia ja toimia, joita ei ole oikeasti tapahtunut. Nämä voivat olla hyvin vakuuttavia ja niitä voi olla vaikea tunnistaa valheellisiksi. Valeuutisissa on vaaroja, ihmiset tekevät usein tärkeitä päätöksiä esimerkiksi ketä äänestävät vaaleissa, mitä lääketieteellisiä hoitoja ottavat sairastuessaan, sen perusteella mitä uutisissa sanotaan. (Kaspersky 2023a).

5 Hybridiuhat ja -vaikuttaminen

> ”Hybridiuhissa on kyse pahantahtoisesta ulkoisesta vaikuttamisesta, jolla valtiollinen toimija pyrkii eri keinoja yhdistelemällä systemaattisesti vaikuttamaan kohteena olevaan maahan. Hybridivaikuttamisen tavoitteena on hyödyntää kohteeksi valitun valtion haavoittuvuuksia ja pyrkiä tekemään se mahdollisimman peitellysti. (Sisäministeriö 2023a).”

Hybridivaikuttamisen keinoja voivat olla mm. disinformaatiokampanjat, vaikutusaseman hankkiminen sijoittamalla rahaa liiketoimintaan tai politiikkaan, sekä valtioiden väliset taloudelliset sanktiot. Yritysten rooli suomalaisen yhteiskunnan suojaamisessa on merkittävä, siksi on tärkeää, että yrityksillä on toimiva yhteistyö viranomaisten kanssa hybridivaikuttamisen tunnistamiseksi sekä sen seurausten torjumiseksi. Vesterisen tekemän selvityksen mukaan hybridivaikuttamisen suhteen suurimmat heikkoudet ovat liika avoimuus ja sinisilmäisyys (67 %), kyky tunnistaa liiketoiminnaksi peitelty vaikuttamisyritys tai hanke, jossa yritystä pyritään hyödyntämään, tarkoituksena vaikuttaa varsinaiseen kohteeseen (56 %), liika riippuvuus kansainvälisistä palveluista tai osaamisesta (39 %) ja työntekijöiden tietoisuuden ja valppauden puute (35 %). Kaikkein todennäköisimmin yrityksiltä tehdyn kyselyn vastauksien perusteella, uskotaan rikollisten tai ulkomaisten tiedustelupalveluiden pääsevän yrityksen tietoihin tietojenkalasteluoperaation kautta (78 %), toiseksi suurin vaihtoehto on USB-laitteiden (esim. muistitikku) tai muiden sähköisten välineiden levittämien haittaohjelmien kautta. Tärkeimmiksi varautumisen toimenpiteiksi yritykset totesivat ohjeiden tai toimintamallien laatimisen riskien varalle, urkkimisen tunnistamisen ja tiedon suojaamisen, luottamuksellisiin ja/tai tärkeisiin yritystietoihin pääsyn rajoittamisen, sekä taustatutkimuksien tekemisen ulkomaisten liikekumppanien ja heidän yhteyksien osalta. (Vesterinen 2022).

Suomessa Sisäministeriössä toimii hybridiuhkaverkosto. Kansallisen turvallisuuden yksikkö koordinoi hybridiuhkaverkostossa tehtävää työtä. Verkoston tehtävänä on vastata koko ministeriön toimialaa kattavan uhka-arvion tekemisestä koskien hybridiuhkia yhdessä suojelupoliisin kanssa. (Kytömaa 2023). Sisäministeriö on joutunut marraskuussa 2023 tekemään ratkaisuja Venäjän käynnistäessä välineellistettyyn maahanmuuttoon perustuvan hybridioperaation. Tilanteen johdosta Suomi on sulkenut kaikki rajanylityspaikat Suomen ja Venäjän rajalla 14.1.2024 saakka. (Sisäministeriö 2023b).

Hybridiuhkien torjumiseen on perustettu kansainvälinen, autonominen verkostopohjainen organisaatio, johon voi osallistua kaikki EU- ja Nato-maat, organisaation nimi on Hybrid CoE. Hybrid CoE johtaa keskustelua hybridiuhkista sekä sen keskeisenä tehtävänä on kehittää valmiuksia ehkäistä ja torjua hybridiuhkia. Keskus suunnittelee ja koordinoi työtä Helsingissä sijaitsevan hybridiosaamiskeskuksen sihteeristön kautta. Keskus tekee yhteistyötä eri alan toimijoiden kanssa sekä julkaisee laajasti aiheesta, auttaen näin yrityksiä olemaan tietoisempi hybridiuhkien tilanteesta. (Hybrid CoE 2023).

6 Tietojenkalastelu

Tietojenkalastelulla tarkoitetaan tilannetta, missä tyypillisesti sähköpostilla tai tekstiviestillä pyritään saamaan henkilötietoja, verkkopankkitunnuksia, maksukorttien tietoja tai tietokoneiden ja ohjelmistojen käyttäjätunnuksia (Kilpailu- ja kuluttajavirasto 2023). Mahdollista on myös, että tietojenkalastelun avulla tartutetaan haittaohjelmia laitteille. Tietojenkalastelussa on eri muotoja, kohdennettu tietojenkalastelu eli spear phishing – mikä tarkoittaa isolle joukolle satunnaisesti lähetettyjä viestejä, tekstiviestihuijaukset eli smishing – mikä tarkoittaa että teksti- tai pikaviestipalveluja käytetään kalastelun välineenä, sekä huijauspuhelut eli vishing – puhelimitse tapahtuvia huijauksia. (F-Secure 2023a).

6.1 Tietojenkalasteluhyökkäykset

Tietojenkalasteluhyökkäyksistä suurin osa tapahtuu sähköpostitse, mutta jonkin verran myös tekstiviestitse, tai muiden viestien kautta esim. Messenger tai vastaava, sekä puhelimitse. Tyypillisesti niissä huijataan jakamaan henkilökohtaisia tietoja, tai lataamaan vaarallisia haittaohjelmia. Glamoslijan laatiman oppaan mukaan sähköpostihuijaukset ovat lisääntyneet yli 400%, viime vuosina (Glamoslija 2023). Artikkelissa ei ole täsmennystä viime vuosien määrään, jolloin kyseessä olevaa prosentuaalista lukua voidaan käyttää lähinnä vain suuntaa antavana mielipiteenä. Kyberturvallisuuskeskuksen julkaiseman kybersää toukokuu 2023 tiedotteessa todetaan, että ilmoitukset sosiaalisen median tilien murroista kasvoi räjähdysmäisesti, noin 300%, alkuvuoden keskiarvoon nähden. Kyberturvallisuuskeskus on myös syyskuun kybersään tiedotteessaan julkaissut, että suomalaiset ovat 2023 ensimmäisen puolen vuoden aikana menettäneet verkkohuijauksissa 19,8 miljoonaa euroa. Vuonna 2022 koko vuoden aikana verkkohuijauksissa menetetty euromäärä oli 10 miljoonaa. (Traficom 2023a). Tietojenkalastelu on ehdottomasti eniten käytetty kyberhyökkäysmenetelmä. (Alkhalil, Hewage, Nafaf & Khan 2021).

Tyypillisimmin tietojenkalasteluhuijaus jäljittelee luotettuja brändejä, eli sähköposti näyttää tulleen Applelta, pankista, verovirastolta, poliisilta tms. Kuitenkin usein, jos viestiä tarkistellaan kriittisesti ja rauhassa, siitä löytyy kirjoitusvirheitä, graafisia virheitä tai siinä on

monenlaisia fontteja. Huijauksen aikana käyttäjää pyritään saamaan toimimaan kiireellä ja/tai pelotellaan, että esimerkiksi pankkitili suljetaan, ellei siihen reagoi nopeasti. Sähköposteissa kannattaa ensimmäiseksi tarkistaa sähköpostiosoite, mistä viesti on tullut ja verrata virallisten verkkosivujen yhteystietoihin ennen vastaamista. Huijausviestit voivat myös luvata, että olet voittanut iPadin, ulkomaanmatkan tai suuren summan rahaa, yleensä huijausviestit ovat liian hyvää ollakseen totta ja voi olla, että et muista edes osallistuneesi mihinkään kilpailuun. (Glamoslija 2023).

Kaspersky tutkii vuosittain, miten tietojenkalasteluhyökkäykset jakaantuivat toimialoittain. Vuonna 2022 tehdystä tutkimuksesta käy ilmi, että jakeluyritysten osuus on ollut selvästi suurin, toisena verkkokaupat ja tämän jälkeen maksujärjestelmät ja pankit. Tutkimuksen ja siitä kootun datan suhteen pitäisi omalla toimialalla pohtia onko olemassa jo kohonnut uhkataso tietojenkalasteluhyökkäysten suhteen. Tutkimus ja siitä kerätty data antaa osviittaa siitä, minkälainen tilanne oman toimialan suhteen yleisesti on ja miettiä onko olemassa olevat toimenpiteet riittäviä. Vuosittainen kyberhyökkäyksien kohdistamisen seuraaminen auttaa yrityksiä olemaan tietoisempi riskeistä ja varautumaan niihin oman yrityksensä osalta. Seuranta myös auttaa ennakoimaan, valmistautumaan ja hakemaan yhteistyökumppaneita kyberhyökkäyksistä aiheutuvien ongelmien ratkaisemiseksi ja mahdollisesti jopa myös ennaltaehkäisevästi. (Kaspersky 2023d). Samalla seurannan avulla voidaan varoittaa käyttäjäryhmiä sen suhteen, millä toimialalla nähdään eniten kyberhyökkäyksiä.

F-Secure varoittaa tänä vuonna erityisesti varomaan tietojenkalastelun osalta sosiaalisen median käyttäjätilien kalastelua, suosituimmat alustat ovat olleet Facebook, WhatsApp, Instagram ja LinkedIn. Huijauksissa pyritään saamaan käyttöön esimerkiksi sosiaalisen median tunnuksia, henkilökohtaisia tai taloudellisia tietoja. Esimerkkeinä mainittakoon mm. Netflixin nimissä tulleissa sähköpostiviesteissä vastaanottajalle on ilmoitettu, että maksu on hylätty. Tilanteen korjaamiseksi vastaanottajaa on houkuteltu päivittämään laskutustiedot väärennetyllä kirjautumissivulla. Ukrainan sotaa on hyödynnetty erilaisin sähköpostitse lähetetyin avustuskampanjaviestein, jossa pyydetään lahjoittamaan kryptovaluuttaa. Huijauksissa on käytetty tunnettuja hyväntekeväisyysjärjestöjen nimiä, kuten Punainen Risti. Toisaalta taas on huijattu ottamaan yhteyttä ”kuumiin ukrainalaisiin tyttöihin”, jotka etsivät rakkautta. Uhrit ovat luoneet maksullisen profiilin deittialustalle ja alustalle liittyneitä henkilöitä on käsketty maksamaan enemmän, jotta voivat jatkaa keskustelua. Hei äiti tai hei isä -huijauksissa ovat smishing- eli tekstiviestihuijauksia. Tuntemattomasta numerosta on lähetetty viesti, joka on alkanut Hei äiti tai Hei isä ja on pyydetty kiireellisesti rahaa esim. laskun maksuun tai uuden puhelimen ostamiseen. Pelialustoilla tapahtuu myös tietojenkalasteluhuijauksia, tämän hetken suosituimmat alustat ovat Steam ja Roblox. (F-Secure 2023b).

6.2 Tietojenkalasteluhyökkäyksen todennäköisyys

Todennäköisyyttä joutua tietojenkalastelun uhriksi on tutkittu paljon. Käytännössä kaikki ovat alttiita tietojenkalasteluhyökkäyksille. Tutkimusten perusteella voidaan kuitenkin vetää erilaisia johtopäätöksiä, jotka vaikuttavat siihen, että onnistuuko hyökkäys. KeepnetLabsin mukaan 82% uhkista jää huomaamatta ja 78% kaikista ilmoitetuista haitallisista sähköposteista on peräisin O365- ja Google workspace -käyttäjiltä. Inhimillinen virhe aiheuttaa jopa 90% tietomurroista. Yhteistyötä tehdään yhä vähän ja tietomurroista ilmoitetaan heikosti. Monia uhkia ei pystytä käsittelemään, sillä suurin osa jää havaitsematta. (KeepnetLabs 2023). Williamsin ym. 2018 tekemän tutkimuksen mukaan 18-25-vuotiaat ovat kaikkein alttiimpia tietojenkalastelulle, kuin muut ikäryhmät. Alttius johtuu siitä, että he ovat kaikkein luottavaisempia ja luottavat verkkoviestintään enemmän kuin muut ikäryhmät. (Williams ym. 2018). Tätä ikäluokkaa vanhemmat käyttäjät ovat usein vähemmän impulsiivisia ja siten eivät niin alttiita avaamaan tietojenkalasteluviestiä (Arnsten, Mazure, April 2012). Ihmisillä on tapana työskennellä kiireessä ja stressaantuneina, jolloin he ovat alttiimpia tietojenkalasteluhyökkäyksille. Hadlingtonin tekemässä tutkimuksessa on todettu, että naiset ovat alttiimpia tietoturvahyökkäyksille kuin miehet, mutta toisaalta taas miehet ovat alttiimpia mobiilihyökkäyksille, sillä he luottavat enemmän mobiiliverkkopalveluihin. Motorinen impulsiivisuus, tarkkavaisuuden heikentyminen ja internet-riippuvuus myös altistavat tutkimuksen mukaan sille, että hyökkäys onnistuu. (Hadlington 2017).

Tietojenkalasteluhyökkäykset ovat kehittyneet aiemmista sähköpostilla saaduista huijauksista, jotka sisälsivät useita kielioppivirheitä ja jotka olivat väärin osoitettuja ja niissä pyydettiin suoraan arkaluontoisia tietoja, sekä niistä, joissa hyökkäykset kohdistuivat tiettyihin ihmisiin ja yrityksiin. Hyökkäyksistä on tullut ammattimaisempia, räätälöidympiä ja todelliset aikomukset ovat taitavammin peitelty. (Nurse 2015). Tutkimuksissa on havaittu, että verkkorikollisilla kestää noin 82 sekuntia saada ensimmäinen tietojenkalastelukampanjan uhri ansaan (BBC 2016).

