Kyberkansalaistaidot ja niiden kehittäminen Euroopan unionissa

Aalto-yliopiston tutkijaryhmä

Suomi, helmikuu 2023

KUVAILULEHTI

Julkaisija ja julkaisuaika	Aalto-yliopiston tutkijaryhmä, helmikuu 2023
Tekijät	Jarno Limnéll, Minna Alasuutari, Niko Candelin, Kaisa Cullen, Oula Halonen, Mika Helenius, Tommi Hermunen, Juha Lappalainen, Sari Latvanen, Marianne Lindroth, Teemu Matilainen, Olli-Pekka Palonen, Janne Riiheläinen, Mirva Salminen ja Pietari Virkkunen
Julkaisun nimi	Kyberkansalaistaidot ja niiden kehittäminen Euroopan unionissa
Asiasanat	Kyberturvallisuus, digitaalinen turvallisuus, kansalaistaidot, kyberkansalaistaidot, turvallisuus, koulutus, Euroopan unioni
Kieliversiot	suomi, englanti **Sivuja** 146

TIIVISTELMÄ

Tutkimus on osa laajempaa kyberkansalaistaitohanketta, jonka ensimmäinen vaihe on tutkimuksellinen ja tuloksena on tämä tutkimusraportti. Kokonaisuutena hanke tuottaa kyberturvallisuuden perustaitojen opettamisen eurooppalaisen mallin ja sen käytännön toteutuksen, joka tapahtuu niin kybertaitojen opetuksen pelillistämisen kuin päivitettävää koulutusmateriaalia tarjoavan toiminnan kautta.

Ensimmäisen vaiheen tavoitteena oli selvittää kyberkansalaistaitojen opettamisen nykytila Euroopan unionin jäsenmaissa ja se, millaisia opetussisältöjä kyberkansalaistaitojen opettamiseen on olemassa. Tutkimuksessa myös selvitettiin EU-maiden kansallisia erityispiirteitä ja vaatimuksia kyberkansalaistaitoihin sekä Euroopan unionin aiheeseen liittyviä virallisia linjauksia. Keskeinen osa tutkimusraportin sisältöä on myös määritelmä siitä, että mitä kyberkansalaistaidoilla käytännössä tarkoitetaan ja miten ne määritellään, sillä pelkästään käsitteestä ”kyberturvallisuus” on eri EU-maissa monenlaisia määritelmiä. Hankkeen seuraavissa vaiheissa luodaan koko EU:n alueelle yhteisiä kyberkansalaistaitojen opetussisältöjä sekä kyberkansalaistaitoja opettava verkkopohjainen peli.

Tutkimustapa oli laadullinen ja tutkimusmenetelmä iteratiivinen suunnittelutieteen menetelmä. Tutkimuksessa hyödynnettiin useita eri aineistoja: taustoittava sisältöanalyysi tehtiin kyberkansalaistaitoja käsittelevistä dokumenteista, maakohtaisessa vertailuanalyysissa koottiin laadullinen primääriaineisto ja kartoittavassa kirjallisuuskatsauksessa kerättiin sekundääriaineisto. Mukana on myös pelianalyysi ja kyberturvallisuuden indeksien arviointi.

Kyberturvallisuuden perusosaaminen vaihtelee Euroopan unionin jäsenmaissa paljon, ja sama koskee kyberturvallisuuden yleistä tasoa. Keskeisimmät tutkimustulokset osoittavat, että Euroopan unionin jäsenmaissa on tahto kyberkansalaistaitojen luomiseen ja opettamiseen, mutta samalla on huomioitava kansallisia kulttuurisia erityispiirteitä pedagogisesti sekä huolehdittava eri ikäryhmien oppimisen edellytyksistä. Tärkeänä myös pidettiin kyberkansalaistaitojen opettamisen sisältöjen jatkuvaa kehittämistä kybertoimintaympäristön jatkuvan kehittymisen takia. Kyberkansalaistaitoja ei koeta pelkästään arkipäivän taitoina ja uhkiin varautumisena, vaan myös mahdollistajana alati digitalisoituvassa Euroopassa. Tässä tutkimuksessa analysoidut kyberkansalaistaitoja opettavat pelit olivat melko yksinkertaisia ja lineaarisia.

Tutkimusryhmän määritelmän mukaisesti kyberkansalaiseksi katsotaan henkilö, joka vakituisesti tai tilapäisesti asuu tai oleskelee EU-jäsenvaltion alueella ja käyttää digitaalisia palveluita tai hyötyy näiden palveluiden tuottamisesta suoraan tai välillisesti. Kybertoimintaympäristössä tarvittavien tietojen, taitojen ja kykyjen yhdistelmää kutsutaan kyberkansalaistaidoiksi. Tutkimuksessa on määritetty sisällöllisesti kyberkansalaistaitoihin yhdistyvät osa-alueet. Tutkimuksessa myös ilmeni, että EU:ssa tulisi olla yhteinen mittari kyberkansalaistaitojen tason määrittämiselle.

Tutkimusryhmä kiittää lämpimästi lukuisia tutkimukseen osallistuneita tahoja ja EU:n jäsenmaita, joiden tuki on ollut mittava tutkimushankkeen onnistumisen ja oleellisten tutkimustulosten havainnollistamisen kannalta.

Sisällys

1. Johdanto

1.1. Tutkimuksen tausta ja tavoitteet

Turvallisuutta ylläpitävä osaaminen ja tieto digitaalisessa ympäristössä on keskeinen osa meidän jokaisen turvallisuutta arkipäivässämme, koko Euroopassa. Kyse on jokaisen kansalaistaidosta tämän päivän maailmassa ja luottamusta vahvistavassa toiminnassa. Kyberturvallisuuden perustaidot kuuluvat kaikille, ja tätä ihmisten osaamiseen ja sivistykseen perustuvaa turvallisuuskulttuurin kehitystä tulee tietoisesti ja määrätietoisesti vahvistaa.

Tämä tutkimushanke pohjautuu käytännön tarpeeseen luoda turvallisuuskulttuuria digitaaliseen toimintaympäristöön, jonka keskiössä on ihminen. Kuten fyysisen maailman liikenteessä, on jokaisen tarpeellista nykymaailmassa osata digitaalisen maailman eli kybertoimintaympäristön perussäännöt ja toimintatavat osatakseen ja voidakseen toimia turvallisesti sekä hyödyntääkseen sen mahdollisuuksia. Tämä koskee kaikkia ikäryhmiä. Kyberympäristö ja ylipäänsä teknologia kehittyy jatkuvasti, uhkineen ja mahdollisuuksineen. Tällöin kyberkansalaistaidot on nähtävä jatkuvasti kehitettävinä ja päivitettävinä taitoina, jolloin jatkuvan oppimisen periaate sekä oikeanlaisen turvallisuuden asenteen luominen on kansalaistaitoja kehitettäessä tärkeää.

Tämä tutkimusraportti on ensimmäinen osa hankkeen kolmevaiheisessa toteutussuunnitelmassa, jolla luodaan yhtenäistä kyberkansalaistaito-opetusta koko Euroopan unionin alueelle ja etenkin kaikille eurooppalaisille. Tavoitteena tässä ensimmäisessä toteutusvaiheessa oli tutkimuksen keinoin selvittää kyberkansalaistaitojen opettamisen tapojen, näkemyksien ja materiaalien nykytila Euroopan unionin kaikissa jäsenvaltioissa. Nykytilan selvittämiseen kuului myös kansallisten pedagogisten ja kulttuuristen erityispiirteiden selvittäminen niin kansallisista lähtökohdista kuin Euroopan unionin yhtenäisvaatimuksien näkökulmista. Tutkimuksessa selvitettiin myös EU-maiden korkeakoulujen kyberturvallisuuskoulutustarjontaa. Korkeakouluissa rakennetaan kansalaistaitoja laajempaa kyberturvallisuusosaamista, mutta koulutettujen määrä (ja heidän suorittamiensa ohjelmasisältöjen laajuus) kuvaa sitä kouluttajakapasiteettia, joka on kyvykäs kouluttamaan kansalaisia ja esimerkiksi opettajia.

Ensimmäisen vaiheen tuloksena syntyi tämä raportti kyberkansalaistaitojen opettamisen nykytilasta koko Euroopan unionin alueella sekä sisällöllisistä vaatimuksista kyberkansalaistaitoihin Euroopan unionissa. Tutkimusraportin pohjalta hankkeen toisessa ja kolmannessa vaiheessa luodaan yhteinen digitaalinen oppimisportaali sekä peli kyberkansalaistaitojen kehittämiseksi. Hankkeella on vahva tutkimuksellinen perusta ensimmäisessä vaiheessa, jonka jälkeen siirrytään enemmän käytännön opetuksen ja oppimisen tuottamiseen tutkimustiedon pohjalta. Tärkeää on, että myös pedagogiset ja määritelmälliset kansalliset erityispiirteet eri EU-maissa tulevat jo tutkimusvaiheessa esille.

Tämän tutkimusraportin ja Aalto-yliopiston tutkimusryhmän tekemän tutkimuksen keskeisimmät tutkimuskysymykset ovat:

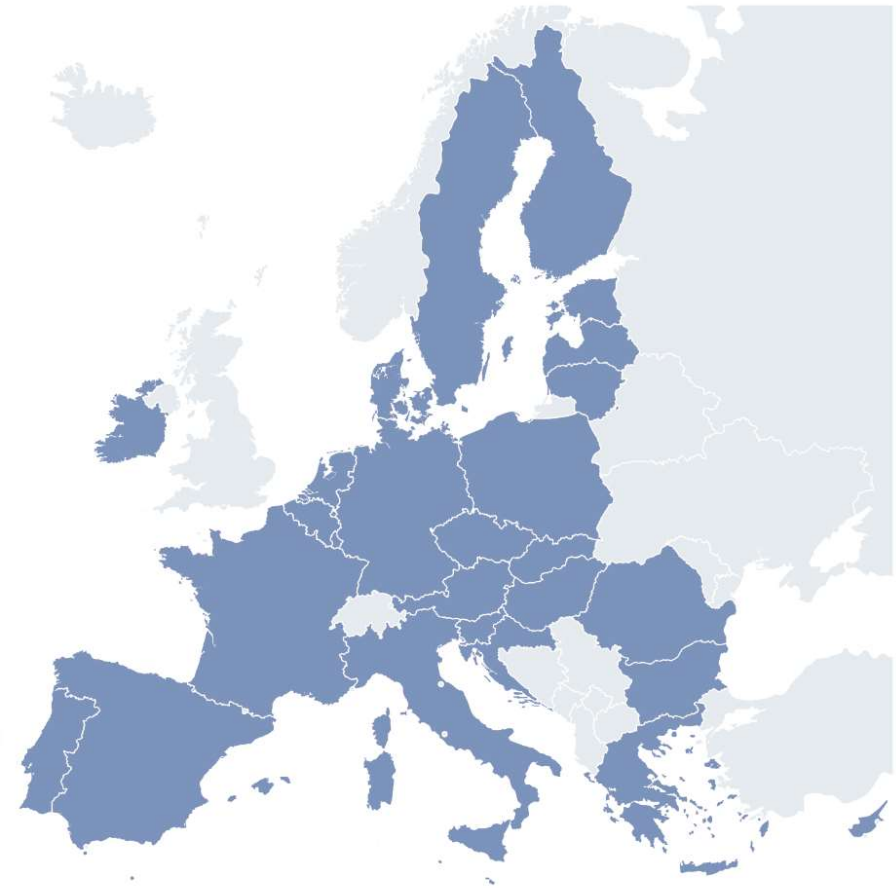
- Mikä on Euroopan unionin jäsenmaissa kyberkansalaistaitojen opettamisen nykytila ja millaisia opetussisältöjä on tällä hetkellä olemassa?

- Mitä kansallisia erityispiirteitä ja vaatimuksia kyberkansalaistaitoihin liittyy sekä eri EU-maissa että Euroopan unionin osalta?

- Millaisia toiveita ja näkemyksiä eri EU-maissa ja Euroopan unionissa yhtenäisiin kyberkansalaistaitojen opetussisältöihin sekä toteutukseen liittyy?

Keskeinen osa tutkimusraportin sisältöä on myös määritelmä siitä, mitä kyberkansalaistaidoilla käytännössä tarkoitetaan ja miten ne määritellään, sillä pelkästään käsitteestä ”kyberturvallisuus” on eri maissa ja eri tahoilla erilaisia määritelmiä. Tämä on ollut yksi keskeinen tutkimusraportin lähtökohta eli pyrkimys ymmärtää, mitä

tietoja ja taitoja eri EU-maissa kyberturvallisuuden kansalaistaitoihin yhdistetään ja millaisia kansallisia erityispiirteitä tähän liittyy.



Kuva 1: EU-maat.

Tutkimuksessa kerättiin laajasti tietoa eri lähteistä sekä henkilöhaastatteluilla tutkimuskysymysten avulla. Tietojen kerääminen tapahtui suorakontakteilla EU-jäsenmaihin (viranomaisiin ja oppilaitoksiin), ja tässä hyödynnettiin myös niin Euroopan unionin kuin Suomen valtion yhteysverkostoja sekä Euroopan unionin kyberturvallisuusviraston (ENISA) verkostoja. Tiedon keräämisessä ja sisältöanalyysissä korostuivat myös henkilöhaastattelut yhtenä tiedon keräämisen ja analysoinnin metodina, jotta ymmärretään paremmin opetusmateriaalien perustana olevia pedagogisia edellytyksiä. Tiedonhankintaa tehtiin systemaattisesti eri menetelmiä käyttäen ja yhdistäen. Kattavan tiedon keräämisen jälkeen tutkimusryhmä arvioi sekä laadullisesti että määrällisesti aineiston sisältöä huomioiden kansalliset erityispiirteet. Tällä varmistettiin jäsenmaiden ja unionin kansalaisten kyberosaamisen ja -tietämyksen lähtötaso sekä käytössä olevien opetusmenetelmien erityispiirteiden ymmärtäminen.

Kokonaisuutena hanke tuottaa kyberturvallisuuden perustaitojen opettamisen eurooppalaisen mallin ja sen käytännön toteutuksen, joka tapahtuu niin kybertaitojen opetuksen pelillistämisen kuin päivitettävää koulutusmateriaalia tarjoavan toiminnan kautta. Hankkeella vahvistetaan eurooppalaista kyberturvallisuutta sekä luodaan yhteisiä toimintatapoja ja -malleja eurooppalaisten perustaitoihin kyberturvallisuudessa. Kyse on sekä nykyhetken että tulevaisuuden kansalaistaidoista, jotka koskettavat kaikkia eurooppalaisia yhä enemmän digitalisoituvissa yhteiskunnissa. Tällöin näiden taitojen opettamiseen ja kouluttamiseen kannattaa panostaa ja samalla hyödyntää uudenlaisiakin oppimisen keinoja, joihin esimerkiksi pelillistäminen kuuluu. Hankkeen

menestyksellinen toteuttaminen Euroopan laajuisesti parantaa Euroopan unionin turvallisuutta sekä kilpailukykyä modernissa teknologiamaailmassa.

1.2. Tutkimuksen menetelmät

Tutkimustapa on laadullinen ja tutkimusmenetelmä iteratiivinen suunnittelutieteen menetelmä. Tutkimuksessa hyödynnettiin useita eri aineistoja: taustoittava sisältöanalyysi tehtiin kyberkansalaistaitoja käsittelevistä dokumenteista, maakohtaisessa vertailuanalyysissa koottiin laadullinen primääriaineisto ja kartoittavassa kirjallisuuskatsauksessa kerättiin sekundääriaineisto. Mukana ovat myös pelianalyysi ja indeksit. Lisäksi tutkimuksessa kartoitettiin Euroopan unionin kyberturvallisuuden kansalaistaitojen kehittämiseen liittyvää tutkimusta, ohjausta sekä toimeenpanoa. Sekundäärisen aineiston avulla pystyttiin arvioimaan primäärisen aineiston pohjalta tehdyn laadullisen tutkimuksen soveltuvuutta määritettyyn käyttötarkoitukseen.

Laadullinen lähestymistapa ja suunnittelutieteellinen menetelmä mahdollistivat teeman laaja-alaisen ja syvällisen, iteroivan tarkastelun. Menetelmän avulla luotiin perusteellinen pohja tulosten vaiheittaiselle rakentumiselle. Suunnittelutieteen tutkimusmenetelmällä voidaan luoda luotettavia ratkaisuja yhteiskunnallisiin ongelmiin, kuten kansalaisten kyberturvallisuustaitojen kehittämiseen. Sen avulla pystytään lähentämään tieteellisen teoriapohjan ja käytännön toiminnan välistä yhteyttä ja vuorovaikutusta. Suunnittelutiede on sekä prosessi että jatkuvaa, vaiheittain tarkentuvaa ongelmanratkaisua. Tuotosten vaiheittainen luominen, jatkuva arviointi (mukaan lukien soveltuvuus ja hyödyllisyys) ja uudelleentarkentaminen tuottavat uutta ymmärrystä tutkittavasta ilmiöstä. Suunnittelutieteen menetelmä on joustava ja sitä voidaan soveltaa monitahoisten ongelmien ratkaisuun.

Tutkimuksessa kartoitettiin, hankittiin, luokiteltiin, kuvattiin ja analysoitiin erilaisia aineistoja. Tieteellisen tutkimustiedon tulee olla luotettavaa ja relevanttia. Kehittävässä suunnittelututkimuksessa tavoitteena on käytännön tiedollisen ymmärryksen lisääminen, toiminnan parantaminen ja ratkaisujen synnyttäminen havaintojen pohjalta. Tässä suunnittelututkimuksessa tutkimusprosessi käynnistettiin laadullisella sisältöanalyysillä, jossa kartoitettiin kyberturvallisuuden kansalaistaitojen opettamisen teoriapohjaa sen yhteiskunnallisen merkityksellisyyden näkökulmasta.

Suunnittelututkimuksessa edetään vaiheittain kehittämällä ”kansalaisten kyberturvallisuuden opettamisen” tietoperustaa arvioimalla ja tarkentamalla tuloksia. Alkuvaiheessa tehtiin sisältökatsaus olemassa olevaan tieto- ja teoria-aineistoon. Tuloksia tarkennettiin arvioimalla niitä kartoittavan kirjallisuuskatsauksen ja haastattelututkimuksen menetelmin. Kehittävää tutkimustulosta arvioitiin sekä relevanssin että täsmällisyyden näkökulmasta lukuisilla kriittisillä tarkasteluilla. Tämä tapahtui peilaamalla löydöksiä kerättyyn empiiriseen haastatteluaineistoon, kirjalliseen aineistoon ja opetuspelianalyyseihin.

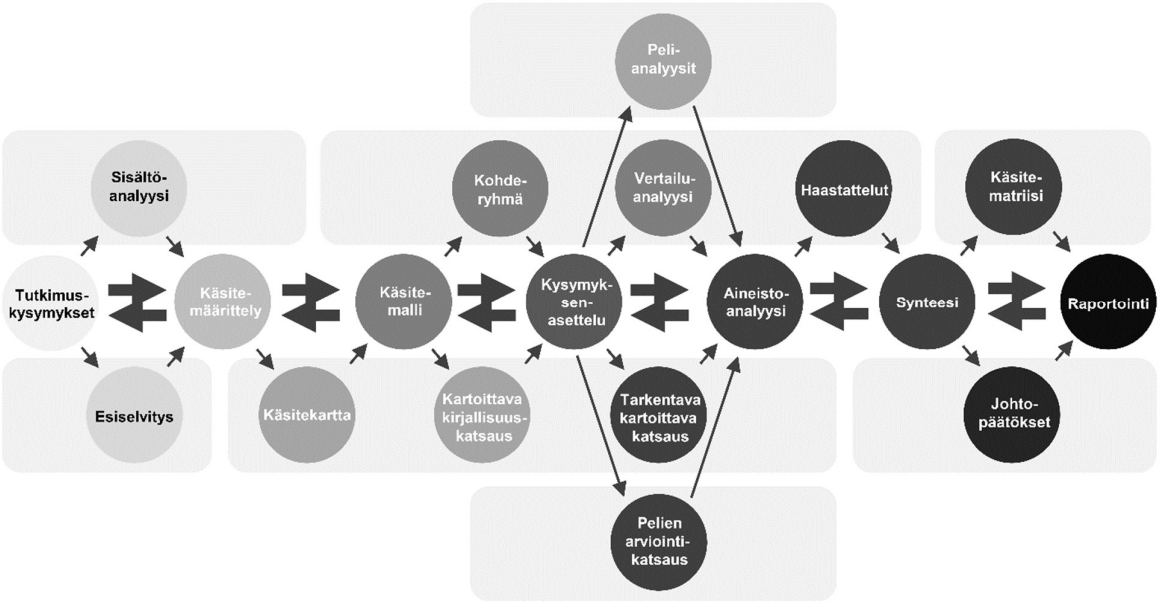
1.2.1. Määritelmät

Ennen tutkimuksen aloittamista ja tutkijaryhmän työn käynnistämistä määriteltiin tutkimuksen kohde laadullisen sisältöanalyysin keinoin. Käsite *kyberkansalaistaidot* on selkeästi määrittelemättä ja eri yhteyksissä täsmentämättä. Tutkimushankkeen käsitteiden analysointi aloitettiin helmikuussa 2022, kun tutkimushanketta käynnistettiin ensimmäisten keskustelujen pohjalta. Projektin aikana käsitteen määritelmää tarkennettiin useita kertoja hankkeen valmistelijoiden parissa, yhdessä tutkimusryhmän kanssa ja muutamien aihepiiriä lähellä olevien tahojen kanssa. Tapaamisten pohjalta syntyi erittäin avara ja laaja määritelmä kyberkansalaistaidoista. Käsitemäärittelyä syvennettiin mentaalikarttatyöskentelyn avulla. Määritelmällä tutkijat haluavat korostaa kyberturvallisuuden laaja-alaisuutta. Tutkimuksessa tarkasteltiin kansalaisten kyberturvallisuustaitojen näkökulmaa laajasti uusien ja kehittyvien uhkakuvien kautta. Laaja-alainen määritelmä mahdollistaa paremmin epävarman ja monitahoisen tulevaisuuden huomioinnin osana tutkimusta. Määritelmän työstäminen saatiin valmiiksi joulukuussa 2022 ja se löytyy luvusta 5.

1.2.2. Menetelmät

Tutkimus on aineistolähtöinen laadullinen tutkimus, jossa hyödynnettiin useita laadullisen tutkimuksen menetelmiä aineistojen keräämiseen ja validointiin. Tämä tutkimus toteutettiin maalis-joulukuussa 2022 neljäntoista tutkijan voimin, ja se koski koko Euroopan unionin aluetta. Tutkimuksessa käytettiin seuraavia aineistolähteitä: tausta-aineisto on muodostettu sisältöanalyysilla, kartoittavan kirjallisuuskatsauksen aineistona ovat aiemmin julkaistut akateemiset tutkimusartikkelit, ja maakohtaisissa analyyseissa aineisto kerättiin laajasti eri julkisista lähteistä ja teemahaastatteluin. Maakohtaisesti selvitettiin kyberturvallisuuden opettamisen ja kouluttamisen nykytilaa, kansallisia ja kielellisiä käsitteitä, painotuksia, toimintamalleja, kyberturvallisuuden toimijoita, olemassa olevia palveluita ja pelejä, kohderyhmiä ja kulttuurin vaikutusta nykytilan sekä tulevaisuuden taitojen näkökulmasta.

Tutkimusryhmä edustaa moninaisesti kyberkansalaistaitojen eri näkökulmia, ulottuvuuksia, toimi- ja oppialoja. Yhteiseen digitaaliseen työtilaan tallennettiin hankkeen kannalta keskeiset Euroopan unionin aluetta koskevat aineistot, hanke- ja toimijatiedot, pelilinkit ja arviointimallit. Hankkeen alussa tutkimusryhmän käyttöön luotiin yhteistyö- ja aineistoalusta, määriteltiin yhteinen lähdeaineistojen hallintamenetelmä, kuvattiin yhteiset tutkimuksen toimintaperiaatteet, laadittiin yhtenäinen maa-analyysien malli ja jalostettiin yhteinen tulosten arviointimalli säännöllisissä tutkimusryhmän tapaamisissa. Tutkimuksessa tukeuduttiin ensisijaisesti primäärilähteisiin ja maiden yleisen kyberturvallisuuden kypsyyden osalta sekundäärisiin lähteisiin. Primääriaineistona olivat haastattelut, dokumentit, viranomaisraportit ja kansalliset selvitykset. Kunkin maan osalta lähteistä saatua informaatiota tarkasteltiin tutkimuskysymysten, kokonaisuuden, teoriapohjan ja tutkimuskirjallisuuden valossa.



Kuva 2: Iteratiivisen tutkimusprosessin vaiheet.

Tutkijat tekivät yli 200 haastattelua eri EU-maissa, analysoivat noin tuhat eri verkkosivustoa ja kartoittivat yli 500 eri tutkimusta, raporttia tai julkaisua. Kartoittavan kirjallisuuskatsauksen laajuus on kuvattu luvussa 2.

1.3. Keskeiset käsitteet

Kybertoimintaympäristö

Euroopan unionin mukaan kybertoimintaympäristöllä tarkoitetaan ihmisten luomaa digitaalista rinnakkaistodellisuutta, joka maailmanlaajuisesti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta toisiinsa ihmisiä ja laitteita valtioiden rajojen yli.[1]

Jo Suomen vuoden 2013 kyberturvallisuusstrategiassa kybertoimintaympäristöstä todettiin: ”Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi sekä yksittäisten kansalaisten, yritysten että koko yhteiskunnan kannalta. Uhkia muodostavat toimijat ovat entistä ammattimaisempia ja niihin voi kuulua myös valtiollisia tahoja. Kyberrikollisuuden ja taloudellisen hyödyn tavoittelun ohella kansalaisiin kohdennettuja toimia voidaan käyttää poliittisen painostuksen välineinä ja sotilaallisena vaikuttamiskeinona.” [2] Kybertoimintaympäristöön viitataan usein myös termillä digitaalinen toimintaympäristö.[3]

Kyberturvallisuus

Suomen Turvallisuuskomitean määritelmän mukaan ”kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.”[4]

Kyberturvallisuuden lähitermi, digitaalinen turvallisuus tai digiturvallisuus (kyberturvallisuuteen viitataan usein tällä, laajemmalla termillä kyberkansalaistaitojen käsittelemisen yhteydessä) on VAHTI-riskienhallintasanaston mukaan ”tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa ja toiminta sekä siellä että siihen liittyen on turvallista ja hallittua, myös häiriötilanteissa” [5] . Digitaalinen turvallisuus voidaan nähdä kattokäsitteenä, joka keskittyy digitaalisen toimintaympäristön lisäksi laajasti siihen, mikä vaikuttaa tähän toimintaympäristöön ja mihin toimintaympäristö vaikuttaa. Esimerkiksi politiikka ja luottamus ovat tällaisia vaikuttavia tekijöitä. OECD on niin ikään määritellyt digiturvallisuuden laajasti ja katsoo siihen kuuluvan muun muassa nämä elementit (eivät tosin aivan kokonaisuudessaan): digiturvallisuuden riskienhallinta, jatkuvuudenhallinta, tietosuoja, tietoturvallisuus sekä kyberturvallisuus. Kun kyberturvallisuuden voidaan nähdä liittyvän kansallisen tai kansainvälisen ulottuvuuden turvallisuuteen, digiturvallisuus on lähempänä kansalaista ja sitä voidaan tarkastella yksittäisen henkilön tavoitteiden ja toiminnan kautta. Digiturvallisuuteen kuuluvat myös tekniset, sosiaaliset ja taloudelliset aspektit.[6]

1.4. Keskeiset indeksit

Digitalisaatioon ja kyberturvallisuuteen liittyvissä tutkimuksissa, arvioinneissa ja tilastoinneissa on tullut tavaksi mitata tarkastelukohteiden maturiteettia ja kehityksen tasoa eri viitekehyksien ja indeksien avulla. Tutkimusryhmä rajasi tutkimusaineiston vertailevaan analyysiin kolme yleistä ja tehtävään parhaiten soveltuvaa indeksiä. Tyypillisesti kyberturvallisuudessa yleiset ja vakiintuneet indeksit mittaavat kansallista varautumista suhteessa kyberhyökkäyksiin ja suhteuttavat varautumisen tasoa kohdemaan digitalisaation tasoon painottaen eri osa-alueita, kuten voimassa olevaa lainsäädäntöä, koulutusohjelmia ja koordinointia.

Global Cybersecurity Index, ITU (GCI)

Kansainvälinen televiestintäliitto (ITU) on Yhdistyneiden kansakuntien (YK) tieto- ja viestintäteknologiaan (ICT) erikoistunut virasto. Viraston vuodesta 2015 alkaen julkaisema maailmanlaajuinen kyberturvallisuusindeksi GCI

(Global Cybersecurity Index) auttaa jäsenvaltioita tunnistamaan parannuskohteita kyberturvallisuuden edistämiseksi.

GCI mittaa eri maiden sitoutumista kyberosaamisen kehittämiseen ja tietoisuuden lisäämiseen. Kyberturvallisuuden soveltamisala on erittäin laaja kattaen monia toimialoja ja eri sektoreita. Kunkin maan kehitys- tai sitoutumistasoa arvioidaan viiden ulottuvuuden avulla: i) lainsäädännölliset toimenpiteet, ii) tekniset toimenpiteet, iii) organisatoriset toimenpiteet, iv) valmiuksien kehittäminen ja v) kansallinen yhteistyö.

GCI mittaa tietoverkkorikollisuutta ja kyberturvallisuutta käsittelevää lainsäädäntöä ja määräaviä käytäntöjä, kuten tietosuojaan tai kriittisen infrastruktuurin turvallisuuteen liittyviä lakeja ja asetuksia. Indeksi arvioi teknisten kyvykkyyksien toteuttamista (mukaan lukien kansallinen CIRT-toiminta) julkishallinnon virastoissa ja toimialakohtaisissa organisaatioissa. Indeksi mittaa kyberturvallisuuden toimeenpanoa kansallisen strategian ja tätä toteuttavan toiminnan organisoinnin kautta. Valmiuksien kehittämistä mitataan olemassa olevien tietoisuuskampanjoiden, kurssien, koulutusten ja kyberturvallisuuden kehittämiseen suunnattujen kannustimien avulla. Kansallisen yhteistyökyvykkyyden mittaamisen ja arvioinnin keskipisteessä on julkishallinnon ja yksityisen sektorin välinen yhteistoiminta, Public Private Partnership (PPP). Indeksi muodostuu yhdistämällä eri osa-alueiden tulokset kokonaispisteytykseksi.

Kyberkansalaistaitojen osaamisen lisäämiseksi turvallisuustietoisuutta tulisi parantaa kansalaisten, hallitusten ja organisaatioiden tasolla. GCI mittaa kyberturvallisuuden sisällyttämistä kansallisiin opetussuunnitelmiin, aina perus- ja toisen asteen koulutuksesta akateemiseen maailmaan saakka. Indeksissä huomioidaan yrityksille, kolmannelle sektorille ja valtion virastoille suunnatut erilliset tietoturvakampanjat sekä saatavilla olevat palvelut.

ITU-viraston ja GCI:n tarkoituksena on sekä edistää hyviä käytäntöjä että kehittää maailmanlaajuista kyberturvallisuuskulttuuria ja -yhteistyötä. Kerättyjen tietojen avulla ITU-virasto tuottaa havaintoja ja käytäntöjä, joita eri jäsenvaltiot voivat soveltaa kansalliseen toimintaansa.[7]

National Cyber Security Index (NCSI)

Vuonna 2002 perustettu e-Governance Academy (eGA) on Viron hallituksen, Open Society Instituten (OSI) ja YK:n kehitysohjelman yhteinen, voittoa tavoittelematon säätiö. eGA:n missiona on lisätä yhteiskuntien kilpailukykyä digitaalisessa muutoksessa läpinäkyvyyden ja avoimuuden keinoin. Se tuottaa, kehittää ja ylläpitää reaaliaikaista kyberturvamittaria, National Cyber Security -indeksiä (NCSI).

NCSI mittaa kohdemaiden ennalta ehkäisevän kyberturvallisuuden tasoa, kuten valmiutta hallita tietoturvatapahtumia ja torjua kyberrikollisuutta, kykyä hallita ja estää laajamittaisia kriisejä sekä osaamisen kehittämistä laaja-alaisesti. NCSI keskittyy olemassa ja mitattavissa oleviin valtionhallinnon kyberturvallisuusohjelmiin ja -toimenpiteisiin, joita ovat: i) voimassa oleva lainsäädäntö (lait, asetukset ja säädökset), ii) perustetut toimielimet (olemassa olevat organisaatiot ja osastot), iii) yhteistyömuodot (komiteat ja työryhmät) ja iv) tulokset (käytännöt, harjoitukset, tekniikat, verkkosivustot sekä kansalliset ohjelmat ja toteutukset). Arvioinnissa kiinnitetään huomiota siihen, miten olemassa olevat ratkaisut ja palvelut sijoittuvat suhteessa palvelunestohyökkäyksiin, tietomurtoihin ja tietovuotoihin. NCSI koostuu yhteensä 46 indikaattorista, joiden suhteelliset painoarvot indeksissä määrittää vuosittain kokoontuva asiantuntijaryhmä.

Kyberkansalaistaitojen näkökulmasta NCSI arvioi koulutusta ja ammatillista kehittymistä eri koulutusasteilla, joita ovat perus- ja toisen asteen koulutus, alempi ja ylempi korkeakoulutus sekä jatkotutkintokoulutus. Koulutusyhteistyön ohella kyberkansalaistaitoihin olennaisesti liittyvän kybertietoisuuden ja resilienssin kannalta merkittävää on kohdemaiden valmius tunnistaa ja analysoida kyberuhkia sekä tuottaa tilannekuvaa ja uhkatietoa kansalaistensa hyväksi. Indeksissä arvioidaan myös kyberturvallisuuden ammatillisten yhdistyksien ja yhteistyöfoorumien toimintaa.

NCSI:n visiona on kehittää kyberturvallisuuden mittaustyökalu, joka tarjoaa tarkkaa ja ajantasaista tietoa kohdemaiden kyberturvallisuudesta ja siihen liittyvistä kehityskohteista.[8]

Digitaalitalouden ja -yhteiskunnan indeksi (DESI)

Euroopan komissio on seurannut jäsenvaltioiden digitaalisen kehityksen tasoa ja edistymistä digitaalitalouden ja -yhteiskunnan indeksiä (DESI) koskevissa raporteissa vuodesta 2014 lähtien.

DESI on yhdistelmäindeksi, joka tiivistää Euroopan digitaalisen suorituskyvyn kannalta merkitykselliset indikaattorit ja seuraa EU:n jäsenvaltioiden kehitystä viidessä ulottuvuudessa: i) tietoliikenneyhteydet, ii) inhimillinen pääoma, iii) internetin käyttö, iv) tekniikan integrointi ja käyttäminen sekä v) julkiset digitaaliset palvelut.

Euroopan komissio on määrittänyt indikaattoreita käytännön toiminnallisiin ryhmiin, jotka kuvaavat joitakin eurooppalaisen tietoyhteiskunnan keskeisiä toimialoja (tietoliikenne, matkaviestintä, internetpalvelut, sähköinen hallinto, sähköinen liiketoiminta, tieto- ja viestintäteknologian koulutus, tutkimus ja kehitys).

Raportissa yhdistetään viiden eri osa-alueen DESI-indikaattorien määrälliset tiedot maakohtaisiin toimintalinjoihin, näitä koskeviin näkemyksiin ja vallitseviin käytäntöihin. Jäsenvaltioiden raportit sisältävät maaprofiileja, jotka auttavat jäsenvaltioita yksilöimään ja tunnistamaan osa-alueita, jotka edellyttävät tehtävien priorisointia ja kehitystoimien kohdistamista.

DESI mittaa digitaalisia taitoja suhteessa henkilöiden kykyyn käsitellä ja ymmärtää tietoa. Indeksi arvioi internetin käytön aktiivisuutta, käyttäjien viestintä- ja yhteistyötaitoja sekä heidän kykyään käyttää digitaalisia palveluita. Se huomioi digitaalisten taitojen kohdalla sisällön tuottamiseen liittyviä kyvykkyyksiä sekä suoraan ongelmanratkaisuun tai kyberturvallisuuteen liittyviä taitoja, kuten käyttäjän kykyä suojata käyttämänsä laitteet, käsittelemänsä tiedon ja kykyä huolehtia yksityisyydestään.[9]

Viitteet

[1] ”Kyberturvallisuus ja kybertoimintaympäristö,” *Ulkoministeriö*, luettu 27.12.2022, https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto.
[2] Turvallisuuskomitea, ”Suomen kyberturvallisuusstrategia,” *Valtioneuvoston periaatepäätös 24.1.2013* (Helsinki: Turvallisuuskomitean sihteeristö, 2013), 1.
[3] Valtiovarainministeriö, ”Julkisen hallinnon digitaalinen turvallisuus, Julkisen hallinnon ICT,” *Valtiovarainministeriön julkaisuja – 2020:23* (Helsinki: Valtiovarainministeriö, 2020), 17.
[4] Turvallisuuskomitea, ”Yhteiskunnan turvallisuus: Yhteiskunnan turvallisuusstrategia”, *Valtioneuvoston periaatepäätös 2.11.2017* (Helsinki: Turvallisuuskomitean sihteeristö, 2017), 10, 22.
[5] Digi- ja väestötietovirasto, *VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta, riskiviestintään* (Digi- ja väestötietovirasto, 2022), 16.
[6] Digi- ja väestötietovirasto*, VAHTI-riskienhallintasanasto*, 16, 68.
[7] “Global Cybersecurity Index,” *ITU,* luettu 1.12.2022, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
[8] “Purpose,” *NCSI*, luettu 1.12.2022, https://ncsi.ega.ee/methodology/.
[9] “The Digital Economy and Society Index (DESI),” *Euroopan komissio*, luettu 1.12.2022, https://digital-strategy.ec.europa.eu/en/policies/desi.

2. Kyberkansalaistaitojen opettaminen ja kouluttaminen EU-tasolla sekä aiempi tutkimus

2.1. Kyberkansalaistaitojen opettamisen ja kouluttamisen ohjaus ja käytännön toimet EU-tasolla

Kyberkansalaistaitoja pyritään parantamaan EU-tasoisella ohjauksella ja kyberturvallisuuden kehittämiskapasiteetin tukemisella. Osaamisen kehittämistä ohjataan esimerkiksi strategioiden, politiikkojen ja viitekehysten avulla. Myös EU-rahoitteiset hankkeet pyrkivät parantamaan kyberosaamista unionin alueella. Käytännön toimenpiteistä EU-tasolla vastaa Euroopan unionin kyberturvallisuusvirasto (The European Union Agency for Cybersecurity, ENISA).[10]

2.1.1. Kyberturvallisuuden kansalaistaitojen koulutuksen ohjaus

Vuonna 2020 julkaistussa Euroopan unionin kyberturvallisuusstrategiassa todetaan, että strategialla vahvistetaan ”Euroopan sietokykyä kyberuhkia vastaan ja varmistetaan, että kaikki kansalaiset ja yritykset voivat hyötyä täysimääräisesti luotettavista palveluista ja digitaalisista välineistä”[11]. Strategian mukaan noin kaksi viidesosaa EU-kansalaisista on kohdannut turvallisuuteen liittyviä ongelmia ja kolme viidestä kokee, etteivät he pysty suojautumaan kyberrikollisuudelta. Kolmannes kansalaisista on saanut huijaussähköposteja tai -puheluita, mutta 83 prosenttia ei ole koskaan ilmoittanut kohtaamastaan kyberrikollisuudesta. Strategiassa linjataan, että EU:n digitaalisen koulutuksen toimintasuunnitelman (The Digital Education Action Plan) avulla pyritään lisäämään kansalaisten tietoisuutta kyberturvallisuudesta; kohderyhminä ovat erityisesti lapset, nuoret ja organisaatiot (erityisesti pienet ja keskisuuret). Siinä todetaan myös, että muodollisen koulutuksen ja opetuksen (mukaan lukien ammatillisen koulutuksen), kyberturvatietoisuuskoulutuksen sekä kyberharjoitusten tulisi entisestään parantaa kyberturvallisuustaitoja EU-tasolla. Tavoitteena on, että kaikki, jotka käyttävät internetiä, ylläpitävät samalla globaalia, avointa, vakaata ja turvallista kyberavaruutta, jossa kaikki voivat elää turvallista digitaalista elämäänsä.[12,13]

EU:n 2030 Digitaalinen kompassi sisältää vision ja tavoitteet digitalisaatiolle vuoteen 2030 mennessä. Riippuvuus EU:n ulkopuolella tuotetuista teknologioista ja muutamista suurista teknologiayrityksistä sekä näiden riippuvuuksien vaikutukset myös kansalaisten elämään mainitaan kompassissa ongelmallisiksi. Siinä todetaan, että Euroopan tulevaisuuden ja kollektiivisen resilienssin kannalta on tärkeää, että kansalaiset ovat digitaalisesti osaavia ja heillä on tarvittavat perustaidot. Tavoitteena on, että Euroopan aikuisista kansalaisista 80 prosentilla on vähintään perustason digitaaliset taidot vuonna 2030. Näihin taitoihin luetaan muun muassa disinformaation ja huijausyritysten tunnistaminen sekä suojautuminen kyberhyökkäyksiltä ja verkkohuijauksilta. Lisäksi todetaan, että lasten on tärkeää oppia ymmärtämään tietotulvaa, jonka keskellä he elävät. Kompassin tavoitteissa mainitaan myös, että kansalaisten tulee kunnioittaa perustavanlaatuisia EU-oikeuksia, kuten henkilötietojen ja yksityisyyden suojaa, oikeutta tulla unohdetuksi ja yksilöiden tekijänoikeuksien suojaamista digitaalisessa ympäristössä.[14]

EU:n digitaalisen koulutuksen toimintasuunnitelmassa (Digital Education Action Planissa) todetaan, että digitaalinen kompetenssi on eurooppalaisessa avaintaitojen elinikäisen oppimisen viitekehyksessä (European Reference Framework of Key Competences for Lifelong Learning) osana tietoja, taitoja ja asenteita, joita ihmiset tarvitsevat elämässään. Näiden oppimisen tulee alkaa yksilön elämän varhaisessa vaiheessa ja jatkua läpi elämän. Teknisten taitojen lisäksi niin kutsuttujen pehmeiden taitojen (soft skills) opetus nähdään tärkeänä. Digitaalisen kompetenssin kehittymiseen tähtäävässä opetuksessa kannustetaan suosimaan avoimia

luokkahuoneita, tosielämän kokemuksia, projekteja, uusia oppimisvälineitä ja materiaaleja sekä kaikille avoimia oppimisresursseja. Myös verkossa tapahtuvaan yhteistyöhön kannustetaan. Digitaaliseen kompetenssiin sisältyvät muun muassa kriittinen ajattelu, medialukutaito, turvallisuustaidot ja yksityisyyteen liittyvät taidot, mutta näiden opettaminen ja kouluttaminen väestölle laajemmin on haaste. Tarvitaan unionin laajuista yhteistyötä parhaiden käytäntöjen vaihdon sekä vertaisoppimisen osalta, jotta koulutusta eri maissa voidaan kehittää.[15]

EU:ssa on määritelty digitaalista kompetenssia DigComp-viitekehyksen (DigComp 2.2, The Digital Competence Framework for Citizens) avulla. Uusin versio viitekehyksestä julkaistiin vuonna 2022, ja se pyrkii parantamaan yhteistä ymmärrystä siitä, mitä digitaalinen kompetenssi tarkoittaa. DigComp-viitekehyksessä on oma osio turvallisuuskompetenssille, mutta myös muihin kompetensseihin sisältyy taitoja, joiden voidaan katsoa olevan kyberkansalaistaitoja.[16] Kompetenssialueet ovat 1) informaatio- ja datalukutaito, 2) viestintä ja yhteistyö, 3) digitaalinen sisällöntuotanto, 4) turvallisuus ja 5) ongelmanratkaisu.[17]

Turvallisuus-kompetenssialueeseen kuuluu laitteiden, sisältöjen, henkilötietojen ja yksityisyyden suojeleminen digitaalisessa ympäristössä, fyysisen ja psyykkisen terveyden suojeleminen, tietoisuus yhteiskunnallista hyvinvointia ja osallisuutta lisäävistä digiteknologioista sekä tietoisuus digiteknologioiden käytön ympäristövaikutuksista. [18] Ongelmanratkaisu-kompetenssialueeseen kuuluu ongelmien ja tarpeiden tunnistaminen, konseptuaalisten ongelmien sekä ongelmatilanteiden ratkaiseminen digitaalisissa ympäristöissä, ajan tasalla pysyminen digitaalisessa kehityksessä sekä digityökalujen käyttö innovointiin. Kaikkien näiden taitojen voidaan nähdä liittyvän myös kyberkansalaistaitoihin.[19] Viestintä ja yhteistyö -kompetenssialue sisältää myös kyberkansalaistaidoiksi liittyviä taitoja, kuten vuorovaikuttamisen ja yhteistyön digitaalisissa kanavissa sekä digitaalisen läsnäolon hallinnan (digijalanjäljen kontrolloinnin sekä identiteetin ja maineen hallinnan).[20] Informaatio- ja datalukutaito -kompetenssialueen osalta mainittavia taitoja ovat erityisesti lähdekritiikki sekä informaation elinkaaren hallinta.[21] Digitaalisen sisällöntuotannon kompetenssialueelta kyberkansalaistaidoiksi voidaan lukea tekijänoikeusperiaatteiden ymmärtäminen sekä se, että yksilö osaa käyttää teknologioita ja palveluita niin, ettei vaaranna sisältöä tai tietoturvallisuutta.[22]

EU:n kyberresilienssisäädös (Cyber Resilience Act, CRA) keskittyy pääasiassa vahvistamaan kyberturvallisuuteen liittyvää sääntelyä, jotta laitteisto- ja ohjelmistotuotteiden turvallisuus voidaan varmistaa. Säädös koskettaa kuitenkin myös kansalaisia, sillä toisena tunnistettuna päätavoitteena on luoda olosuhteet, joissa käyttäjät voivat huomioida kyberturvallisuuden valitessaan ja käyttäessään digitaalisia tuotteita. Erityisinä tavoitteina mainitaan digitaalisten tuotteiden turvaominaisuuksien läpinäkyvyyden parantaminen sekä kuluttajien mahdollisuuksien lisääminen sen osalta, että he voivat käyttää digitaalisia palveluita turvallisesti.[23]

2.1.2. Kyberturvallisuustaitojen kehittämiseen liittyvät EU-organisaatiot ja yhteistyötahot

EU:n kyberturvallisuusvirasto ENISA jatkaa Euroopan unionin verkko- ja tietoturvaviraston työtä ja perustuu sen rakenteisiin, mutta sillä on vahvempi asema ja pysyvä toimeksianto. ENISA tuottaa ohjeistuksia ja raportteja kyberkansalaistaitojen kehittämisestä ja julkaisi joulukuussa 2022 raportin, joka käsittelee kyberopetuksen (perusopetuksessa) tilaa EU-jäsenvaltioissa. Tämän raportin pohjalta ENISA luo tiekartan, joka ohjaa työtä kyberturvallisuusopetuksen lisäämiseksi EU-jäsenvaltioissa.[24,25]

ENISAlla on paljon kyberturvallisuuskoulutukseen ja -tietoisuuteen liittyvää toimintaa. Se on päävastuussa vuosittaisesta Euroopan kyberturvallisuuskuukaudesta ja tuottaa siihen liittyvää materiaalia suoraan kansalaisille sekä eri toimijoiden käyttöön ja järjestää tapahtumia. Se järjestää vuosittain Euroopan kyberturvallisuushaasteen (European Cybersecurity Challenge, ECSC) kyberturvallisuudesta kiinnostuneille nuorille. Tapahtuma kokoaa yhteen nuoria ympäri Eurooppaa verkostoitumaan, tekemään yhteistyötä ja kilpailemaan. ECSC:n tavoitteena on kannustaa nuoria kyberturvallisuusuralle kehittämällä heidän taitojaan ja tarjoamalla kontaktipinnan alaan.[26] ENISA järjestää myös kansainvälisen, globaalin kyberturvallisuushaasteen

(International Cybersecurity Challenge, ICC)[27] yhdessä kansainvälisten organisaatioiden kanssa. Myös tämän tapahtuman tavoitteena on houkutella nuoria kyberturvallisuusalalle ja lisätä ylipäätään tietoisuutta kyberturvallisuuskoulutuksen tarpeesta ja kyberturvallisuudessa tarvittavista taidoista globaalilla tasolla. ENISAn tuottama eurooppalainen kyberturvataitojen viitekehys (European Cyber Security Skills Framework, ECSF) [28] pyrkii luomaan yhteisen ymmärryksen kyberturvallisuuteen liittyvistä rooleista, kompetensseista, taidoista ja tiedoista, jotta kyberosaajapulaan pystytään vastaamaan ja tukemaan kyberturvallisuuteen liittyvien koulutusohjelmien suunnittelua. ENISA on myös luonut kyberkorkeakoulutustietokannan (Cyber Higher Education Database, CyberHEAD)[29], jossa on lueteltuna akateemiset kyberturvallisuustutkinnot EU:n alueella.

ENISA organisoi erilaisia kyberturvallisuustietoisuuskampanjoita, joiden kohderyhmänä ovat EU-kansalaiset ja -organisaatiot. Näistä tunnetuin on aiemmin mainittu Euroopan kyberturvallisuuskuukausi, jossa on vuosittain vaihtuva teema.[30] Lisäksi se järjestää muun muassa terveydenhuoltosektorilla toimiville ja heidän potilailleen kohdistettua kyberterveysviikkoa (Cyber Health Week). [31] ENISA myös järjestää eri kohderyhmille tarpeen mukaan kyberturvallisuustietoisuuskampanjoita.[32] ENISAlla on parhaillaan tekeillä lisämateriaalia kansalaisten kyberturvatietoisuuden kasvattamiseen. Organisaatiossa toimii myös äskettäin kybertietoisuuden lisäämiseksi perustettu Ad hoc -työryhmä, jossa on mukana henkilöitä eri sidosryhmäorganisaatioista ympäri Eurooppaa. Työryhmän tavoitteena on muun muassa kehittää kyberturvallisuuden koulutusta ja koulutusmateriaaleja, auttaa suunnittelemaan ajankohtaisia tiedotuskampanjoita ja mitata niiden vaikuttavuutta.[33,34,35]

Vuonna 2021 perustettiin EU:n kyberturvallisuuden kompetenssikeskus (The European Cybersecurity Competence Centre, ECCC), jonka päätoimipaikka on Romanian Bukarestissa. Tällä hetkellä Euroopan komissio toimii keskuksen virkaatekevänä pääjohtajana, kun sen rakenteita luodaan. Keskus tulee ohjaamaan EU-maiden kansallisten kyberkoordinaatiokeskusten verkostoa ja unionin kyberturvallisuuteen liittyvää rahoitusta. Sen tavoitteena on lisätä kybertutkimuksen huippuosaamista ja EU:n kilpailukykyä kyberturvallisuuden alalla. Euroopan komission puheenjohtaja Ursula von der Leyen kertoi syyskuussa 2022 vuonna 2023 kompetenssikeskuksen yhteyteen perustettavasta kybertaitoakatemiasta (Cybersecurity Skills Academy) liittovaltion tilaa koskevassa aiekirjeessään.[36,37]

EU-tasolla kyberturvallisuustaitoja kehittää myös European Cyber Security Organisation (ECSO), joka on Euroopan komission yhteistyötaho kyberturvallisuuden julkisen ja yksityisen sektorin kumppanuuden toteuttamisessa. Se on useiden sidosryhmien ja alojen muodostama kumppanuusorganisaatio, joka yhdistää suuret yritykset, pk-yritykset ja start-upit, tutkimuskeskukset, yliopistot, keskeisten palvelujen loppukäyttäjät ja operaattorit, klusterit ja yhdistykset sekä paikallisen, alueellisen ja kansallisen yleisön. ECSO tukee kyberturvallisuuden ja ICT-turvallisuusekosysteemin kehitystä ja etuja (mukaan lukien koulutus ja kyberturvallisuustietoisuus).[38] Mainittava taho on myös Council of European Professional Informatics Societies (CEPIS), jonka tarkoituksena on tarjota riippumatonta ammatillista asiantuntemusta IT-alan lainsäädännöstä ja kyberturvallisuuskysymyksistä. Ryhmä on aktiivisesti mukana myös muissa organisaatioissa, kuten ENISAssa ja ECSOssa.[39]

EU-tasolla kyberturvallisuuden kehittämiseen liittyvää yhteistyötä tehdään myös Yhdistyneiden kansakuntien (YK), Euroopan turvallisuus- ja yhteistyöjärjestön (ETYJ), Pohjois-Atlantin puolustusliiton (Nato), Taloudellisen yhteistyön ja kehityksen järjestön (OECD), Euroopan unionin lainvalvontayhteistyöviraston (Europol) ja erityisesti sen yhteyteen perustetun Euroopan kyberrikostorjuntakeskuksen sekä Global Forum of Cyber Expertise -järjestön (GFCE) kanssa.[40]

2.1.3. Kyberturvallisuustaitojen kehittämiseen liittyviä EU-hankkeita ja toimenpiteitä

Digitaalinen Eurooppa -hanke (The Digital Europe Programme, DIGITAL) avustaa EU:ta saavuttamaan korkean kyberturvallisuustason kyberturvallisuusstrategian mukaisesti. Se on investointiohjelma, joka tukee erityisesti eurooppalaisen ”kyberkilven” rakentamista. DIGITAL edistää uusimpien turvallisuuskäytäntöjen laajaa käyttöönottoa ja digitaitojen kehittämistä erilaisten työohjelmiensa avulla. Sen tavoitteena on resilienssin

kasvattaminen, riskitietoisuuden lisääminen ja kyberturvallisuuden perustason parantaminen. Hankkeessa on käynnissä työohjelmia, joissa on myös EU-kansalaisia koskettavia toimenpiteitä, kuten tietoisuuden lisäämistä kyberturvallisuusteknologioista. DIGITALin työohjelmassa on myös kyberturvallisuuden korkeakoulutuksen ja lyhyemmän kyberkoulutuksen tukeminen sekä koulutusta ja työpaikkoja esittelevän ja välittävän alustan rakentaminen. Tämän, jo luodun Digital Skills and Jobs Platform -nimeä kantavan alustan kautta jaetaan myös digitaitoihin liittyviä kansalaisille suunnattuja koulutuksia.[41,42,43]

Cybersecurity Skills Alliance – A New Vision for Europe -hanke (REWIRE)[44] pyrkii luomaan konkreettisen eurooppalaisen kyberturvallisuustaitojen strategian kybertoimialalle. Hanke kehittää erityisesti kyberturvallisuuden ammatillista osaamista ja tarjoaa keinoja pienentää alan osaamisvajetta. Hanke kokoaa yhteen eri puolilta EU:ta 25 kumppania, jotka edustavat koulutuslaitoksia, teollisuus- ja sertifiointiorganisaatioita sekä ammatillisen koulutuksen verkostoja. REWIRE-hanke rakentuu neljä muun kyberturvallisuuteen liittyvän Horizon2020-hankkeen työn päälle. Ne ovat CONCORDIA, SPARTA, ECHO ja CyberSec4Europe.

Cyber security competence for research and innovation -hankkeessa (CONCORDIA) on rakennettu kyberturvallisuuden verkostoa, joka yhdistää eri sidosryhmät ja luo eurooppalaisen ekosysteemin kyberturvallisuuskoulutukselle. Hankkeen avulla pyritään muun muassa kouluttamaan kybertaitoja ammattilaisille, selittämään kyberturvallisuuteen liittyviä asioita yleiskielisesti ja visuaalisesti sekä kannustamaan naisia kyberalalle. Suunnitteilla on tuottaa materiaalia myös opettajille kyberturvallisuuden kouluttamiseen.[45] Jo päättynyt SPARTA-hanke rakensi verkoston kehittämään kyberturvallisuuden tutkimusta, innovaatioita ja kouluttamista tavoitteenaan kyberrikollisuuden ehkäiseminen ja kyberturvallisuuden parantaminen EU:ssa. Hankkeessa muun muassa tehtiin sisältöjä yliopistojen kyberturvallisuusopetukseen.[46] The European network of Cybersecurity centres and competence Hub for innovation and Operations -hankkeessa (ECHO) rakennettiin myös verkostoa kyberalan kehittämiseksi. Tässä verkostossa on mukana 30 kumppania eri aloilta, mukaan lukien liikenne, alkutuotanto, ICT, koulutus, tutkimus, televiestintä, energia, avaruus, terveydenhuolto, puolustus ja pelastuspalvelu. Hankkeessa kehitettiin Euroopan kyberturvallisuuden ekosysteemiä niin, että se mahdollistaa turvallisen yhteistyön, tuettiin Euroopan markkinoiden kehitystä ja pyrittiin löytämään keinoja EU-kansalaisten suojelemiseksi kyberuhkilta ja -häiriöiltä.[47] CyberSec4Europe-hanke suunnittelee, testaa ja esittelee mahdollisia hallintorakenteita tulevalle Euroopan kyberturvallisuuden osaamisverkostolle käyttämällä parhaita käytäntöjä, jotka on johdettu CERNin kaltaisista konsepteista (organisaatio, jonka jäsenvaltiot muodostavat yhdessä ja jonka päätäntävalta on jaettu valtionhallinnon edustajien sekä tieteellisen yhteisön edustajien kesken) sekä kumppaneiden asiantuntemuksesta ja kokemuksista. Tavoitteena on kaikkien EU-kansalaisten turvallisuuden parantaminen. Hankkeessa on muun muassa tutkittu kyberturvatietoisuuskoulutuksen vaikuttavuutta. CyberSec4Europe-hanke päättyi joulukuussa 2022.[48,49]

2.1.4. EU-tason koulutustarjontaa

Digital Skills and Jobs Platformilta löytyy oma sivu kyberturvallisuustaitojen opiskeluun. Sivustolla on kansalaisille suunnattuja ilmaisia kyberturvallisuuskursseja, kyberkansalaistaitoihin liittyviä artikkeleita sekä ohjeistuksia. Myös tämän Cyber Citizen -hankkeen materiaaleja saadaan levitykseen alustan kautta.[50,51]

EU-rahoitteinen Cyberwiser.eu tarjoaa kursseja lähinnä ammattilaisille tai kyberalan opiskelijoille, mutta sen Primer-kurssi sopii myös henkilöille, joilla ei ole aiempaa kyberturvallisuusosaamista. Sivustolta löytyy kyberturvallisuuteen liittyviä uutisia sekä tietoa tapahtumista.[52] Myös aiemmin mainittu REWIRE-hanke julkaisee sivustollaan kyberturvallisuuden VOOC-kursseja (Vocational Open Online Courses) loppuvuodesta 2023.

Euroopan unionin Learning corner -sivusto tarjoaa pelejä ja muita sisältöjä lapsille ja nuorille. Sivustolta löytyy muun muassa kyberturvallisuuspeli (Cyber Chronix), sarjakuva 12–15-vuotiaille kybertaitojen opettamiseen, 9–

12-vuotiaille opas turvalliseen toimintaan verkossa sekä Happy Onlife -peli, jossa opetellaan toimimaan turvallisesti internetissä ja suojautumaan esimerkiksi hyväksikäytöltä.[53,54]

2.1.5. Tulevaisuus

Keväällä 2023 EU:n puheenjohtajamaana toimiva Ruotsi on ilmoittanut haluavansa lisätä EU-kansalaisten turvallisuutta, torjua organisoitua rikollisuutta ja suojella EU:n arvoja ja rakentaa resilienttiä Eurooppaa. Se aikoo jatkaa edellisten puheenjohtajamaiden Ranskan ja Tšekin kanssa luotua strategista ohjelmaa, jossa pyritään erityisesti torjumaan disinformaatiota ja vaalivaikuttamista.[55]

2.2. Huomioita aiemmasta tutkimuksesta

2.2.1. Kirjallisuuskatsauksen tavoite, tutkimuskysymys, lähtökohta ja metodi

EU-tason toimien ohella jäsenvaltioraportteja taustoittaa jo julkaistua akateemista tutkimusta kartoittava kirjallisuuskatsaus (scoping review). [56] Katsauksen tavoitteena on tuottaa tietoa siitä, miten kyberkansalaistaitojen opettamista on aiemmin tutkittu, erityisesti Euroopassa. Koska 'kyberkansalaistaidot' ei ole tutkimuksessa vakiintunut käsite, muotoiltiin varsinainen tutkimuskysymys ja tiedonhaussa käytetyt hakusanat ja -lausekkeet vakiintuneempien käsitteiden avulla. Tarkemmaksi tutkimuskysymykseksi siten muodostui se, miten digitaalinen kansalaisuus (digital citizenship)[57] ymmärretään akateemisessa tutkimuksessa, erityisesti kyberturvallisuuden yhteydessä.