6.3 Tietojenkalastelun seuraukset

Yleisesti voidaan mainita, että tietojenkalasteluhyökkäyksien perimmäisenä tarkoituksena on useimmiten saada taloudellista hyötyä. Cranen artikkelissa on koottu 12 kalleinta tietojenkalastelun esimerkkejä, nämä ovat:

1. 100 dollaria miljoonaa — Facebook ja Google
2. 75 dollaria miljoonaa — Crelan Bank
3. 61 dollaria miljoonaa — FACC
4. 50 dollaria miljoonaa — Upsher-Smith Laboratories
5. 47 dollaria miljoonaa — Ubiquiti Networks
6. 44 dollaria miljoonaa — Leoni AG

7. 31 dollaria miljoonaa — Xoom Corporation
8. 21 dollaria miljoonaa — Pathé
9. 18 dollaria miljoonaa — Tecnimont SpA
10. 17 dollaria miljoonaa — Scoular Company
11. 11,8 dollaria miljoonaa — MacEwanin yliopisto
12. 3 dollaria miljoonaa — Mattel

Kalleimman huijauksen osalta eli Facebook ja Google menetykset tapahtuivat liettualaisen hakkerin lähettämien väärennettyjen laskujen kautta. Hakkeri esiintyi suurena aasialaisena valmistajana, jota ko. yritykset käyttivät. Listan neljä seuraavaa yritystä joutuivat ns. toimitusjohtajahuijauksen uhriksi, eli yhtiöiden talousosastot saivat yrityksen toimitusjohtajan nimissä laskuja tai varojen siirtoon liittyviä ohjeita. Artikkelin perusteella voidaan sanoa, että tietojenkalasteluhyökkäyksellä saadut taloushaitat voivat olla yritykselle erittäin merkittävät. (Crane 2021).

Kyberturvallisuuskeskuksen julkaisussa todettiin, että sillä on tiedossaan Suomessa useita tapauksia, jossa kiristyshaittaohjelma on aiheuttanut merkittäviä kustannuksia organisaatiolle ja ainakin yksi suomalainen yritys on joutunut kokonaan lopettamaan liiketoimintansa näiden johdosta. (Traficom 2023a).

Tietoisuus siitä, miten huijausviestit etenevät, voivat auttaa käyttäjää huomaamaan milloin on joutumassa huijauksen uhriksi. Se, missä vaiheessa hyökkäys on käyttäjälle itselleen vahingollinen, on hyvä myös huomata. Ehdottomasti käyttäjätunnuksia ja salasanoja ei tule luovuttaa missään tilanteessa eteenpäin. Tervettä epäluuloa kaikkea kohtaan on hyvä olla ja vain tietoisuus lisää huijauksien epäonnistumista. (Kuluttajaliitto 2023).

Erilaiset tiedot, mitä hyökkääjä saa käyttäjästä, auttavat taloudellisen hyödyn saamiseksi tai saamia tietoja voi käyttää seuraavassa huijauksessa, tekeytymällä toiseksi. Käytännössä hyökkääjällä on usein taloudellinen hyöty päämääränä, mutta saadakseen taloudellista hyötyä hän voi käyttää siihen saamiaan tietoja, joko seuraavaan huijaukseen tai myydä saamiaan tietoja eteenpäin tai jopa kiristää saamillaan tiedoilla. Tietoja saadaan erilaisten valetietoon perustuvien selitysten ansiosta. Tietojenkalastelu on ehdottomasti eniten käytetty kyberhyökkäysmenetelmä. (Alkhalil ym. 2021).

6.4 Suojautuminen tietojenkalastelulta

Tietojenkalasteluhyökkäyksiltä tehokkain suojautuminen on koulutus. Koulutus sekä tietoisuus on ensimmäinen torjuntamenetelmä, mutta nekään eivät kuitenkaan anna täydellistä suojaa. (Hong 2012). Käyttäjä on suurin riskitekijä, joten on tärkeää olla tietoinen tietojenkalastelusta. Mikäli jokin ei näytä, tunnu tai vaistomaisesti epäilet jonkin olevan pielessä, voi kyseessä olla tietojenkalasteluhyökkäys (F-Secure 2023a). Oleellista on, että yrityksessä

selvitetään mikä tieto on tärkeää liiketoiminnan kannalta, määritellä lähtötila, sekä kriittiset tietotekniset resurssit, sekä yhteistyö palveluntarjoajien ja kumppanien kanssa. Näiden perusteella voidaan tehdä riskikartoitus ja suunnitella tarvittavat toimenpiteet. (Kyberturvallisuuskeskus 2020). Kasperskyn mukaan tärkeintä on henkilökunnan kouluttaminen, sekä tietoisuuden varmistaminen kyberturvallisuuden tärkeydestä. Tiedot tulee varmuuskopioida ja arkaluontoiset ja luottamukselliset tiedot tulee salata. Kybersuojaus on tarkistettava säännöllisesti. Kyberturvallisuuskäytännöt ja ohjelmat, sekä järjestelmät ja palvelimet tulee tarkistaa säännöllisesti suojauksen varmistamiseksi. Käyttämättömät ohjelmat on hyvä poistaa ja etsiä mahdollisia heikkouksia, joita kyberrikolliset voisivat hyödyntää. Pääsyä on hyvä rajoittaa, kaikkien ei ole hyvä päästä kaikkeen tietoon käsiksi. Järjestelmänvalvojan oikeudet tulee olla rajoitetusti käytössä, vain niillä henkilöillä, joilla siihen tarve. Ohjelmistojen asennus vain näiden toimesta. Palomuuri on yksi tehokkaimmista keinoista puolustautua kyberhyökkäyksiltä. Hyökkäyksiä tapahtuu, mikäli ohjelmat, laitteet ja käyttöjärjestelmät eivät ole ajantasaisia, huolehdi siis päivityksistä. Asianmukaiset, järkevät salasanakäytänteet, sekä monivaiheinen tunnistautuminen lisäävät turvallisuutta. (Kaspersky 2023c).

Tietojenkalasteluhyökkäyksien tapoja ja keinoja on olemassa siis monenlaisia. Käyttäjän tarkkaavaisuuden lisäksi on tärkeää, että käytetyt tietokoneet tai mobiililaitteet ovat koko ajan päivitettyinä sekä turvaamiseksi on tehty teknisiä ratkaisuja, joita voivat olla mm. palomuuri, virusturvaohjelmistot, vahvempi käyttäjien tunnistaminen, sekä seuranta. Käyttäjien koulutus, sekä teknisestä turvallisuudesta huolehtiminen hankaloittaa hyökkäysten onnistumista. Valitettavasti usein myös oppiminen hyökkäyksistä toimii opettajana. Oppia voisi kuitenkin myös toisten ratkaisuista, eli aktiivinen seuranta siitä, mitä on liikkeellä, oman yrityksen ulkopuolella on tärkeää. (Alkhalil ym. 2021).

6.5 Tietojenkalastelu ja tekoäly

Kyberturvallisuuskeskuksen toukokuun kyberturvallisuussään tiedotteessa nostetaan pidemmän aikavälin seurattavaksi asiaksi tekoälyn käyttö kyberrikollisuudessa (Traficom 2023a).

Tekoäly ei ole uusi asia, sen tutkiminen aloitettiin Dartmouthin yliopistolla kesällä 1956, josta voidaan sanoa alkaneen tekoälyn moderni historia, historian juuret kuitenkin juontavat jo antiikin aikoihin 400-301 Ekr (Mäntylä 2023). Pahantahtoiset toimijat ja innovaattorit pyrkivät kummatkin parantamaan toistensa työtä (Enisa 2023). Tekoälyllä tarkoitetaan koneen kykyä käyttää perinteisesti ihmisen älyyn liitettyjä taitoja, kuten päättelyä, oppimista, suunnittelemista ja luomista (Guillot 2023).

Valeuutiset voivat sisältää syvävääreennöksiä. Syväoppiminen on edistynyt tekoälymenetelmä. Syväoppiminen käyttää koneoppimisen algoritmeja usealla tasolla ja poimii raakamateriaalista progressiivisesti korkeamman tason ominaisuuksia, tämä mahdollistaa sen, että se kykenee oppimaan jäsentämätöntä dataa, kuten ihmiskasvoja. Tekoäly pystyy keräämään tietoja

fyysisistä liikkeistäsi. Syvähuijauksen hyvä esimerkki on näyttelijä Jordan Peelen varoittavaksi esimerkiksi luoma video Barack Obamasta, jossa hän itse esittää Obamaa. Videolla hän näyttää, miten kaksi erillään olevaa videota sulautetaan yhdeksi. Syvähuijausvideoita on käytetty lisääntyvässä määrin mustamaalaus- ja petostapauksissa, niitä on käytetty myös poliittisiin tarkoituksiin sekä henkilökohtaiseen kostoon. Syvähuijausvideoiden aiheuttamia uhkia on ryhdytty käsittelemään lainsäädännössä, esim. Kaliforniassa on hyväksytty kaksi lakisäädöstä, jotka tekivät syvähuijauksen tietyt osat laittomiksi. Lakisäädös AB-602 kieltää ihmisen kuvien syntetisoinnin pornografian tekemiseksi ilman kuvissa esiintyvien henkilöiden lupaa. Säädös AB730 kieltää poliittisten ehdokkaiden kuvien manipuloinnin 60 päivää ennen vaaleja. Kyberturvallisuuteen erikoistuneet yritykset kehittävät parempia tunnistusalgoritmeja. Nykyiset syvähuijaussyntetisaattorit mallintavat kaksiulotteiset kasvot ja väärentävät ne sopimaan kolmiulotteiseen perspektiiviin. Helpoiten väärennöksen huomaa tarkkailemalla mihin suuntaan henkilön nenä osoittaa. Muita syvähuijausvideoiden ominaisuuksia on liikkeiden nykiminen, valaistuksen muutokset kuvien välillä, ihonvärin muutokset, outo silmien räpsyttely tai ei lainkaan silmien räpsyttelyä, huulet eivät mukaile puhetta ja/tai kuvan sisältämät digitaaliset virheet. Syvähuijaus kehittyy kuitenkin koko ajan edelleen paremmaksi. (Kaspersky 2023b).

Gartnerin haastattelussa vara-analyytikko Avivah Litanin kertoo että, generatiivinen tekoäly aiheuttaa yrityksille uusia riskejä. Tekoälyn chatbot-ratkaisut ovat uskottavampia ja niihin luotetaan, tämän vuoksi virheellisiä, vääriä ja puolueellisia tietoja on vaikea havaita. Syväväärennökset, joiden avulla väärennetään kuvia, videoita ja äänitallenteita ja näitä voidaan käyttää hyökkäämään julkkiksia ja poliitikkoja vastaan. Väärennöksillä pyritään levittämään ja luomaan harhaanjohtavaa tietoa ja jopa luomaan väärennettyjä tilejä tai murtautumaan olemassa oleville laillisille tileille. Tietosuojan osalta on haasteellista, kun generatiiviset tekoälypohjaiset tekoälybotit tallentavat loputtomasti käyttäjän syötteiden kautta kaapattuja tietoja ja jopa käyttävät tietoja muiden mallien kouluttamiseen. Työntekijät voivat helposti paljastaa arkaluonteisia ja omistusoikeudellisia yritystietoja. Ongelmallisia ovat myös tekijänoikeuskysymykset, ilman lähdeviitteitä tai läpinäkyvyyttä miten generatiivisen tekoälychatbotin tuottamaa materiaalia käytetään, on mahdollista, että nämä tekoälychatbotin luomat tuotokset rikkovat tekijänoikeuksia tai immateriaalioikeuksien suojaa. Kyberturvallisuuteen liittyy huolenaiheita, sillä hyökkääjät voivat käyttää haitallisen koodin luomisen helpottamiseen ChatGPT:tä, koskien mm. tietojenkalastelua tai kehittyneempää sosiaalista manipulointia. Yritysten tulisikin valvoa ChatGPT:n käyttöä olemassa olevilla turvatarkastuksilla ja koontinäytöillä käyttörikkomusten havaitsemiseksi. (Rimol 2023).

EU-jäsenmaat ovat hyväksyneet tekoälyasetuksen. Asetuksen tavoitteena on luoda yhteiset pelisäännöt, siten että tekoälyn käyttö on turvallista kaikille yrityksille ja ihmisille. Asetuksella kielletään tietyt haitalliset käyttötapaukset, esim. ihmisten sosiaalinen pisteytys tekoälyn avulla. Asetuksella on tarkoitus säädellä myös tekoälyjärjestelmien markkinavalvontaa sekä tekoälyn sääntelyn testiympäristöjä. (Alanko & Hauptmann 2022).

Kyberturvallisuuskeskus on tutkinut tekoälyn mahdollistamia kyberhyökkäyksiä ja pohtinut tulevaisuuden skenaarioita eteenpäin. Sen mukaan lyhyellä aikavälillä tekoälyä ei luultavasti sisällytetä haittaohjelmiin itsenäisesti, sillä tekoälyyn pohjautuvien ohjelmien kehittäminen on monimutkainen prosessi. Keskipitkällä 2-5 vuoden aikavälillä tekoälyn mahdollistama tiedonkeruu ja avoimista lähteistä tiedon louhinta muodostuu uskottavaksi uhaksi. Pitkällä aikavälillä eli yli 5 vuoden kuluttua, tekoälyn mahdollistama hyökkäysten joustavuus, sekä vaikeasti havainnoitavuus dataa generoivien mallien avulla ja itsenäiset haittaohjelmat ovat mahdollisia. Samaan aikaan kuitenkin tekoälyä kehitetään havaitsemaan ja analysoimaan mahdollisia hyökkäyksiä ja torjumaan niitä. (Traficom 2023b).

Tekoälyn riskienhallintaa on standardoitu, ISO ja IEC ovat perustaneet yhteisen teknisen komiteansa alakomitean ISO/IEC JTC 1/SC 42 standardisoimaan tekoälyn käyttöä. Alakomitean tekoälyn luotettavuuden työryhmä (WG) 3 työskentelee useiden etiikkaan, riskiin ja vikasietoisuuteen liittyvien hankkeiden parissa. Alakomitea on kesällä 2021 ilmoittanut työstävänsä seuraavia standardeja (suomenkieliset nimet epävirallisia käännöksiä):

- ISO/IEC 23894, Riskienhallinta
- ISO/IEC 24028, Katsaus tekoälyn luotettavuuteen
- ISO/IEC 24029, Neuroverkojen vikasietoisuuden arviointi
- ISO/IEC 24368, Katsaus eettisiin ja yhteiskunnallisiin kysymyksiin
- ISO/IEC 5469, Toiminnallinen turvallisuus (safety) ja tekoälyjärjestelmät

Standardoimista on tapahtunut myös maaliikenteen, merenkulun, ilmailun sekä muuta sektorikohtaista säätelyä mm. datapohjaisille terveyteen liittyville järjestelmille. (Traficom 2023c).