Kartoittavan kirjallisuuskatsauksen tavoitteena on tuottaa keskeisiin julkaisuihin perustuva yleiskuva olemassa olevan tutkimuksen laajuudesta ja syvyydestä. Se on yleisluontoinen lähestymistapa, joka auttaa muun muassa tunnistamaan keskeiset käsitteet ja käytössä olevat lähestymistavat sekä nostamaan esiin keskeisiä huomioita tutkimuskirjallisuudesta. Se ei pyri arvioimaan yksittäisten tutkimusten laatua eikä tuottamaan hienojakoista analyysia tutkimuskentästä vaan keskittyy nimenomaan yleiskuvaan. [58] Tutkimusmetodi mahdollistaa kirjallisuuskatsauksen tekemisen käytettävissä olevan ajan ja muiden resurssien puitteissa, mutta kuitenkin niin, että se vastaa tutkimusprojektin tarpeisiin.

2.2.2. Työskentelyn kuvaus

Kirjallisuuskatsauksen tietokantahaut tehtiin erilaisilla yhdistelmillä taulukossa 1 listatuista hakusanoista. Yhdistävänä Boolen operaattorina käytettiin AND-operaattoria. Haut kohdistettiin artikkelin otsikkoon, avainsanoihin ja abstraktiin. Tietokannoissa, joissa kohdistusta otsikkoon, avainsanoihin ja abstraktiin ei voitu tehdä, haut kohdistettiin koko tekstiin.

Taulukko 1: Käytetyt hakusanat.

civic* / citizen* / native*	Cybersecurity / "cyber security" / cybersafety / "cyber safety" / "digital security" / "digital safety"	skill* / competen*	train* / educat*
cyber* / digital*	citizen*		

Artikkelihaut päätettiin tehdä kuudesta tietokannasta (ks. taulukko 2). Tietokantavalinnat tehtiin useissa tietokannoissa tehtyjen alustavien hakujen perusteella, eli arvioitiin, mistä tietokannoista löytyisi keskeisiä tutkimusartikkeleita. Haut kohdistettiin kuuteen tieteenalaan: kasvatustieteisiin, yhteiskuntatieteisiin, tietotekniikkaan, johtamiseen, viestintä- ja informaatiotutkimukseen sekä psykologiaan. Näistä tieteenaloista

oletettiin löytyvän kyberkansalaistaitojen opettamiseen liittyvää tutkimusta. Tietokantahaut rajattiin englanninkielisiin artikkeleihin, jotka oli julkaistu vuonna 2010 tai sen jälkeen, jotka olivat läpikäyneet arviointiprosessin ja jotka olivat saatavilla Aalto-yliopiston digitaalisissa kokoelmissa. Siten muun muassa kirjat, kirjan luvut, konferenssijulkaisut, populäärikirjoitukset ja internetlähteet rajattiin hakujen ulkopuolelle. Käytännössä tutkimusprosessi eteni iteratiivisesti ja joustavasti, kun muun muassa hakulausekkeita muokattiin hakutulosten mukaan tavoitteena saada tietokannoista mahdollisimman kattava otanta. Taulukossa 2 on esitetty tietokannoista edellä mainittuja hakusanoja yhdistelemällä saadut hakutulokset.

Taulukko 2: Hakutulokset eri tietokannoista.

Tietokanta	Hakutulokset	1. kierroksella valitut	2. kierroksella valitut
SCOPUS (Elsevier)	995	130	Euroopasta 16
Springer Link – Springer Compact	270	26	
Science Direct (Elsevier)	172	31	
Business Source Complete (EBSCO)	469	21	
Proquest Databases	924	197	
IEEE Electronic Library IEL (IEEE Xplore)	40	7	
Yhteensä	2870	430	

Artikkelivalinnat tehtiin kahden tutkijan järjestelmällä, jossa ensimmäinen tutkija teki ja dokumentoi tietokantahaut sekä teki alustavat artikkelivalinnat otsikon ja abstraktin perusteella. Toinen tutkija kävi alustavat valinnat läpi ja luki artikkelit kokonaan.[59] Toisessa vaiheessa artikkeli poistettiin otoksesta muun muassa siksi, että artikkeli käsitteli digitaalista kansalaisuutta, muttei kyberturvallisuutta tai että se keskittyi rinnakkaisilmiöihin, kuten opettajien halukkuuteen integroida digitaalinen kansalaisuus omaan opetukseensa, kansalaisten sähköisiä julkispalveluita kohtaan tuntemaan luottamukseen, kyberrikollisuuteen tai yksilöiden internethakustrategioihin. Tutkimus on verrattain viimeaikaista, sillä esimerkiksi SCOPUS-tietokannan 130 artikkelista 91 on julkaistu vuosina 2019–2022. Rajallisen tilan vuoksi tässä raportissa käsitellään vain SCOPUS-tietokannan 16:ta valittua, eurooppalaisia valtioita käsittelevää artikkelia.

2.2.3. Keskeisiä huomioita tutkimuksesta

EU-kansalaisten kyberkansalaistaitoihin liittyvää tutkimusta on tehty verrattain vähän. Artikkeleista kuusi keskittyy joko yksittäiseen EU-jäsenvaltioon (Suomi[60], Ruotsi[61], Bulgaria[62], Puola[63], Kreikka[64] ja Kypros[65]), EU-jäsenvaltioon ja eurooppalaiseen ei-jäsenvaltioon (Yhdistynyt kuningaskunta-Irlanti-Kreikka [66] ja Espanja-Yhdistynyt kuningaskunta[67]) tai koko Euroopan unioniin[68]. Laajennettaessa tarkastelua unionin ulkopuolelle löytyy seitsemän Euroopan valtioihin keskittyvää artikkelia lisää (Yhdistynyt kuningaskunta[69], Turkki[70], Serbia[71] ja Venäjä[72]).

Suurin osa tutkimuksesta kohdistuu lapsiin ja nuoriin, nuoriin aikuisiin tai näiden kasvattajiin. Artikkeleista kahdeksan keskittyy korkeakouluopiskelijoihin, neljä opettajiin/akateemiseen henkilöstöön, kolme koululaisiin/lapsiin tai nuoriin, kaksi koko väestöön ja yksi sekä työttömiin että eläkeläisiin. Yksi tutkimus on pelkästään kirjallisen aineiston analyysia.[73] Oppilaitoksilla ja opettajilla katsotaan olevan merkittävä rooli osaavien digitaalisten kansalaisten kasvattamisessa. Tällöin opettajien digi- ja kyberturvallisuusosaaminen nousee keskeiseen asemaan[74] – samoin kuin opetussuunnitelmat, joissa ei vielä ole riittävästi huomioitu

digitaalista osaamista[75], ja koulujen erilaisuudet muun muassa sisäisissä politiikoissa ja tarvittavien laitteiden, ohjelmien ja yhteyksien tarjoamisessa oppilaille, opiskelijoille ja opettajille[76]. Oppilaitosympäristöissä tehty digitaalisen kansalaisuuden opettaminen ja sen tutkimus eivät kuitenkaan kerro paljoa koko väestön kyberkansalaistaidoista. Tämä koskee varsinkin väestöä, joka on käynyt koulunsa ennen kuin digitalisaatio muutti lähestulkoon kaikkia elämän osa-alueita ja on opetellut digitaalisia taitoja itsekseen, läheisten avustuksella, erilaisilla kursseilla tai työnantajan järjestämässä koulutuksessa.

Artikkeleissa käytetyt tutkimusmetodit ovat moninaisia, esimerkiksi monimenetelmätutkimusta, kehittämistutkimusta, toimintatutkimusta, haastattelututkimusta ja kohderyhmähaastatteluita, assosiaatiosäännön avulla tehtyä tiedonlouhintaa, tilastollista analyysia, kirjallisuuskatsauksia, asiakirja-analyysia ja selittävää yhdistelmämenetelmäsuunnittelua. Suurin osa tutkimusaineistoista (puolessa artikkeleista) on kerätty informanteille lähetetyillä tai annetuilla itsearviointilomakkeilla. Yksi artikkeli keskittyy pelkästään tällaisen itsearviointilomakkeen rakentamisprosessiin.[77] Vaikka itsearvioinneilla ei saada tarkkaa kuvaa esimerkiksi tutkimuskohteiden kyberturvallisuusosaamisesta, se on usein onnistuneesti käytetty tapa kerätä ihmisten kokemuksista, tarpeista ja toiminnasta tietoa, jota voidaan hyödyntää eri yhteyksissä.[78]

Tutkimuksesta merkittävä osa keskittyy ihmisten digi- ja kyberturvallisuustietoisuuteen (awareness) ja käyttäytymiseen (behaviour). Turvallisuuden nimissä usein kerrotaan asioista, joista jokaisen tulisi huolehtia ja joita ovat esimerkiksi salasanat, digijalanjäljet, järkevästi tehty omien tietojen jakaminen, virustorjunta ja yksityisyysasetusten tarkistaminen. Yksi artikkeleista listaa digitaaliseen turvallisuuteen, oikeuksiin ja velvollisuuksiin sekä lakiin liittyvät odotetunlaiset käyttäytymistavat ja keskittyy digitaalisen turvallisuuden osaamiseen kahdella osa-alueella eli henkilökohtaisiin varotoimiin ja teknisiin varotoimiin.[79] Yleisesti ottaen tutkimuksessa kuvataan kuitenkin hyvin vähän sitä, mitä ja miten kyberkansalaistaitoja opetetaan tai tulisi opettaa. Laskennallisen ajattelun oppimista tarkasteleva tutkimus on ainoa, joka (1) katsoo laskennallisen ajattelun kansalaistaidoksi ja (2) selkeästi käsittelee ongelmaa, miten opettaa laskennallista ajattelua oppilaille, jotka eivät vielä kykene riittävän abstraktiin ajatteluun – tässä pelaaminen ja pelin muokkaaminen antavat lupaavia alustavia tuloksia.[80]

Koko Euroopan unioniin ja tietosuojalainsäädännön tuntemiseen keskittyvä tutkimus määrittelee neljä digitaalisen kansalaisen tyyppiä: offline-kansalainen (alhaisin internetin käyttö ja GDPR-tietoisuus), verkkokansalainen (keskiverto käyttäjänä ja GDPR-tietoisuudessa), sosiaalinen nettikansalainen (erittäin aktiivinen sosiaalisen median käyttö, mutta alhainen GDPR-tietoisuus) ja datakansalainen (korkeimman tason internetin käyttäjä ja GDPR-osaaja).[81] Digitaalista kansalaisuutta on jäsennelty myös (1) lähdekritiikiksi ja kriittiseksi ajatteluksi, (2) digitaalisten teknologioiden eettiseksi, turvalliseksi ja virheettömäksi käytöksi sekä (3) materiaalisiksi ja immateriaalisiksi keinoiksi demokraattiseen osallistumiseen.[82] Teknologian hallintaa (osaaminen, kyvyt, taidot) on määritelty digitaalisesta kansalaisuudesta (asenteet ja käyttäytyminen) hieman erilliseksi osa-alueeksi.[83] Digitaalisten taitojen on saatettu katsoa käsittävän taitoja, jotka edistävät luovaa, kriittistä, turvallista, eettistä ja vastuullista tieto- ja viestintäteknologioiden käyttöä jonkin tavoitteen saavuttamiseksi. Samalla ne tarkoittavat kykyä sopeutua uuteen tietoon ja asennetta, jolla pärjää nykyisessä digitaalisessa ympäristössä.[84] Yksi tutkimus nostaa selkeästi esiin digitaaliset ihmisoikeudet ja työnantajan tarjoaman koulutuksen merkityksen[85]; toinen taas huomioi ihmisten haluttomuuden muuttaa omaa käytöstään tai opetella lisää kyberturvallisuudesta, vaikka he näkisivät, etteivät heidän tietonsa ole nykyisellään turvassa[86].

2.2.4. Digitaalinen kansalaisuus ja kyberturvallisuus

Yleisesti ottaen digitaalisella kansalaisuudella viitataan yksilön mahdollisuuksiin ja kykyihin käyttää digitaalista teknologiaa yhteiskuntaan osallistumiseen. Käsitteellistys kattaa yksilön taidot, tiedot, asenteet ja käyttäytymisen.[87] Kun käytetään digitaalista kansalaisuutta teoreettisena viitekehyksenä, Ribblen ynnä muiden ja Choin ynnä muiden mallit ovat suosituimmat.[88]

Ribblen ynnä muiden mallissa digitaalinen kansalaisuus muodostuu yhdeksästä osa-alueesta. Ne ovat etiketti (käyttäytymisen ja toimenpiteiden mallit), viestintä (sähköinen tiedonvaihto), koulutus (teknologiasta ja sen käytöstä oppiminen ja opettaminen), osallisuus (osallistuminen digitaaliseen yhteiskuntaan), kaupankäynti (sähköinen ostaminen ja myyminen), oikeudet (kaikille kuuluvat vapaudet digitaalisessa ympäristössä), turvallisuus (safety) (fyysinen ja henkinen hyvinvointi) ja turvallisuus (security) (itsesuojelu eli toimenpiteet oman turvallisuuden varmistamiseksi). Malli korostaa yksilöiden moraalista käyttäytymistä ja yksinkertaisimmillaan määrittelee digitaalisen kansalaisuuden käytösnormeiksi, jotka ohjaavat tieto- ja viestintäteknologioiden käyttämistä.[89]

Choin ynnä muiden digitaalisen kansalaisuuden mallista on olemassa kaksi hieman erilaista versiota. Ensimmäisessä digitaalinen kansalaisuus koostuu neljästä osa-alueesta. Ne ovat etiikka (internetin käyttäjien sitoutuminen turvalliseen, eettiseen ja vastuulliseen nettikäyttäytymiseen), media- ja tiedon lukutaito (käyttäjien pääsy internetiin ja digitaalisiin palveluihin sekä kyky arvioita tietoa, viestiä ja tehdä yhteistyötä muiden kanssa), osallisuus (internetin käyttäminen poliittisiin, taloudellisiin, sosiaalisiin tai kulttuurisiin aktiviteetteihin) ja kriittinen vastustus (muutosta edistävä osallistuminen, joka haastaa vallitsevat voimasuhteet ja edistää sosiaalista oikeudenmukaisuutta). Näiden osa-alueiden pohjalta on rakennettu toinen malli, digitaalisen kansalaisuuden asteikko (digital citizenship scale), jota voidaan käyttää arvioitaessa yksilön digitaalisen kansalaisuuden tasoa. Asteikon viisi pääosa-aluetta ovat poliittinen aktiivisuus internetissä, tekninen osaaminen, paikallinen/globaali tietoisuus, kriittinen lähestymistapa ja toimijuus verkostoissa.[90]

Useissa eurooppalaisissa tutkimuksissa viitekehyksenä on myös DigComp[91] tai DigComp yhdessä jonkin muun kehyksen kanssa[92]. Tutkimuksessa lähes järjestään kyberturvallisuuden (cyber security/safety) eri osa-alueet, kuten tietosuoja ja yksityisyys, kriittinen ajattelu tai taidolliset ja tekniset tietoturvatoimet, ovat vain yksi osa digitaalisen kansalaisuuden kokonaiskehystä. Yleensä turvallisuus liittyy läheisesti yksilöiden velvollisuuksiin tai odotetunlaiseen, usein moraaliseen käyttäytymiseen. Digitaalisessa ympäristössä tarvittavien kansalaistaitojen määritelmät ovat kuitenkin muuttuvia eikä luotettavaa tapaa niiden mittaamiseen ole.[93] Siksi tarvitaan lisää tutkimusta muun muassa kyberkansalaistaitojen oppimisesta ja opettamisesta sekä niiden kehittämisestä.

Viitteet

[10] Henkilökohtainen tiedonanto tutkijalle, 21.7.2022.
[11] ”Kyberturvallisuus: miten EU torjuu kyberuhkia?,” *Euroopan unionin neuvosto*, luettu 20.6.2022, https://www.consilium.europa.eu/fi/policies/cybersecurity/.
[12] Euroopan komissio, *The EU's Cybersecurity Strategy for the Digital Decade* (Brysseli: European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2020), 2, 12, 25.
[13] Henkilökohtainen tiedonanto tutkijalle, 31.8.2022.
[14] Euroopan komissio, *2030 Digital Compass: the European way for the Digital Decade* (Brysseli: Euroopan komissio, 2021), 1-4, 13.
[15] Euroopan komissio, *The Digital Education Action Plan* (Brysseli: Euroopan komissio, 2018), 1–4, 7.
[16] Riina Vuorikari, Stefano Kluzer ja Yves Punie, *DigComp 2.2: The Digital Competence Framework for Citizens*, EUR 31006 EN (Luxemburg: Publications Office of the European Union, 2022), 2.
[17] Vuorikari ym., *DigComp 2.2*, 3. Viitekehyksessä kansalaisten kyberturvallisuuskompetenssiin viitataan termillä ”Safety”, eikä niinkään termillä ”Security”, mikä voi aiheuttaa sekaannusta. Termit eivät myöskään tarkoita samaa asiaa.
[18] Vuorikari ym., *DigComp 2.2*, 37-42.
[19] Vuorikari ym., *DigComp 2.2*, 43-50.
[20] Vuorikari ym., *DigComp 2.2*, 15-26.
[21] Vuorikari ym., *DigComp 2.2*, 13-14.
[22] Vuorikari ym., *DigComp 2.2*, 27-28.
[23] Euroopan komissio, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (Brysseli: Euroopan komissio, 2022), 1-2.
[24] ”Cybersecurity Education Initiatives in the EU Member States”, *ENISA*, luettu 21.12.2022, https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states.
[25] Henkilökohtainen tiedonanto tutkijalle, 6.10.2022.
[26] ”European Cyber Security Challenge (ECSC),” *ENISA*, luettu 8.10.2022, https://www.enisa.europa.eu/topics/education/eu-cyber-challenge.
[27] ”International Cybersecurity Challenge (ICC),” *ENISA*, luettu 8.10.2022, https://www.enisa.europa.eu/topics/education/international-cybersecurity-challenge-icc.

[28] "ECSF European Cybersecurity Skills Framework," *ENISA*, luettu 7.10.2022, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.
[29] "CYBERHEAD - Cybersecurity Higher Education Database," *ENISA*, luettu 9.10.2022, https://www.enisa.europa.eu/topics/education/cyberhead#/.
[30] "European Cybersecurity Month," *ENISA*, luettu 29.10.2022, https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month.
[31] "Cyber Health Week," *ENISA*, luettu 30.10.2022, https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals.
[32] "Cyber Energy Week," *ENISA*, luettu 26.11.2022, https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/cyber-energy-week. Esimerkiksi vuonna 2022 järjestettiin Kyberenergiaviikko-kampanja, joka oli kohdistettu energia-alalla toimiville ja heidän kanssaan yhteistyötä tekeville.
[33] Henkilökohtainen tiedonanto tutkijalle, 6.10.2022.
[34] Henkilökohtainen tiedonanto tutkijalle, 21.7.2022.
[35] Henkilökohtainen tiedonanto tutkijalle, 31.8.2022.
[36] Henkilökohtainen tiedonanto tutkijalle, 22.9.2022.
[37] Henkilökohtainen tiedonanto tutkijalle, 8.12.2022.
[38] "Europan Cyber Security Organisation," *ECSO*, luettu 29.4.2022, http://www.ecs-org.eu/.
[39] "Council of European Professional Informatics Societies," *CEPIS*, luettu 15.7.2022, https://cepis.org/.
[40] Henkilökohtainen tiedonanto tutkijalle, 20.6.2022.
[41] Henkilökohtainen tiedonanto tutkijalle, 9.9.2022.
[42] "Digital Skills and Jobs Platform," *Euroopan unioni*, luettu 10.9.2022, https://digital-skills-jobs.europa.eu/en.
[43] Euroopan komissio, *Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021 – 2022* (Brysseli: Euroopan komissio, 2021), 98, 106-110.
[44] "Cybersecurity skills alliance," *REWIRE*, luettu 18.8.2022, https://rewireproject.eu/.
[45] "Concordia," *CONCORDIA*, luettu 18.8.2022, https://www.concordia-h2020.eu/.
[46] "Cybersecurity training and awareness," *SPARTA*, luettu 19.8.2022, https://www.sparta.eu/training/.
[47] "The European network of Cybersecurity centres and competence Hub for innovation and Operations," *ECHO*, luettu 19.8.2022, https://echonetwork.eu/.
[48] "Cyber Security for Europe," *CyberSec4Europe*, luettu 19.8.2022, https://cybersec4europe.eu/.
[49] Henkilökohtainen tiedonanto tutkijalle, 16.8.2022.
[50] Henkilökohtainen tiedonanto tutkijalle, 9.9.2022.
[51] "Cybersecurity," *Digital Skills & Jobs Platform*, luettu 1.10.2022, https://digital-skills-jobs.europa.eu/en/cybersecurity.
[52] "Cyberwiser.eu," luettu 15.10.2022, https://www.cyberwiser.eu/.
[53] Henkilökohtainen tiedonanto tutkijalle, 9.9.2022.
[54] "Learning corner," *Euroopan unioni*, luettu 11.9.2022, https://learning-corner.learning.europa.eu/index_en.
[55] "Sweden's Presidency of the Council of the EU," *Government Offices of Sweden*, luettu 29.11.2022, https://www.government.se/government-policy/swedens-eu-presidency-2023/.
[56] Esim. Andrew Booth, Anthea Sutton ja Diana Papaioannou, *Systematic Approaches to a Successful Literature Review*, 2nd ed. (London: SAGE, 2016); Danielle Levac, Heather Colquhoun ja Kelly K O'Brien, "Scoping studies: advancing the methodology", *Implementation Science* 5, no. 69 (2010), doi: 10.1186/1748-5908-5-69.
[57] Esim. Moonsun Choi, "A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age", *Theory & Research in Social Education* 4, no. 4 (2016): 565-607, doi: 10.1080/00933104.2016.1210549; Moonsun Choi, Michael Glassman ja Dean Cristol, "What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale", *Computers and Education* 107 (2017): 100-112, doi: 10.1016/j.compedu.2017.01.002.
[58] Booth ym., *Systematic Approaches*, 23, 38, 84.
[59] Ks. Levac ym., "Scoping Studies", 5-6.
[60] Maiju Kyytsönen, Jonna Ikonen, Anna-Mari Aalto ja Tuulikki Vehko, "The self-assessed information security skills of the Finnish population: A regression analysis", *Computers and Security* 118 (2022): 102732, doi: 10.1016/j.cose.2022.102732.
[61] Alex Örtegren, "Digital Citizenship and Professional Digital Competence — Swedish Subject Teacher Education in a Postdigital Era", *Postdigital Science and Education* 4: 467-493, doi: 0.1007/s42438-022-00291-7.
[62] Valentina Milenkova ja Vladislava Lendzhova, "Digital Citizenship and Digital Literacy in the Conditions of Social Crisis", *Computers* 10, no. 40 (2021), doi: 10.3390/computers10040040.
[63] Aleksandra Pawlicka, Renata Tomaszewska, Ewa Krause, Dagmara Jaroszewska-Choraś, Marek Pawlicki ja Michał Choraś, "Has the pandemic made us more digitally literate? Innovative association rule mining study of the relationships between shifts in digital skills and cybersecurity awareness occurring whilst working remotely during the COVID-19 pandemic", *Journal of Ambient Intelligence and Humanized Computing*, online ahead of printing, doi: 10.1007/s12652-022-04371-1.
[64] Marianthi Grizioti ja Chronis Kynigos, "Code the mime: A 3D programmable charades game for computational thinking in MaLT2", *British Journal of Educational Technology* 52 (2021): 1004-1023, doi: 10.1111/ bjet.13085.
[65] Hasan Tangül ja Emrah Soykan, "Comparison of Students' and Teachers' Opinions Toward Digital Citizenship Education", *Frontiers in Psychology* 12 (2021): 752059, doi: 10.3389/fpsyg.2021.752059.
[66] Konstantina Martzoukou, Crystal Fulton, Petros Kostagiolas ja Charilaos Lavranos, "A study of higher education students' self-perceived digital competences for learning and everyday life online participation", *Journal of Documentation* 76, no. 6 (2020): 1413-1458, doi: 10.1108/JD-03-2020-0041.
[67] Mark Thomas Peart, Prudencia Gutiérrez-Esteban ja Sixto Dubo-Delgado, "Development of the digital and socio-civic skills (DIGISOC) questionnaire", Education Technology Research and Development 68 (2020): 3327-3351, doi: 0.1007/s11423-020-09824-y.

[68] Răzvan Rughiniș, Cosima Rughiniș, Simona Nicoleta Vulpe ja Daniel Rosner, ”From social netizens to data citizens: Variations of GDPR awareness in 28 European countries”, *Computer Law and Security Review* 42 (2021): 105558, doi: 10.1016/j.clsr.2021.105585.
[69] Konstantina Martzoukou, Petros Kostagiolas, Charilaos Lavranos, Thorsten Lauterbach ja Crystal Fulton, ”A study of university law students’ self-perceived digital competences”, *Journal of Librarianship and Information Science* 54, no. 4 (2021): 1-19, doi: 10.1177/09610006211048004; D. McGillivray, G. McPherson, J. Jones ja A. McCandlish, ”Young people, digital media making and critical digital citizenship”, *Leisure Studies* 35, no. 6 (2016): 724-738, doi:10.1080/02614367.2015.1062041.
[70] Filiz Elmali, Ahmet Tekin ja Ebru Polat, ”A Study on Digital Citizenship: Preschool Teacher Candidates vs. Computer Education and Instructional Technology Teacher Candidates”, *Turkish Online Journal of Distance Education* 21, no. 4 (October 2020): 251-269; Ridvan Ata ja Kasim Yildirim, ”Turkish Pre-service Teachers’ Perceptions of Digital Citizenship in Education Programs”, *Journal of Information Technology Education: Research* 18 (2019): 419-438, doi: 10.28945/4392; Nuri Kara, ”Understanding University Students’ Thoughts and Practices about Digital Citizenship: A Mixed Methods Study”, *Educational Technology and Society* 21, no. 1 (2018): 172–185, http://www.jstor.org/stable/26273878.
[71] Ana Kovačević, Nenad Putnik ja Oliver Tošković, ”Factors Related to Cyber Security Behavior”, *IEEE Access* 8 (2020): 125140-125148, doi: 10.1109/ACCESS.2020.3007867.
[72] L. V. Astakhova, ”Issues of the Culture of Information Security under the Conditions of the Digital Economy”, *Scientific and Technical Information Processing* 47, no. 1 (2020): 56–64, doi: 10.3103/S0147688220010062.
[73] Astakhova, ”Issues of the Culture”.
[74] Esimerkiksi McGallivray ym., ”Young people”, 724; Martzoukou ym., ”A study of university law”, 3; Örtegren, ”Digital citizenship”, 471, 479, Martzoukou ym., ”A study of higher education”, 1419, pitävät opettajien digi- ja kyberturvallisuusosaamista puutteellisena. Sen sijaan Elmali ym., ”A Study on Digital Citizenship”, 262, tulee johtopäätökseen, että opettajaopiskelijoiden digitaalisen osaamisen taso on keskimääräistä parempaa.
[75] Martzoukou ym., ”A study of higher education”, 1418, 1434; Elmali ym., ”A Study on Digital Citizenship”, 264.
[76] McGallivray ym., ”Young people”, 724; Örtegren, ”Digital citizenship”, 471, 480.
[77] Peart ym., ”Development of the digital”.
[78] Marzoukou ym. ”A study of university law”, 6.
[79] Elmali ym., ”A Study on Digital Citizenship”, 253-254, 264.
[80] Grizioti ja Kynigos, ”Code the mime”.
[81] Rughiniș R. ym., ”From social netizens to data citizens”.
[82] Örtegren, ”Digital citizenship”, 480; McGallivray ym., ”Young people”.
[83] Martzoukou ym., ”A study of higher education’”, 1419, 1436.
[84] Peart ym., ”Development of the digital”, 3329.
[85] Pawlicka ym., ”Has the pandemic made us”.
[86] Kovačević ym., ”Factors Related to Cyber”, 125147.
[87] Örtegren, ”Digital citizenship”, 470.
[88] Örtegren, ”Digital citizenship”; Elmali ym., ”A Study on Digital Citizenship”; Martzoukou ym., ”A study of higher education”; Tangül ja Soykan, ”Comparison of Students’”; Milenkova ja Lendzhova, ”Digital Citizenship”; Kara, ”Understanding University Students’”; Ata ja Yıldırım, ”Turkish Pre-Service Teachers’”.
[89] Esim. Mike S. Ribble, Gerald D. Bailey ja Tweed W. Ross, ”Digital Citizenship. Addressing Appropriate Technology Behavior*”, Learning & Leading with Technology* 32, no.1 (2004): 6-11, https://files.eric.ed.gov/fulltext/EJ695788.pdf. (19.12.2022); Mike S. Ribble ja Gerald D. Bailey, *Digital citizenship in schools: Nine elements all students should know* (Washington DC: International Society for Technology in Education, 2007).
[90] Choi, ”A Concept Analysis”; Choi ym., ”What it means to be a citizen”.
[91] Riina Vuorikari, Stefano Kluzer and Yves Punie, DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 EN (Luxembourg: Publications Office of the European Union, 2022).
[92] Martzoukou ym., ”A study of higher education”; Marzoukou ym., ”A study of university law;” Örtegren, ”Digital Citizenship”; Peart et al., ”Development of the digital”; Pawlicka ym., ”Has the pandemic made us”. Milenkova ja Lendzhova, ”Digital Citizenship”, taas viittaa DigCompin taustalla oleviin julkaisuihin.
[93] Peart ym., ”Development of the digital”, 3329.