7 Tulevaisuus

Datatalouden uskotaan kuluvan vuoden 2023 aikana EU:ssa kasvavan yli 600 miljardiin. Suomen osuus tästä arvioidaan olevan noin 9 miljardia. EU:n datan kaupallistamisen on arvioitu kasvaneen tällä vuosikymmenellä jopa 30 prosentin vuosivauhtia. Suomen lähes puolta pienempi kasvuluku on herättänyt huolta Suomen kyvystä tuottaa arvonlisää datalla palveluina, tuotteistamalla tai vaihdantana. Kasvua hidastaa pula dataosaajista. Osaamisen puute näkyy myös siinä, että suomalaisista yrityksistä vain 12 prosenttia ilmoittaa hyödyntävänsä tekoälyä. Osaamisen puutteen lisäksi esteinä nähdään ongelmat ohjelmien ja järjestelmien yhteensopivuudessa sekä datan saatavuudessa ja laadussa. Datayhteistyö organisaatioiden välillä on vasta kehittymässä. Data-avaruudet ja dataekosysteemit kasvavat voimakkaasti, mutta tieto niistä on vielä hajanaista ja rajallista. Ekosysteemisyyden arvo syntyy perinteiset arvoketjut

ylittävissä yhteenliittymissä ja palvelukokonaisuuksissa ja haastaa liiketoimintamallien lisäksi taloudellisen toiminnan mittaamisen. (Rastas 2023).

Euroopan digitaalisen median seurantakeskus (EDMO) julkaisee kuukausittain tiedotteen faktantarkistuksen osalta. Kesäkuun tiedotteessa on todettu, että tällä hetkellä tekoälyn luoma disinformaatio on alhaista ja vakaata, kesäkuun osalta 4% kaikesta havaitusta disinformaatiosta oli tekoälyn tuottamaa ja muuta 96%. Tekoälyn tuoma väärä tieto perustui enimmäkseen kuviin, tästä esimerkkinä Elon Musk suutelemassa naisrobottia. (EDMO 2023).

Supersovellusten päivittäisiä ja aktiivisia käyttäjiä on Gartnerin ennusteen mukaan vuoteen 2027 mennessä yli 50% maailman väestöstä. Organisaatiot, jotka hallitsevat aktiivisesti tekoälyn riskejä, yksityisyyttä ja tietoturvaa, saavuttavat parempia tekoälyprojektien tuloksia. Organisaatioiden tulisi ottaa käyttöönsä uusia ominaisuuksia luotettavuuden, tietoturvan ja tietosuojan varmistamiseksi. Tämä edellyttää, että koko yritys osallistuu yhdessä toimenpiteiden toteuttamiseksi. Digitaalisen immuniteetin rakentamiseen investoiminen vuoteen 2025 mennessä vähentää järjestelmän seisokkeja jopa 80% ennustaa Gartner. Digitaalinen immuunijärjestelmä yhdistää dataan perustuvan näkemyksen toiminnasta, automatisoidusta testauksesta, automatisoidusta tapahtumien ratkaisemisesta, ohjelmistosuunnittelusta IT-toiminnoissa ja sovellusten toimitusketjun turvallisuudesta järjestelmien joustavuuden ja vakauden lisäämiseksi. (Rimol & Howley 2022).

Perinteiset sähköpostilla tapahtuvat tietojenkalasteluhyökkäykset ovat muuttuneet sosiaalisen median pohjaiseen tietojenkalasteluun. Tutkimus sosiaalisen median, äänitietojenkalastelun sekä tekstiviestien osalta on vähäistä, mutta näiden uhkien ennustetaan lisääntyvän merkittävästi seuraavien vuosien aikana. (Alkhalil ym. 2021).

Julkaisemattoman tutkimuksen mukaan tekoälyä mahdollisesti kehitetään olemaan sellainen, että se estäisi jakamasta väärää tietoa ja loukkaavia kommentteja, joka tietysti disinformaation kitkemisen kannalta on positiivinen uutinen. Mallin GBT-4 kesäkuun 2023 uusissa testeissä havaittiin, että sen vastaukset olivat vähemmän monisanaisia sekä siitä oli tullut turvallisempi, kuin minkälainen se oli ollut saman vuoden maaliskuussa. (Leffer 2023).

8 Pedagogiset ratkaisut

Uuden opintojakson laatiminen alkaa aina suunnittelulla. Opintojakson laatijalla tulee olla tavoite ja tieto siitä, mitä osaamista opintojakson jälkeen opiskelijalla tulisi olla, vastaako työmäärä osaamispisteitä, sekä onko opintojakso opiskelijan tutkinnon mukaisen vaatimustason mukainen. Suunnittelun jälkeen valitaan menetelmät ja työskentelytavat, millä tavalla saadaan digitaaliselle alustalle luodusta opintojaksosta vuorovaikutteinen ja työelämälähtöinen. Sisältöä ja materiaalia tuotetaan siten, että opiskelijalla on mahdollisuus tutustua aiheeseen

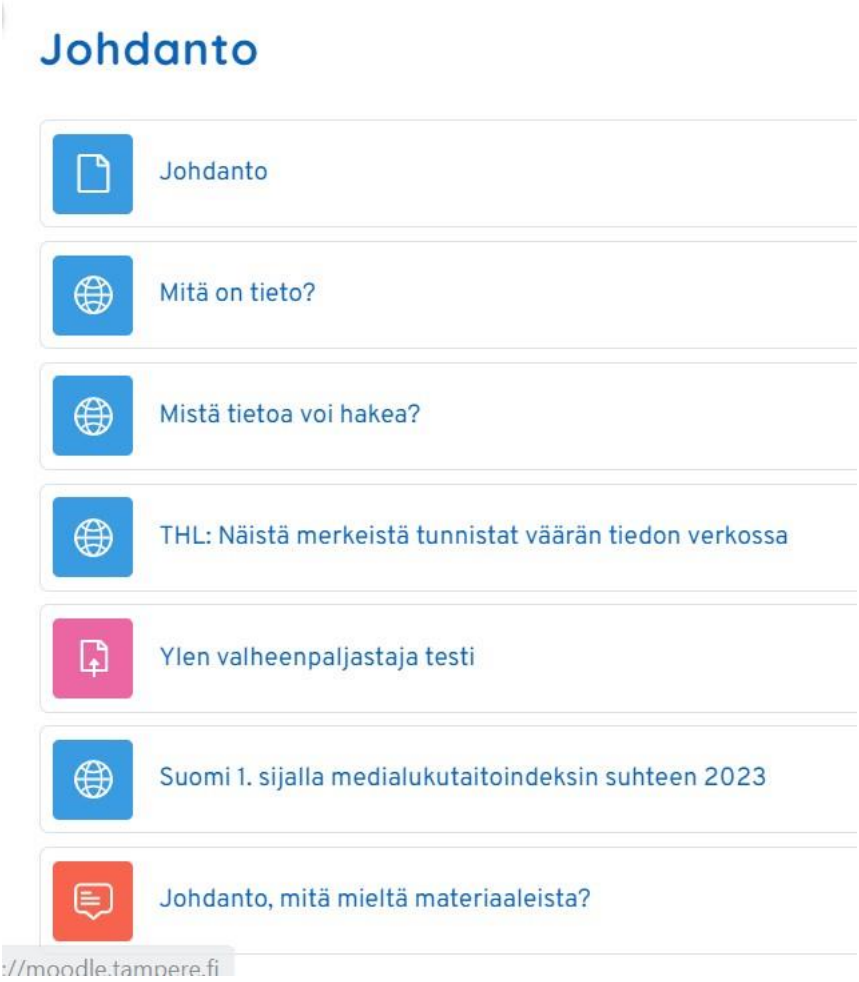
tarpeeksi monipuolisesti tutkinnon osan puitteissa ja saada uutta osaamista opintojakson aikana. (Tampereen yliopisto, Tampereen ammattikorkeakoulu 2023). Oppimisympäristön valinta kohdeorganisaatiossa oli selvää, sillä käytössä Moodle (Tampereen seudun ammattiopisto 2023b). Etukäteen oli tärkeää suunnitella, miten materiaali viedään Moodleen, jotta se on selkeää ja opiskelijalla on mahdollisuus edetä kurssilla siten, että oppimisympäristö ei ole liian haasteellinen. Ja lopuksi, miten opintojakson suorittaminen arvioidaan, sekä ohjeistus sillä tasolla, että opiskelija myös tietää opintoja tehdessään mihin arvosanaan hänen tekemänsä työ voi yltää. (Tampereen yliopisto, Tampereen ammattikorkeakoulu 2023). Opiskelijoilla on jo lähtökohtaisesti hyvät valmiudet opiskella verkossa. Omaan tahtiin suoritettavien verkko-opintojen tulee kuitenkin olla erittäin selkeästi ohjeistetut ja ongelmatilanteissa pitää olla mahdollisuus saada mahdollisimman pian vastauksia esiin tulleisiin ongelmiin. Kohdeorganisaatiossa verkossa tapahtuvassa oppimisessa tulee olla opettajan tuki tarjolla.

Pedagogiseksi ratkaisuksi tehtävien osalta on päädytty ongelmalähtöiseen oppimiseen, sillä se sopii hyvin verkko-opintoihin itseohjautuvuuden ja tosielämän tilanteita jäljittelevällä tavalla oppia. Tehtävien tueksi on laadittu materiaalia ja annettu verkkolinkkejä, joten mikäli opiskelija innostuu aiheesta enemmän, on hänellä mahdollisuus laajentaa osaamistaan mielenkiintonsa mukaisesti, mutta vähintään suoriutua annetuista tehtävistä. Verkko-opintojen hyvä puoli on se, että opiskelija voi omaan tahtiin, omassa paikassaan keskittyä ja tehdä tehtäviä oman aikataulun mukaisesti. Tarkoitus on, että opiskelijoilla on ryhmän tuki, sekä säännölliset tapaamiset opettajan kanssa, jotta opettaja voi auttaa esiin tulevien kysymysten kanssa, mahdollisesti innostaa tehtävien tekemiseen ja auttaa pulmissa opintojakson suorittamisen suhteen. (Marstio 2020). Omaan tahtiin tekeminen on kuitenkin mahdollistettava selkeällä työskentelyalustalla.

9 Tutkinnon osan sisältö

Valetiedon tunnistaminen on viiden (5) osaamispisteen turvallisuusalan perustutkinnon paikallinen tutkinnon osa, joka on laadittu verkko-opiskelualusta Moodleen. Paikallinen tutkinnon osa tarkoittaa sitä, että Tampereen seudun ammattiopisto, Tredussa, perustutkintoa opiskeleva opiskelija voi sen sisällyttää opintoihinsa, mikäli hänen oman perustutkinnon muodostuminen sen sallii. Tutkinnon osa on laadittu turvallisuusalan perustutkintoon, mutta on tutkinnon muodostumissääntöjen puitteissa yhtä hyvin käytettävissä kaikkien alojen perustutkintoa opiskelevien opiskelijoiden opintoihin. Henkilökohtainen opiskelun kehittämissuunnitelma mahdollistaa opiskelijalle hänen henkilökohtaisen tavan koostaa oma tutkinto. Perustutkinnon opiskelijalla on usein perustutkinnon muodostumissäännön mukaisesti mahdollista sisällyttää omaan perustutkintoon tutkinnon osa toisesta tutkinnosta, sekä paikallisia tutkinnon osia 5-15 osaamispisteen verran.

Tutkinnon osan Moodleen on ollut kehitysvaiheessa mahdollisuus päästä vieraana, tämä ominaisuus poistuu, kun opiskelijat aloittavat tutkinnon osan suorittamisen, siksi ohessa joitain kuvankaappauksia sisällöstä. Kuten usein, tutkinnon osa alkaa johdanto -osiolla, jossa opiskelija pääsee aiheeseen orientoitumaan suoritettavaan tutkinnon osaan ja sen tehtävänä on pyrkiä saamaan opiskelijat samanlaiselle lähtötasolle tutkinnon osan suorittamisen aloittamisen suhteen, perustutkinnosta riippumatta. Johdannon sisältönä on tiedot tutkinnon osan käytännön suorittamisesta, valetiedon tunnistamiseen liittyvää yleistä ohjeistusta sekä mielipiteiden keräämistä aloituksen materiaalien osalta. Johdannon jälkeen, jokainen osio on oma kokonaisuutensa, sisältäen johdannon, linkkejä aiheeseen, keskustelualueen, sekä osioon liittyvän ongelmanratkaisutehtävän. Tutkinnon osassa on oma työelämälähtöinen näyttötehtävä, laatia valetietoon liittyvää ohjeistusta opiskelijan todelliseen tai kuvitteelliseen työpaikkaan.



Kuva 1: Johdanto

Johdannon tehtävä on saada opiskelijat samalle lähtötasolle. Johdannon osiossa orientoidutaan aiheeseen tiedon osalta, mitä se on ja mikä on tiedon merkitys yksilön kannalta

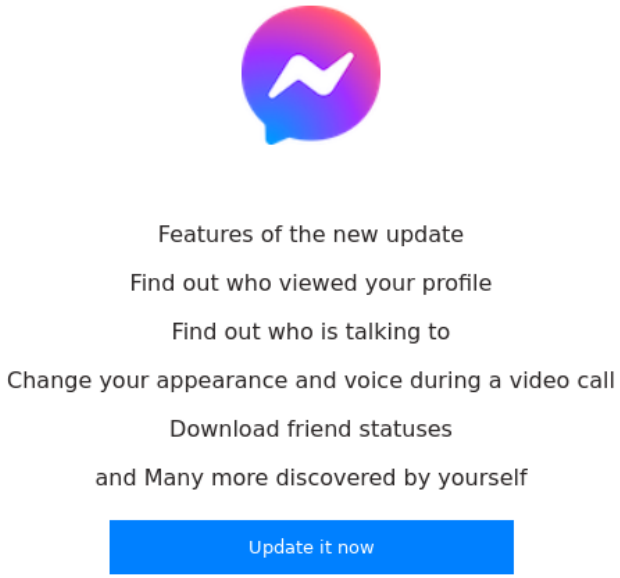
sekä yritystoiminnassa. Johdannossa on myös Ylen valheenpaljastajatestiin linkki, joka on osa aiheeseen orientoitumista tutkinnon osan sisältöön, valetiedon tunnistamiseen.

Jokaisella eri tehtäväosioilla oma aihekohtainen kokonaisuutensa herättämään ajatuksia kyseisen aiheen osalta. Sosiaalisen median osalta sisältönä on aiheita, jotka voivat opiskelijan omaa sosiaalisen median käyttämistä laittaa pohtimaan, sekä tekemään tarkastuksia. Sosiaalisen median osion osuus on laajahko, johtuen siitä, että se on aiheista kohderyhmää ajatellen tutuin ja toisaalta se missä valetietoa tulee opiskelijoille todennäköisimmin vastaan.

Kuva 2: Sosiaalinen media

Erilaiset tahot esimerkiksi Kyberturvallisuuskeskus ja Kuntaliitto, ovat jo kiinnittäneet huomiota turvalliseen sosiaalisen median käyttämiseen, ohjeistuksia löytyy hyvin valmiina. Tehtävien tekeminen vaatii näihin ohjeistuksiin tutustumista. Luotettavien tahojen hyvää ohjeistusta on kannattavaa käyttää, ennemmin kuin laatia omaa, mikäli sitä on olemassa. Valmiit ohjeistukset tulevat opiskelijoille tutuiksi, kun tehtävien tekemisen osalta niitä tarvitaan. Osiossa on joitain esimerkkejä turvallisuuden lisäämiseen sosiaalisen median palveluissa ja

omien sosiaalisen median alustojen ja julkaisujen turvallisuuden lisäämiseen. Osiosta löytyy myös keskustelualue sosiaalisen median osalta, täällä on tarkoituksena jakaa hyviä käytänteitä, vinkkejä sekä kokemuksia. Sosiaalisen median tehtävän tarkoitus on olla jokin oikea, lähiaikoina liikkeellä ollut sosiaalisen median palveluissa ollut huijaus. Ensimmäisenä sosiaalisen median tehtävänä on Messengerin päivitysilmoitus, joka on ns. liian hyvää ollakseen totta. Kyseinen huijaus on ollut 2023 vuonna liikkeellä Messengerin käyttäjien keskuudessa. Kyseessä on siis aito olemassa oleva huijaus.



Kuva 3: Sosiaalinen media, tehtävä

Tehtävä on seuraava: Facebookin Messenger pyytää päivitystä ja vaatii yllättäen tätä varten käyttäjätunnusta ja salasanaa. Lisäksi päivitys lupaa, että voisi muun muassa muuttaa käyttäjän ulkonäköä ja ääntä videopuheluiden aikana ja seurata, sekä päivityksen jälkeen kertoa kuka on katsellut profiilia. Innostut asiasta, mutta sitten alatkin pohtimaan, että onko tämä totta vai huijaus. Miten on? Huijataanko tällä, vai voiko tämä olla totta. Tehtävänantona on pohtia myös mitä motiiveja tällä huijauksella voisi olla.

Paikallinen tutkinnon osa Valetiedon tunnistaminen 5 osp on siis verkossa, Moodle verkko-oppimisympäristössä ja mahdollista suorittaa myös omaan tahtiin. Muita osioita sosiaalisen median lisäksi on painettu media, kriittinen infrastruktuuri, EU vaalit 2019, sekä kyberhyökkäykset. Jokainen osio mukailee sosiaalisen median osion mukaista etenemistä. Osiosta löytyy siis lyhyt alustus aiheeseen, aiheen mukaisia linkkejä, joiden käytössä suositaan valmiita hyviä ja selkeitä ohjeistuksia, keskustelualue, jossa voi keskustella aiheen mukaisista kokemuksista ja näkemyksistä, sekä ongelmaratkaisutehtävä aiheesta. Osion tehtävä on herättää opiskelijoissa

sen osion aiheen mukaisesti ajattelemaan valetietoa ja sen merkitystä. Tehtäviä tekemällä opiskelija tutustuu erilaisiin kyberturvallisuuden toimijoihin ja heidän laatimiin ohjeisiin, jotta voi tehtävät tehdä. Opiskelija oppii samalla käyttämään luotettavia lähteitä ja hankkimaan luotettavaa valmista ohjeistusta.

Tutkinnon osan osiot voi suorittaa missä järjestyksessä tahansa, eli opiskelija voi johdanto osion jälkeen suorittaa osiot haluamassaan järjestyksessä, vaikka oman mielenkiinnon mukaan, mutta kaikki osiot tulee tehdä. Jokaisessa osiossa on käytännössä kaksi tehtävää, jotka tulee tehdä. Ensimmäinen tehtävä on keskustelu aiheesta, keskusteluun voi tuoda jotain uutta tai mieleen jäänyttä aiheen tiimoilta ja toisena tehtävänä ongelmanratkaisutehtävä, jossa opiskelija on joko omana opiskelija minänään ratkaisemassa pulmaa, tai yrityksen turvallisuudesta vastaavana henkilönä. Opiskelija voi yritykselle näin tuottaa jokaisen osion mukaista materiaalia ja ohjeistusta jo ennen varsinaista näyttötehtävää.

Moodlessa olevassa näyttö osiossa on paikallisen tutkinnon osan näyttöön liittyvää ohjeistusta, sekä linkkejä, jotta ohjeistuksen voi laatia laadukkaasti. Osiosta löytyy myös näyttöpohja, jolle työelämälle suunnatun ohjeistuksen voi laatia. Pohja on laadittu siten, että on mahdollista sen täyttämällä saavuttaa arvioitava osaaminen taso yksi (1). Perusteellisemmalla valmiin pohjan täyttämisellä arvosanan saaminen hyvän ja kiitettävän tasolle on mahdollista. Näyttöpohjassa on erilaisia kysymyksiä aiheeseen valetietoon ja sen tunnistamiseen liittyen, joihin vastaamalla osaamisen taso saavutetaan. Vastaamiseen on annettu useita hyviä linkkejä ja mitä monipuolisemmin opiskelija on annettuja ohjeistuksia käyttänyt, sen parempi arvosana hänelle on mahdollista antaa, sillä osaamisen voi täten näyttää laajempana.

Moodlessa olevassa info osiossa on tutkinnon osan arviointiin liittyviä asioita. Osiosta löytyy myös ammattitaitovaatimukset ja arvioinnin kriteerit sekä Turvallisuusalan perustutkinnon osaamisen arvioinnin toteutussuunnitelma. Turvallisuusalan perustutkinnon osaamisen arvioinnin toteutussuunnitelmassa on paljon tietoa turvallisuusalan perustutkinnon suorittamisesta yleisesti. Osaamisen arvioinnin toteutussuunnitelmassa kerrotaan mm. osaamisen tunnistamisesta ja tunnustamisesta, työpaikalla tapahtuvan oppimisen arvioinnista, sekä arvosanoista mm. uusimisesta ja korottamisesta.

9.1 Sosiaalinen media

Ihmiset käyttävät sosiaalista mediaa erittäin aktiivisesti, Pandasecurity listasi jo vuonna 2018 että Facebookilla oli yli 2 miljardia käyttäjää, Instagramilla 1 miljardia käyttäjää ja LinkedIn 590 miljoonaa käyttäjää. Määrät ovat tästä kasvaneet huomattavasti. Internetiä käytti vuonna 2021 4,66 miljardia ja sosiaalisten verkostojen käyttäjien määrä oli 4,2 miljardia. Tammikuussa 2021 maailman väkiluku on 7,83 miljardia (Stanislavsky 2021). Käyttäjämäärien ja sosiaalisen median alustojen kehittyminen sekä lisääntyminen tekee sen, että sosiaalisen median käyttäjiä tavoitetaan erittäin suuri määrä kerralla nopeasti. Käyttäjät myös lataavat paljon

tietoa itsestään alustoille, tämä tieto on erittäin käyttökelpoista esim. tietojenkalasteluhyökkäystä ajatellen. Hyökkääjä saa paljon sellaista tietoa käyttäjästä, joka helpottaa huijausten läpimenoa. Vastaisuudessa tekoälyn käyttö tulee mahdollisesti vaikuttamaan siten, että tietojen keräämisen tehokkuuden ja sen jäsentelyn, sekä suoran käyttökelpoisuuden vuoksi, kyberhyökkäykset tulevat olemaan enemmän henkilökohtaisia ja paremmin suunnattuja.

Calabrese on laatinut ohjeita sosiaalisen median valeuutisten havaitsemiseen. Ohjeiden tarkoitus on, että sosiaalisen median valeuutiset havaitaan, jolloin niiden jakaminen jätetään tekemättä ja valeuutiset raportoidaan sivuston ylläpitäjälle niiden poistamiseksi. Calabresen mukaan paras neuvo on, että käyttäjä pysähtyy hetkeksi miettimään ennen uutisen jakamista eteenpäin ja pohtii mm. seuraavia asioita, kuka loi tai jakoi uutisen, onko sen luojan/jakajan alkuperäinen tili. Artikkelin/sisällön osalta; milloin se on luotu ja miksi se on jaettu. Ennen uutisen jakamista on hyvä tarkistaa vähintään edellä mainitut asiat. Artikkelissa mainitaan ilmainen faktantarkistustyökalu Bellingcat, joka suorittaa visuaalista tutkimusta verkossa ja joka on voittoa tavoittelemattoman järjestön ylläpitämä. Suurin osa valeuutisista voidaan kuitenkin hylätä käyttämättä mitään faktantarkistustyökalua, kysymällä onko uutinen totta ja harkitsemalla ennen kuin jaamme sen. Ongelmana on, että käyttäjä vaistomaisesti painaa jakopainiketta. (Calabrese 2020). Faktantarkastusohjelmat jäävät monelta peruskäyttäjältä käyttämättä, mutta jo harkitsemalla ja kysymällä edellä mainittuja kysymyksiä, voidaan välttää ainakin osa valeuutisten leviäminen. Käyttäjien tulee vastaisuudessa kyseenalaistaa enemmän internetissä tai verkossa löytämäänsä tietoa ja osata arvioida sen oikeellisuutta tai vähintään jättää jakamatta uutinen, mikäli epäilee sen oikeellisuutta.

Kyberrikollisille sosiaalinen media on erinomainen tietolähde. Sosiaalisessa mediassa jaetut tiedot ovat merkittävässä osassa taustatietoja kerätessä. Käyttäjän manipulointi (social engineering) on metodi, jolla kyberrikollinen saa käyttäjän tekemään asioita, joita hän ei normaalisti tekisi. Yleisin manipuloinnin tapa on tietojenkalasteluhyökkäys. (Lehto, Limnell, Innola, Pöyhönen, Rusi & Salminen 2017). Tulevaisuudessa sosiaalisen median käyttäjien tulee pohtia minkälaisia henkilökohtaisia tietoja lisään erilaisiin sosiaalisen median verkostoihin, koska se voi johtaa siihen, että tekoälyllä on mahdollisuus poimia sellaisia henkilökohtaisia tietoja, joiden avulla on parempi mahdollisuus onnistua manipuloimaan käyttäjä erehtymään tietojenkalasteluhyökkäyksen uhriksi.

Traficomin julkaiseman kybersään toukokuun 2023 tiedotteessa todetaan, että ilmoitukset sosiaalisen median tilien murroista kasvoi räjähdysmäisesti, noin 300%, alkuvuoden keskiarvoon nähden (Traficom 2023a). Sosiaalinen media on siten aiheena tutkinnon osan osalta lähes välttämätön, kohderyhmän käyttäessä sosiaalisen median palveluita ahkerasti. Sosiaalisen median osalta myös erilaisten käytännön esimerkkien esittäminen on perusteltua tutkinnon osaa suorittaessa. Tehtävänanto voi antaa samalla ajankohtaisen varoituksen huijauksista, ellei tehtävän sosiaalisen median huijaus ole vielä opiskelijalle tuttu.

9.2 Painettu media

Uutismedian liiton tuoreen tutkimuksen mukaan suomalaisten mielestä sanomalehdet (painettu ja digitaalinen) ovat yhä luotettavin media. Tutkimuksen mukaan kuitenkin 29 % vastaajista törmää valeuutisiin viikoittain. Nuoremmat vastaajat, alle 25-vuotaat kokevat törmäävänsä valeuutisiin useammin, jopa lähes puolet (46 %) viikoittain. Eteenpäin valheellisiksi tietämiään uutisia kertoi jakaneen 12 % nuorista vastaajista iältään 18-24-vuotta. (Uutismedian liitto 2022). Kyselyyn vastanneista 75 % luottaa kykyynsä tunnistaa valeuutinen (Herranen 2017). Painettu media pitää pintansa luotettavana mediana, johtuen Suomen lainsäädännöstä, sekä mm. Julkisen sanan neuvoston seurannasta ja sanktioista. Suomessa luotetaan painettuun mediaan, koska meillä on ollut jo pitkään sen osalta seurantaa ja sääntöjä. Valeuutisia julkaisevat tahot jo osin tunnistetaan ja tiedostetaan niiden levittämät valheelliset uutiset.

Euroopan parlamentti on yhteisessä rintamassa jakanut jäsenmailleen ohjeistuksia, miten valeuutiset tunnistetaan, tästä konkreettisena esimerkkinä tunnista valeuutiset kompassi, joka voi toimia käytännön työkaluna valeuutista tunnistettaessa (Bentzen & Chahri 2019). Toimittajille on laadittu myös ilmainen faktantarkistustyökalu InVid-hankkeessa, jonka avulla voi tehdä käänteisen kuvahaun Google-, Baidu- tai Yandex hakukoneissa, sekä tehdä Twitter-kyselyjä tehokkaammin, sekä pirstoa videoita eri alustoilta (Facebook, Instagram, YouTube, Twitter, Daily Motion). Työkalusta on laadittu erinomainen ohjeistus, jotta työkalun käyttö itsessään on helppoa ohjeiden avulla (Mezaris 2020). Jokaiselle kansalaiselle on myös tarjolla tietoa valeuutisten tunnistamiseen ja toimimiseen, jos sellaisen havaitsee. Valeuutisten johdosta on koettu tarpeen erilaiset helposti käytettävät faktantarkistuspalvelut, suomalainen faktantarkistuspalvelu on Faktabaari. Faktabaarissa voi pyytää faktantarkistusta, sekä lukea jo tehtyjä faktantarkistuksia. Siellä on myös valetiedosta aiheena erilaisia näkökulmia, sekä opetusmateriaalia valmiiksi laadittuna (Faktabaari 2023). Kansainvälisesti faktantarkistustyötä edistää International Fact-Checking Network (IFCN). European Digital Media Observatory (EDMO) kokoavat yhteen faktantarkastajia ja akateemisia tutkijoita. EDMO pyrkii ammattilaisten avulla ymmärtämään ja analysoimaan disinformaatiota.