3. Maakohtaiset analyysit

3.1. Alankomaat

ITU, Global Cybersecurity Index (GCI) 2020	16/182 (Global), 10/46 (Europe)
National Cyber Security Index (NCSI) 2022	18/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	3/27

3.1.1. Strategiset kyberkoulutuslinjaukset

Alankomaiden hallitus julkaisi vuonna 2022 uuden kansallisen kyberturvallisuusstrategian vuosille 2022–2028 (National Cyber Security Strategy 2, From awareness to capability). Strategia sisältää toimintasuunnitelman, jossa on konkreettisia toimia Alankomaiden digitaalisen turvallisuuden parantamiseksi. Kyberturvallisuusstrategiassa hallitus kuvaa näkemystään digitaalisesta yhteiskunnasta ja hallituksen, yritysten ja kansalaisten roolia sekä vastuuta siinä. Strategia sisältää neljä päätavoitetta. Ensimmäisenä tavoitteena on hallituksen, yritysten ja kansalaisyhteiskunnan organisaatioiden digitaalisen sietokyvyn lisääminen. Toiseksi tavoitteeksi nostetaan turvallisten ja innovatiivisten digitaalisten tuotteiden ja palveluiden tarjonta koko maassa. Kolmas tavoite on osavaltioiden ja rikollisten aiheuttamien digitaalisten uhkien torjunta. Lopuksi neljäntenä tavoitteena on taata riittävästi kyberturvallisuuden asiantuntijoita, kehittää koulutusta digitaalisesta turvallisuudesta, ja lisäksi pyritään lisäämään kansalaisten valmiutta sekä sietokykyä digitaalisen ympäristön uhkiin varautumisessa.[94,95]

Tuoreimman kyberturvallisuusstrategian tavoitteiden saavuttamiseksi vahvistetaan digitaalisen turvallisuuden järjestelmää ja koulutusta sekä yrityksille että Alankomaiden kansalaisille. Kansallinen kyberturvallisuuskeskus NCSC (National Cyber Security Centrum), Digitaalisen luottamuksen keskus (Digital Trust Center, DTC) ja digitaalisten palveluntarjoajien kyberturvallisuushäiriöiden reagointiryhmä (Cyber Security Incident Response Team voor digitale dienstverleners, CSIRT-DSP) yhdistetään yhdeksi kansalliseksi kyberturvallisuusviranomaiseksi. Kansallisen kyberturvallisuusviranomaisen tehtävänä on ymmärtää digitaalisen maailman haavoittuvuudet ja uhat. Lisäksi pyritään muodostamaan yhteys eri osapuolten tietoihin tiedonjaolla julkisen ja yksityisen sektorin kesken. Tavoitteena on myös estää yhteiskunnalliset vahingot ja lieventää uhkia. Tutkimusklusteri myötävaikuttaa näihin tavoitteisiin arvioimalla tieteellisiä innovaatioita ja määrittelemällä asiaankuuluvat tutkimuskysymykset. Tutkimusohjelmassa on neljä teemaa: kriisinhallinta, riskienhallinta, kyberturvallisuuden strategiset ja sosiaaliset näkökohdat sekä teknologia ja kyberturvallisuus (tekniset innovaatiot). Näiden teemojen avulla pyritään tehostamaan kyberturvallisuuteen liittyvää koulutusta. [96,97,98]

3.1.2. Kyberkansalaistaitojen opettamisen nykytila

Alankomaiden perus- ja keskiasteen opetussuunnitelmien uudistus on jatkunut useiden vuosien ajan. Painopisteenä on luoda digitaaliselle lukutaidolle rakenteellinen paikka koko opetussuunnitelmassa tasapainossa muiden oppimistavoitteiden kanssa. Vuonna 2022 perustettiin Alankomaiden opetussuunnitelmien kehittämisinstituutti SLO (Stichting Leerplanontwikkeling), joka on voittoa tavoittelematon järjestö. SLO on määritellyt digitaaliselle lukutaidolle, aivan kuten muillekin perusopetuksen oppimisalueille, sisällön: tiedot, taidot ja asenne. Viitekehykset on jaettu eri osa-alueisiin: 1) internetin tutkiminen turvallisessa ympäristössä, 2) huolellisen toiminnan tärkeys sosiaalisissa verkostoissa ja harkittu

toiminta internetissä, 3) turvallisten salasanojen käyttäminen ja niiden tärkeyden ymmärtäminen, 4) muiden jakamien tietojen käsittely turvallisesti ja 5) tietoisuus evästeistä, boteista ja GPS-seurantalaitteista. Toiveena on, että digitaalisen lukutaidon koulutuksen tehostaminen on täyttä todellisuutta lukuvuodesta 2024/2025 alkaen.[99]

Kansallisen kyberturvallisuusviranomaisen tehtävänä on projektien käynnistäminen tutkimuslaitosten kanssa, joita ovat esimerkiksi Alankomaiden soveltuvan tieteen tutkimusorganisaatio TNO (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) ja tutkimus- ja dokumentointikeskus WODC (Wetenschappelijk Onderzoek- en Documentatiecentrum). Kyberturvallisuusviranomainen osallistuu myös erilaisiin tutkimuksiin jakamalla tietoa, mentoroimalla jatko-opiskelijoita ja tohtoriehdokkaita sekä järjestämällä luentoja. Se myös arvioi tutkimusehdotuksia, jotka liittyvät vaatimusten mukaisesti projekteihin ja teemoihin, joihin se on kyberturvallisuusviranomaisena sitoutunut. TNO järjestää kyberturvallisuuden koulutuswebinaareja yrityksille ja julkisille organisaatioille. WODC tekee riippumatonta tieteellistä tutkimusta tai teettää sitä tunnustetuilla instituuteilla ja yliopistoilla.[100,101]

Haagin yliopiston kampuksella sijaitsee The Hague Security Delta (HSD). Yli 275 yritystä, valtion organisaatiota ja osaamislaitosta on tehnyt yhteistyötä vuodesta 2013 lähtien edistääkseen digitalisoituvan yhteiskunnan turvaamista. Kyseessä on voittoa tavoittelematon yhteisö, joka jakaa tietojaan ja tekee yhteistyötä innovatiivisten tietoturvaratkaisujen parissa, joita voidaan skaalata Alankomaissa ja kansainvälisesti. HSD "ajattelee, uskaltaa ja toimii" tarjoamalla pääsyn tietoon, innovaatioihin, markkinoihin, rahoitukseen ja lahjakkuuksiin kyberturva-alalla. HSD järjestää kyberturvallisuusohjelmia, -koulutuksia ja -tapahtumia, myös kansainvälisiä.[102] HSD on julkaissut inhimillisen pääoman kyberturvallisuuden toimintaohjelman vuonna 2016 (Human Capital Actieagenda Cyber Security 2016–2018). [103] Samalla se julkaisi myös web-sivuston securitytalent.nl. [104] Tavoitteena on vastata kyberturva-ammattilaisten puutteeseen. Agendalla pyritään toteuttamaan seuraavat tavoitteet: Ensinnäkin kasvatetaan koulutustarjontaa tarvittavien opettajien lisäämiseksi. Toiseksi vahvistetaan yhteyksiä koulutusohjelmien ja yritysten tarpeiden räätälöimiseksi. Kolmanneksi lisätään houkuttelevuutta kyberturvallisuuden opiskelijoiden saamiseksi. Neljänneksi kyberturvallisuuden ammattilaisten osaamista kehitetään edelleen. Lisäksi stimuloidaan uudelleen koulutusohjelmia lahjakkuuksien lisäämiseksi kyberturvallisuuden alalla.

Indo Netherlands Cyber Security School 2022 (IDCSS) järjestää 20 luentoa laajasta valikoimasta kyberturvallisuuteen liittyviä aiheita tunnetuilta asiantuntijoilta sekä mahdollisuuden työskennellä johtavien hollantilaisten ja intialaisten organisaatioiden tarjoamien todellisten tapaustutkimusten parissa. [105] Kybermaisteritutkintoja Alankomaissa järjestetään seuraavissa yliopistoissa: University of Amsterdam, Security and Network Engineering[106]. Vrije Universiteit Amsterdam, Computer Security[107]. Radboud University Nijmegen, Cyber Security[108] ja Computing Science[109]. Leiden University, Intelligence and National Security[110], Cybersecurity Governance[111], Crisis and Security Management[112] ja Cyber Security[113]. University of Twente and TU Delft, 4TU Cybersecurity Master Specialization[114]. Eindhoven University of Technology, Information Security Technology track[115].

Alankomaista löytyy erityisesti lapsille ja nuorille suunnattuja kyberturvallisuuspelejä. Hackshield on kyberturvallisuuspeli 8–12-vuotiaille. Sen on kehittänyt Alankomaiden rikostentorjunta- ja turvallisuuskeskus (Centrum voor Criminaliteitspreventie en Veilighet, CCV). Sivustolta löytyy myös kyberprojektitietokanta eri ikäryhmien ja yhteisöjen kunnallisista projekteista. Lapset oppivat kohtaamaan digitaalisen maailman kyberturvauhkia leikkisällä tavalla, ja heitä rohkaistaan välittämään oppimaansa vanhemmilleen ja isovanhemmilleen. Kunnilla on tärkeä rooli tässä hankkeessa. Pormestari kutsuu lapsia videoviestillä pelaamaan peliä ja ryhtymään nuoremmaksi kyberagentiksi. Myöhemmin pormestari osoittaa kunnioitusta lapsille henkilökohtaisesti, mikä antaa heille lisämotivaatiota soveltaa oppimaansa.[116] Pakopeli Cyber24 on suunnattu 12–21-vuotiaille lapsille ja nuorille aikuisille. Sen on kehittänyt Mooveteam yhdessä Alankomaiden poliisin ja kyberturva-ammattilaisten kanssa. Peli opettaa olemaan tietoinen, miten verkossa käyttäytyminen vaikuttaa omaan kyberturvaan ja sen seurauksiin. Se on moderni vuorovaikutteinen pakopeli, jossa on eri aiheita, kuten

seksuaalinen häirintä, identiteettivarkaudet, rahahuijaukset, sosiaalisen median huijaukset ja hakkerointi. Pakokokemuksen aikana pienten ryhmien pelaajien on estettävä tarinan hahmoja joutumasta pelissä verkossa tapahtuvien rikosten uhreiksi. Tällä tavoin he ovat sekä "tekijän" että "uhrin" rooleissa ja kokevat molemmat puolet itse. He näkevät oman toimintansa vaikutukset sekä asenteensa ja käyttäytymisensä muutokset. Pelin jälkeinen haastattelu varmistaa, että kokemukset jaetaan ja tieto jalostuu paremmin. Lyhyesti sanottuna Cyber24 on ainutlaatuinen yhdistelmä leikkiä ja oppimista.[117]

Netherlands Cyber Security Awareness Training e-learning Course sample on interaktiivinen moduuli, jossa on 3D-pohjaisia kyberturvallisuusriskisimulaatioita.[118] Sen on tuottanut Alankomaiden vaatimuksenmukaisuuskoulutuksen ministeriö (Ministry Of Compliance opleidingen van charco & dique).[119] Moduuli haastaa pelaajan mukaan todellisiin skenaarioihin lisäämällä kyberturvallisuustietoutta ja osoittaa positiivisen kyberturvallisuuskäyttäytymisen merkityksen. Pelimäisen haasteen soveltaminen kyberturvallisuuskoulutuskokemuksiin voi merkittävästi parantaa kykyä omaksua uusia kyberturvallisuustaitoja ja parantaa havaintoja kyberriskeistä. Pelillistäminen käyttää kineettisiä liikkeitä ulkoa muistamisen sijaan, mikä auttaa pelaajaa saamaan positiivisen oppimiskokemuksen turvallisessa ympäristössä.

Kyberturvallisuuskuukausi järjestetään vuosittain lokakuussa. Järjestävä taho on SIDN (Stichting Internet Domeinregistratie Nederland), joka hallitsee Alankomaiden verkkotunnuksia ja verkon toimialueita. Vuotuisen kyberturvallisuuskuukauden tavoitteena on edistää kyberturvallisuustietoisuutta julkisen ja yksityisen sektorin organisaatioissa sekä järjestää koulutuskursseja ja harjoituksia. Tavoitteena on saada oma henkilöstö, asiakkaat ja kontaktit ajattelemaan kyberturvallisuutta, myös hauskasti esittäen, tarjoamalla muun muassa valmis pubivisa tai tietokilpailu organisaatioille ja tiimeille. Lisäksi se jakaa ajantasaista tietoa kyberturvallisuuden nykytilasta sekä kyberturvallisuusaiheisiin liittyviä työkaluja.[120, 121] Kyberturvallisuusviikko järjestettiin 17.–21.10.2022 Haagissa. Sen järjestää vuosittain suurin piirtein samaan aikaan HSD. Kyberturvallisuusviikko järjestetään Euroopan kyberturvallisuuskuukauden aikana. Se on EU:n vuotuinen tiedotuskampanja, joka järjestetään lokakuussa eri puolilla Eurooppaa. Tavoitteena on lisätä tietoisuutta kyberturvallisuusuhkista ja edistää kyberturvallisuutta kansalaisten ja organisaatioiden keskuudessa.[122] Safer Internet Centre Nederland on osa eurooppalaista Better Internet for Kids -ohjelmaa. Se kehittää yhdessä hallituksen, yritysten ja yhteiskunnallisten instituutioiden kanssa materiaaleja ja toimintoja sekä antaa nuorille ja heidän sosiaaliselle verkostolleen, kuten vanhemmille, opettajille ja hoitopalvelujen tarjoajille, välineitä, joiden avulla he voivat kehittyä digitaalisesti taitaviksi kansalaisiksi.[123,124]

3.1.3. Kansalliset erityispiirteet

Kyberturvallisuuden lisäämiseksi kolme kyberturvallisuusklusteria on yhdistetty Alankomaissa yhdeksi kyberturvallisuusviranomaiseksi. Tällä pyritään tehostamaan tiedon saantia sekä sen jakamista julkisen ja yksityisen sektorin kesken sekä panostamaan tutkimukseen ja innovaatioihin. Lisäksi pyritään varmistamaan asiantuntijoiden määrä riittävällä koulutuksella sekä kehittämään kansalaisten kyvykkyyttä ja sietokykyä kyberturvallisuusuhkiin varautumisessa. Europolin ec3 (kyberrikoskeskus) sijaitsee Haagissa Alankomaissa. Alankomaiden kyberturvallisuusstrategiassa halutaan siirtyä niin sanotusta tietoisuudesta seuraavalle tasolle eli kyvykkyyteen. Tavoitteena on, että ohjelmistot ja laitteet ovat kyberturvallisia jo lähtökohtaisesti.[125]

3.1.4. Kyberkansalaistaitojen määrittäminen

Alankomaat ei ole erityisesti määritellyt kyberkansalaistaitoja. Käsitteen ”kansalaistaidot” määritelmä perustuu kansalaisille suunnattujen koulutuskokonaisuuksien sisältöihin, jotka keskittyvät digitaalisessa maailmassa tarvittaviin perustaitoihin, joilla voidaan vaikuttaa omaan ja muiden turvallisuuteen. Taidot perustuvat aiemmin mainittuihin SLO-viitekehyksiin. Painotetaan myös jokaisen omaa vastuuta, jolla voi vaikuttaa kaikkien muidenkin kyberturvallisuuteen. Jokaisen tulee ymmärtää omien henkilökohtaisten tietojen ja laitteiden suojaamisen tärkeys ja perusperiaatteet. Tavoitteena on ymmärtää digitaalisen ympäristön riskit ja uhat

(esimerkiksi haittaohjelmat, sosiaalinen manipulointi, identiteettivarkaudet) ja tiedostaa tarvittavat toimenpiteet (esimerkiksi virustorjuntaohjelman ja verkon palomuurin käyttö).

Viitteet

[94] Minister of Justice and Security, *National Cyber Security Strategy 2, From awareness to capability* (2022).
[95] "Cabinet presents new cybersecurity strategy," *Government of the Netherlands,* luettu 9.2.2023, https://www.government.nl/latest/news/2022/10/10/cabinet-presents-new-cybersecurity-strategy.
[96] "National Cyber Security Centrum (NSCS)," *Ministerie van Justitie en Veiligheid*, luettu 29.10.2022, https://www.ncsc.nl/.
[97] "Digital Trust Center," *Ministerie van Economische Zaken en Klimaat*, luettu 22.11.2022, https://www.digitaltrustcenter.nl/.
[98] "CSIRT-DSP," *Ministerie van Economische Zaken en Klimaat,* luettu 19.11.2022, https://www.csirtdsp.nl/.
[99] Henkilökohtainen tiedonanto tutkijalle, 19.7.2022.
[100] "Towards Digital Life: Een toekomstvisie op AI anno 2032," *TNO*, luettu 26.11.2022. https://www.tno.nl/nl/.
[101] "WODC," *Wetenschappelijk Onderzoek- en Documentatiecentrum*, luettu 26.11.2022, https://www.wodc.nl/.
[102] "The Dutch security cluster", *HSD*, luettu 26.11.2022, https://securitydelta.nl/.
[103] The Hague Security Delta, *Human Capital Actieagenda Cyber Security 2016-2018*, (2016).
[104] "Security Talent," *HSD*, luettu 6.12.2022, https://securitytalent.nl/.
[105] "Indo Netherlands Cyber Security School 2022," *HCSS*, katsottu 26.11.2022, https://www.youtube.com/watch?v=jkNbbm2OYCA.
[106] "Master Education SNE/OS3", Security & Network Engineering, luettu 30.11.2022, https://www.os3.nl/.
[107] "Build tomorrow's hacker-proof computer systems", *Vrije Universiteit Amsterdam*, luettu 8.12.2022, https://vu.nl/nl/onderwijs/master/computer-security.
[108] "Master Cyber Security," *Radboud Universiteit*, luettu 8.12.2022, https://www.ru.nl/opleidingen/masters/cyber-security.
[109] "Bachelor Informatica," *Radboud Universiteit*, luettu 8.12.2022, https://www.ru.nl/opleidingen/bachelors/informatica.
[110] "Intelligence and National Security (MSc)", *Universiteit Leiden,* luettu 8.12.2022, https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management/intelligence-and-national-security.
[111] "Cybersecurity Governance (MSc)", *Universiteit Leiden*, luettu 8.12.2022, https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management/cybersecurity-governance.
[112] "Crisis and Security Management (MSc)," *Universiteit Leiden,* luettu 8.12.2022, https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management.
[113] "Cyber Security (MSc)," *Universiteit Leiden,* luettu 8.12.2022, https://www.universiteitleiden.nl/en/education/study-programmes/master/cyber-security.
[114] "4TU.Cyber Security," *4TU*.Federation, luettu 30.11.2022, https://www.4tu.nl/cybsec/.
[115] "Master track in cyber security, Information Security Technology," *Eindhoven University of Technology track*, luettu 30.11.2022, https://ist.win.tue.nl/.
[116] "Hackshield," *CCV*, luettu 27.10.2022, https://hetccv.nl/onderwerpen/cybercrime/database-lokale-cyberprojecten/hackshield/.
[117] "Cyber24", *CCV*, luettu 27.10.2022, https://hetccv.nl/onderwerpen/cybercrime/cyber24/.
[118] "Dutch (Nederlands) - Cybersecurity Awareness Training e-Learning Course Sample," *Security Quotient*, luettu 3.12.2022, https://www.youtube.com/watch?v=fuse2GVw15I.
[119] "Laws and regulations translated into practice," *Ministry of Compliance, opleidingen van Charco & Dique*, luettu 5.12.2022, https://www.ministryofcompliance.nl/en/.
[120] "SIDN and .nl registrars support Cybersecurity Month in October," *SIDN*, luettu 27.10.2022, https://www.sidn.nl/en/news-and-blogs/sidn-and-nl-registrars-support-cybersecurity-month-in-october.
[121] "Zorgeloos online," *SIDN*, luettu 26.11.2022, https://www.sidn.nl/.
[122] "Cyber Security Week in the Haque," *The Hague & Partners,* luettu 26.11.2022, https://www.cybersecurityweek.nl/.
[123] "SIC Nederland Safer Internet Centre," luettu 18.10.2022, https://saferinternetcentre.nl/.
[124] "Safer Internet Forum 2022," *Better Internet For Kids*, luettu 18.10.2022, https://www.betterinternetforkids.eu/policy/safer-internet-forum.
[125] Minister of Justice and Security, *National Cyber Security Agenda: A cyber secure Netherlands* (2018).

3.2. Belgia

ITU, Global Cybersecurity Index (GCI) 2020	19/182 (Global), 12/46 (Europe)
National Cyber Security Index (NCSI) 2022	3/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	16/27

3.2.1. Strategiset kyberkoulutuslinjaukset

Belgian kyberturvallisuusstrategia [126] on vuodelta 2021 ja siinä kyberturvallisuus nähdään ensisijaisesti digitalisaation jouhevoittajana ja mahdollistajana. Strategia erottaa kohderyhmikseen väestön, elinkeinoelämän, julkisen sektorin ja erikseen vielä elintärkeiden toimintojen tarjoajat. Viimeisimpään ryhmään kuuluviksi lasketaan yhteiskunnan toiminnalle keskeiset toimijat sekä julkisella että yksityisellä sektorilla.

Suurimmiksi uhkatekijöiksi kyberturvallisuudelle nimetään verkkorikolliset, ulkovaltojen turvallisuuspalvelut, terroristiryhmät ja haktivistit. Myös teknologioiden kehityksen luomat uudet riskit nostetaan strategiassa esiin, esimerkkinä pilvipalveluiden tai IoT:n potentiaaliset haavoittuvuudet. Inhimillisten voimavarojen puute nostetaan Belgian kyberturvallisuusstrategiassa voimakkaasti esiin. Alan osaajien riittämättömyys kuvataan uhaksi, johon pitää suhtautua vakavasti. Korkean osaamisen asiantuntijat nähdään kyberturvallisuuden perustana, ja he osaamisellaan turvaavat muiden verkonkäyttöä. Vaatimus asiantuntijoista koskee luonnollisesti erityisesti maan koulujärjestelmää, mutta kysyntä saa muotoja myös yritystoiminnassa. RHEA-niminen kyberturvallisuusyritys on avaamassa[127] 300 henkeä työllistävää kyberturvallisuuden osaamiskeskusta vuoden 2023 aikana. Belgia aikoo käyttää kyberturvallisuuden parantamiseen noin 61 miljoonaa euroa [128] EU:n elpymispaketin varoja.

Strategiassa asetetaan kuusi tavoitetta, joihin panostetaan erityisesti sen voimassaolon (2021–2025) ajan. Niitä ovat digitaalisen ympäristön vahvistaminen ja luottamuksen lisääminen siihen, käyttäjien ja palveluntarjoajien varustaminen uhkia vastaan, elintärkeiden toimintojen tuottajien suojeleminen sekä neljäntenä kyberuhkiin vastaaminen. Viidentenä päätavoitteena on julkisen, yksityisen ja koulutus- ja tutkimussektorin yhteistyön parantaminen ja kuudentena sitoutuminen kansainväliseen yhteistyöhön. Strategiassa kansalaiset ovat siis yksi neljästä pääkohderyhmästä. Lähtökohtana on, että kukin kantaa kyberturvallisuuden kannalta itse vastuuta omista laitteistaan, sovelluksistaan ja niiden sisältämästä tiedosta. Julkisen vallan ja median tehtävänä taas on pitää kansalaiset ajan tasalla näitä kohtaan kohdistuvista uhista. Näin voidaan sanoa, että belgialainen kyberturvallisuuden malli vastuuttaa kansalaista hyvin voimakkaasti. Strategian toteuttamisen kannalta keskeinen toimija on Belgian kyberturvallisuuskeskus CCB. Sen vastuulla on maan kyberturvallisuustoimien koordinointi ja valvonta.

3.2.2. Kyberkansalaistaitojen opettamisen nykytila

Belgian kyberturvallisuuskeskus on keskeinen valtiollinen toimija, jonka alla toimii myös Belgian CERT. Keskus jakaa kyberturvallisuuden neljään osaan: kotiin, työhön, kouluun ja julkiseen hallintoon. Vuonna 2014 perustettu virasto toimii suoraan pääministerin alaisuudessa.

Kyberturvallisuuden koalitio (CSC) on kyberturvallisuutta edistävä yhteistyötaho, jossa mukana ovat niin julkisen kuin yksityisen sektorin toimijat. CSC tuottaa muun muassa oppimateriaaleja, oppaita, raportteja ja kampanjoita kyberturvallisuuden edistämiseksi. CSC:n uusin vuosiraportti tiivistää kyberturvallisuuden kohentamisen keskeisiksi tavoitteiksi tietoisuuden nostamisen ja alan ammattilaisten määrän lisäämisen. CSC myös valitsee vuoden kyberturvallisuushenkilön ehdolle asetetusta kymmenen kyberturvallisuusvaikuttajan joukosta. Vuonna

2022 valinta kohdistui[129] kymmenen finalistin joukosta Sebastien Deleersnyderiin, joka on Toreon-nimisen kyberturvallisuusyrityksen teknologiajohtaja (CTO).

Valtiollinen Safeonweb.be-sivusto kokoaa kansalaisille tarkoitettua kyberturvallisuustietoa yhteen. Sivuston sisältö on neljällä kielellä: flaamiksi, ranskaksi, saksaksi ja englanniksi. Se tarjoaa paitsi vinkkejä ja testejä, myös ”ensiapua” erilaisiin kyberturvallisuuteen liittyviin tilanteisiin. Näissä toimintaohjeissa käydään läpi erilaisia kyberturvallisuuden kannalta vaarallisia käytännön tilanteita roskapostista kiristykseen ja älylaitteen katoamisesta väärän linkin klikkaukseen. Sivustolle voi myös edelleen lähettää saamansa epäilyttävän sähköpostin.

Kysyntää tiedolle ja tuelle on, sillä Safeonweb.be-sivusto saa päivittäin keskimäärin noin 12 000 viestiä kansalaisilta.[130] Samalla tämä luku kertoo palvelun hyvästä tavoittavuudesta. Safeonweb-palvelun sovelluksen on ladannut noin 200 000 ihmistä[131] ja he saavat näin varoituksia uusista kyberturvallisuusuhista suoraan matkapuhelimeensa. Safeonweb-palvelun vuosittaisten kampanjoiden tunnettuus on noin 55 prosenttia.

Kyberturvallisuus mielletään jo osaksi arkielämän turvallisuutta. Besafe.be-sivusto on ylipäätään kodin turvallisuuteen keskittynyt valistussivusto, jossa yksi uusimmista kampanjoista keskittyy kodin älylaitteiden aiheuttamiin riskeihin.[132] Myös varautumiseen ja turvallisuuteen keskittyneellä risk-info.be-sivustolla esillä ovat kyberturvallisuuden perusasiat. Finanssialan keskusjärjestö Febelfin tarjoaa kuluttajille tietoa[133] rahaliikenteen turvallisuudesta verkossa. Myös teleoperaattorit toimivat[134] koordinoidusti verkkohuijauksia vastaan ja tiedottavat aktiivisesti asiakkailleen uhista.

Belgian koulujärjestelmä[135] jakautuu kolmen kielen (ranska, flaami, saksa) pohjalta eri järjestelmiin, jotka tosin ovat hyvin lähellä toisiaan. Koulujärjestelmä jakautuu myös koulujen taustan mukaan. Koulujen taustalla voi olla kieli- tai hallintoalue tai muu yhteisö, yleensä katolinen kirkko. Tietotekniikkaan liittyvissä asioissa kouluilla on käytännössä valta päättää itse opetuksen sisällöistä ja menetelmistä. Liittovaltio päättää ainoastaan kouluiästä ja epäsuorasti koulujen rahoituksesta. Tämän jakautuneisuuden myötä on mahdotonta antaa edes viitteellistä kuvaa koulujen kyberturvallisuuden tilanteesta tai oppisisällöistä. Voidaan esittää oletus, että kyberturvallisuuden opetuksessa on hyvin suuria eroja. Tähän viittaa myös se, että NCSI:n kyberturvallisuusindeksissä Belgia saa ensimmäisen ja toisen asteen opetuksen kohdalla vain yhden pisteen kahdesta[136], kun muilla oppiasteilla ja muissa koulutukseen liittyvissä kysymyksissä tulos on kaikissa 2/2.

Belgiassa noin kahdeksan prosenttia korkeakouluissa opiskelevista on ICT-alalla[137] ja kyberammattilaisten tarve maassa on unionin mittakaavassa suurta[138]. Kyberturvallisuuden korkeakoulututkintoja voi Belgiassa suorittaa yli 20 yliopistossa ja ammattikorkeakoulussa.[139] Lähes kaikki ovat yhden oppilaitoksen järjestämiä, mutta mukana on myös kuuden oppilaitoksen yhdessä rakentama kyberturvallisuuden kaksivuotinen maisteriohjelma.[140] Se on lähes kokonaan englanninkielinen, mutta pieni osa opetuksesta on ranskaksi. Nämäkin osat on mahdollista korvata englanninkielisillä kursseilla.

Lastensuojelujärjestö Child Focusin Click safe -sivusto keskittyy nimenomaan lasten turvallisuuskysymyksiin verkossa. Järjestön toiminnan keskiössä ovat lasten hyväksikäytön ja lapsikaupan ehkäisy. Child Focus on keskeisenä toimijana mukana myös kaksi kertaa vuodessa järjestettävässä Internet Safe and fun -päivässä[141], jolloin järjestön kouluttamat vapaaehtoiset puhuvat koululaisille kyberturvallisuudesta. Vuoden 2010 jälkeen tapahtuma on tavoittanut 93 000 koululaista.[142]

Vanhemmilla verkon käyttäjillä on tutkitusti enemmän epävarmuutta[143] omasta osaamisesta kuin nuoremmilla. Tämän takia vanhemmalle väelle on kohdistettu heille suunnattuja kampanjoita[144] opastamaan ja rohkaisemaan verkon käytössä.