Suomessa toimiva Julkisen sanan neuvosto, on tiedotusvälineiden kustantajien ja toimittajien perustama. Sen tehtävänä on tulkita hyvää journalistista tapaa ja puolustaa sanan- ja julkaisemisen vapautta. Neuvosto arvioi journalistien työtä journalistien ohjeita tulkitsemalla. Ohjeet koskevat kaikkea journalistista työtä. Kuka tahansa voi tehdä kantelun, jos havaitsee, että mediassa on loukattu hyvää journalistista tapaa. Julkisen sanan neuvosto käsittelee ja ratkaisee kaikki tapaukset, joista sille on kanneltu. Mikäli tiedotusväline on neuvoston mielestä rikkonut hyvää journalistista tapaa, annetaan sille huomautus, joka on julkaistava lyhyessä määräajassa. Neuvosto voi omasta aloitteestaan ottaa myös käsittelyyn asioita. Julkisen sanan neuvoston määräämät sanktiot ja uutisten oikaisut ovat hyviä, mutta tosiasia on, että

lukijat usein muistavat paremmin valeuutisen, kuin oikean uutisen. (Julkisen sanan neuvosto 2023).

9.3 Kriittinen infrastruktuuri

Pöyhösen, Nuojuan, Lehdon ja Rajamäen julkaisussa kriittisen infrastruktuurin rakenne on palvelut, tiedonsiirtoverkot sekä sähköverkot. Suomessa yksityisten yritysten merkitys korostuu kriittisen infrastruktuurin osalta, sillä noin 80 prosenttia toiminnoista arvioidaan kuuluvan heidän vastuulleen. (Pöyhönen, Nuojua, Lehto & Rajamäki 2019, 236-256). Suomessa Valtioneuvosto asettaa huoltovarmuudelle yleiset tavoitteet. Keskeinen tavoite on turvata kriittinen infrastruktuuri, tuotannon ja palveluiden toimivuus. Suomessa on valtion ja kuntien viranomaisilla lakisääteinen velvollisuus varautua poikkeus- ja häiriötilanteisiin. Huoltovarmuuskeskus tekee yhteistyötä viranomaisten, elinkeinoelämän ja toimialajärjestöjen kanssa. Se koordinoi, edistää ja mahdollistaa huoltovarmuustyötä, niillä alueilla, jotka ovat kriittisiä huoltovarmuuden kannalta. Huoltovarmuuskeskuksen yksi tehtävä on varmistaa varastoinnilla esimerkiksi viljan ja öljyn osalta puskurit yhteistyöllä muiden organisaatioiden kanssa. (Huoltovarmuuskeskus 2023). Huoltovarmuuskeskus on osaltaan huolehtimassa Suomen informaatioturvallisuudesta. Vihamielinen informaatiovaikuttaminen tunnistetaan salakavalaksi aseeksi, joka voi lamaannuttaa elintärkeitä toimintoja ja yhteiskunnan toimintakykyä, ellei sitä tunnisteta ajoissa. Informaatioturvallisuus on tärkeä osa Suomen kokonaisturvallisuutta, joka syntyy yhteistyössä viranomaisten, yritysten ja organisaatioiden kanssa. Huoltovarmuuskeskus on vahvistanut informaatioturvallisuutta ja perustanut informaatioturvallisuuden osaamiskeskustoiminnon, projekti on käynnissä 2022-2024 ja auttaa elinkeinoelämää, viranomaisia ja kansalaisia tunnistamaan, ehkäisemään ja saamaan tietoa informaatiovaikuttamisesta. (Kangasniemi 2022).

Euroopan komissio julkaisi Euroopan turvallisuusunionistrategian vuonna 2020. Strategiassa linjattiin, että EU-maiden tulee yhdenmukaisin menettelyin määrittää ja tunnistaa yhteiskunnan toimintakyvyn kannalta kriittiset toimijat ja parantaa niiden kriisinsietokykyä. Direktiiviehdotuksen tarkoitus on parantaa EU:n ja sen jäsenmaiden varautumista laaja-alaiseen vaikuttamiseen, kuten hybridiuhkiin. CER-direktiivi (Critical Entities Resilience), tuli voimaan joulukuussa 2022 ja se edellyttää Suomelta toimia, kuten kriittisten toimijoiden tunnistamiseen ja valvontaan liittyviä viranomaistehtäviä. Tämän johdosta Suomessa ensimmäistä kertaa määritetään kansallista kriittistä infrastruktuuria, kriittisiä sektoreita, sekä toimijoita lainsäädännön tasolla. (Valtioneuvosto 2023a). Lainsäädännön tavoitteena on vahvistaa kriittisen infrastruktuurin kriisinkestävyyttä, parantaa toimijoiden häiriönsietokykyä sekä jatkuvuudenhallintaa ja siten vahvistaa yhteiskunnan kriisinkestävyyttä ja kansallista turvallisuutta. Hanke on asetettu joulukuussa 2022 ja sen toimikausi päättyy joulukuun loppuun 2024. (Valtioneuvosto 2023b).

Valtioneuvostolla on hanke kyberturvallisuuden NIS2-direktiivin velvoitteisen saamiseksi osaksi kansallista lainsäädäntöä. Hankkeen tarkoitus on yhdenmukaistaa eräiden yhteiskunnan kriittisten sektoreiden vähimmäistason kyberturvallisuusriskienhallinta- ja raportointivelvoitteita. Hankkeeseen liittyy muita kyberturvallisuuteen liittyviä hankkeita mm. lainsäädäntöhanke Kriittisen infrastruktuurin tunnistaminen ja kriisinkestävyyden parantaminen. (Valtioneuvosto, 2023c).

Koronaviruspandemian aikana disinformaation määrä lisääntyi. EU neuvosto havaitsi, että koronaviruspandemia tekee EU:sta ja sen jäsenmaista alttiimpia hybridiuhkille ja sen vuoksi neuvosto kehotti tehostamaan EU tason toimia hybridiuhkien, myös disinformaation, torjumiseksi. Koronaviruspandemiaan liittyvän disinformaation vuoksi, Euroopan komissio ja EU:n ulkoasiainedustajat antoivat tiedonannon, jossa ehdotettiin konkreettisia toimia EU:n selviytymiskyvyn vahvistamiseksi disinformaatioon liittyen. Euroopan komissio lähti torjumaan disinformaatiota, tarjoamalla luotettavia tietolähteitä. Maailman terveysjärjestö (WHO) myös kokosi koronaviruspandemiaa koskevia laajimmin levinneitä myyttejä, sekä pyrki oikaisemaan niitä. Toimien aikana syntyi myös EUvsDisinfo - sivusto, joka seuraa disinformaatiota ja tiedottaa tästä suurta yleisöä. Kaikkien näiden toimien tarkoituksena on tarjota ihmisille luotettavia tietolähteitä. (Eurooppa-neuvosto 2023).

9.4 EU vaalit 2019

Ennen EU-vaaleja oli disinformaation torjumisen suhteen ollut suuret toimenpiteet koronapandemian vuoksi ja havaittiin, että on tarvetta tehdä toimia disinformaation torjumiseksi myös vaalien aikana. Tämä johtikin erilaisiin EU:n yhteistyön perusteella tehtäviin ohjeistuksiin ja käytänteiden yhdenmukaistamiseen sekä turvaamiseen mm. tietosuojaa koskevissa kysymyksissä. Vaaleissa oli ennätyskorkea äänestysprosentti, mutta samalla havaittiin, että ulkomailla asuvien EU-kansalaisten äänioikeus tulee turvata jatkossa paremmin. Vuoden 2019 EU-vaalien jälkeen Yhdistyneiden kansakuntien ja Romanian kansalaiset tekivät useita kanteluita EU:n kansalaisten äänestysvaikeuksista. Tämän johdosta Euroopan komissio esitteli joulukuussa 2020 eurooppalaisen demokratian toimintasuunnitelman, jonka tarkoituksena on lisätä kansalaisten vaikutusmahdollisuuksia, rakentaa kestävämpiä demokratioita kaikkialla EU:ssa edistämällä vapaita ja oikeudenmukaisia vaaleja, sekä vahvistaa tiedotusvälineiden vapautta ja torjua disinformaatiota. (Wigand, Mercier & Kolanko 2023).

Euroopan komissio antoi tiedonannon ja ohjeistuksia vuonna 2018, jotta vapaat ja oikeudenmukaiset vaalit voidaan turvata. Vaalipaketin ohjeilla oli tarkoitus antaa erityisiä ohjeita henkilötietojen käsittelystä, sekä suositella parhaita käytäntöjä disinformaation ja kyberhyökkäysten riskeihin puuttumiseksi, sekä edistää avoimuutta ja vastuuvelvollisuutta verkossa EU:n vaaliprosessissa. Tehtyjen toimien tarkoitus oli että, toimivaltaisten viranomaisten välisen yhteistyö tehostuu ja sellaisten välineiden käyttöönotto, joiden avulla viranomaiset voivat

puuttua asiaan ja tarvittaessa ottaa käyttöön seuraamuksia vaaliprosessin rehellisyyden turvaamiseksi. Vaalipaketissa oli myös ehdotettuja toimenpiteitä, joilla voidaan puuttua tilanteisiin, joissa tarkoituksellisest rikotaan tietosuojasäännöksiä tai yritetään vaikuttaa Euroopan parlamentin vaalien tulokseen. (Euroopan komissio 2018).

Verkkoon laadittiin tämän johdosta uusia faktantarkistusjärjestelmiä, mm. FactCheck.org ja PolitiFact.com. Suurin osa nykyisistä faktantarkastusresursseista keskittyy juuri poliittisten uutisten todentamiseen. (Euroopan komissio 2018).

EU asioihin liittyen on paljon väärinkäsityksiä ja -tietoa, tätä oikaisemaan on lähtenyt Schuman-seura, joka julkaisee tosiasioita käsittelevän julkaisun vastaamaan urbaanilegendojen väittämiin. Julkaisusta on juuri julkaistu 6. painos, jossa käsitellään perusasioiden lisäksi esim. mistä EU päättää tai mitä Euroopan parlamentti tekee, sekä myös ajankohtaisia ongelmia esim. kyberuhkilta suojautuminen. (Elo, Eskola, Lappalainen, Laurila, Martikainen, Mikkola, Nieminen, Nousiainen, Oikarinen, Puranen, Raikas, Rosas & Tuusvuori 2019).

Kyseinen osio on palautteen jälkeen todettu olevan haastavin ja hieman jo perusaiheeltaan vanhentunut, vaikkakin vaalien aikana ja jälkeen tehdyt havainnot ja toimenpiteet ovat vahvistaneet ja yhdenmukaistaneet toimintatapoja EU:n sisällä. Tämä osio tullaan jatkossa korvaamaan opiskelijan omavalinnaisella panoksella aiheen ajankohtaisista tai mieleen jääneistä asioista valetietoon ja sen tunnistamiseen liittyen, joita opiskelija haluaa jakaa opintojen aikana. Osiossa on esimerkkejä aiheista, joista opiskelija voi oman tehtävän koostaa valmiiksi, mutta opiskelijalla on mahdollisuus tässä osiossa myös oman mielenkiinnon mukaan tehdä aiheen mukainen tehtäväsuoritus.

9.5 Kyberhyökkäykset

Yritysverkkoihin tehtyjen hyökkäysyritysten määrä nousi 50% vuodesta 2020 vuoteen 2021. Kyberrikollisuus aiheuttaa taloudellisia tappioita, mainehaittoja, imagotappioita ja asiakkaiden vähentynyttä luottamusta. Kyberuhka ei enää ole pelkästään isojen yritysten asia, tänä päivänä se on tärkeää huomioida myös ihan yksilötasolta saakka. Kyberhyökkäyksessä kyberrikolliset pyrkivät poistamaan tietokoneet käytöstä, varastamaan tietoja tai käyttämään murrettuja tietokonejärjestelmiä uusien hyökkäysten käynnistämiseen. Kyberhyökkäykset ovat tulleet viime vuosina hienostuneemmiksi ja kehittyneemmiksi, sen lisäksi että ne ovat lisääntyneet. Kyberrikollisuus perustuu heikkouksien tehokkaaseen hyväksikäyttöön. Tavanomaisia kyberhyökkäyksiä ovat haittaohjelmat, palvelunestohyökkäykset, tietojenkalastelu, SQL-injektiohyökkäykset, sivustojen väliset komentosarjahyökkäykset, sekä bottiverkot. (Kaspersky 2023c).

Helsingin seudun kauppakamarin (2022) tekemän kyselyn mukaan ylivoimaisesti suurin kyberuhka on tietojenkalastelu (phishing)- ja haittaohjelmahyökkäykset 77 % osuudellaan, muut

uhat yritysten kyberturvallisuuden osalta ovat tietoverkkoon tunkeutumiset (37 %), palvelunestohyökkäykset (32 %), yhtiön sisäinen uhka (omat työntekijät) 29 % ja loput 9 % jakaantuivat 8 % hyökkäyksiin, jotka kohdistuivat teollisiin tuotantoprosesseihin ja 1 % muut. Tietojenkalastelu- ja haittaohjelmahyökkäykset ovat näin ollen yli kaksi kolmasosallaan suurin uhka yrityksille. Kyselyn mukaan suurimmat esteet tehokkaan kyberturvallisuuden toteuttamisessa on 51 % osuudella nykyisen henkilökunnan tietotaidon ylläpitäminen kyberuhkien suhteen, 41 % käyttäjien piittaamattomuus tietoturvallisuudesta ja kyberuhkista, 38 % kyberuhkiin liittyvän tiedon riittämättömyys sekä 35 % turvallisuustoimiin ja menetelmiin liittyvän tiedon riittämättömyys. Näiden lisäksi mm. rahoitus, osaavien ammattilaisten löytämisen vaikeus koettiin haasteina. Raskaimpina seurauksina kyberhyökkäysien suhteen todettiin olevan 59 % yksityisyyden (henkilökunnan tai asiakkaiden tiedot) loukkaus, 42 % tuoton menetys (suora tai epäsuora), 34 % aineettoman omaisuuden menetys, 29 % negatiivinen julkisuus, 24 % kansallisen turvallisuuden vaarantuminen sekä markkinaosuuden menetys. (Vesterinen ym. 2022).

Kyberturvallisuuskeskuksen julkaiseman helmikuun kybersää tiedotteessa kerrottiin, että vuonna 2022 pankkitunnuskalastelulla suomalaisilta huijattiin 10 miljoonaa euroa. Tämä on suuri summa, ajatellen että Tilastokeskuksen ennakkotietojen mukaan Suomen väkiluku oli joulukuun 2022 lopussa 5 565 519 miljoonaa. Väkimäärään suhteutettuna siis erittäin suuri summa. Huolestuttavampaa kuitenkin on kehitys, sillä Kyberturvallisuuskeskus julkaisi syyskuun 2023 kybersään tiedotteessa, että vuoden 2023 ensimmäisen puolen vuoden aikana suomalaiset menettivät erilaisissa verkkohuijauksissa 19,8 miljoonaa euroa. (Traficom 2023a).

Osaajapula vaivaa kyberturvallisuusalaa, vaikka tällä hetkellä ala työllistää koko ajan enemmän ihmisiä, tämän hetken arvion mukaan 4,7 miljoonaa henkilöä kansainvälisesti. ISC² tekemän tutkimuksen mukaan tämän hetken työntekijävaje alalla on 3,4 miljoonaa henkilöä. Tutkimuksessa selvitettiin organisaatioiden keinoja työvoimapulaan vastaamiseksi. Vastanneista 57% kertoi investoivansa monimuotoisuutta, tasa-arvoa ja inklusiivisuutta lisääviin aloitteisiin, kuten naisten ja vähemmistöjen osallisuuden lisäämiseen. Uuden henkilöstön rekrytointiin, palkkaamiseen ja perehdyttämiseen oli valmis panostamaan 62% vastanneista. Henkilöstön koulutukseen ja joustavien työolojen tarjoamiseen panosti 64% vastanneista. (ISC² 2022). McKinseyn tekemän analyysin mukaan tilanne ei ole paranemassa, vaan päinvastoin osaajapula tulee nousemaan 3,9 miljoonaan ihmiseen vuoteen 2027 mennessä. Analyysi oli myös huolissaan naisten vähyydestä alalla, sillä huolimatta osaajapulasta vain hieman yli 20% kaikista Euroopan teknologia-alan tehtävistä on nykyisin naisten täyttämiä. McKinseyn arvioin mukaan, yksinkertaisin ja vaikuttavuudeltaan kauaskantoisin tapa vastata osaajapulaan on lisätä naisten osuutta alalle. Analyysin mukaan, mikäli Eurooppa pystyisi kaksinkertaistamaan naisten osuuden teknologia-alan työvoimasta ja kohottamaan naisten osuuden vastaamaan noin 45% työntekijöistä, riittäisi tämä kattamaan EU:ta uhkaavan teknologia-alan osaajapulan ja kasvattamaan BKT:tä jopa 600 miljardilla eurolla. (Blumberg, Krawina, Mäkelä & Soller 2023).

10 Johtopäätökset ja kehittäminen

Opinnäytetyö yhdisti tutkimuksen ja kehitystyön toimintatutkimuksen mukaisesti. Aiheeseen perehtyminen toimintatutkimuksen kautta osoittautui hyväksi valinnaksi. Lopputuloksena voidaan päätellä, että paikallinen tutkinnon osa valetiedon tunnistaminen on hyvä tiedon välineenä, jotta valetiedon osalta tiedon lisääntyminen kohdeorganisaatiossa lisääntyy tutkinnon osan suorittamisella ja valmistunut tutkinnon osa on hyödynnettävyydeltään hyvä. Tämän kaltaisen opintomateriaalin laatiminen valetiedon tunnistamiseen perustutkinnon opiskelijoille on monelta näkökulmalta järkevää ja suositeltavaa. Ikäryhmä (18-25-vuotiaat) on suurin, joka joutuu tilastollisesti onnistuneiden hyökkäyksien kohteeksi, sekä tutkitusti myös se, joka eniten välittää valetietoa eteenpäin erilaisissa kanavissa, miettimättä edes mitä ovat levittämässä. Ikäryhmä on myös aloittamassa työuraansa, joten he voivat viedä mennessään tietoisuutta aiheesta työpaikoille ja lisäävät siellä osaamista. Opiskelijat, osaamisen karttuessa valetiedon tunnistamisen osalta, osaavat itse työelämässä pohtia erilaisista medioista tulevan tiedon oikeellisuutta ja vaikuttavuutta yrityksen toimintaan. Opiskelijat tiedostavat tutkinnon osan suorittamisen jälkeen, mitä havaituista vahingollisista valeuutisista voi seurata, sekä mahdollisia erilaisia toimintamalleja, miten yrityksessä tulisi toimia, jos huomaa joutuneensa valeuutisten kohteeksi. Valetiedon tunnistamisen lisäksi valmiudet toimia kasvavat tietoisuuden lisääntyessä. Käytännön toimia voivat olla mm. valetiedon tunnistaminen ja sen jakamatta jättäminen, sekä vahingollisesta valetiedosta mahdollisimman nopea tiedottaminen yrityksessä, jotta siihen voidaan reagoida nopeasti. Kun turvallisuusalan perustutkinnon sisältöjä tarkasteltiin, huomattiin, että tämän työn aihepiiriä ei ole käsitelty aiemmin. Itseasiassa valetiedon osalta perustutkinnoissa ei ole suoranaisesti aihetta järjestelmällisesti missään tutkinnossa mainittu, eikä siten opintojen aikana aiheesta ole ollut opetusta. Artikkeli julkaistiin Osaava Tredussa, jonka jälkeen valetieto on herättänyt kiinnostusta myös muissa Tredussa järjestettävissä perustutkinnoissa opettavien henkilöiden osalta. Artikkelin julkaisun jälkeen valetiedon osalta on kohdeorganisaatiossa oltu aiheesta paremmin tietoisia, sekä kiinnostuneita hyödyntämään valmistunutta materiaalia.

Kyberosaajien pula on huolestuttavaa. Pulaan on pyritty EU tasoisesti vastaamaan, mutta tässä hetkessä olisi erittäin suositeltavaa yrityksissä katsoa omaa henkilöstöä ja pyrkiä kouluttamaan sieltä osaajia vastaamaan oman yrityksen kyberosaamisesta. Suositus siksi, että osaajat yleisistä koulutuksista tulevat olemaan pitkään niin haluttuja, että heidän saaminen vapailta markkinoilta voi olla haastavaa. Valmiin osaajan palkkaaminen on käytännössä tällä hetkellä mahdotonta. Opiskelijoiden innostaminen monesta eri lähtökohdista kouluttautumaan kyberosaajiksi on siksikin järkevää. Turvallisuusalan perustutkinnon koulutukseen toisella asteella kuuluu turvallisuuteen liittyvien riskien tunnistaminen ja niiden osalta toimenpidesuositusten laatiminen. Paikallinen tutkinnon valetiedon tunnistaminen on siis hyvä lisä jo olemassa oleviin ammatillisiin riskien tunnistamiseen käsittelevissä opintokokonaisuuksissa. Tutkinnon osan suorittamisen keskeinen ajatus on, että tietoisuus lisääntyy. Toisen asteen

opiskelijat ovat siirtymässä työelämään, jolloin he vievät oppilaitoksessa saavutettua osaamistaan mukanaan ja mahdollisesti pääsevät siellä sitä käyttämään, hyödyntämään ja jakamaan. Perustutkinnosta valmistuneet opiskelijat saattavat myös jatkaa myöhemmin opintojaan ja mahdollisesti jopa aiheeseen liittyen tieto- ja kyberturvallisuuden aiheita, jos ovat saaneet siihen innostuksen perustutkinnon suorittamisen aikana.

Kehittämisehdotuksiksi tutkinnon osan muokkaamisen lisäksi löytyi monta uutta tutkittavaa asiaa, sekä mahdollisesti myös kohdeorganisaatiossa huomioon otettavia seikkoja. Uusia tutkittavia asioita esimerkiksi ohjeiden, määräysten ja lainsäädännön kokonaisvaltaisempi huomioiminen. Tarve pysyä ajan vaatimusten mukaisesti monipuolisesti tiedon, kyberturvallisuuden ja hybridivaikuttamisen osalta on valtava. Osaamisen kehittäminen, vaikka pieninkin askelin, on aina suunta eteenpäin. Tietoisuuden lisääntyminen, opintojakson materiaaleihin tutustuminen ja opintojakson näytön laatimisella on mahdollisuus laatia yrityksiin hyvinkin konkreettisia tulevaisuuden suuntakuvia sekä -arvioita ja käytännön torjuntakeinoja ja -malleja, mikäli tähän ei ole jo kohdeorganisaatiossa ryhdytty. Nämä toimet ovat pääosin jatkumoa tutkinnon osan suorittajan aloittamasta työstä. Kehitystyötä tulee siis jatkaa opiskelijan suorittaman näyttötyön jälkeen.

Tampereen seudun ammattiopisto on hyötynyt laaditun tutkinnon osan valmistumisessa myös oman henkilöstön tietoisuuden lisäämisessä, aiheen ollessa ajankohtainen myös kohdeorganisaation henkilöstön keskuudessa julkaistun artikkelin johdosta. Tutkinnon osa on kaikkien Tredun ammatillisen perustutkinnon opiskelijoiden mahdollista tehdä halutessaan. Verkkototeutuksena tutkinnon osan suoritus ei ole aikaan tai paikkaan sidottu, joka tekee siitä hyödynnettävyydeltään hyvän ja käytettävyydeltään joustavan. Kohdeorganisaatio on myös kokoamassa verkkototeutukset ns. tarjottimelle, jolloin niihin on helpompaa liittyä, sekä opiskelijat voivat tehdä valintoja oman mielenkiinnon mukaan.

Valetiedon tunnistamisen osaamisen merkitys henkilökohtaisen elämän, organisaation ja yritys elämän osalta on tärkeää. Hankimme paljon tarvittavaa tietoa erilaisista medioista, jolloin harkinta, oikeellisuuden punnitseminen ja mahdollisesti tiedon oikeellisuuden tarkistamisen osaaminen on oleellinen kansalaistaito. Teemme päätöksiä saamamme tiedon pohjalta, jolloin tiedon oikeellisuus on arvokasta. Tiedon saaminen ei ole ongelma – sen oikeellisuus on. Nimenomaan ymmärrys, että virheellistä tai valheellista tietoa on julkaistu ja julkaistaan ja jopa sen löytäminen mediavirrassa on tärkeää. Valetietoa voidaan käyttää vaikuttavasti ja varsinkin mikäli esimerkiksi sosiaaliset verkostot ovat laajat, jolloin kaikki tieto on jaettavissa silmänräpäyksessä eteenpäin ja taas eteenpäin.

Hybridivaikuttamisen osalta valetieto on suuressa osassa myös. Valheellisin tiedoin pyritään vaikuttamaan ihmisten mielipiteisiin esimerkiksi Venäjän ja Ukrainan välisessä sodassa. Kyberturvallisuuden osalta on huomioitavaa, että pääosa kyberhuijauksista perustuu nimenomaan

valheellisiin tietoihin, joiden avulla käyttäjä saadaan tekemään hänelle epäedullisia ratkaisuja esim. antamalla käyttäjätunnukset. Toisaalta halutaan tietoa, jotta voidaan käyttää sitä hyödyksi huijauksien tekemisessä. Erilaisissa kyberhuijauksissa on viime vuonna (2022) Suomessa menetetty noin 10 miljoonaa euroa, tämän vuoden (2023) ensimmäisellä puoliskolla summa oli jo lähes 20 miljoonaa euroa, eli vain puolessa vuodessa summa on tuplaantunut vuodesta 2023. Ainakin yksi suomalainen yritys on mennyt konkurssiin kyberhuijauksen vuoksi ja yrityksistä, jotka ovat joutuneet vaikeuksiin kyberhuijauksien vuoksi on raportoitu. Taloudellisesta näkökulmasta aihe on siis merkittävä. Valheellinen tieto on hybridivaikuttamisessa ja kyberhuijauksessa oleellisesti vaikuttamassa siihen, miten niihin uskotaan ja ne ovat viime vuosina kehittyneet koko ajan uskottavimmiksi. Tietoisuuden lisääminen valetiedon osalta auttaa siinä, ettei tule huijatuksi, sekä osaa jatkossa hankkia luotettavaa ja oikeaa tietoa päätösten tueksi.