Vuoden 2022 aikana B-BICO-projekti kokosi eri alojen asiantuntijoita pohtimaan haavoittuvassa asemassa olevien ryhmien medialukutaitoa ja sen tukemista. Loppuvuodesta 2022 ilmestyneessä raportissa annetaan yhdeksän politiikkasuositusta. Niistä ensimmäiset neljä koskevat lapsia ja ovat verkkopalvelujen saavutettavuuden korostaminen, kouluissa annettavien digitaitojen tärkeys, opetusmateriaalien toimivuus ja digitaalisen mentoroinnin tärkeyden tunnistaminen ja tunnustaminen. Loput viisi koskevat vanhempia.

Ensimmäinen on selkokielen, videoiden ja muiden vastaavien ilmaisukeinojen käyttö valistusmateriaaleissa. Nämä auttavat usein vanhempia, joiden kielitaito on puutteellinen. Lisäksi tuodaan esiin joustavuuden ja monimuotoisuuden tärkeys opetuksessa, vanhempien oman tieto- ja taitotason kohottaminen, vanhempien kiinnostuksen herättäminen lastensa digitaaliseen ympäristöön ja vinkkien antaminen perheen sisäisten sääntöjen ja toimintatapojen muodostamiseen.[145]

Verkkohuijauksiin liittyvää valistustyötä on ranskaksi traquelarnaque.be-sivustolla [146] ja flaamiksi spotdescam.be-sivustolla [147] . Cyber Security Challenge [148] on vuonna 2015 aloitettu, nelihenkisille opiskelijajoukkueille tarkoitettu kilpailu, jonka tavoitteena on lisätä tietoisuutta kyberuhista ja innostaa opiskelijoita alalle. Yleiseurooppalaisen kilpailun tärkeyttä korostetaan sillä, että Belgian finaali järjestetään Kuninkaallisessa sotilasakatemiassa.

3.2.3. Kansalliset erityispiirteet

Belgian hallintomalli on belgialaisten omien määritelmiensäkin mukaan monimutkainen. Maata jakaa myös kaksi virallista kieltä, flaami ja ranska. Maan kyberturvallisuusstrategiassa [149] mainitaan erikseen tämän tekevän yhteisistä ja kattavista kyberturvallisuuskäytännöistä hankalia. Belgian kyberturvallisuuskeskuksen ohjeet ja opastukset ovatkin maassa nimenomaan vain ohjeita ja opastuksia, eivät määräyksiä. Sinällään turvallisuuteen liittyvät asiat, kuten myös kyberturvallisuus, ovat Belgiassa liittovaltion hoidettavia asioita.

Oman sävynsä kyberturvallisuudelle antaa se, että Belgiassa sijaitsee useita kansainvälisten toimijoiden keskuksia, päällimmäisinä Euroopan unioni ja Naton päämaja. Maa tukee näiden toimijoiden kyberturvallisuutta ja laskee ne samaan kategoriaan kuin omat elintärkeät toimintonsa.

Belgian puolustusministeriöön kohdistui kyberhyökkäys joulukuussa 2021. Tämän jälkeen, alkuvuonna 2022 maa sitoutui käyttämään yli sata miljoonaa euroa kyberturvallisuuden ja kyvykkyyksien parantamiseen.[150]

3.2.4. Kyberkansalaistaitojen määrittäminen

Belgian kyberturvallisuusstrategiassa kansalainen velvoitetaan olemaan itse vastuussa hallussa olevasta tietotekniikasta ja siinä olevista sovelluksista ja tiedoista. Vaadittavat kyberkansalaistaidot määritellään näin vastuun kautta. Tämän voi ajatella ainakin osittain johtuvan Belgian yhteiskunnan voimakkaasti sirpaloituneesta luonteesta, jossa konkreettisempien tavoitteenasettelujen saatikka määräysten toteuttaminen ei ole mahdollista.

Viitteet

[126] Centre for Cybersecurity Belgium, *Cybersecurity Strategy Belgium 2.0 – 2021-2025* (2021).
[127] "RHEA Group Announces New European Cybersecurity Centre of Excellence," *RHEA Group,* luettu 25.11.2022, https://www.rheagroup.com/rhea-group-announces-new-european-cybersecurity-centre-of-excellence/.
[128] "Belgium to spend millions improving national cyber security," *The Brussels Times*, luettu 3.1.2023, https://www.brusselstimes.com/203570/belgium-to-spend-millions-improving-national-cyber-security.
[129] Cathy Suykens, "Sebastien Deleersnyder is Belgium's Cyber Security Personality of the Year 2022!," *Cyber Security Coalition.be,* 7.10.2022 blog, https://blog.cybersecuritycoalition.be/sebastien-deleersnyder-is-belgiums-cyber-security-personality-of-the-year-2022/.
[130] "2021: Activity report of the Cyber Security Coalition," *Cyber Security Gazette*, luettu 25.11.2022, https://annualreport.cybersecuritycoalition.be/nl/annualreportcybersecuritycoalitionbe/.
[131] "Ambitions and achievements in the field of cyber security in Belgium," *Centre for Cyber Security Belgium*, luettu 14.12.2022, https://ccb.belgium.be/en/news/ambitions-and-achievements-field-cyber-security-belgium.
[132] "Appareils connectés," *ibz*, luettu 25.11.2022, https://www.besafe.be/fr/vol/appareils-connectes.
[133] "Payer par voie digitale et la banque digitale," *Febelfin*, luettu 14.12.2022, https://www.febelfin.be/fr/themes/payer-par-voie-digitale-et-la-banque-digitale.
[134] Krystina Sferlazza, "What is Proximus doing to counter online and telephone fraud?," *Proximus*, 28.4.2022 blog, https://www.proximus.com/news/2022/20220428-blogpost-ksferlazza-fraud-prevention.html.
[135] "Education Structure in Belgium", *belgiumeducation.info*, luettu 25.11.2022, https://www.belgiumeducation.info/education-system/education-structure.html.
[136] "Belgium," *NCSI*, luettu 25.11.2022. https://ncsi.ega.ee/country/be/.
[137] "Distribution of graduates and new entrants by field," *OECD.Stat*, luettu 3.1.2023, https://stats.oecd.org/Index.aspx?datasetcode=EAG_GRAD_ENTR_FIELD.
[138] Borka Jerman Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?," Education and Information Technologies 27 (2022): 3011–3036, https://doi.org/10.1007/s10639-021-10704-y.
[139] "ICT security education in Belgium," *Centre for Cyber Security Belgium*, luettu 14.12.2022, https://ccb.belgium.be/en/ict-security-education-belgium.
[140] "Master in Cybersecurity," *Ecole Royale Militaire, Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Haute Ecole de Bruxelles, Haute Ecole Libre de Bruxelles*, luettu 20.12.2022, https://masterincybersecurity.ulb.ac.be/.
[141] "Internet safe and fun," luettu 14.12.2022, https://internetsafeandfun.be.
[142] "Internet Safe & Fun Days," *Proximus*, luettu 14.12.2022, https://www.proximus.com/digital-society/trust/internet-safe-and-fun-child-focus.html.
[143] Karel Vandendriessche, Eva Steenberghs, Ann Matheve, Annabel Georges ja Lieven De Mare, *imec.digimeter 2020: Digitale trends in Vlaanderen*, (Belgia: imec, 2020).
[144] "Cybersecurity campaign for elderly people," *DNS Belgium*, luettu 14.12.2022, https://www.dnsbelgium.be/en/news/cybersecurity-campaign-elderly-people.
[145] "Creating a better internet for all - How to include and support vulnerable groups?," *Belgian Better Internet Consortium (B-BICO), CSEM, Média Animation, Mediawijs*, luettu 20.12.2022, https://b-bico.be/IMG/pdf/policy_brief_better_internet_for_all_eng.pdf.
[146] "Traque l'Arnaque," luettu 14.12.2022, https://www.traquelarnaque.be/.
[147] "Spot De Scam," luettu 14.12.2022, https://www.spotdescam.be/.
[148] "Cyber Security Challenge Belgium," luettu 14.12.2022, https://www.cybersecuritychallenge.be/.
[149] Centre for Cybersecurity Belgium, *Cybersecurity Strategy Belgium 2.0 – 2021-2025* (2021).
[150] "Belgium to spend millions improving national cyber security," *The Brussels Times*, luettu 27.12.2022, https://www.brusselstimes.com/203570/belgium-to-spend-millions-improving-national-cyber-security.

3.3. Bulgaria

ITU, Global Cybersecurity Index (GCI) 2020	77/182 (Global), 37/46 (Europe)
National Cyber Security Index (NCSI) 2022	26/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	26/27

3.3.1. Strategiset kyberkoulutuslinjaukset

Bulgarian ministerineuvosto (Министерски съвет) julkaisi kansallisen kyberturvallisuusstrategian, Cyber Resilient Bulgaria 2020:n, vuonna 2016. Huhtikuussa 2021 päivitetyn strategian voimassaoloa on jatkettu vuoteen 2023 asti. Yksi päätavoitteista on kaikkien sidosryhmien tietoisuuden, tietämyksen ja osaamisen lisääminen, kyberturvallisuuskulttuurin vahvistaminen sekä kannustavien tutkimus- ja innovointipuitteiden luominen. Kyberturvallisuus sekä tieto- ja viestintäteknologioiden vastuullinen ja turvallinen käyttö sisällytetään kaikkien koulutusasteiden opetukseen, ja opettajien koulutusta lisätään. Opetuksessa ja kampanjoinnissa käytetään nykyaikaisia, innovatiivisia, osallistavia ja innostavia menetelmiä, kuten pelillistämistä. Suunnitteilla on useita tietoisuuskampanjoita, joiden tavoitteena on parantaa kansalaisten kyberhygienian tasoa. Kyberturvallisuustietoisuuden lisääminen on keskeinen tavoite, jotta kansalaiset olisivat tietoisia kyberturvallisuusriskeistä ja ennalta ehkäisevistä toimenpiteistä.[151,152]

Digitaalinen Bulgaria 2025 -ohjelman yhtenä tavoitteena on kyberturvallisuusvalmiuksien vahvistaminen. Keskeisenä toimenpiteenä on lisätä tieto- ja viestintätekniikan käyttäjien tietoisuutta kyberturvallisuuden merkityksestä ja turvallisesta verkkokäyttäytymisestä.[153] Digitaalisten taitojen strategia on osa Digitaalinen muutos 2020–2030 -suunnitelmaa. Koulutusjärjestelmää uudistetaan, jotta työvoiman digitaalista osaamista saadaan kohennettua. Vuonna 2021 opettajien ja akateemisten laitosten henkilöstön lisäkoulutukseen budjetoitiin kaksi miljoonaa euroa. Aikuisväestölle on suunnitteilla digitaalinen oppimisalusta, jota kautta tarjotaan ilmaista digitaalisten taitojen opetusta. Bulgaria investoi 2,9 miljoonaa euroa 21 koulutuskeskukseen ympäri maata. Niissä annetaan opiskelijoille ja nuorille ilmaista digitaalisten taitojen opetusta, johon sisältyy myös kyberturvallisuutta. Työttömien, senioreiden, toimintarajoitteisten ja muiden riskiryhmien digitaalisten taitojen parantamiseen panostetaan. Kansalaisia kannustetaan käyttämään sähköisiä palveluita, ja samalla tarjotaan kyberturvallisuuskoulutusta, jotta luotto sähköisiin palveluihin vahvistuisi. Suunnitelmassa todetaan, että koska kyberavaruudessa on haavoittuvuuksia, joiden kaikkia mahdollisia vaikutuksia ei voida tietää, on tärkeää kehittää koko yhteiskunnan kyberturvallisuuskulttuuria.[154,155]

3.3.2. Kyberkansalaistaitojen opettamisen nykytila

Digitaalinen Bulgaria 2025 -ohjelmalla nykyaikaistetaan kouluissa annettavaa tietotekniikan opetusta. Tehtäviin toimenpiteisiin kuuluu opetussuunnitelman ja opetusmenetelmien uudistukset ja opettajien lisäkoulutukset.[156] Tietoteknisten taitojen opetus alkaa Bulgarian koulujärjestelmässä peruskoulun kolmannella luokalla tietokonemallinnuksen opinnoilla ja jatkuu tietotekniikan opinnoilla yläkoulussa ja lukion ensimmäisellä luokalla. Turvallisuuteen liittyvää opetusta annetaan osana näitä oppiaineita kaikilla luokka-asteilla. Turvallisuuteen liittyvät oppimistavoitteet koskevat kaikkia. Opetuksen sisältö ja opetusmenetelmät vaihtelevat kohderyhmän iän mukaan.[157,158]

Luokilla III–IV opiskellaan turvallisuuden edellytyksiä digitaalisessa ympäristössä ja luokilla V–VII internetin toimintaa ja tietosuojaa. Oppilaat saavat valmiudet noudattaa internetin turvallisen käytön ohjeita ja sähköisen viestinnän eettisiä sääntöjä. Luokilla VIII–X keskitytään siihen, miten digitaalisuus vaikuttaa terveyteen ja ympäristöön ja miten haitallisia vaikutuksia ehkäistään. Luokkien XI–XII opinnot painottuvat media- ja

informaatiolukutaitoihin. Kriittinen ajattelu ja medialukutaito ovat oppiainerajat ylittävä, monialainen teema Bulgarian kouluissa. Tavoitteena on kouluttaa valveutuneita ja ajattelevia kansalaisia, jotka osaavat analysoida mediaviestintää ja toimia mediaympäristöissä. Monissa kouluissa on laadittu internetin turvallisuutta ja tietoturvaa koskevat toimintaperiaatteet. Niihin sisältyy eettisen verkkokäyttäytymisen ja verkkoturvallisuuden sääntöjä sekä toimenpiteitä riskialttiin verkkokäyttäytymisen ehkäisemiseksi. Bulgarian lastensuojeluviranomainen on tehnyt päiväkodeille ja kouluille verkon turvallisuussäännöt. Bulgarian Safer Internet Centre (SIC) on puolestaan antanut suosituksia kyberturvalliseen etäopiskeluun.[159]

Sähköisen hallinnon virasto (Електронно управление) ja opetus- ja tiedeministeriö (Министерството на образованието и науката) ovat yhteistyössä laatineet kouluihin digitaalisen kyberhygienian tuntisuunnitelman ja opettajan oppaan. Vuorovaikutteiseen opetukseen sisältyy kyberturvallisuustietoa, videoita ja testejä. Vanhemmille on oma verkkohygienian moduuli.[160] Bulgarian sähköisen hallinnon ministeriön (Министерството на електронното управление) yksi päätehtävistä on huolehtia lasten ja nuorten turvallisuudesta internetissä. Ministeriö toteuttaa tehtäväänsä erilaisilla tapahtumilla ja aloitteilla.[161] Monet kansalaisjärjestöt tarjoavat eri kohderyhmille kyberturvallisuuskoulutusta ja -materiaaleja. Lapsille ja nuorille on kerhoja, joissa on esillä myös kyberturvallisuuteen liittyviä asioita. Useat yliopistot tarjoavat kyberturvallisuuskoulutusta. Esimerkiksi University of National and World Economyssa, Varna Free Universityssa ja National Military University "Vasil Levskissä" voi opiskella kyberturvallisuuden maisterintutkinnon. Myös yritykset kouluttavat työntekijöitään.[162,163]

Applied Research and Communications Fundin (ARC Fund) vuonna 2005 perustama Bulgarian Safer Internet Centre (SIC) edistää informaatioteknologioiden ja internetin turvallista, vastuullista ja positiivista käyttöä. Toiminnan jatkuminen on epävarmaa riittämättömän rahoituksen vuoksi. Tärkeimmät kohderyhmät ovat lapset, nuoret ja opettajat. SIC on osa Euroopan komission tukemia kansainvälisiä Insafe-, INHOPE- ja Better Internet for Kids -verkostoja. Sen neuvottelukunnassa on mukana noin 30 bulgarialaisen ja kansainvälisen tahon edustajaa muun muassa ministeriöistä. SIC järjestää yhdessä koulujen ja kuntien kanssa erilaista toimintaa, kuten kampanjoita, työpajoja ja koulutuksia. Vuonna 2021 SIC koulutti opettajia ympäri maata oppilaiden medialukutaidon kohentamiseksi. Koulutus perustui Digital Competence Framework for Citizens -viitekehykseen (DigComp), jonka yksi osa-alueista on turvallisuus. SICin SafeNet-verkkosivustolla on käytännönläheistä tietoa verkkoturvallisuuden riskeistä. Sivustolla on erilaisia oppaita, julkaisuja, esityksiä, uutisia ja tuntisuunnitelmia. SICillä on oma hotline, johon voi raportoida internetin laittomasta ja haitallisesta sisällöstä, helpline, josta saa apua verkkoturvallisuuden ongelmiin, ja SafeNet-sovellus mobiililaitteisiin. YouTube-kanavalla on verkkoturvallisuuden riskeistä kertovia videoita, joita voidaan käyttää kouluissa opetuksen tukena. Vuonna 2021 tehdyssä kuusiosaisessa animaatiosarjassa (Кибер сбирка) käsitellään internetin keskeisimpiä riskejä.[164,165]

Vuonna 2021 ARC Fund ja SIC kehittivät ja jalkauttivat kouluissa uusia opetusmenetelmiä, joiden tarkoituksena on ehkäistä kyberrikollisuutta ja verkossa tapahtuvaa hyväksikäyttöä sekä parantaa lasten digitaalista lukutaitoa. Noin 1 500 lasta, 200 opettajaa, 270 vanhempaa ja 1 160 ammattilaista osallistui vuonna 2021 ARC Fundin ja SICin järjestämiin koulutuksiin ja tietoisuuskampanjoihin. Vuodesta 2010 lähtien SICillä on ollut oma 14–18-vuotiaiden vapaaehtoisten nuorisopaneeli. Nuorisopaneeli toteutti Bulgarian vuoden 2021 Safer Internet Dayn, johon osallistui yli 20 000 ihmistä. Vuodesta 2015 lähtien SIC on ylläpitänyt Cyberscout-koulutusohjelmaa sisäministeriön (Министерство на вътрешните работи) ja Telenor Bulgarian tuella. Suurta suosiota kymmenissä kouluissa saanut koulutusohjelma on suunnattu viidesluokkalaisille lapsille. Osallistujat käyvät kaksipäiväisen kyberturvallisuusvalmennuksen. Sertifioitu Cyberscout-oppilas kertoo ikätovereilleen, miten internetissä toimitaan vastuullisesti ja turvallisesti, antaa neuvoja internetiin liittyvissä pulmissa ja järjestää kyberturvallisuustilaisuuksia.[166,167]

Media Literacy Coalitionin tehtävänä on edistää kaikenikäisten kansalaisten medialukutaitoa. Liitto on järjestänyt vuodesta 2018 alkaen vuotuisia medialukutaitopäiviä. Vuoden 2021 medialukutaitopäivillä pidettiin ilmaisia yhden päivän kyberturvallisuustyöpajoja kolmella eri paikkakunnalla. Liitto kouluttaa mentoreita, jotka opastavat muita kansalaisia omissa verkostoissaan. Koulutuksissa käsitellään esimerkiksi valeuutisia,

verkkohuijauksia ja tietosuojaa. Mentoreita on koulutettu yli 200 ympäri maata. Lisäksi liitto tarjoaa räätälöityjä koulutuksia yli 55-vuotiaille kansalaisille, joilla on pääsy internetiin, muttei vielä tarvittavia taitoja. Koulutuksessa käsiteltäviä aiheita on muun muassa disinformaation, propagandan, valeprofiilien, salaliittoteorioiden ja huijausten tunnistaminen.[168,169]

UNICEF Bulgaria auttaa lapsia ja nuoria kehittämään digitaalisia taitoja ja kriittistä ajattelua, jotta he oppisivat suojautumaan kyberhyökkäyksiltä, -rikoksilta ja -väkivallalta, tunnistamaan valeuutiset ja tekemään järkeviä päätöksiä internetissä. Viime vuosina UNICEF Bulgaria on panostanut erityisesti nuorten kyberturvallisuusosaamiseen. Vuonna 2019 julkaistiin nuorille tarkoitettu ”My Right to an Opinion” -opas, jossa puhutaan muun muassa sosiaalisen median turvallisuudesta. Vuonna 2020 UNICEF Bulgaria järjesti Hackathonin, jossa nuoret saivat tilaisuuden esitellä omia medialukutaitoon ja kyberturvallisuuteen liittyviä ratkaisujaan. Suunnitteilla on 11–14-vuotiaille suunnattu, pelillistämistä hyödyntävä Cyber Survivor -sovellus.[170,171]

Vuonna 2021 Bulgarian valtion sähköisen hallinnon virasto järjesti kansallisen kyberturvallisuuskuukauden (ECSM) neljättä kertaa. Euroopan yhteisten kyberturvallisuusteemojen lisäksi kampanjoihin sisällytetään kansallisia teemoja. Vuoden 2021 kampanjan lähettiläinä oli kaksi tunnettua bulgarialaista näyttelijää, Aleksandra Sarchadjieva ja Kitodar Todorov. Kyberturvallisuuskuukauden aikana he jakoivat sosiaalisessa mediassa kampanjaviestejä, infografiikkaa ja neuvoja ja kutsuivat asiantuntijavieraita keskustelemaan kyberturvallisuuskysymyksistä. Julkkiskumppaneiden ansiosta kampanjan näkyvyys oli suuri, ja kampanja sai kansalaisilta positiivista palautetta. Kampanjavideoita esitettiin koko lokakuun ajan Sofian kaikilla metroasemilla 30 kertaa päivässä. Bulgariassa on pohdittu, että vastaavanlaisia kampanjoita voitaisiin järjestää ympäri vuoden, koska tieto ja tietoisuus ovat edellytys käyttäytymisen muutokselle. Kampanjoiden strategiana on toiminnallinen oppiminen, kuten aitojen esimerkkien antaminen, jatkuvan ajantasaisen tiedon välittäminen sekä perustermien ja -käytäntöjen opettaminen. [172] Vuoden 2022 ECSM:n pääteemana oli lasten suojeleminen kyberturvallisuusrikollisuudelta.[173]

3.3.3. Kansalliset erityispiirteet

Sofia Security Forum tutki vuonna 2019 11–18-vuotiaiden bulgarialaisten verkkoturvallisuusosaamista. Tutkimuksen mukaan lapset ja nuoret viettävät yhä enemmän aikaa internetissä. Internetin merkitys lasten ja nuorten vapaa-aikaan on suuri. Suurin osa 11–18-vuotiaista kertoi tietävänsä internetin riskit ja turvallisuusohjeet. Monet eivät kuitenkaan noudata ohjeita. Noin 30 prosenttia vastaajista olikin joko itse altistunut verkkorikollisuudelle tai tunsi jonkun, joka oli altistunut. Yli neljäsosa vastaajista ei tiennyt, kenelle tai miten verkkorikollisuudesta pitäisi ilmoittaa. Tutkimuksen mukaan tämä osoittaa, että verkkoturvallisuuden tietoisuuskampanjoita ja koulutusta tarvitaan Bulgariassa lisää. Lähes puolet vastanneista ei ollut saanut verkkoturvallisuuteen liittyvää opetusta. Eniten heitä oli 17–18-vuotiaiden ryhmässä. Vastaajat olivat saaneet opetusta erityisesti koulussa, mutta 17–18-vuotiaista lähes puolet oli opetellut verkkoturvallisuutta itse.[174]

3.3.4. Kyberkansalaistaitojen määrittäminen

Sähköisen hallinnon ministeriö antaa kansalaisille ohjeita turvalliseen verkkokäyttäytymiseen. Verkkosivuilla on Europolin julkaisemia materiaaleja, joissa neuvotaan, miten kodista tehdään kyberturvallinen (esimerkiksi varmuuskopiointi, salasanat, virustorjunta), miten internetissä tehdään ostoksia turvallisesti (esimerkiksi luotettavat verkkokaupat ja luottokortin käyttö), kuinka pysyä varuillaan (esimerkiksi tietojen jakaminen, linkit ja liitteet) ja mitä kyberturvallisuus lasten kanssa tarkoittaa (esimerkiksi älylelujen turvallisuus). [175] Sisäministeriön alainen järjestäytyneen rikollisuuden torjunnan kyberrikollisuuden yksikkö neuvoo verkkosivuillaan kansalaisia seuraavissa asioissa: salasanat, kalastelu, henkilötiedot, lisensoidut ohjelmistot, virustorjunta, rahaliikenteen seuranta, käyttöjärjestelmien ja ohjelmistojen päivittäminen, varmuuskopiointi, kaksivaiheinen tunnistautuminen ja netiketti. [176] Kyberkansalaistaitoja määritellään myös DigComp-viitekehyksen pohjalta.

Viitteet

[151] Министерски съвет, *Национална стратегия за киберсигурност Киберустойчива България 2020* (2016).
[152] Министерски съвет, *Актуализирана Национална стратегия за киберсигурност КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023* (2021).
[153] ”НАЦИОНАЛНА ПРОГРАМА „ЦИФРОВА БЪЛГАРИЯ 2025, ПЪТНА КАРТА ЗА ПЕРИОДА ДО 2025, Отчет към декември 2021г.,” luettu 16.11.2022, https://egov.government.bg/wps/wcm/connect/egov.government.bg-2818/ea3fa5bc-f762-479e-8fcd-472cc8af68da/patna_karta_2021_24jan2022.docx?MOD=AJPERES&CVID=ofQZ43R.
[154] European Commission, *Digital Economy and Society Index (DESI) 2022: Bulgaria* (2022), 6-18.
[155] Council of Ministers, *Digital Transformation of Bulgaria for the Period 2020-2030* (2020), 9.
[156] “National Program "Digital Bulgaria 2025" and Road map for its implementation are adopted by CM Decision №730/05-12-2019,” *Republic of Bulgaria, Ministry of Transport and Communications*, luettu 1.9.2022, https://www.mtc.government.bg/en/category/85/national-program-digital-bulgaria-2025-and-road-map-its-implementation-are-adopted-cm-decision-no73005-12-2019.
[157] Henkilökohtainen tiedonanto tutkijalle, 31.10.2022.
[158] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 10-58.
[159] Henkilökohtainen tiedonanto tutkijalle, 31.10.2022.
[160] “УЧЕНИЦИТЕ ЩЕ УЧАТ ЗА СИГУРНОСТТА В ИНТЕРНЕТ ОТ ДОГОДИНА,” *Republic of Bulgaria, Ministry of Education and Science*, luettu 16.11.2022, https://web.mon.bg/bg/news/3136.
[161] “МЕУ обучава тийнейджъри как да различават фалшивите новини в Интернет,” *Министерство на електронното управление*, luettu 16.11.2022, https://egov.government.bg/wps/portal/ministry-meu/press-center/news/learning.hackthefake.
[162] Henkilökohtainen tiedonanto tutkijalle, 5.10.2022.
[163] Henkilökohtainen tiedonanto tutkijalle, 30.9.2022.
[164] Bulgarian Safer Internet Centre Safenet.bg, *Public report* (2021), 2-20.
[165] ”Safenet.bg,” *The Bulgarian Safer Internet Center*, luettu 1.9.2022, https://www.safenet.bg/en/.
[166] Applied Research And Communications Fund, *Annual Report 2021*, 31-34.
[167] ”The Cyberscout Training Programme,” *Safenet.bg*, luettu 1.9.2022, https://www.safenet.bg/en/initiatives/173-cyberscouts.
[168] Henkilökohtainen tiedonanto tutkijalle, 21.7.2022.
[169] ”Media Literacy Coalition,” luettu 1.9.2022, https://gramoten.li/home/.
[170] ”UNICEF launches digital literacy campaign - 'New generation with critical thinking',” *UNICEF Bulgaria*, luettu 2.11.2022, https://www.unicef.org/bulgaria/en/unicef-launches-digital-literacy-campaign-new-generation-critical-thinking.
[171] Henkilökohtainen tiedonanto tutkijalle, 27.10.2022.
[172] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 69-93.
[173] Metodi Yordanov, ”Child Protection at Focus of European Cybersecurity Month in October,” *BTA*, 27.09.2022, https://www.bta.bg/en/news/bulgaria/334269-child-protection-at-focus-of-european-cybersecurity-month-in-october.
[174] Sofia Security Forum, *Оценка на познанията за сигурността в интернет*, Survey on the Knowledge and Aptitudes of Young People for their Security Online” (2019).
[175] ”Бъдете виртуални и защитени,” *EGOV.BG*, luettu 3.11.2022, https://egov.bg/wps/portal/egov/kibersigurnost.
[176] ”БОРБА С КИБЕРПРЕСТЪПНОСТТА, ГДБОП-МВР,” luettu 17.11.2022, https://www.cybercrime.bg/.

3.4. Espanja

ITU, Global Cybersecurity Index (GCI) 2020	4/182 (Global), 3/46 (Europe)
National Cyber Security Index (NCSI) 2022	9/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	7/27

3.4.1. Strategiset kyberkoulutuslinjaukset

Espanjan asema kyberturvallisuudessa on Euroopassa ja myös maailmanlaajuisesti omaa luokkaansa ja sillä on myös omat kyberturvallisuuteen erikoistuneet organisaatiot.[177] Kansallinen kyberturvallisuusstrategia (2019) alleviivaa yksityisen ja julkisen sektorin yhteistyötä ja kannustaa siihen kansallisen kyberturvallisuusfoorumin kautta. Foorumin kolme työryhmää on keskittynyt 1) kyberturvallisuuskulttuuriin, 2) teollisuuteen ja tutkimus-, kehitys- ja innovaatiotoimintaan sekä 3) kyberturvallisuuskoulutukseen. [178] Kyberturvallisuusstrategiassa esitetään yleiset toimintaohjeet kyberturvallisuudelle, ja siksi Espanjan täytyy edelleen vahvistaa taitoja, joilla kyberuhkia torjutaan. Kyberturvallisuuskulttuurin luomisen tulisi olla yksi pääteemoista, ja siihen kuuluu kyberturvallisuustietoisuuden kasvattaminen yhteiskunnassa ja oikeus turvalliseen, luotettavaan ja vastuulliseen toimimiseen kyberavaruudessa. Koska kyberturvallisuus on koko ajan kehittyvää, tarvitaan espanjalaiselle kyberturvallisuusalalle jatkuvaa tukea ja kannustusta. Tähän tarvitaan tietoa ja erilaisia taitoja.[179]

Kyberturvallisuuskulttuuria ja siihen sitoutumista tulisi edistää ja samalla vahvistaa inhimillisiä ja teknologisia taitoja. Kyberturvallisuuskulttuuria kehitetään kansalaisille ja yrityksille kohdennetuilla tietoisuutta lisäävillä kampanjoilla, joissa tietoa jaetaan kullekin kohderyhmälle räätälöiden, huomioiden erityisesti yksityisyrittäjät ja pienet ja keskisuuret yritykset. Yhteiskuntavastuuta kyberturvallisuudesta lisätään ja kannustetaan aloitteisiin ja suunnitelmiin kyberturvallisuuden ja digitaalisen lukutaidon edistämiseksi. Myötävaikutetaan totuudenmukaiseen ja korkealaatuiseen informaatioon, jossa valeuutiset ja disinformaatio erottuvat joukosta. Kyberturvallisuustietoisuutta ja -koulutusta lisätään kouluissa, joissa ne mukautetaan eri koulutusasteille sopiviksi. Yhteistyötä tiedotusvälineiden kanssa lisätään niin, että kansalaiskampanjoille saadaan lisää näkyvyyttä.[180] Kansallinen kyberturvallisuuskulttuuri on Espanjalle erittäin tärkeä asia. Yhteiskunnan jäseniä kannustetaan rakentamaan kyberturvallisuuskulttuuria, jossa kansalaiset ovat yhteisvastuussa kansallisesta kyberturvallisuudesta. [181] Espanjassa tehdään paljon työtä kyberturvallisuuskulttuurin parantamisen eteen kaikilla tasoilla. Työtä tehdään muun muassa erilaisten koulutusten avulla, tietoisuuskampanjoin ja aiheelle omistetuin portaalein. Tarkoituksena on tunnistaa aukkokohdat ja ”suojata” ne uusilla kampanjoilla sen mukaisesti, mikä tilanne kullakin hetkellä kybermaailmassa vallitsee. Espanjassa on paljon materiaalia, verkkosivustoja, ohjeistusta ja kampanjoita eri kohderyhmille. Aina on kuitenkin parantamisen varaa ja siksi ainut oikea lähestymistapa kyberturvallisuuskulttuurin parantamiseen on tehdä se 360°:ssa.[182] INCIBEn 2021–2025 strategian mottona onkin ”De miles a millones” (Tuhansista miljooniin). INCIBEn toimenpiteiden kerrannaisvaikutusten avulla halutaan tavoittaa yhä enemmän kansalaisia ja yrityksiä, jotta kansalaisten ja yritysten kyberturvallisuuden taso nousisi. Tahtotilana on asemoida Espanja johtavaksi toimijaksi kansainvälisesti ja esimerkilliseksi eurooppalaiseksi benchmarking-valtioksi kyberturvallisuuden alalla. Tulevaisuudessa kansalaisten ja yritysten kyberturvallisuuden tason halutaan olevan viiden parhaan joukossa maailmassa. Lisäksi INCIBE halutaan asemoida kyberturvallisuusalan esimerkkitoimijaksi.[183,184]

3.4.2. Kyberkansalaistaitojen opettamisen nykytila

Kyberturvallisuustietoisuuden tulisi olla osa koulutusohjelmia, jotta jokaisella olisi tietyt kyberturvallisuustaidot. Ihmiset kotona ja organisaatioissa muodostavat kyberturvallisuuden ensimmäisen puolustuslinjan ja siksi heidän

on oltava tietoisia riskeistä, joita he kohtaavat.[185] Kyberturvallisuuskulttuurin nykytilasta ja toteutettujen aloitteiden vaikutuksista ei ole olemassa kattavaa ja tarkkaa kuvaa, koska monien tietoisuutta lisäävien kampanjoiden ja valistusaloitteiden välillä on epäjohdonmukaisuuksia, sillä niitä ei arvioida eikä raportoida. Kouluissa esimerkiksi, sen lisäksi että nykyisissä opetussuunnitelmissa ei ole riittävästi kyberturvallisuutta, kyberturvallisuustietoisuuden lisäämiseen tähtäävät toimet eivät tavoita kohderyhmäänsä, vaikka materiaalia on runsaasti saatavilla. Osa tärkeistä hankkeista ja palveluista on yleisölle tuntemattomia.[186]

Espanjassa tietojenkäsittely on aluksi osana muita oppiaineita perusopetuksessa yläkouluissa ja myöhemmin erillisenä oppiaineena. Tietojenkäsittelyyn kuuluu kymmenen eri osa-aluetta, joista neljä on Espanjassa yläkouluissa integroituna ja kaikille oppilaille pakollisena. Yksi niistä on turvallisuus (safety and security). Vaikka alakoulujen perusopetuksessa tietojenkäsittelyn oppimistavoitteita ei ole Espanjassa määritelty kansallisella tasolla, osa autonomisista alueista kuitenkin käyttää niitä. Andalusiassa esimerkiksi ”kulttuuri ja digitaaliset käytännöt” -oppiaineessa osa-alueena on turvallisuus.[187] ENISAn CyberHEAD-tietokannan mukaan Espanjan korkeakouluissa kyberturvallisuutta opetetaan 23 eri ohjelmassa.[188]

Espanjan kansallinen kyberturvallisuusinstituutti INCIBE pyrkii vahvistamaan digitaalista luottamusta, lisäämään kyberturvallisuutta ja sietokykyä. Sen toiminta perustuu tutkimustoimintaan, palvelujen tarjontaan ja koordinointiin, joiden avulla se edistää kyberturvallisuutta kansallisesti ja kansainvälisesti. Sen kohderyhmänä ovat kansalaiset, akatemia ja tutkimusverkosto (RedIRIS), kyberalan ammattilaiset sekä yritykset. Sen slogan on ”INCIBE es ciberseguridad” (INCIBE on kyberturvallisuus).[189,190] Jotta voidaan luoda kyberturvallisuuskulttuuri, johon kuuluu kansalaisten ja yritysten digitaalisen luottamuksen ja kyberturvallisuusvalmiuksien vahvistaminen, on panostettava tietoisuuteen digitalisaatioon liittyvistä riskeistä ja kyberturvallisuuskoulutukseen. Kaikkia näitä toimia kehitetään INCIBEn eri yleisöille suunnattujen kanavien kautta. Kampanjoihin kuuluu tietoisuuden lisäämistä ja viestintää, kuten laajat kampanjat eri kohderyhmille, tapahtumia ja toimia itsehallintoalueilla, myös pelillistämisen avulla, sekä koulutuksia.[191]

OSI (Oficina de Seguridad del Internauta) [192] on kanava kyberturvallisuustietoisuuden lisäämiseen. Sen kohderyhmänä ovat kansalaiset, jotka käyttävät internetiä ilman riittävää tietoa tietotekniikasta, viestinnästä ja kyberturvallisuudesta. Tietoisuuden lisäämistä varten on käytössä paljon erilaisia työkaluja.[193] Sivusto sisältää muun muassa 19 erilaista tietoisuuskampanjaa, kuten senioreille suunnatun ”Experiencia Senior” -osion. Senioreille löytyy tietoa, harjoituksia ja tehtäviä, kuten sanaristikoita. Sivustolta löytyy myös kattava kyberturvallisuusopas (Guía de ciberseguridad La ciberseguridad al alcance de todos), joka soveltuu kaikille, vaikka onkin osa seniorisarjaa. Kirjassa käsitellään laiteturvallisuutta, tilien ja henkilökohtaisten tietojen suojausta, internetin turvallista käyttöä, erilaisia petoksia ja sosiaalisen median riskitöntä käyttöä. Se sisältää myös turvallisuuden tarkistuslistan, linkkejä lisätietoihin ja ohjeet raportointiin sekä kansallisen poliisin yhteystiedot. INCIBE on tehnyt kirjan OSIn kautta yhdessä kansallisen poliisin kanssa. [194] Espanjassa kyberturvallisuutta opetetaan myös pelien avulla. Näin kyberturvallisuutta voi oppia hauskalla tavalla, vaikka perheen kesken tai ystävien kanssa, esimerkiksi erilaisten tee-se-itse-pöytäpelien avulla. Salasanoja opitaan ¡Contraseñas seguras! – turvalliset salasanat -pelin avulla, joka ensin askarrellaan. Sitten sitä pelataan ja näin opitaan tekemään salasanoista turvallisempia.[195,196]

INCIBEn hallinnoima alaikäisille suunnattu Safer Internet Centerin (SIC) Internet Segura for Kids (IS4K) toimii osana Euroopan unionin Better Internet for Kids (BIK) -ohjelmaa sekä Insafe- ja INHOPE-verkostoja. Kohderyhmänä ovat lapset ja nuoret sekä heidän kauttaan vanhemmat ja muut kasvattajat.[197,198] Vuonna 2021 yli 40 000 ihmistä osallistui yli 200 erilaiseen IS4K:n koulutus- ja tietoisuutta lisäävään tapahtumaan. [199] Ohjelmassa järjestettäviin tapahtumiin kuuluu esimerkiksi vuotuinen ”Safer Internet Day”. [200] Koulunaloituskampanja Kyberturvallisuutta reppuusi opettaa vastuulliseen laitteiden käyttöön koulussa. Lasten vanhemmille on suunnattu Lastenvalvontatyökaluja-kampanja, josta löytyy ohjeistusta ja sovelluksia esimerkiksi ruutuajan tai sisällön hallintaan. [201] INCIBE on myös tehnyt lapsille ja perheille opetuksellisia verkko- ja mobiilipelejä. Cyberscouts-verkkopelissä, joka on suunnattu koko perheelle, opitaan käyttämään internetiä turvallisemmin. Pelissä on eri tasoja ja omat osiot lapsille ja aikuisille. Pelin avulla opitaan muun muassa hyviä ja

huonoja salasanoja, kyberturvallisuuden termejä, turvallisia ja turvattomia tilanteita ja salauksen peruskäsitteitä. [202] , [203] Toisessa Hackers vs Cybercrook -mobiilipelissä opitaan tietoturvaa jokapäiväisissä tilanteissa pelaamalla Sergion kanssa.[204]

Yrityksille ja ammattilaisille on tarjolla muun muassa MOOC-verkkokursseja kouluttautumiseen sekä ilmainen Hackend-peli, jonka avulla opitaan yritysten kyberturvallisuutta. Peli voitti ”Paras vakava peli” -palkinnon vuonna 2016 Fun&Serious Game Festival -tapahtumassa.[205,206] Hackend-pelin avulla (verkko/mobiilipeli) opetellaan pk-yritysten kyberturvallisuutta. Tehtävät liittyvät pk-yrityksen päivittäisiin tilanteisiin (kuten sähköpostin käyttö) ja tilanteisiin, joissa yrityksen tiedot tai resurssit ovat vaarantuneet (kuten tietovuoto, sosiaalinen manipulointi tai haittaohjelmatartunta). [207] Yrityksille on myös alakohtaista kyberturvallisuuskoulutusta. [208] Esimerkiksi turismille löytyy 29-kohtainen koulutuspaketti, joissa jokaisessa on lisätietoa ja koulutusmateriaaleja.

INTEF eli Espanjan kansallinen opetusteknologian ja opettajankoulutusinstituutti tarjoaa verkkokursseja AprendeINTEF, the education meeting point -sivustolla, kuten #SeguDig. Kurssilla opiskellaan digitaalista turvallisuutta ja yksityisyyttä. Se on suunnattu opettajille alaikäisten turvallisen ja vastuullisen internetin käytön opettamiseen. Käsiteltäviä aihealueita ovat muun muassa viraalihaasteet, valeuutiset, digitaalinen hyvinvointi ja riippuvuutta aiheuttava käyttäytyminen verkossa. Tämä MOOC-kurssi on tehty yhteistyössä INCIBEn ja Espanjan tietosuojaviraston (AEPD) kanssa. [209] INTEF:n AseguraTIC-sivusto tarjoaa kasvattajille, perheille, opiskelijoille, kouluille ja hallinnolle koulutuksellista sisältöä, ohjeita, koulutuskursseja ja muuta hyödyllistä.[210]

#ExploradorINCIBE-kyberturvallisuustietoisuuskampanja[211] sai paras video -EU-palkinnon 2021. Kampanja oli suunnattu 14–64-vuotiaille, mutta sävyltään sen erityiskohderyhmänä olivat nuoret. Kampanjan aiheena olivat kiristyshaittaohjelmat, verkkourkinta ja syvävärennökset. Kampanjalla oli yli 75 miljoonaa katselukertaa.[212]

Tulevaisuuden toimenpiteitä ja toiveita tietoisuuden lisäämiseen (esimerkkejä): Kaikkien eri aiheista järjestettävien kurssien kokoaminen samaan paikkaan ja tietoisuutta lisäävät laajat kansalliset kampanjat. Opetuspelejä voisivat olla digitaaliset tietokilpailut, pakohuonetyyliset pelit, klassiset ajattomat ajanvietepelit ja virtuaalitodellisuuskokemukset. Tukipalveluihin voitaisiin koota usein kysytyt kysymykset, luoda kyberturvallisuutta koskeva Wikipedia tai koota kirjastoja kyberturvallisuussovelluksista ja mielenkiintoisista sisällöistä ja resursseista.[213]

3.4.3. Kansalliset erityispiirteet

Kaikki Espanjan itsehallintoalueet (kuten Andalusia [AndalucíaCERT], Katalonia [Agencia de Ciberseguridad de Cataluña], Galicia [CIBER.gal] ja Kastilia-León [Cybersecurity Innovation HUB] kehittävät tai tukevat aloitteita, jotka liittyvät kyberturvallisuuteen tai kyberturvallisuuskulttuurin edistämiseen ja CSIRT-ryhmien perustamisesta lähtien erilaisten tietoisuuskampanjoiden toteuttamiseen.

3.4.4. Kyberkansalaistaitojen määrittäminen

Kansalainen määritellään INCIBEn strategiassa 2021–2025 jokaiseksi, joka käyttää teknologiaa ja laitteita. Erityisenä huomion kohteena ovat alaikäiset, koska he ovat erittäin haavoittuvainen ryhmä. [214] Kyberkansalaistaitoja voidaan tarkastella opettajien yhteisen digitaalisen osaamisen viitekehyksen (CDCFT) kautta, joka on mukautettu kansalaisille suunnatusta The European Digital Competence Framework for Citizens- ja opettajille suunnatusta The European Digital Comptence Framework for Educators -viitekehyksestä. Viitekehys on jaettu viiteen osaamisalueeseen ja yhteensä 21 kompetenssiin. Yksi osa-alueista on turvallisuus, johon kuuluu muun muassa laitteiden, digitaalisen identiteetin, datan, terveyden ja ympäristön suojaaminen. Aihealueita ovat esimerkiksi salasanat, yksityisyyden suojaaminen ja verkkokiusaaminen. Ne ovat aiheita, joita käsitellään myös tietoisuuskampanjoissa ja koulutuksissa.[215]

Viitteet

[177] Pedro Sánchez Castejón, President of the government of Spain, *National Cybersecurity Strategy 2019* (2019), 14.
[178] National Cybersecurity Forum, *Global report activities carried out in the first phase*, 6, 10.
[179] Pedro Sánchez Castejón, President of the government of Spain, *National Cybersecurity Strategy 2019* (2019), 29-30.
[180] Pedro Sánchez Castejón, President of the government of Spain, *National Cybersecurity Strategy 2019* (2019), 38, 56-57.
[181] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 131.
[182] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 133.
[183] Gobierno de Espãna, INCIBE, *Plan Estratégico INCIBE 2021-2025 'De miles a millones'* (2021), 4-5.
[184] Gobierno de Espãna, INCIBE, *Plan Anual de Actividad INCIBE 2021*, 5.
[185] Foro Nacional de Ciberseguridad, *Foro Nacional de Ciberseguridad, Motor de la colaboración público-privada* (2021), 31.
[186] Foro Nacional de Ciberseguridad, *Foro Nacional de Ciberseguridad, Motor de la colaboración público-privada* (2021), 40.
[187] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 10, 59-60.
[188] "CYBERHEAD – Cybersecurity Higher Education Database," *ENISA*, luettu 15.11.2022, https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=esp.
[189] "What is INCIBE," *INCIBE*, luettu 14.11.2022, https://www.incibe.es/en/what-is-incibe.
[190] "Qué es INCIBE," *INCIBE*, luettu 14.11.2022, https://www.incibe.es/que-es-incibe.
[191] Gobierno de Espãna, *España Digital 2026* (2022), 49.
[192] "OSI, Oficina de Seguridad del Internauta," luettu 14.11.2022, https://www.osi.es.
[193] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 131.
[194] "Guía de ciberseguridad," *OSI*, luettu 22.9.2022, https://www.osi.es/es/guia-de-ciberseguridad-la-ciberseguridad-al-alcance-de-todos.
[195] "Juegos mesa," *OSI*, luettu 14.11.2022, https://www.osi.es/es/juegos-mesa.
[196] "Mejora tus contraseñas,"*OSI*, luettu 14.11.2022 https://www.osi.es/sites/default/files/docs/c3_pdf_rp_mejora_tus_contrasenas.pdf.
[197] "Spanish Safer Internet Centre," luettu 17.11.2022, https://www.betterinternetforkids.eu/sic/spain.
[198] "Internet Segura for Kids (IS4K)," luettu 17.11.2022, https://www.is4k.es/.
[199]"Cybersecurity Balance 2021 INCIBE," *INCIBE*, luettu 16.8.2022, https://www.incibe.es/sites/default/files/paginas/que-hacemos/cybersecurity_balance_2021_incibe.pdf?utm_source=google&utm_medium=web&utm_campaign=cybersecurity_balance_2021&utm_id=Cybersecurity+Balance+2021.
[200] "Día de Internet Segura 2023," *INCIBE*, luettu 30.11.2022, https://www.incibe.es/sid.
[201] "Internet Segura for Kids (IS4K)," luettu 17.11.2022, https://www.is4k.es/.
[202] "INCIBE lanza Cyberscouts, un juego online para aprender a hacer un uso más seguro de Internet," *INCIBE*, luettu 15.7.2022, https://www.incibe.es/sala-prensa/notas-prensa/incibe-lanza-cyberscouts-juego-online-aprender-hacer-uso-mas-seguro.
[203] "Juego Cyberscouts," *is4k*, luettu 17.11.2022, https://www.is4k.es/de-utilidad/cyberscouts.
[204] "Hackers vs Cybercrook,"*OSI*, luettu 17.11.2022, https://www.osi.es/es/hackers.
[205] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 131.
[206] "Hackend, se acabó el juego,"*INCIBE*, luettu 15.11.2022, https://www.incibe.es/protege-tu-empresa/hackend.
[207] "Hackend: se acabó el juego,"*INCIBE*, luettu 15.7.2022, https://www.incibe.es/protege-tu-empresa/blog/hackend-se-acabo-el-juego.
[208]"Bienvenidos, Selecciona el sector al que pertenece tu empresa," *INCIBE*, luettu 30.11.2022, https://itinerarios.incibe.es/.
[209] "AprendeINTEF, the education meeting point," *INTEF*, luettu 18.11.2022, https://enlinea.intef.es/?status=in-progress.
[210] "AseguraTIC," *INTEF*, luettu 18.11.2022, https://intef.es/aseguratic/.
[211] "Explorador INCIBE," *INCIBE*, luettu 30.11.2022, https://www.incibe.es/exploradorincibe.
[212] "#ExploradorINCIBE," *ECSM*, luettu 17.11.2022, https://cybersecuritymonth.eu/countries/spain/exploradorincibe/.
[213] Foro Nacional de Ciberseguridad, *Foro Nacional de Ciberseguridad, Motor de la colaboración público-privada* (2021), 42-42.
[214] Gobierno de Espãna, INCIBE, *Plan Estratégico INCIBE 2021-2025 'De miles a millones'* (2021), 10.
[215] INTEF, *Common Digital Competence Framework for Teachers* (2017).

3.5. Irlanti

ITU, Global Cybersecurity Index (GCI) 2020	46/182 (Global), 28/46 (Europe)
National Cyber Security Index (NCSI) 2022	30/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	5/27

3.5.1. Strategiset kyberkoulutuslinjaukset

Irlannissa kyberturvallisuudesta vastaavat viranomaiset ovat kansallinen kyberturvallisuuskeskus (National Cyber Security Centre, NCSC)[216], joka toimii ympäristö- ja viestintäministeriön (Department of the Environment, Climate and Communications DECC)[217] alaisuudessa, sekä Irlannin tietokonehätätilatiimi (Computer Emergency Response Team, IRISS-CERT)[218]. Irlannin viimeisin kansallinen kyberturvallisuusstrategia koskee vuosia 2019–2024. Kyberturvallisuusstrategiassa on määritelty 20 mittaria, joiden perusteella kyberturvallisuuden kehitystä on tarkoitus Irlannissa kehittää. Kyseisestä 20 mittarista viisi viittaa jollain tavalla kansalaisten kyberturvallisuuspääoman kehittämiseen, ennen kaikkea liiketoiminnallisesta näkökulmasta (korkea- ja jatkokoulutus työelämän tarpeisiin; osaajien houkutteleminen työelämän tarpeisiin; kumppanuuksien löytäminen kyberturvallisuuden tutkimustyön rahoittamiseksi; teollisuuden sekä hallinnon ja korkeakoulutuksen erityisosaajien keskinäinen yhteistyö ja tämän rahoitus; sekä tutkimus- ja yritysmaailman yhteen törmäyttäminen käytännön innovaatioiden ja tutkimusläpimurtojen saavuttamiseksi). Irlannin julkilausuttu visio kyberturvallisuusstrategian mukaisesti on yhteiskunta, joka nauttii digitalisaation eduista ja on mukana muokkaamassa tulevaisuuden internetiä. Tämä on strategiassa jaettu tarkemmin kolmeen osioon: suojaamiseen, kehittämiseen ja osallistumiseen. Suojaamisosio viittaa sekä kansalliseen infrastruktuuriin että kansalaisten turvallisuuteen; kehittämisosiossa mainitaan instituutioiden, julkisen ja yksityisen sektorin lisäksi myös kansalaiset; osallistumisosiossa viitataan lähinnä kansainväliseen yhteistyöhön ja kansainvälisen kybertoimintaympäristön kehittämiseen. Strategiassa on seitsemän määriteltyä tavoitetta. Näistä yksi ottaa kantaa kyberkansalaistaitoihin, ja tavoitteena on parantaa kansalaisten kyberturvallisuuteen liittyvää tieto- ja taitotasoa sekä auttaa tavallisia ihmisiä ymmärtämään paremmin näitä taitoja tiedotuksen ja koulutuksen avulla. Myös vaalivaikuttamista ja disinformaatiota käsitellään, samoin kuin identiteettivarkauksien ja kiristyshaittaohjelmien uhkaa. Strategian kansalaisille suunnattua koulutusta käsittelevässä osuudessa mainitaan muun muassa kansalaisille suunnatun kyberturvallisuuskampanjan rakentaminen (teemoina kyberhygienia ja sosiaalinen manipulointi). Strategia huomioi myös Irlannissa työskentelevät 6 500 tietoturva-alan ammattilaista (2015) sekä heidän vastuunsa ja potentiaalinsa kansallisen kyberturvallisuuden takaajina sekä yleisemmin kyberturvallisuusalan työllistävän potentiaalin tulevina vuosina.[219]

3.5.2. Kyberkansalaistaitojen opettamisen nykytila

Digitaalinen osaaminen on monialainen teema Irlannin peruskoulussa ja toisella asteella, ja digitekniikan käytön sulauttaminen opetukseen on osa opetussuunnitelman kehittämisprosessia. Digitaalinen osaaminen yhdistetään muihin pakollisiin oppiaineisiin ja valinnaisiin oppimisalueisiin, esimerkiksi perusasteella digitaaliseen medialukutaitoon. Peruskoulun ylemmillä luokilla (lower secondary school) voi opiskella valinnaista ainetta ”Digital media literacy” ja toisella asteella on yhtenä valinnaisena aineena ”Computer science”. DigCompin ”Safety”-osa-alue on viety opetussuunnitelmaan peruskoulun ylempien luokkien osalta[220], ja yksi keskeinen näkökohta opetussuunnitelman kehittämistyössä on ollut nimenomaan kyberturvallisuushygienia.[221] Kansallinen opetussuunnitelma- ja arviointineuvosto (National Council for Curriculum and Assessment) on opetusministeriön alainen toimielin, joka tuottaa tukimateriaalia Irlannin opetussuunnitelmaan, yhtenä

esimerkkinä 12–15-vuotiaille suunnattu ”Digital media literacy” -kurssi. Kurssilla pyritään parantamaan opiskelijoiden mahdollisuuksia käyttää digitaalitekniikkaa, viestintävälineitä ja internetiä luovasti, kriittisesti ja turvallisesti. Opettajien ja koulujen tueksi verkossa on ”Assessment Toolkit”, jossa on mukana muun muassa oppimista, opetusta, arviointia ja raportointia tukevaa aineistoa.[222] Myös muutamat yksityiset yritykset tukevat Irlannin koulujen tietotekniikan opetusta. Cyber school.ie tekee yhteistyötä peruskoulujen ja toisen asteen koulujen kanssa tarjoamalla verkkokoulutuksia. Yhtenä esimerkkinä on vuorovaikutteinen, itsenäistä opiskelua edellyttävä verkkokurssi, jossa käydään läpi kaikki tärkeimmät verkkoturvallisuuden osa-alueet ja joka sopii niin oppilaille, vanhemmille kuin peruskoulun ja lukion henkilökunnallekin.[223] Computing at schools -yritys järjestää esimerkiksi 15–18-vuotiaille cyber safety & digital citizenship -opetusta joko Zoomissa tai paikan päällä oppilaitoksessa. Cyber safety -kursseja on myös 2.–6. luokan oppilaille. [224] Korkeakouluasteella kyberturvallisuuteen liittyvää koulutusta järjestää Dublinin yliopiston (University College Dublin) maisteriohjelma ”Forensic Computing and Cybercrime Investigation”[225], ja Dublinin teknologisessa yliopistossa (Technological University Dublin) on ohjelma ”Bachelor of Science (Honours) in Computing in Digital Forensics & Cyber Security”[226]. Aikuisille kohdennettua kyberturvallisuuskoulutusta toteuttavat myös kansanopistot. Ainakin Dublinin jatkuvan koulutuksen kansanopistolla (People's College for Continuing Education and Training) on aikuisille käytäntöön pohjautuva, 12 viikkoa kestävä kurssi ”Computers/phones: protect yourself online-keeping your personal information safe”.[227]

Kolmannen sektorin panostus kyberturvallisuuden koulutukseen on Irlannissa merkittävä. CyberSafeKids (aiemmin CyberSafeIreland) on irlantilainen rekisteröity hyväntekeväisyysjärjestö, jonka tavoitteena on opettaa lapsille, vanhemmille ja opettajille turvallista ja vastuullista verkkokäyttäytymistä. Järjestön koulutukset ovat joko live-koulutuksia tai ne järjestetään järjestön portaalin kautta webinaarina. Cyberacademy-portaali sisältää lyhyitä internetin turvallisuuteen liittyviä videoita, materiaaleja ja tehtäviä 7–10-vuotiaille lapsille, vanhemmille ja opettajille.[228] Cyber threat task force puolestaan on voittoa tavoittelematon kyberturvallisuusalan yhteisö, joka ylläpitää kansalaisten ja organisaatioiden verkkokoulutuskampusta nimeltään ”Cyber risk academy”. Kampuksen ”Interactive cyber awareness training” on tarkoitettu kaikille, jotka ovat huolissaan verkkoturvallisuudesta ja haluavat muuttaa käytöstään välttääkseen kyberhyökkäysten uhriksi joutumisen.[229] Irlannin tiedesäätiön (Science Foundation Ireland) tavoitteena on sitouttaa irlantilaista suurta yleisöä mukaan tieteeseen, teknologiaan, tekniikkaan ja matematiikkaan (STEM). Tähän kuuluu monenlaista lasten ja perheiden kanssa tapahtuvaa toimintaa, yhtenä esimerkkinä ”Mid-term online workshop in cyber security for children” eli työpaja lapsille ja vanhemmille turvallisista verkkokäytännöistä.[230] Kansallinen vanhempainneuvosto (National Parents Council Primary, NPC) puolestaan on perus- tai varhaiskasvatuksessa olevien lasten vanhempien edustusjärjestö. Sen portaalin kautta voi osallistua verkkokoulutukseen ”Internet safety”, jonka tarkoitus on opettaa vanhemmille keinoja lastensa turvallisempaan ja vastuullisempaan internetin käyttöön. [231]

Webwise - Internet Safety Awareness Centre on toteutettu EU-yhteistyössä, ja sen tavoite on edistää nuorten internetin itsenäistä, tehokasta ja turvallisempaa käyttöä erilaisilla vanhempiin, opettajiin ja itse lapsiin kohdennetuilla tiedotustoimenpiteillä. Keskus kehittää ja välittää resursseja, jotka auttavat opettajia integroimaan internetin turvallisuusasioita opetukseensa, ja tarjoaa vanhemmille tietoa, neuvoja ja työkaluja, joilla he voivat tukea lastensa turvallista verkkokäyttäytymistä. Nuorison tietoisuutta lisätään Webwise Youth Advisory Panelin avulla, jossa kehitetään muun muassa kampanjoita verkkokiusaamisen ehkäisemiseksi. [232]

Kampanjat ovat Irlannissa sekä kansallisia että EU-vetoisia. ”Be Safe Online” on hallituksen kampanja, jonka tarkoituksena on tuoda esiin menettelytapoja turvalliseen verkkokäyttäytymiseen. Kampanjan portaalissa on saatavilla laaja valikoima verkkoturvallisuusresursseja kaikkien kansalaisten verkkoturvallisuuden tukemiseksi, esimerkiksi henkilökohtaisten laitteiden ja tilien suojaamiseen. [233, 234] ”Be Media Smart” on Irlannin medialukutaitoyhdistyksen (Media Literacy Ireland) jäsenten kehittämä disinformaatioon painottuva kampanja, jonka tavoitteena on auttaa ihmisiä erottamaan toisistaan luotettava ja tarkka sekä tarkoituksellisesti väärä tai harhaanjohtava tieto toisistaan.[235] Kansallisten kampanjoiden lisäksi Irlanti osallistuu EU:n kampanjoihin kuten Safer Internet day[236] ja ECSM[237]. Safer Internet day -päivää tuetaan esimerkiksi tapahtumilla ja sosiaalisen median kampanjoilla. ECSM-kampanjan yhteydessä Kansallinen kyberturvallisuuskeskus (National Cyber

Security Centre, NCSC) on julkaissut lehdistötiedotteen kampanjan käynnistämiseksi ja tiedotusgrafiikoita hallituksen "Be Safe Online" -verkkosivuilla sekä Twitter-, Facebook- ja LinkedIn-kanavilla.[238]

Irlannin valtiollinen poliisi ja turvallisuuspalvelu (Irelands national police and security service) ylläpitää ”Cyber Crime” -portaalia, johon on koottu kansalaisille yksityiskohtaista tietoa erilaisista verkkoympäristön uhista ja konkreettisista toimenpiteistä siltä varalta, että joutuu esimerkiksi huijauksen kohteeksi.[239] Poliisi on mukana myös kansallisessa palvelussa ”CheckMyLink”, jota se toteuttaa yhdessä Cyber Skillsin ja ScamAdviserin kanssa. Tavoitteena on lisätä kuluttajien luottamusta verkkosivustojen aitouteen ja turvallisuuteen esimerkiksi haittaohjelmien suhteen. Palvelua käytetään kirjoittamalla palveluun verkkosivuston URL-osoite, jonka turvallisuuden se tarkistaa.[240]

Kyberturvallisuuteen liittyviä pelejä on MediaLiteracy Irelandin portaalissa. Portaalin Training & development -välilehdeltä [241] voi hakea tietoa ja koulutusmateriaalia sekä medialukutaidosta että digitaalisesta turvallisuudesta aiheen, ikäryhmän ja toivotun formaatin perusteella. Esimerkiksi disinformaatiota käsittelevät ”Fake news game”- ja ”GoViral”-peli, joka auttaa suojautumaan vääriltä COVID-19:ää koskevilta tiedoilta. ”#For You” -peli keskittyy internetin algoritmien perusteisiin.