Lähteet

Painetut

Hirsijärsi, S., Remes, P., Sajavaara, P. 1997. 18. painos. Tutki ja kirjoita. Porvoo: Bookwell Oy

Tuomi, J. Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Vantaa: Hansaprint Oy

Sähköiset

Alanko, Kristine. Hauptmann, Maria. 9.12.2022. Valtioneuvosto. EU-jäsenmaat yhteisymmärrykseen tekoälyasetuksesta – mitä se käytännössä tarkoittaa. Viitattu 19.7.2023 https://valtioneuvosto.fi/-//1410877/eu-jasenmaat-yhteisymmarrykseen-tekoalyasetuksesta-mita-se-kaytannossa-tarkoittaa-

Alkhalil, Zainab. Hewage Chaminda. Nawaf, Liqaa. Khan, Imtiaz. 9.3.2021. Frontiers. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Viitattu 14.7.2023 https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#h5

Arnsten, B. A., Mazure, C. M. ja April, R. S. (2012). Everyday stress can shut down the brain's chief command center. Scietific American. Viitattu 3.7.2023. https://www.scientificamerican.com/article/this-is-your-brain-in-meltdown/

BBC. 2015. Phishing catches victims 'in minutes'. Viitattu 16.7.2023 https://www.bbc.com/news/technology-32285433

Bentzen, Naja. Chahri, Samy. 2019. Euroopan parlamentti. Tunnista valeuutiset kompassi. Viitattu 8.7.2023 https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_FI.pdf

Blumberg, Sven. Krawina, Melanie. Mäkelä, Elina. Soller, Henning. 24.1.2023. McKinsey & Company. Women in tech: The best bet to solve Europe's talent shortage. Viitattu 22.7.2023 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/women-in-tech-the-best-bet-to-solve-europes-talent-shortage

Calabrese, Erin. 29.5.2020. 5 ways to spot disinformation on your social media feeds. Viitattu 8.7.2023 https://abcnews.go.com/US/ways-spot-disinformation-social-media-feeds/story?id=67784438

Crane Casey. 2021. The 12 most expensive phishing attacks in history. Viitattu 3.7.2023. https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/#:%7E:text=At%20some%20level%2C%20everyone%20is%20susceptible%20to%20phishing,outright%20trick%20you%20into%20performing%20a%20particular%20task

EDMO. 2023. Fact-checking Briefs. Viitattu 22.7.2023 https://edmo.eu/fact-checking-briefs/

Elo, Kimmo. Eskola, Anna. Lappalainen, Emma. Laurila, Iida. Martikainen, Tuomas. Mikkola, Maritta. Nieminen, Hannariikka. Nousiainen, Ilkka. Oikarinen, Jarmo. Puranen, Tomi. Raikas, Terhi. Rosas, Allan. Tuusvuori, Ossi. 2019. Schuman-seura ry. EU ja käyrät kurkut. Tosiasioita urbaanilegendojen sijaan. Viitattu 22.7.2023 https://www.schuman-seura.fi/fi/kayrat-kurkut/

Enisa. 2023. Artificial Intelligence and Cybersecurity Research. Viitattu 9.7.2023 https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research

Eperusteet. 2023. Ammatillinen koulutus. Turvallisuusalan perustutkinto. Tutkinnon osat Viitattu 21.12.2023 https://eperusteet.opintopolku.fi/#/fi/ammatillinen/7659530/tutkinnon-osat

Euroopan komissio. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. 12.9.2018. Viitattu 8.7.2023 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0637&from=EN

Eurooppa-neuvosto. Euroopan unionin neuvosto. EU:n toimet koronaviruspandemian johdosta. Disinformaation torjunta. Viitattu 6.7.2023 https://www.consilium.europa.eu/fi/policies/coronavirus/fighting-disinformation/

European Digital Media Observatory. EDMO. 2023. ADMO at a Glance. Viitattu 11.7.2023 https://edmo.eu/edmo-at-a-glance/

Faktabaari. Viitattu 28.8.2023 https://faktabaari.fi/

F-Secure. 2023a. Mitä on tietojenkalastelu?. Viitattu 9.7.2023 https://www.f-secure.com/fi/articles/what-is-phishing

F-Secure. 2023b. Vältä näitä 5 tietojenkalasteluhuijausta vuonna 2023. Viitattu 17.7.2023 https://www.f-secure.com/fi/articles/5-phishing-scams-to-avoid-in-2023

Glamoslija, Katarina. Mitä on tietojenkalastelu? Yksinkertainen opas esimerkkeineen. SafetyDetectives. 2023. Viitattu 12.7.2023 https://fi.safetydetectives.com/blog/mita-on-tietojenkalastelu-yksinkertainen-opas-esimerkeilla-varustettuna/

Grinberg, N., Joseph, K., Friedland, L., Swire-Thompson, B., & Lazer, D. (2019). Fake news on Twitter during the 2016 U.S. presidential election. Science, 363(6425), 374–378. https://doi.org/10.1126/science.aau2706

Guillot, Jean. 2023. Euroopan parlamentti. Mitä tekoäly on ja mihin sitä käytetään. Viitattu 29.11.2023 https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200827STO85804/20200827STO85804_fi.pdf

Hadlington, L. (2017). Heliyon. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behavioours. Viitattu 3.7.2023 https://www.cell.com/heliyon/fulltext/S2405-8440(17)30998-2?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844017309982%3Fshowall%3Dtrue

Herranen, Tanja. Medialiitto. Valeuutistutkimus 2017. 14.11.2017. Viitattu 6.7.2023 https://www.medialiitto.fi/wp-content/uploads/2020/06/Valeuutistutkimus_14.11.2017.pdf

Hong, J. (2012). The state of phishing attacks. Viitattu 14.7.2023 https://dl.acm.org/doi/10.1145/2063176.2063197

Hybrid CoE. What is Hybrid CoE. 2023. Viitattu 14.7.2023 https://www.hybridcoe.fi/who-what-and-how/

Huoltovarmuuskeskus. Huoltovarmuus Suomessa. 2023a. Viitattu 5.7.2023 https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/huoltovarmuus-suomessa

IMMUNE 2 INFODEMIC -hanke. 2013. Viitattu 25.11.2023 https://immune2infodemic.eu/index.html

ISC². 2022. Cybersecurity workforce study. A critical need for cybersecurity professionals persist amidst a year of cultural and workplace evolution. Viitattu 22.7.2023 https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

Jyväskylän yliopisto. 2015. Laadullinen tutkimus. Viitattu 28.11.2023 https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

Julkisen sanan neuvosto. Mikä on JSN. 2023. Viitattu 8.7.2023. https://jsn.fi/mika-on-jsn/julkisen-sanan-neuvosto/

Kallinen, Timo & Kinnunen, Taina. 2021. Etnografia. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 29.11.2023 https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/

Kangasniemi, Hanna. Huoltovarmuuskeskus. 2022. Informaatioturvallisuus keskeinen osa digitaalista turvallisuutta. Viitattu 18.7.2023 https://www.varmuudenvuoksi.fi/artikkeli/informaatioturvallisuus-keskeinen-osa-digitaalista-turvallisuutta

Karanian, Jessica M, Rabb, Nathaniel, Wulff, Alia N, Race, Elizabeth. Protecting memory from misinformation: Warnings modulate cortical reinstatement during memory retrieval. 31.8.2020. Viitattu 2.7.2023 https://www.pnas.org/doi/abs/10.1073/pnas.2008595117

Kaspersky. 2023a. Kuinka tunnistat valeuutiset. Viitattu 13.7.2023 https://www.kaspersky.fi/resource-center/preemptive-safety/how-to-identify-fake-news

Kaspersky. 2023b. Huijausvideot ja syvähuijaus – kuinka käyttäjät voivat suojautua? Viitattu 13.7.2023 https://www.kaspersky.fi/resource-center/threats/protect-yourself-from-deepfake

Kaspersky. 2023c. Kyberhyökkäysten estäminen. Viitattu 13.7.2023 https://www.kaspersky.fi/resource-center/preemptive-safety/how-to-prevent-cyberattacks

Kaspersky.16.2.2023d. Spam and phishing in 2022. Viitattu 17.7.2023 https://securelist.com/spam-phishing-scam-report-2022/108692/

Keepnet LABS (2023). Viitattu 3.7.2023 www.keepnetlabs.com

Kilpailu- ja kuluttajavirasto. Kuluttaja-asiat. Huijaukset. Tietojenkalastelu. 2023. Viitattu 9.7.2023 https://www.kkv.fi/kuluttaja-asiat/huijaukset/tietojenkalastelu/

Kuluttajaliitto. 2023. Varo, varmista ja varoita: Nettihuijaukset ja tietojenkalastelu muuttavat muotoaan, mutta niiltä on mahdollista suojautua. Viitattu 17.7.2023 https://www.kuluttajaliitto.fi/varo-varmista-varoita/

Kyberturvallisuuskeskus. Kyberturvallisuus ja yrityksen hallituksen vastuu. 2020. Viitattu 12.7.2023 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kytömaa, Eero. 2023. Sisäministeriö. Hybridiuhat ja hybridivaikuttaminen. Viitattu 21.12.2023 https://intermin.fi/kansallinen-turvallisuus/hybridiuhat

Leffer, Lauren. 2023. Yes, AI Models can get worse over time. Scientific American. Viitattu 9.8.2023. https://www.scientificamerican.com/article/yes-ai-models-can-get-worse-over-time/

Lehto, Martti. Limnell, Jarno. Innola, Eeva. Pöyhönen, Jouni. Rusi, Tarja. Salminen, Mirva. 2017. Valtioneuvoston selvitys- ja tutkimustoiminta. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Viitattu 11.7.2023 https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila,+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Marstio, Tuija. 2020. Verkko-opinnon muotoilu. Käsikirja. Viitattu 15.7.2023 https://peda.net/ksao/digituki/verkkopedagogiikka/verkko-pedagogiikan-materiaali-pankki/verkko-pedagogiikan-materiaaleja/laurea-julkaisut-134-verkko-oppimisen-ka:file/download/9df99d33cd79468a6f37589479d514769eedb3c7/Laurea%20Julkaisut%20134_verkko-oppimisen%20k%C3%A4sikirja.pdf

Mezaris, Vasileios. InVid-hanke. European Union's Horizon 2020 research and innovation programme under grant agreement No 687786. 2020. Viitattu 8.7.2023 https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

Moodle. 2014. Tietoa moodlesta. Viitattu 29.11.2023 https://docs.moodle.org/2x/fi/Tietoja_Moodlesta

Mäntylä, Jussi. Skycode Oy. 2023. Tekoälyn historia. Viitattu 9.7.2023 https://xn--tekoly-eua.info/tekoaly_historia/

Nurse, Jason R.C. 27.3.2015. Exploring the Risks to Identity Security and Privacy in Cyberspace. Viitattu 16.7.2023 https://dl.acm.org/doi/10.1145/2730912

Opetushallitus. 2023a. Tutkintojen perusteet. Viitattu 19.12.2023. https://www.oph.fi/fi/koulutus-ja-tutkinnot/tutkintojen-perusteet

Opetushallitus. 2023b. Ammatillisten tutkinnon osien arviointikriteeristö. Viitattu 19.12.2023 https://www.oph.fi/fi/koulutus-ja-tutkinnot/ammatillisten-tutkinnon-osien-arviointikriteeristo

Pandasecurity. 10 Social media scams and how to spot them. 2.4.2019. Viitattu 8.7.2023 https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/

Pöyhönen, J., Nuojua, V., Lehto, M. & Rajamäki, J. 2019, "Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations", Information & Security, vol. 43, no. 1, pp. 236-256. Viitattu 5.7.2023 https://www.researchgate.net/publication/335995107_Cyber_Situational_Awareness_and_Information_Sharing_in_Critical_Infrastructure_Organizations

Rastas, Taru. 19.4.2023. Sitra. Datatalouden kehittymisen seuranta helpottuu – koostimme työkalun tarkkailemaan mittareita. Viitattu 17.7.2023 https://www.sitra.fi/artikkelit/datatalouden-kehittymisen-seuranta-helpottuu-koostimme-tyokalun-tarkkailemaan-mittareita/

Richards, Abbie. 2021. The conspiracy chart. 2021. Detached from reality. Viitattu 11.7.2023 https://www.conspiracychart.com/

Rimol, Meghan. 20.4.2023. Why Trust and Security are Essential for the Future of Generative AI. Viitattu 16.7.2023 https://www.gartner.com/en/newsroom/press-releases/2023-04-20-why-trust-and-security-are-essential-for-the-future-of-generative-ai

Rimol, Meghan. Howley, Catherine. 17.10.2022. Gartner. Gartner Identifies the Top 10 Strategic Technology Trends for 2023. Viitattu 17.7.2023 https://www.gartner.com/en/newsroom/press-releases/2022-10-17-gartner-identifies-the-top-10-strategic-technology-trends-for-2023

Sisäministeriö. 2023a. Hybridiuhat ja hybridivaikuttaminen. Viitattu 14.7.2023 https://intermin.fi/kansallinen-turvallisuus/hybridiuhat

Sisäministeriö. 2023b. Itärajan tilanne. Viitattu 21.12.2023 https://intermin.fi/ajankohtaista/itarajan-tilanne

Stanislavsky, Juri. 28.1.2021. Root Nation. Internetin käyttäjien määrä maailmassa oli 4,66 miljardia. Viitattu 15.7.2023 https://root-nation.com/fi/ua/news-ua/it-news-ua/ua-new-internet-records/

Tampereen seudun ammattiopisto, Tredu. 2023a. Tietoa meistä. Viitattu 9.7.2023 https://www.tredu.fi/tredu/tietoa-meista/

Tampereen seudun ammattiopisto, Tredu. 2023b. Millaiset opiskeluvalmiudet täytyy olla? Viitattu 19.12.2023. https://www.tredu.fi/dial_tredu/parjaanko-opinnoissa/opiskelutaitoni-ovat-ruosteessa/

Tampereen yliopisto, Tampereen ammattikorkeakoulu. 2023. Digipedagogiikka. Viitattu 15.7.2023 https://www.tuni.fi/tlc/suunnittelu/digipedagogiikka/

Tepa-termipankki. 2023a. Informaatiovaikuttaminen. Viitattu 9.7.2023 https://termipankki.fi/tepa/fi/haku/disinformaatio

Tepa-termipankki. 2023b. Hybridivaikuttaminen. Viitattu 9.7.2023 https://termipankki.fi/tepa/fi/haku/hybridivaikuttaminen

Tilastokeskus. 2023. Väestön ennakkotilasto. Viitattu 5.7.2023 https://www.stat.fi/tilasto/vamuu

Toikko, Timo. Rantanen, Teemu. 2009. Tampereen Yliopistopaino Oy. Tutkimuksellinen kehittämistoiminta. Viitattu 24.11.2023 https://trepo.tuni.fi/bitstream/handle/10024/100802/Toikko_Rantanen_Tutkimuksellinen_kehittamistoiminta.pdf

Traficom. 2023a. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. Kybersää. Viitattu 5.7.2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202023

Traficom. 2023b. Tekoälyn mahdollistaman kyberhyökkäykset. Viitattu 2.8.2023. https://www.traficom.fi/sites/default/files/media/publication/TRAFICOM_Teko%C3%A4lyn_mahdollistamat_kyberhy%C3%B6kk%C3%A4ykset%202022-12-12_web.pdf

Traficom. 2023c. Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta. Viitattu 3.8.2023 https://www.traficom.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf

Uutismedian liitto. Sanomalehtien luotettavuus tutkimus 2022. Viitattu 2.7.2023 https://www.uutismediat.fi/ajankohtaista/sanomalehdet-ovat-suomalaisten-mielesta-ylivoimaisesti-luotettavin-media/

WHO, World Health Organication. 2023. Infodemic. Viitattu 29.11.2023 https://www.who.int/health-topics/infodemic#tab=tab_1

Wigand, Christian, Mercier, Guillaume, Kolanko, Katarzyna. 19.6.2020.European Comission. Comission reports on 2019 European elections: fostering European debates and securing free and fair elections. Viitattu 6.7.2023 https://ec.europa.eu/commission/presscorner/detail/fi/ip_20_1123

Williams, E. J., Hinds, J. ja Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. Viitattu 3.7.2023 https://www.sciencedirect.com/science/article/pii/S1071581918303628?via%3Dihub

Valtioneuvosto. Sisäministeriö. 8.12.2022a. Kriittisen infrastruktuurin häiriönsietokykyä parannetaan ja yhteiskunnan toimintakyvyn kannalta kriittiset toimijat tunnistetaan. Viitattu 5.7.2023 https://valtioneuvosto.fi/-/1410869/kriittisen-infrastruktuurin-hairionsietokykya-parannetaan-ja-yhteiskunnan-toimintakyvyn-kannalta-kriittiset-toimijat-tunnistetaan-

Valtioneuvosto. 8.12.2022b. Lainsäädäntöhanke: Kriittisen infrastruktuurin tunnistaminen ja kriisinkestävyyden parantaminen. Viitattu 5.7.2023. https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022

Valtioneuvosto. 2023. Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä. Viitattu 9.8.2023 https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022

Valtioneuvoston kanslia. 2019. Informaatiovaikuttamiseen vastaaminen. Opas viestijöille. Viitattu 9.7.2023 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161512/VNK_11_2019_Informaatiovaikuttamisen%20vastaaminen_web.pdf?sequence=1&isAllowed=y

Vehkoo, Johanna. Valheenpaljastaja: Miksi uskomme valheisiin? Näin tunnistat psykologiset mekanismit, joiden takia sinäkin lankeat väärään tietoon. 15.12.2019a. Viitattu 9.7.2023 https://yle.fi/aihe/artikkeli/2019/12/15/valheenpaljastaja-miksi-uskomme-valheisiin-nain-tunnistat-psykologiset

Vehkoo, Johanna. Valheenpaljastaja: Varoituslista valemedioista – älä luota näihin sivustoihin. 16.9.2016b. Viitattu 9.7.2023 https://yle.fi/aihe/artikkeli/2016/09/16/valheenpaljastaja-varoituslista-valemedioista-ala-luota-naihin-sivustoihin

Vesterinen, P. & Korslow, P. 2022. Yrityksiin kohdistuvat kyberuhat. Helsingin Seudun Kauppakamari. Viitattu 5.7.2023. https://view.taiqa.com/helsinki.chamber/yrityksiin-kohdistuvat-kyberuhat--selvitys-2022#/page=4

Vesterinen, Panu. 2022. Keskuskauppakamari. Huoltovarmuuskeskus. Yrityksiin kohdistuva hybridivaikuttaminen. Viitattu 14.7.2023 https://kauppakamari.fi/wp-content/uploads/2022/06/Yrityksiin-kohdistuva-hybridivaikuttaminen-selvitys.pdf

Julkaisemattomat lähteet

Pirinen Rauno, Ruoslahti Harri. 2023. Opinnäytetyön laatimiseen liittyvä haastattelu 22.05.2023. Laurea ammattikorkeakoulu. Teams/Espoo

Salin, Ossi. 2020. Laadullisista analyysimenetelmistä. Opinnäytetyö. 3.2.1. Laadulliset analyysimenetelmät. Laurea ammattikorkeakoulu. Espoo

Kuvat

Liitteet

Liite 1: Valetiedon tunnistaminen, 5 osp. Ammattitaitovaatimukset, arviointi ja ammattitaidon osoittamistavat

Tampereen seudun ammattiopisto, hyväksytty 06.09.2023 § 157, johtaja, ammatillinen koulutus. Turvallisuusalan perustutkinto (OPH-4815-2021) Paikallisiin osaamisvaatimuksiin perustuva yhteisen tutkinnon osa: Valetiedon tunnistaminen 5 osp

Ammattitaitovaatimukset, arviointi ja ammattitaidon osoittamistavat

Valetiedon tunnistaminen, 5 osp

Ammattitaitovaatimukset

Opiskelija

- noudattaa työelämän säädöksiä ja sopimuksia sekä aikatauluja
- noudattaa perusoikeuksiin liittyviä lakeja ja säädöksiä
- tunnistaa aiheeseen liittyvät viranomaisorganisaatiot, yhteisöt sekä niiden toimintaympäristön ja toimintaan vaikuttavat säädökset
- ymmärtää valetiedon (mis- ja disinformaation) merkityksen osana yrityksen tieto- ja kyberturvallisuutta
- tunnistaa valetietoa eri medioissa
- osaa toimia valetietoa havaitessaan ja näin estää sen leviämisen
- oppii kriittisyyttä ja etsimään luotettavia lähteitä tiedon oikeellisuuden varmistamiseksi
- arvioi valetietoon liittyviä turvallisuusriskejä
- toimii ratkaisukeskeisesti
- ymmärtää valetiedon merkityksen vaikuttamisen välineenä
- toimii työssään luottamuksellisesti ja asiakassuhteita edistäen
- tunnistaa miten valetieto voisi vaikuttaa organisaation/yrityksen toimintaan
- ymmärtää valetiedon haitallisen vaikutuksen laajemman merkityksen mm kriittinen infrastruktuuri
- osaa ohjeistaa luotettavan tiedon pariin
- raportoi oikealle taholle havaitessaan valetietoa

Arviointi

Opiskelija

Tyydyttävä 1	• toteuttaa työn ohjeiden mukaisesti • toimii yhteistyökykyisesti • tarvitsee joissakin tilanteissa lisäohjeita • hyödyntää työssä tarvittavaa perustietoa • muuttaa toimintaansa saamansa palautteen mukaisesti
Tyydyttävä 2	• toteuttaa työn oma-aloitteisesti ja ohjeiden mukaisesti • toimii yhteistyökykyisesti ja vuorovaikutteisesti • tarvitsee vain harvoissa tilanteissa lisäohjeita • hyödyntää työssä tarvittavaa tietoa tarkoituksenmukaisesti • muuttaa toimintaansa saamansa palautteen ja omien havaintojen mukaisesti
Hyvä 3	• toteuttaa työkokonaisuuden itsenäisesti • toimii yhteistyökykyisesti ja aloitteellisesti vuorovaikutustilanteissa • selviytyy tavanomaisista ongelmanratkaisutilanteista • hyödyntää työssä tarvittavaa tietoa monipuolisesti • arvioi suoriutumistaan realistisesti
Hyvä 4	• suunnittelee ja toteuttaa työkokonaisuuden itsenäisesti • toimii yhteistyökykyisesti ja rakentavasti vuorovaikutustilanteissa • selviytyy ongelmanratkaisutilanteista hyödyntäen monipuolisia ratkaisutapoja • soveltaa työssä tarvittavaa tietoa monipuolisesti ja perustellusti • arvioi suoriutumistaan realistisesti sekä tunnistaa vahvuuksiaan ja kehittämisen kohteitaan
Kiitettävä 5	• suunnittelee ja toteuttaa työkokonaisuuden itsenäisesti ottaen huomioon muut toimijat • toimii yhteistyökykyisesti ja rakentavasti haastavissakin vuorovaikutustilanteissa • soveltaa työssä tarvittavaa tietoa ongelmanratkaisutilanteissa monipuolisesti ja kriittisesti • esittää työhön ja toimintaympäristöön liittyviä perusteltuja kehittämisehdotuksia • arvioi suoriutumistaan realistisesti ja esittää perusteltuja ratkaisuja osaamisensa kehittämiseen • ymmärtää oman työnsä merkityksen osana laajempaa kokonaisuutta

Osaamisen osoittaminen

Opiskelija osoittaa ammattitaitonsa näytössä käytännön työtehtävissä laatimalla valetiedon tunnistamisesta ja toimenpiteistä ohjeen asiakaskohteeseen. Siltä osin kuin tutkinnon osassa vaadittua ammattitaitoa ei voida arvioida näytön perusteella, ammattitaidon osoittamista täydennetään yksilöllisesti muilla tavoin. Näitä voivat olla esimerkiksi laajempi kirjallinen ohjeistus tai infotuokio valetiedosta ja sen vaikutuksesta.

Liite 2: Artikkeli: Osaava Tredu

Turvallisuusala kehittää: Valetiedon tunnistaminen

Valeuutiset eivät ole uusi ilmiö, mutta 2016 Yhdysvaltojen presidentinvaaleissa ne herättivät paljon huomiota ja niistä huolestuttiin (Grinberg ym. 2016). Huoli ei niinkään johtunut demokratian toteutumisesta tai vaalien merkityksestä, vaan siitä että se oli niin valtavan laajaa. Sosiaalinen media on mahdollistanut viestinnän osalta uusia toimintoja, joita ovat mm nopea leviäminen, helppo saatavuus, kohdeyleisön ja kontrollin puutteen. Yhdysvaltojen presidentin vaalien lisäksi toinen valeuutisten aalto oli COVID-19-kriisin aikana. Valeuutisista kirjoitan tällä kertaa siksi, että tein siitä omiin opintoihin opinnäytetyön ja aiheesta syntyi Turvallisuusalan perustutkinnon paikallinen tutkinnon osa Valetiedon tunnistaminen 5osp, koimme aiheen ajankohtaisena ja tärkeänä.

Valeuutiset

Valeuutiset voidaan jakaa eri kategorioihin. Kasperskyn internetsivuilla nämä ovat jaettu seuraaviin, klikkiotsikot; oudot tarinat, vääristyneet kuvat tai sensaationtavoittelu myy ja houkuttelee käyttäjiä avaamaan tarinan, usein näissä ei ole muuta hurjaa kuin otsikko. Propaganda; yleisön harhauttamiseksi, poliittisen agendan tai puolueellisen näkökulman mainostamiseksi on laadittu valheellisia tai vääristeltyjä tarinoita. Heikkolaatuinen journalismi; journalistin virheen tai väärien faktojen vuoksi muodostunut valeuutinen. Usein journalisti korjaa virheen ja tiedottavat siitä. Harhaanjohtavat otsikot; sensaatiomaisella tai harhaanjohtavalla otsikolla houkutellaan lukijoita. Joskus juttu voi olla suurilta osin tottakin, mutta otsikkoa jakamalla saadaan johdatettua käyttäjiä harhaan. Huijareitten sisältö; huijauksen tai harhautuksen vuoksi valheelliset ja keksityt jutut, usein imitoivat uutislähteitä. Satiiri tai parodia; Viihteenä julkaistu valeuutinen. Nämä eivät pyri huijaamaan, eikä niitä ole tarkoitettu otettavan tosissaan, vaan ne on laadittu huumorilla (Kaspersky, 2023).

Tutkimuksen mukaan sosiaalinen media mahdollistaa valeuutisten nopean leviämisen. Sosiaalisessa mediassa ne itseasiassa leviävät paljon nopeammin kuin todelliset uutiset. Valeuutiset ovat tyypillisesti laadittu vetoamaan tunteisiin ja kiinnittämään huomiota, tämä selittää niiden nopean leviämisen. Valeuutiset ovat usein omituisia väitteitä ja tarinoita ja ne lietsovat vihaa ja pelkoa. Sosiaalisen median botit massatuottavat ja levittävät artikkeleita verkossa ottamatta huomioon niiden lähteiden luotettavuutta. Botit voivat luoda verkossa valetilejä, jotka saavat seuraajia, tunnustusta ja auktoriteetteja, näistä osa on ohjelmoitu levittämään

virheellistä tietoa. Internetin käyttäjissä on myös trolleja, jotka tarkoituksella yrittävät aloittaa riitoja tai suututtaa ihmisiä ja osaltaan myös levittävät valeuutisia. Trolleille voidaan myös maksaa tästä toiminnasta. Poliittiseen päätöksentekoon pyrkiviä vakiintuneita trolliryhmistä käytetään termejä ”trollifarmi” tai ”trollitehdas”. Valeuutiset voivat sisältää syvävääärennöksiä, ne ovat digitaalisella ohjelmistolla, koneoppimisella ja kasvojen vaihdolla luotuja valevideoita. Kuvia yhdistelemällä luodaan uutta kuvamateriaalia, jotka esittävät tapahtumia ja toimia, joita ei ole oikeasti tapahtunut. Nämä voivat olla hyvin vakuuttavia ja niitä voi olla vaikea tunnistaa valheellisiksi (Kaspersky 2023).

Valeuutisissa on vaaroja, ihmiset tekevät usein tärkeitä päätöksiä esimerkiksi ketä äänestävät vaaleissa, mitä lääketieteellisiä hoitoja ottavat sairastuessaan, sen perusteella mitä uutisissa sanotaan (Kaspersky, 2023).

Internetissä on erilaisia valetiedon luontiohjelmia, joilla todella nopeasti ja vaivattomasti luot oman valeuutisen tai äänen tai videon. Ohessa malli (melko mielikuvitukseton ja huonolla kuvalla) luotu valeuutinen, valeuutisgeneraattorin kautta. Tekemiseen meni alle minuutti ja toki se lopputuloksessa näkyy, helppoa ja hauskaa se oli. Valetietoa käytetään kyberhyökkäyksissä, yleisimmin tietojenkalasteluyrityksissä.

Breaking news-kuva jossa opettaja uutisoidaan seuraaviin vaaleihin presidenttiehdokkaaksi.

Terveisin Turvallisuusalan lehtori Marika Peuraniemi

Lähteet

Grinberg, N., Joseph, K., Friedland, L., Swire-Thompson, B., & Lazer, D. (2019). Fake news on Twitter during the 2016 U.S. presidential election. Science, 363(6425), 374–378. https://doi.org/10.1126/science.aau2706

Kaspersky. 2023. Kuinka tunnistat valeuutiset. Viitattu 13.7.2023 https://www.kaspersky.fi/resource-center/preemptive-safety/how-to-identify-fake-news

Linkki: https://osaava.tredu.fi/2023/11/06/turvallisuusala-kehittaa-valetiedon-tunnistaminen/