Erityistä Irlannin kyberturvakoulutukselle on lisäksi se, että kirkot ja aktiiviset vapaaehtoiset, esimerkiksi seniorit, osallistuvat kouluttamiseen. Vodafone Ireland Foundation -säätiö järjestää yhteistyökumppaniensa kanssa digitaalisen osaamisen kursseja, joissa kouluttajina toimivat aktiiviset eläkeläiset Active Retirement Ireland -hyväntekeväisyysjärjestöstä. He tarjoavat henkilökohtaista opetusta erilaisissa yhteisöllisissä tiloissa eri puolilla maata. Tarkoitus on auttaa ikäihmisiä hoitamaan turvallisesti päivittäisiä toimintoja verkossa.[242] Irlannin kirkon osallisuudesta kouluttamiseen yhtenä esimerkkinä on online-koulutusseminaari ”Cybersecurity for the Bewildered: How to keep your computers safe, your data secure and private information out of sight”, joka oli kohdennettu Corkin, Cloynen ja Rossin papeille ja kansalaisille ja jonka olivat toteuttaneet alueen piispa ja Corkin yliopiston liiketalouden tietojärjestelmien koulutusohjelma (Business Information Systems at University College Cork).[243]

3.5.3. Kansalliset erityispiirteet

Irlannissa on havaittavissa digitaalinen kahtiajako kansalaisten välillä, eli osa hallitsee digitaidot hyvin, toiset eivät (”haves and have-nots”). Vuonna 2020 tehdyn tutkimuksen mukaan irlantilaisista 42 prosenttia kuvailee olevansa digitaalisten taitojen keskiarvon alapuolella. [244] Haasteena kyberturvallisuuden kehittämisessä pidetään epäilyksiä siitä, muuttavatko tiedotuskampanjat todella käyttäytymistä. Epävarmuutta on myös siitä, olisiko kyberasiaa edistettävä koulutusjärjestelmän, työnantajien vai yksityisten tahojen kautta. [245] Merkillepantavaa on, että Irlannissa on alettu kiinnittää erityistä huomiota kyberalan työvoimapulaan. Kansalaiset voivat erilaisilla kursseilla ja ohjelmissa kouluttautua teollisuuden työtehtäviin, vaikka ei olisi alalta aiempaa kokemusta. [246] Esimerkiksi Generation: You Employed Inc. järjestää yhteistyössä Microsoftin ja Verizonin kanssa ”IT Support with Cyber Security” -koulutuksia aloittelijoille, jotka haluavat pätevöityä kyberalalle.[247] CareerEran kurssit on suunniteltu teollisuuden tarpeita ajatellen ja tarjoavat väylän esimerkiksi alanvaihtajille kyberturva-alan tehtäviin.[248] ICT Skillnet CISCO Networking Academy järjestää ilmaisia kyberalan kursseja niin aloittelijoille kuin edistyneemmillekin.[249] Myös Fortify institutella on kursseja, ja se on koonnut portaaliinsa keskeisiä koulutusyrityksiä Irlannissa.[250]

3.5.4. Kyberkansalaistaitojen määrittäminen

Irlannin kyberturvallisuusstrategiassa ei määritellä yksityiskohtaisesti kyberkansalaistaitoja. DigCompin Safety-osa-alue on kuitenkin hyväksytty opetussuunnitelmaan peruskoulun ylempien luokkien (lower secondary school) osalta. Tämän osa-alueen taitojen opetusta kansalaisille siis Irlannin hallinnossa kannatetaan.[251]

Viitteet

[216] ”National Cyber Security Centre NCSC,” *NCSC,* luettu 4.1.2023, https://www.ncsc.gov.ie/.
[217] ”Department of the Environment, Climate and Communications,” *gov.ie*, luettu 4.1.2023, https://www.gov.ie/en/organisation/department-of-the-environment-climate-and-communications/.
[218] “About IRISS,” *Irish Reporting and Information Security Service*, luettu 4.1.2023, https://iriss.ie/.
[219] Government of Ireland, *National Cyber Security Strategy 2019-2024* (2019).
[220] European Commission, / EACEA / Eurydice, Informatics education at school in Europe, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45, 118.
[221] ENISA, EGA*, Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 28.
[222] ”Digital Media Literacy,” *National Council for Curriculum and Assessment,* luettu 25.12.2022, https://curriculumonline.ie/Junior-cycle/Short-Courses/Digital-Media-Literacy/.
[223] ”ABOUT CYBERSCHOOL.IE,” *CyberSchool.ie*, luettu 14.12.2022, https://cyberschool.ie/aboutus/.
[224] ”Welcome to Computing At Schools,” *Computing At Schools*, luettu 25.12.2022, https://computingatschools.ie/.
[225] "MSc Forensic Computing and Cybercrime Investigation," *University College Dublin*, luettu 13.12.2022, https://hub.ucd.ie/usis/!W_HU_MENU.P_PUBLISH?p_tag=PROG&MAJR=T146.
[226] "Digital Forensics and Cyber Security," *Technological University Dublin*, luettu 13.12.2022, https://www.tudublin.ie/study/undergraduate/courses/computing-dig-forensics-and-cyber-sec-tu863/.
[227] ”Course Description,” *Courses.ie*, luettu 25.12.2022, https://www.courses.ie/course/computers-phones-protect-yourself-online-keeping-your-personal-information-safe/#.
[228] ”CyberSafeKids: Our Story,” *CyberSafeKids*, luettu 25.12.2022, https://www.cybersafekids.ie/about-us/.
[229] ”CYBER RISK ACADEMY,” *ICTTF International Cyber Threat Task Force*, luettu 25.12.2022, https://community.icttf.org/courses.
[230] ”Mid-term online workshop in cyber security for children,” *Science Foundation Ireland*, luettu 14.12.2022, https://www.sfi.ie/research-news/news/cyber-security-for-kids/.
[231] ”Internet Safety – Online,” *National Parents Council*, luettu 25.12.2022, https://www.npc.ie/training-and-resources/training-we-offer/internet-safety.
[232] “About us,” *Webwise*, luettu 14.12.2022, https://www.webwise.ie/welcome-to-webwise/us/.
[233]ENISA, EGA*, Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 43.
[234] "Be safe online," *Government of Ireland*, luettu 13.12.2022, https://www.gov.ie/en/campaigns/be-safe-online/.
[235] ”We need a vaccine against misinformation,*” Media Literacy Ireland*, luettu 15.12.2022, https://www.bemediasmart.ie/.
[236] ”Irish Safer Internet Centre - Webwise Ireland,” *European Schoolnet*, luettu 25.12.2022, https://www.saferinternetday.org/in-your-country/ireland.
[237] ”Cybersecurity Resources,” *ENISA*, luettu 25.12.2022, https://cybersecuritymonth.eu/countries/ireland.
[238] ENISA, *European Cybersecurity Month (ECSM) 2020 Deployment Report* (2021), 51.
[239] ”Cyber crime,”*An Garda Síochána (AGS), Ireland’s national police and security service*, luettu 14.12.2022, https://www.garda.ie/en/crime/cyber-crime/cyber-crime-awareness-campaign-2022.html.
[240] ”Cyber Skills Ireland launches new service for consumers to support safer online shopping,” *CyberSkills Ireland*, luettu 25.12.2022, https://www.cyberskills.ie/explore/news/name-13692-en.html.
[241] ”Training & Development,” *Media Literacy Ireland*, luettu 25.12.2022, https://www.medialiteracyireland.ie/training-development/.
[242] ”Digital skills training classes for over 65-year-olds launched | Vodafone Ireland,” *Vodafone Ireland Limited*, luettu 25.12.2022, https://n.vodafone.ie/aboutus/press/multi-million-euro-digital-skills-programme-for-older-people-lau.html.
[243] ”Cybersecurity training session in Cork, Cloyne and Ross attracts a lot of interest,” *Church of Ireland*, luettu 25.12.2022, Cybersecurity training session in Cork, Cloyne and Ross attracts a lot of interest - Church of Ireland - A Member of the Anglican Communion.
[244] Accenture, *BRIDGING THE GAP: Ireland’s Digital Divide* (2020), 9, 15.
[245]ENISA, EGA*, Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 43.
[246] Carmel Somers and Eoin Byrne, *Cyber security skills report 2021: National survey* (2021), 11.
[247] ”IT Support and Cyber Security,” *Generation: You Employed Inc.*, luettu 14.12.2022, https://ireland.generation.org/programs/it-support-2/.
[248] ”Cyber Security Course Online,” *Careerera*, luettu 14.12.2022, https://www.careerera.com/cyber-security.
[249] ”ICT Skillnet CISCO Networking Academy,” *Technology Ireland ICT Skillnet,* luettu 15.12.2022, https://www.ictskillnet.ie/training/ict-skillnet-cisco-networking-academy/.
[250] ”Cybersecurity Training and Education in Ireland – Where do I start?,” *Fortify Institute,* luettu 14.12.2022, https://www.fortifyinstitute.com/blogs/cybersecurity-training?hsLang=en.
[251]European Commission, / EACEA / Eurydice, Informatics education at school in Europe, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45.

3.6. Italia

ITU, Global Cybersecurity Index (GCI) 2020	20/182 (Global), 13/46 (Europe)
National Cyber Security Index (NCSI) 2022	21/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	18/27

3.6.1. Strategiset kyberkoulutuslinjaukset

Italian kansallinen kyberturvallisuusvirasto ACN (Agenzia per la Cybersicurezza Nazionale) julkaisi toukokuussa 2022 Italian uuden kyberturvallisuusstrategian vuosille 2022–2026 ja sen toimeenpanosuunnitelman. Kyberturvallisuusstrategiassa on kolme päälinjaa: suojaaminen, reagointi ja kehittäminen. Niiden tukena on mahdollistavia tekijöitä: kyberturvallisuuskoulutus, kyberturvallisuuskulttuurin edistäminen ja yhteistyö.[252] Yksi strategian päätavoitteista on kyberturvallisuustietoisuuden parantaminen koko yhteiskunnassa. Tavoitteen saavuttamiseksi on suunniteltu erilaisia toimenpiteitä. [253] Kyberturvallisuuskoulutusta tehostetaan eri koulutusasteilla, kuten peruskouluissa, lukioissa, yliopistoissa ja täydentävissä koulutusohjelmissa. Kansalaisille avataan ACN e-Academy -oppimisalusta. Ensimmäiseksi otetaan käyttöön verkkotyökalu, jolla kansalaiset voivat testata omaa kyberturvallisuusosaamistaan ja ansaita sertifikaatin. Julkisen ja yksityisen sektorin työntekijöille tarjotaan aiempaa enemmän kyberturvallisuuden kursseja ja koulutusohjelmia. Kyberturvallisuuskulttuurin edistämiseksi käynnistetään kampanjoita tieto- ja viestintätekniikoiden käytön riskeistä ja yksityisyyden suojaamisesta verkossa. Niissä huomioidaan senioreiden, toimintarajoitteisten ja muiden ryhmien erityistarpeet. Lasten suojelemiseksi verkkorikollisuudelta laaditaan itsenäinen kansallinen strategia ja toimeenpanosuunnitelma, johon sisältyy alaikäisille sekä heidän vanhemmilleen, huoltajilleen ja opettajilleen suunnattuja kampanjoita.[254]

Vuonna 2020 julkaistun kansallisen digitaalisen osaamisen strategian (Strategia Nazionale per le Competenze Digitali) ja sitä täydentävän toimeenpanosuunnitelman tavoitteena on, että 70 prosentilla Italian kansalaisista on vähintään perustason digitaaliset taidot vuonna 2025. Tärkeässä roolissa on Repubblica Digitale -hanke, jonka julistuksessa todetaan, että kansalaisen velvollisuus on toimia digitaalisessa ekosysteemissä tietoisesti, turvallisesti ja kestävästi.[255] Hankkeella oli vuonna 2021 yli 260 erilaista aloitetta, joiden piirissä oli yli kaksi miljoonaa opiskelijaa, 90 000 opettajaa, 240 000 työntekijää ja 1,6 miljoonaa muuta kansalaista. Vuoden 2022 tammikuussa perustetusta rahastosta sijoitetaan 350 miljoonaa euroa kahden miljoonan kansalaisen digitaalisten taitojen parantamiseen vuosina 2022–2026.[256]

3.6.2. Kyberkansalaistaitojen opettamisen nykytila

Italian kansallinen kyberturvallisuusvirasto ACN perustettiin elokuussa 2021. Sillä on vastuu koordinoida kyberturvallisuusstrategiassa linjattuja opetukseen ja kampanjointiin liittyviä tavoitteita. ACN:n tavoitteena on kehittää systemaattinen lähestymistapa kyberturvallisuuden opetukseen kartoittamalla ensin olemassa olevaa tarjontaa ja sovittamalla sitä sitten yhteen. Italiassa onkin useita julkisia ja yksityisiä toimijoita, jotka tarjoavat kyberturvallisuuteen liittyvää koulutusta. [257] Tietojenkäsittelyä, johon sisältyy digitaalisten taitojen ja kyberturvallisuustaitojen opetusta, opetetaan vaihtelevasti koulujen perusopetuksessa osana muita aineita. Toisen asteen opetuksessa tietojenkäsittely on pakollinen ja erillinen oppiaine osalle oppilaista ja pakollista kaikille osana matematiikan opintoja.[258] ENISAn CyberHEAD-tietokannan mukaan Italian korkeakouluissa on tarjolla 17 kyberturvallisuuden koulutusohjelmaa.[259] ACN ja Lazion alue ovat hiljattain solmineet neljän vuoden sopimuksen kyberturvallisuuskoulutusohjelmien järjestämisestä. Koulutusohjelmat on suunnattu toisen asteen oppilaitoksille, korkeakouluille ja jatkokoulutuksiin. Yhteistyössä on mukana italialaisia IT-alan yrityksiä. Opetus

järjestetään uudessa kyberturvallisuuskoulutuskeskuksessa. Koulutushankkeella on määrä vahvistaa koko Italian turvallisuutta.[260,261]

Italian poliisin posti- ja viestintäpoliisin erikoisyksikkö (Polizia Postale e delle Comunicazioni) valvoo Italian viestintäverkon turvallisuutta, ehkäisee verkkorikollisuutta ja huolehtii kansalaisten kirjesalaisuuden ja viestintävapauden toteutumisesta. Se levittää kyberturvallisuustietoisuutta italialaisiin kouluihin ja tavoittaa tällä toiminnalla noin 500 000 koululaista vuosittain.[262] Commissariato di P.S. online -verkkosivujen ja sosiaalisen median kanavien kautta kansalaiset voivat pyytää apua kyberturvallisuusongelmiin ja tehdä niistä ilmoituksia kotoa käsin. Verkkosivuilla julkaistaan kyberturvallisuuteen liittyviä uutisia, varoituksia, vinkkejä ja tietoiskuja kansalaisille.[263]

Italian Safer Internet Center (SIC), Generazioni Connesse, on osa Euroopan komission tukemia Insafe-, INHOPE- ja Better Internet for Kids -verkostoja. Sen toimintaa koordinoi Italian opetusministeriö (Ministero dell'istruzione). Yhteistyössä on mukana muun muassa Italian poliisi ja yliopistoja. Generazioni Connesse antaa tukea ja tietoa lapsille, nuorille, vanhemmille, opettajille ja kasvattajille internetiin ja sen aiheuttamiin ongelmiin liittyvissä asioissa. Se on kehittänyt kouluille Kit Didattico -opetuspaketin, jonka tavoitteena on tarjota oppilaille digitaalisen osaamisen kansalaistaidot. Opetuspaketti pohjautuu Digital Competence Framework for Citizens -viitekehykseen (DigComp), johon kuuluu yhtenä osa-alueena turvallisuus. Generazioni Connessen verkkosivuilla ja sosiaalisen median kanavilla on uutisia ja tietoa kyberturvallisuudesta, kuten haittaohjelmista, kalastelusta ja yksityisyydensuojasta. SuperErrori-videoissa ja -oppaissa seikkailee verkon seitsemän supersankaria, joiden kommellusten kautta lapset ja nuoret oppivat, miten internetissä toimitaan turvallisesti.[264]

CINI-kyberturvallisuuslaboratorio (Consorzio Interuniversitario Nazionale per l'Informatica) ja Italian opetusministeriö käynnistivät vuonna 2014 Programma il Futuro -koulutushankkeen. Hankkeen tavoitteena on tarjota kouluille yksinkertaisia, tehokkaita ja helppokäyttöisiä välineitä, joiden avulla oppilaat voivat perehtyä digitaalisten teknologioiden tieteellisiin perusperiaatteisiin ja opetella digitaalisten teknologioiden vastuullista käyttöä. Opintoihin kuuluu myös kyberturvallisuutta. Hankkeen tärkeimmät kohderyhmät ovat koululaiset ja opettajat, mutta materiaalit soveltuvat myös muiden kansalaisten käyttöön. Niitä on hyödynnetty muun muassa aikuiskoulutuskeskuksissa ja senioreiden itseopiskelussa. Italialaisten peruskoulujen opettajat kutsutaan aina lukuvuoden alussa mukaan hankkeeseen. Osallistuminen on kouluille vapaaehtoista. Opettajien käyttöön tarkoitetut oppaat sisältävät tuntisuunnitelmia, opetussisältöjä ja harjoituksia. Kirjallisten materiaalien tueksi on luotu verkkosivusto. Jokaista oppituntia varten on tehty myös videomateriaaleja.[265,266]

Ludoteca del Registro.it on Registro.it:n (.it-verkkotunnusrekisterin ylläpitäjä) toteuttama hanke, jonka tavoitteena on opettaa lapsille ja nuorille internetin vastuullista käyttöä. Pääpaino on kyberturvallisuudessa. Tähän mennessä hanke on tavoittanut noin 500 koululuokkaa ja 14 000 oppilasta ympäri Italiaa. Ludoteca del Registro.it on suunnattu kaikenikäisille koululaisille. Myös koululaisten vanhemmille ja opettajille on tarjolla tietoa ja materiaaleja. Opetus järjestetään tyypillisesti työpajoissa, joiden pääteemana on kyberturvallisuus, mutta niissä käsitellään myös internetin teknistä infrastruktuuria. Opetusmenetelmät vaihtelevat kohderyhmän iän mukaan. Internetopoli-verkkosovellus on suunnattu alakouluikäisille, Nabbovaldo e il ricatto dal cyberspazio -videopeli (Nabbovaldo ja kiristys kyberavaruudesta) sekä siihen liittyvä opetuspolku yläkouluikäisille ja Cybersecurity4Teens 11–19-vuotiaille. Presente Digitale -portaali on tarkoitettu opettajille. Materiaalit ovat ilmaisia ja kaikkien käytettävissä.[267]

Emilia-Romagnan paikallishallinnon vuonna 2009 käynnistämä Pane e Internet (PEI, Leipä ja internet) on yksi esimerkki alueellisesta koulutushankkeesta. Opetus pohjautuu DigComp-viitekehykseen. Hankkeen tavoitteena on opettaa Emilia-Romagnan alueen kansalaisille digitaalisia taitoja perusteista syvempään osaamiseen. Pääkohderyhmänä ovat kansalaiset, jotka käyttävät muita vähemmän internetiä, kuten työttömät ja kotiäidit, sekä kansalaiset, jotka käyttävät internetiä, mutta joiden tietoturvallisuusosaaminen ja kriittinen medialukutaito eivät ole riittävällä tasolla, kuten nuoret. Kyberturvallisuuteen liittyviä aiheita ovat esimerkiksi laiteturvallisuus, virustorjunta, salasanat ja huijaukset. Viimeisen viiden vuoden aikana yli 30 000 kansalaista on saanut opetusta

hankkeen kautta. Opetus on ilmaista Emilia-Romagnan alueen kansalaisille. PEI järjestää myös erilaisia työpajoja, konferensseja ja tapahtumia, joissa edistetään digitaalisten teknologioiden turvallista käyttöä.[268,269]

Cybercity Chronicles on Dipartimento delle Informazioni per la Sicurezzan (DIS) ja opetusministeriön yhteistyössä kehittämä oppimispeli. Pelin tavoitteena on opettaa erityisesti nuorille, miten internetiä, sosiaalista mediaa ja uusia teknologioita käytetään vastuullisesti ja positiivisesti. Toimintaseikkailu sijoittuu vuoteen 2088 ja pitkälle kehittyneeseen kyberkaupunkiin, jossa digitaalisen vallankumouksen ihmeet ovat tuoneet mukanaan erilaisia riskejä. Peliin kuuluu Cyberbook-sanasto, jossa selitetään kyberturvallisuuden keskeisimmät termit.[270,271] Idea.labin ja Lombardian alueellisen koulutusryhmän toteuttama Digitalscape on digitaalisen turvallisuuden taitoja kehittävä peli. Se sopii kouluihin läsnä- ja etäopetukseen. Pelistä on tehty kaksi versiota: helpommassa on 15 osaa ja se on suunnattu 13–14-vuotiaille oppilaille, vaikeammassa on 21 osaa ja se on suunnattu 15–18-vuotiaille. Pelin ideana on virtuaalinen pakohuonepeli. Käsiteltäviä aiheita ovat muun muassa tietojenkalastelu, roskapostitus, digitaalinen identiteetti, turvalliset salasanakäytännöt, laitteiden turvallisuus, kyberkiusaaminen ja valeuutiset. Tällä hetkellä noin 900 opettajaa hyödyntää peliä opetuksessa.[272,273]

CyberHighSchools on CINIn koordinoima koulujen verkosto, joka edistää italialaisten nuorten kyberturvallisuusosaamista ja -yhteistyötä. Koulut voivat osallistua CyberChallenge.IT-koulutusohjelmaan ja OliCyber.IT-tietoturvaolympialaisiin. Osallistuminen on vapaaehtoista ja ilmaista.[274] CyberChallenge.IT on 16–24-vuotiaille nuorille suunnattu koulutusohjelma, jossa etsitään tulevia kyberturvallisuusammattilaisia. Vuonna 2022 tavoitteena on ollut saada koulutusohjelmaan vähintään 5 000 opiskelijaa. Koulutusohjelma hyödyntää perinteisiä opetusmenetelmiä ja pelillistämistä. ENISA järjestää vuosittain European Cyber Security Challenge -kilpailun, johon Italian edustusjoukkueen jäsenet valitaan karsintakierrosten kautta CyberChallenge.IT-koulutusohjelmasta.[275] CyberTrials on ilmainen peli- ja koulutusohjelma, joka on suunnattu italialaisille lukiolaistytöille. Se edistää tietoturvallisuuden ja verkkokansalaisuuden teemoja.[276] OliCyber.IT, CyberChallenge.IT ja CyberTrials muodostavat yhdessä Big Game at the Laboratory -hankkeen, jonka puitteissa yliopistojen asiantuntijat ja alan johtavat yritykset kouluttavat nuoria kyberturvallisuuden osaajiksi.[277]

Viranomaisten ja finanssialan toimijoiden yhdessä toteuttama kyberturvallisuuskampanja I Navigati - Informati e Sicuri (Kybertietoinen perhe – ajan tasalla ja turvassa) käynnistettiin vuonna 2021. Kampanja kannustaa digitaalisten kanavien ja välineiden turvallisempaan ja tietoisempaan käyttöön sekä levittää tietoisuutta rahoituspalveluihin kohdistuvien verkkohyökkäysten ja petosten riskeistä. Kaikille kansalaisille osoitetussa kampanjassa hyödynnetään televisiota, radiota, sosiaalista mediaa, sanomalehtiä ja kampanjan omaa verkkosivustoa. Kokonaisuuteen kuuluu kahdeksanosainen minisarja, haastatteluja ja tietoiskuja. Kampanjaa on uudistettu vuoden 2022 Euroopan kyberturvallisuuskuukautta varten.[278]

3.6.3. Kansalliset erityispiirteet

Samanlaiset kybermaailman haasteet koskettavat Italiaa kuin koko muuta Eurooppaa. Yleisesti ottaen kansalaisten kyberturvallisuusosaamista pitäisi parantaa. Sukupuolten ja sukupolvien välisiä eroja olisi kavennettava. Eritasoisia kyberturvallisuuskoulutuksia tarvitaan lisää: korkeakoulututkintoja on paljon, mutta lyhyempien kyberturvallisuuskurssien tarjontaa vähemmän.[279]

3.6.4. Kyberkansalaistaitojen määrittäminen

Kyberkansalaistaitojen määritelmää on pohdittu, mutta virallisia linjauksia ei ole toistaiseksi tehty.[280] Kyberkansalaistaitoja on määritelty muun muassa DigComp-viitekehyksen pohjalta. Agenzia per l'Italia Digitale on julkaissut DigComp 2.1 -version italian kielellä.[281] Yleisenä tavoitteena on, että kansalaiset ymmärtävät henkilötietojensa ja laitteidensa suojaamisen perusperiaatteet, ovat tietoisia eri turvallisuustoimista, osaavat huomioida luotettavuuden ja yksityisyyden vaatimukset GDPR:n mukaisesti ja huolehtivat fyysisestä ja henkisestä hyvinvoinnistaan.[282]

Viitteet

[252] ACN, *National Cybersecurity Strategy 2022-2026* (2022).
[253] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[254] ACN, *Implementation Plan, National Cybersecurity Strategy 2022-2026* (2022).
[255] ”Il manifesto per la Repubblica Digitale,” *Repubblica Digitale*, luettu 21.10.2022, https://repubblicadigitale.innovazione.gov.it/it/il-manifesto/.
[256] European Commission, *Digital Economy and Society Index (DESI) 2022: Italy* (2022), 7-8.
[257] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[258] European Commission, / EACEA / Eurydice, Informatics education at school in Europe, Eurydice report (Luxembourg: Publications Office of the European Union, 2022).
[259] ”CYBERHEAD - Cybersecurity Higher Education Database,” *ENISA*, luettu 21.10.2022, https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/.
[260] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[261] ”Cybersicurezza: nel Lazio una scuola per professionisti esperti,” *Regione Lazio*, luettu 14.11.2022, https://www.regione.lazio.it/notizie/cybersicurezza-nel-lazio-una-scuola-per-professionisti-esperti.
[262] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[263] ”Commissariato di P.S. online,” *Polizia Postale e delle Comunicazioni*, luettu 24.10.2022, https://www.commissariatodips.it/index.html.
[264] ”Generazioni Connesse,” luettu 24.10.2022, https://www.generazioniconnesse.it/site/it/home-page/.
[265] ”Programma il Futuro,” luettu 21.10.2022, https://programmailfuturo.it/.
[266] Henkilökohtainen tiedonanto tutkijalle, 24.5.2022.
[267] Giorgia Bassi, Stefania Fabbri ja Anna Vaccarelli, ”Ludoteca del Registro.it: Cybersecurity in Education,” *Ercim News,* nro 129, huhtikuu 2022, 39-40.
[268] ”PEI pane e internet,” luettu 21.9.2022, https://www.paneeinternet.it/public/pei-en.
[269] Henkilökohtainen tiedonanto tutkijalle, 8.7.2022.
[270] ”Cybercity: arriva il primo videogioco ambientato nel cyberspazio,” *Sistema di informazione per la sicurezza della Repubblica*, luettu 24.10.2022, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybercity-arriva-il-primo-videogioco-ambientato-nel-cyberspazio.html.
[271] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[272] Henkilökohtainen tiedonanto tutkijalle, 12.7.2022.
[273] ”Digitalscape,” luettu 14.11.2022, https://www.digitalscape.it/.
[274] ”Cyber High Schools,” *cini*, luettu 24.10.2022, https://cybersecnatlab.it/cyber-high-schools/?lang=en.
[275] ”CyberChallenge.IT,” *cini,* luettu 24.10.2022, https://cyberchallenge.it/.
[276] ”CYBER TRIALS,” *cini,* luettu 24.10.2022, https://www.cybertrials.it/.
[277] ”17 Oct Aperte le iscrizioni di OliCyber e CyberTrials: riparte il grande gioco degli hacker etici,” *cini*, luettu 26.10.2022, https://cybersecnatlab.it/aperte-iscrizioni-olicyber-cybertrials-riparte-il-grande-gioco-degli-hacker-etici/.
[278] ”I NAVIGATI, INFORMATI E SICURI,” *CERTFin*, luettu 24.10.2022, https://inavigati.certfin.it/.
[279] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[280] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[281] Stephanie Carretero, Riina Vuorikari ja Yves Puni, *DigComp 2.1 Il quadro di riferimento per le competenze digitali dei cittadini*, AGID Agenzia per l’Italia Digitale (2017).
[282] AGID Agenzia per l’Italia Digitale, *Competenze digitali per i cittadini: proposte operative*, 11.

3.7. Itävalta

ITU, Global Cybersecurity Index (GCI) 2020	29/182 (Global), 17/46 (Europe)
National Cyber Security Index (NCSI) 2022	32/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	10/27

3.7.1. Strategiset kyberkoulutuslinjaukset

Uusin Itävallan valtiollinen kyberstrategia (ÖSCS 2021) hyväksyttiin 2021, kun edellinen oli vuodelta 2013. Strategian korostetaan olevan osa EU:n yhteisiä ponnisteluja kyberturvallisuuden parantamiseksi. Lähtökohtana on, että koska kaikki elämänalueet digitalisoituvat vauhdilla, ovat valtavien mahdollisuuksien kääntöpuolena suuret uhat. Näitä uhkia vastaan on strategian mukaisesti toimittava järjestelmällisesti ja joustavasti. Strategisella tasolla kyberturvallisuus on liittovaltion säätelemää ja johtamaa toimintaa. Kyberstrategian laatimisesta vastasi liittokanslerin virasto ja sen toteuttamisesta liittovaltion sisäministeriö. Strategia jakautuu kahteen osaan, varsinaiseen strategiaan ja konkreettisempaan toimintasuunnitelmaan. Näin halutaan turvata mahdollisuus nopeaan reagointiin muuttuvissa tilanteissa. Tästä huolimatta maan liittovaltiorakenne tekee sen, että valtakunnalliset toimet myös kyberturvallisuuden suhteen kouluissa ovat väkisinkin vaihtelevia. Liittovaltioilla on autonomiaa koulutusstrategioidensa suhteen, mikä tekee kansallisten aloitteiden implementoinnin mahdottomaksi ja paikallisten aloitteiden seuraamisen vaikeaksi.[283,284]

Kyberturvallisuusuhat luokitellaan strategiassa neljään kategoriaan: tahallinen ja tahaton väärinkäyttö, riippuvaisuus tietojärjestelmistä ja teknologisen kehityksen myötä syntyvät uudet uhat. Kansalaisten kyberturvallisuustaidot eivät tässä luokittelussa ole esillä, vaan strategiassa hahmotetaan turvallisuus ennen kaikkea organisaatioiden kautta. Sama toistuu strategian tavoitteissa, joissa ainoa kansalaisiin edes etäisesti viittaava tavoite on, että kaikki toimijat kantaisivat vastuunsa kyberturvallisuudesta. Toisaalta sitten yksi tavoitteista on se, että itävaltalaisille voidaan tarjota mahdollisuus turvalliseen osallistumiseen sosiaaliseen ja poliittiseen elämään verkon kautta.[285]

Strategian kohderyhmiksi on määritelty yhteiskunta kokonaisuutena, yrityselämä, koulutussektori sekä tutkimus- ja kehitystoiminta. Kansalaisten kyberturvallisuustaidot kuuluvat ensimmäiseen kokonaisuuteen ja siellä aiheen ”tietoisuus” alle. Siinä yhteydessä strategia korostaa, että verkonkäyttäjien itsenäisesti vastuullinen toiminta parantaa Itävallan resilienssiä kyberturvallisuudessa. Koulutuksen teemassa korostetaan alati muuttuvan kentän edellyttävän elinikäistä oppimista digitalisaatioon liittyvissä asioissa. Strategian toteuttamisesta vastaavat kunkin alan ministeriöt omilla vastuualueillaan. Kerran puolessa vuodessa tehdään tarkastelu, jonka lisäksi määritellään uudet, konkreettiset välitavoitteet strategian toteuttamisessa. Työtä ohjaa Kyberturvallisuuden ohjausryhmän sihteeristö.[286]

Digitaalinen osaaminen ja medialukutaito ovat keskeisesti läsnä myös Itävallan nuorisostrategiassa.[287] Siinä korostetaan erityisesti kykyä suhtautua kriittisesti tarjottuun informaatioon. Liittokanslerinvirasto julkaisee vuosittain kyberturvallisuusraportin, jossa käydään mennyttä vuotta läpi paitsi hallinnonaloittain, myös kansainvälisesti.[288]

3.7.2. Kyberkansalaistaitojen opettamisen nykytila

Vuonna 2022 toiselle asteelle tuli pakolliseksi oppiaine nimeltä Digitale Grundbildung digitaalisuuden perusteet. Vaiheittain eri luokka-asteille tulevina vuosina laajenevan oppiaineen taustalla on käynnistetty myös opettajien täydennyskoulutus sekä uuden oppiaineen sisällyttäminen opettajien koulutukseen. Ylipäätään

kyberturvallisuus on lisätty kiinteäksi osaksi pedagogista opetusta Itävallassa. Peruskoulussa digitaalisten taitojen painopisteenä on mediakasvatus ja internetin reflektiivinen käyttö. Alemmilla luokilla olennaista on leikkisä lähestymistapa teknologiaan ja ongelmanratkaisuun. [289] Osaksi opetussuunnitelmaa liitetään "Ajattelua, oppimista ja ongelmanratkaisua" -nimen alle erilaisia hankkeita, jotka liittyvät alakoululaisten digitaalisten taitojen kehittämiseen. Yläkoulussa (5.–8. luokka) digitaalista perusopetusta on vähintään yksi tunti viikossa. [290] Oppiaineeseen on myös tuotettu jo oppimateriaaleja ja sisältöjä eri toimijoiden yhteistyönä. Valtion, Itävallan Punaisen Ristin ja koululaisten lukemista edistävän Buch Klubin yhteistyönä on julkaistu oppiaineeseen sopivaa materiaalia eri-ikäisille CyberSPACE- ja CyberSPOT-nimillä. [291]

Itävallan opetusministeriön koulujen digitalisaation pääsuunnitelmassa jaetaan kehitystoimet sisältöön, kalustoon ja opettajien osaamiseen liittyviin kokonaisuuksiin. Kyberturvallisuuden eri ulottuvuudet käytöstavoista ja kyberuhista ovat mukana sisällöissä, vaikka kysymys on enemmän rakenteiden, toimintatapojen ja sisältöjen kehittämisestä. [292]

Julkisten ja yksityisten kyberturvallisuustoimijoiden yhteistyöelimenä toimii Kyberturvallisuusyhdistys (CSP). Sen työryhmissä muun muassa muotoillaan suosituksia turvallisesta verkon käyttämisestä. Se on myös mukana julkaisemassa kyberturvallisuuden vuosiraporttia. Raportissa käydään läpi vuoden aikana esiin nousseita kyberturvallisuuteen vaikuttaneita ilmiöitä ja tapahtumia niin kotimaassa kuin muuallakin maailmassa. [293]

Wienin kyberturvallisuuden ja yksityisyyden tutkimusklusteri (Vienna Cybersecurity and Privacy Research Cluster, ViSP) tekee parhaillaan yhteistyötahojensa (the Learners programme, the Austrian Computer Society, Saferinternet.at ja Teach for Austria) kanssa suunnitelmaa siitä, kuinka verkossa turvallisesti toimimista opetetaan itävaltalaisille lapsille ja nuorille pelien avulla. Suunnitteluvaiheen jälkeen tavoitteena on luoda verkkopelejä ja haasteita.[294]

Vuonna 2013 perustettu Onlinesicherheit-sivusto tarjoaa runsaasti kyberturvallisuustietoa kansalaisten tarpeisiin: valistusvideoita, linkkejä turvallisuutta lisääviin ohjelmistoihin, ajankohtaisia varoituksia ja niin edelleen. Sivusto on valtiollisten toimijoiden vetämä, mutta siinä on mukana yli 40 yhteistyökumppania. Sivustolla on erilaisia kohderyhmiä eri-ikäisistä kansalaisista yrityksiin. Sivustolla on kansalaisille suunnattuja kyberturvallisuusuutisia, turvallisuusvaroituksia, julkaisuja ja linkkejä erilaisia suojausohjelmiin. Sivuston kautta voi myös osallistua webinaareihin, joiden aiheet käsittelevät kyberturvallisuuden eri osa-alueita. [295]

Saint Pöltenin teknillisen koulun ja Wienin yliopiston yhdessä rakentamassa PenQuest-pelissä kaksi pelaajaa on vastakkain, toinen hyökkääjänä ja toinen puolustajana. Pelin realistisuutta rakennetaan käyttämällä hyökkäyksessä MITRE ATT&CK- ja puolustuksessa MITRE D3FEND -tietokantaa sekä NIST SP 800-53 -turvallisuusstandardia. [296] Itävallan keskuskauppakamari järjestää vuosittain eDay-tapahtuman, jossa edistetään Itävallan yritysten digitalisointia. Kyberturvallisuus on vahvasti mukana tapahtumassa. [297]

Linziin on parhaillaan perusteilla Institute of Digital Sciences Austria (IDSA), jonka on tarkoitus toimia maan digitalisaation vauhdittajana. Vuoden 2023 jälkipuoliskolla toimintansa aloittavan monitieteisen yliopiston akateemisessa konseptissa kyberturvallisuus on sijoitettu kaikille yhteisiin perusopintoihin. Tavoitteena on 5 000 opiskelijaa vuosikymmenen vaihteessa ja noin 150 professoria 2030-luvun puolessavälissä. [298]

Korkeakouluopetusta kyberturvallisuudessa on Itävallassa saatavissa tämän lisäksi reilussa kymmenessä oppilaitoksessa. Osa koulutusohjelmista on englanninkielisiä. [299] Suurten kaupunkien yliopistot ovat kärjessä tässä joukossa tieteellisiin viittauksiin perustuvassa arvioinnissa.[300] Itävallan Tietokoneyhdistyksen lehden 4/22 teemana oli turvallisuus. Ammattilaisille suunnatun lehden sisällössä korostettiin sertifikaattien merkitystä turvallisuustason noston välineinä. [301]

Valtionhallinnon digitalisaatio edellyttää myös laaja-alaista virkakoneiston kouluttamista kyberturvallisuuskysymyksissä. Esimerkiksi sisäministeriö kouluttaa poliiseja ja muita alaisuudessaan toimivia noin 40 000:ta viranhaltijaa omassa e-Campus-oppimisympäristössään.[302] Poliisilla on oma kyberrikollisuuden osaamiskeskus, joka palvelee neuvoilla ja ohjeilla kansalaisia. Varsinaiset rikosilmoitukset on tehtävä tavalliselle poliisiasemalle.[303]

Eurooppalaisesta kyberturvallisuuskuukaudesta on Itävallassa vastuussa liittokanslerin virasto, joka koordinoi vuosittaista kampanjaa ENISAn tuottamien ohjeistusten ja materiaalien avulla. Virasto järjestää myös yhteistyössä Itävallan liittovaltion sisäministeriön sekä Itävallan liittovaltion puolustusministeriön kanssa Itävallan kyberturvallisuushaastetta (Austria Cybersecurity Challenge, ACSC), joka on kilpailu, jossa lahjakkaat nuoret sekä IT-alan ammattilaiset voivat esitellä taitojaan ja asiantuntemustaan. Kilpailu myös tuo näkyvyyttä kyberturvallisuuden teemoille. Kohderyhmänä ovat 14–25-vuotiaat nuoret.[304,305]

Österreichische Institut für angewandte Telekommunikation (ÖIAT) on hankkeiden kautta toimiva, digitalisaatiota edistävä yleishyödyllinen taho. Moni sen hankkeista on keskittynyt juuri kansalaisten kyberturvallisuuden eri ulottuvuuksiin.[306]

ÖIAT on muun muassa kehittänyt laatumerkinnän itävaltalaisille verkkokaupoille, valistanut verkkopetosten tunnistamisessa ajoissa ja kehittänyt kyberturvallisuussisältöjä vanhemmalle väestölle. ÖIAT:n luoma malzwei.at-sivusto on keskittynyt feikkiverkkokauppoihin ja muihin huijauksiin. Sen näkökulma kansalaisten kyberturvallisuuden edistämisessä on painottunut hyvin voimakkaasti juuri verkossa tapahtuvaan kaupankäyntiin liittyviin ongelmiin. ÖIAT antaa kuluttajalle parempia valmiuksia tunnistaa mahdollisia turvallisuusuhkia, ja sen toiminta luo edellytyksiä digitalisaation vaatimalle turvallisuudentunteen kasvulle.[307]

ÖIAT:n Fake Off -kampanja oli suunnattu nuorille, tavoitteenaan parantaa medialukutaitoa. Kampanjaan kuului paitsi sivusto ja kirjallista materiaalia, myös kännykkäsovellus. Sovelluksen avulla oli mahdollista harjoitella lähdekritiikkiä ja disinformaation tunnistamista.[308]

Samantyyppistä digitalisaatiota edistävää toiminta-ajatusta viljelee fit4internet-yhdistys, joka ilmoittaa tavoitteekseen itävaltalaisten digitaalisten taitojen edistämisen.[309] Yhdistyksen sivuilla voi testata oman tilanteensa eri osaamisalueilla, joista yksi on turvallisuus (safety).[310] Eri tasoisille käyttäjille on muotoiltu omat testinsä.

Saferinternet.at-sivustolla on eri kohderyhmille tietoa turvallisesta toiminnasta internetissä. Sisällöt on eritelty kohderyhmittäin, jotka ovat opettajat, vanhemmat, nuoret ja nuorten parissa työskentelevät. Sivustolta löytyy muun muassa kyberkiusaamiseen liittyvä tietovisailutyyppinen peli sekä sarjakuvia nuorille, valmennusta vanhemmille sekä verkostoitumis- ja keskustelumahdollisuuksia nuorten kanssa työskenteleville.[311]

3.7.3. Kansalliset erityispiirteet

Itävallan digitalisoitumisen strategioissa voi nähdä vahvan painotuksen valtiollisiin toimenpiteisiin (lainsäädäntö ja organisointi) sekä asiantuntijoiden merkitykseen. Kansalaisten tiedot ja taidot eivät ole juurikaan esillä, vaikka niiden merkitys resilienssin keskeisenä tekijänä tunnustetaankin. Esimerkiksi kyberturvallisuuden ammattilaisten kouluttamista pidetään tärkeämpänä kuin laajojen kansalaispiirien osaamisen tason kohottamista.

3.7.4. Kyberkansalaistaitojen määrittäminen

Itävaltalaisissa aineistoissa kyberkansalaistaitoihin viitataan järjestelmällisesti hyvin yleisellä tasolla. Kansalaisten kyky ja halu toimia virtuaalisessa maailmassa nähdään ennen kaikkea kilpailutekijänä maan taloudelle ja hallinnon tehokkuudelle.[312] Eri toimijoiden valistus- ja koulutusohjelmat toki ovat konkreettisempia, mutta niiden taustalla olevia ajatuksia vaadittavista kyberkansalaistaidoista ei suoranaisesti avata. Kouluopetuksessa taustalla on kuitenkin DigComp-kehys.[313]

Viitteet

[283] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022), 25.
[284] ÖSCS, *Austrian Strategy for Cybersecurity 2021* (2021).
[285] ÖSCS, *Austrian Strategy for Cybersecurity 2021* (2021).
[286] ÖSCS, *Austrian Strategy for Cybersecurity 2021* (2021).
[287] "Austrian Youth Strategy," *The Federal Ministry of Education, Science and Research*, luettu 25.11.2022, https://www.bmbwf.gv.at/en/Topics/youth_strategy.html.
[288] "Cybersecurity Report," *Federal Chancellery of Republic of Austria,* luettu 4.1.2023, https://www.bundeskanzleramt.gv.at/en/topics/cybersecurity/cybersecurity-report.html.
[289] "Digitale Grundbildung," *Bundesministerium*, Luettu 25.11.2022, https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/dgb.html.
[290] "Denken lernen, Probleme lösen - Digitale Grundbildung in der Primarstufe und der Sekundarstufe I," *Bundesministerium*, luettu 14.12.2022, https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/dgb/dlpl.html.
[291] "Mehr als nur Lesen," *Gemeinsam lesen*, luettu 14.12.2022, https://www.gemeinsamlesen.at/sekundarstufe.
[292] "8-Point Plan for Digital Learning," *The Federal Ministry of Education, Science and Research*, luettu 25.11.2022, https://www.bmbwf.gv.at/en/Topics/school/krp/8_p_p.html.
[293] "Nationale Cybersicherheitsstrukturen," *Bundeskanzleramt*, luettu 14.12.2022, https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/nationale-strukturen.html.
[294] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022).
[295] "Onlinesicherheit," luettu 14.12.2022, https://www.onlinesicherheit.gv.at/.
[296] "PenQuest," luettu 4.1.2023, https://www.pen.quest/.
[297] "E-Day," *WKO*, luettu 14.12.2022, https://www.wko.at/Content.Node/kampagnen/E-Day/index.html.
[298] "Institute of Digital Sciences Austria (IDSA)," *Austrian Federal Ministry of Education, Science and Research: Institute of Digital Sciences*, luettu 14.12.2022, https://www.bmbwf.gv.at/en/Topics/Higher-education---universities/Institute-of-Digital-Sciences-Austria-(IDSA)-%E2%80%93-A-new%2C-innovative-University-of-Technology-for-Digitalisation-and-Digital-Transformation-in-Austria.html.
[299] "Top – Security University´s / Applied Siences / Security Research in Austria," *Cyber Security Austria*, luettu 20.12.2022, https://verbotengut.at/center-of-excellence/top-security-studies-in-austria/.
[300] "7 Best universities for Cyber Security in Austria," *EduRank*, luettu 20.12.2022, https://edurank.org/cs/cybersecurity/at/.
[301] Die Österreichische Computer Gesellschaft (OCG), *OCG Journal* (4/22), https://www.ocg.at/sites/ocg.at/files/medien/pdfs/OJ2022-04.pdf.
[302] "eCampus," luettu 14.12.2022, https://e-campus.st/moodle/.
[303] "Delikte & Ermittlungen," *Bundesministerium*, luettu 14.12.2022, https://bundeskriminalamt.at/306/start.aspx.
[304] "Cybersecurity Activities and Iniatives," *Federal Chancellery Republic of Austria*, luettu 27.12.2022, https://www.bundeskanzleramt.gv.at/en/topics/cybersecurity/activities-and-initiatives.html.
[305] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022), 7-8.
[306] "Kompetenz für die digitale Welt," *ÖIAT*, luettu 14.12.2022, https://www.oiat.at/.
[307] "Malzwei," luettu 14.12.2022, https://www.malzwei.at/.
[308] "Fake Off," luettu 20.12.2022, https://www.fake-off.eu/fake-off/.
[309] "Fit4internet," luettu 14.12.2022, https://www.fit4internet.at/view/verein.
[310] "Safety," *Fit4internet*, luettu 14.12.2022, https://www.fit4internet.at/page/assessment/sicherheit.
[311] "Saferinternet.at", luettu 27.12.2022, https://www.saferinternet.at/.
[312] Republic of Austria, *Digitalisation Report #1: NOW FOR TOMORROW Digitalisation for growth and futureproofing* (2021).
[313] "Digi.komp," *Bundesministerium*, luettu 20.12.2022, https://digikomp.at/.

3.8. Kreikka

ITU, Global Cybersecurity Index (GCI) 2020	28/182 (Global), 16/46 (Europe)
National Cyber Security Index (NCSI) 2022	1/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	25/27

3.8.1. Strategiset kyberkoulutuslinjaukset

Kreikan digitaalisen hallinnon ministeriön (Υπουργείο Ψηφιακής Διακυβέρνησης) alaisuudessa toimiva kansallinen kyberturvallisuusviranomainen (NCSA) julkaisi vuonna 2020 kansallisen kyberturvallisuusstrategian vuosille 2020–2025. Visiona on nykyaikainen ja turvallinen tieto- ja verkkoinfrastruktuurien, sovellusten ja palvelujen digitaalinen ympäristö, joka edistää taloudellista ja sosiaalista hyvinvointia ja suojelee kansalaisten perusoikeuksia. Digitaalisten palvelujen ja sovellusten turvallisen käytön kulttuuria kehitetään ja kansalaisten luottamusta digitaalisiin teknologioihin vahvistetaan. Yhtenä strategisena päätavoitteena on valmiuksien kehittäminen, tiedon lisääminen ja tietoisuuden parantaminen. Siihen kuuluu kansalaisten kyberturvallisuustietoisuuden ja -osaamisen jatkuva ja järjestelmällinen kehittäminen. Keskeisenä toimenpiteenä on laatia koulutuksen ja tietoisuuden toimintasuunnitelma. Kyberturvallisuusstrategiassa suositellaan yhteistyössä kehitettävää kansallista kyberturvallisuuden tietoisuusohjelmaa, jossa huomioidaan kaikki ikä- ja yhteiskuntaryhmät ja käytetään ajantasaisia tietomateriaaleja. Tavoitteena on luoda kyberhygienian viitekehys ja kansallinen kyberturvallisuustietoisuuden kulttuuri.[314]

Vuonna 2021 julkaistiin Kreikan digitaalisen muutoksen strategia vuosille 2020–2025 ja sen toteuttamista tukeva digitaalisen muutoksen operatiivinen ohjelma vuosille 2021–2027. Strategiassa panostetaan vahvasti maan kansalaisiin. Kansalaisten digitaalisten taitojen parantaminen onkin yksi Kreikan digitaalisen muutoksen strategian kulmakivistä. Tähän liittyviä toimenpiteitä ovat esimerkiksi tietotekniikan viikkotuntien lisääminen peruskouluissa, digitaalisten taitojen kurssit korkeakouluissa, työntekijöiden digitaalisen osaamisen vahvistaminen ja kansalaisille suunnattu digitaalisten taitojen verkkokoulutusalusta. Strategiassa huomioidaan myös eri riskiryhmät, kuten toimintarajoitteiset ja seniorit, sekä ryhmät, joilla on tyypillisesti enemmän haasteita päästä työmarkkinoille, kuten naiset ja työttömät.[315,316]

3.8.2. Kyberkansalaistaitojen opettamisen nykytila

Kreikassa ei ole tällä hetkellä yhtä tahoa, jolla olisi kokonaisvastuu kansalaisten kyberturvallisuusosaamisesta, vaan vastuu jakautuu usealle virastolle ja ministeriölle. Yksi suurimmista haasteista onkin yhteistyön koordinointi. Ongelmia voi syntyä, jos roolit ja tehtävät menevät ristiin ja useammalla kuin yhdellä taholla on samankaltaisia koulutusohjelmia ja kampanjoita. Yhteistyö on välttämätöntä, jotta opettaminen olisi tehokasta. Kansalaisten osaamistasoon vaikuttaa merkittävästi myös kansalaisten omat resurssit ja kiinnostus kyberturvallisuutta kohtaan.[317]

Tietojenkäsittely on pakollinen ja erillinen oppiaine perusopetuksessa ensimmäiseltä luokalta alkaen ja toisen asteen opetuksessa. Kyberturvallisuuteen liittyvää opetusta annetaan peruskoulun kaikilla luokka-asteilla osana tietojenkäsittelyä. [318] Peruskoulussa annettava kyberturvallisuuskoulutuksen määrä ei ole asiantuntijoiden mukaan vielä riittävä. [319] Kyberturvallisuuden korkeakoulutusta on tarjolla useassa eri yliopistossa, kuten University of Aegeanissa, Athens University of Economics and Businessissä ja University of Piraeusissa.[320]

Kreikan Safer Internet Center of FORTH (SIC) perustettiin vuonna 2016 tutkimuskeskus Foundation for Research and Technology – Hellasin (FORTH) tuella. Se on osa Euroopan komission tukemia kansainvälisiä Insafe-, INHOPE-

ja Better Internet for Kids -verkostoja. SIC on vastannut vuodesta 2016 lähtien suuresta osasta koulujen kyberturvallisuuden opetusmateriaaleista ja tietoisuuskampanjoista. Tärkeimmät kohderyhmät ovat lapset, nuoret, vanhemmat ja opettajat, mutta materiaaleja on myös yleisesti kaikille kansalaisille. SIC tuottaa esimerkiksi erilaisia tietoiskuja, opetusvideoita, tuntisuunnitelmia, webinaareja, MOOC-kursseja, artikkeleita ja tutkimuksia. SICin verkkosivuilla ja sosiaalisen median kanavilla on runsaasti kyberturvallisuuteen liittyvää tietoa. SIC on järjestänyt yli 800 vierailua kreikkalaisissa kouluissa, seitsemän kansallista Safer Internet Day -tapahtumaa ja seitsemän kansallista, koulujenvälistä verkkoturvallisuuden kilpailua, ja sillä on 200 lähettilästä ympäri maata. SICin tärkeimpiä yhteistyökumppaneita ovat Kreikan opetus- ja uskontoasiainministeriö (Υπουργείο Παιδείας και Θρησκευμάτων), Kreikan digitaalisen hallinnon ministeriö ja sen alla toimiva Kreikan kansallinen kyberturvallisuusviranomainen, ENISA ja Kreikan poliisi.[321,322]

Kreikan Safer Internet Center of FORTH ja Kreikan kyberturvallisuusviranomainen ovat toteuttaneet yhdessä kyberturvallisuuskampanjoita ja niihin liittyviä opetusvideoita. ”Smishing”-videolla kerrotaan, miten erityisesti tekstiviestien välityksellä tapahtuvan tietojenkalastelun tunnistaa ja miten siltä suojaudutaan. ”Do you know what a strong password is?” -videolla puhutaan hyvästä salasanahygieniasta. ”Don’t click – don’t click” -videolla kuvataan tilanne, jossa iäkkään henkilön käyttäjätili on hakkeroitu. Katsojalle neuvotaan, miten tilanteessa tulisi toimia, mihin tapahtuneesta voi ilmoittaa ja miksi on hyödyllistä jakaa kokemus perheen ja ystävien kanssa. Nämä esimerkkivideot on suunnattu kaikille kansalaisille. [323] SIC toimii ENISAn vuotuisten kyberturvallisuuskuukausien Kreikan maakoordinaattorina. Vuoden 2022 kyberturvallisuuskuukauden yhteydessä ENISA valitsi vuoden parhaaksi oppiaineistoksi Kreikan SICin tuottaman ”Aarteenetsintäpelit alakoululaisille” -opetusmateriaalin. Voiton myötä materiaali käännetään kaikille EU:n virallisille kielille.[324]

Kreikan digitaalisen hallinnon ministeriön alainen Kreikan tutkimus- ja teknologiaverkosto GRNET S.A. koordinoi ja jalkauttaa ministeriön suunnitteleman digitaalisen muutoksen strategian. GRNET S.A:han on perustettu tätä tehtävää varten erityinen digitaalisten taitojen osasto, Directorate of Digital Skills. Sen vastuulla on myös ministeriön kehittämän National Academy for Digital Skills -alustan toteutus ja ylläpito. Alusta on suunnattu Kreikan kansalaisille ja sen tarkoituksena on parantaa kansalaisten digitaalisia taitoja erilaisten kurssien avulla. National Academy for Digital Skills on ilmainen alusta, joka kokoaa yhteen kaikki digitaalisen koulutuksen yksityiset ja julkiset palveluntarjoajat. Hanke käynnistettiin vuoden 2020 alussa.[325,326]

National Academy for Digital Skillsin kurssivalikoimaan kuuluu tällä hetkellä noin 300 kurssia, joista erityisesti 20 kurssia liittyy kyberturvallisuuteen. Kansalaiset voivat valita itselle sopivan opintopolun itsearviointiin tarkoitetun työkalun avulla. GRNET S.A. tarjoaa lisäksi itse kehittämäänsä viiden kurssin Digitaalinen kansalainen -opintopolkua, joka perustuu Euroopan komission Digital Competence Framework for Citizens -viitekehykseen (DigComp). Kokonaisuus on tarkoitettu erityisesti kansalaisille, joiden digitaalinen osaaminen on vielä hyvin perustasoa. Tavoitteena on vahvistaa kansalaisten digitaalista ajattelutapaa ja kehittää heidän taitojaan ja asenteitaan, jotta jokainen voisi toimia digitaalisessa ympäristössä tuottavalla, turvallisella ja vastuullisella tavalla. Kursseilla käsitellään myös kyberturvallisuutta, kuten turvallista verkkoselausta, hyviä salasanakäytäntöjä ja yksityisyyden suojaamista.[327]

Kreikan poliisin elektronisten rikosten yksikön (Cyber Crime Division: Unit of Innovative Actions and Strategy) vastuulla on lisätä tietoisuutta verkkorikollisuuden eri muodoista ja verkkoturvallisuudesta.[328] Kohderyhminä ovat kansalaiset, yritykset, julkisen sektorin laitokset ja korkeakoulut. Osasto toteuttaa tehtäväänsä monin eri tavoin. Lukuvuonna 2021 ja 2022 järjestettiin 330 luentoa ja työpajaa eri kohderyhmille. Osasto julkaisee kyberrikoksista ja internetin vaaroista kertovia lehtisiä, videoita ja muita materiaaleja. Lasten verkkoturvallisuutta käsitteleviä tietoiskuja esitetään valtakunnallisilla televisio- ja radiokanavilla. Tunnettu näyttelijä ja kirjailija Carmen Rouggeri loi yhteistyössä osaston kanssa alle kymmenenvuotiaille suunnatun Sifis the Mouse and the Internet -sadun internetin vaaroista. CyberKid on yksikön lanseeraama verkkoturvallisuuden kampanja, jota päivitetään jatkuvasti. Se on suunnattu erityisesti lapsille, nuorille, vanhemmille ja opettajille. Kampanjan verkkosivustoa on käytetty kouluissa IT-opetuksen tukena. Panhellenic School Network on nostanut CyberKidin näkyvyyttä. CyberKid sisältää muun muassa kyberturvallisuustietoa ja minipelejä.[329,330] CyberAlert-

ja FeelSafe-sivustot on suunnattu kansalaisille ja yrityksille. Sivustoilla on ajankohtaista tietoa verkkorikollisuudesta ja internetin riskeistä. FeelSafe keskittyy elektronisen kaupankäynnin turvallisuuteen. Sivustot on tehty yhteistyössä poliisin, kansalaistensuojeluministeriön ja ESEE-kauppajärjestön kanssa.[331]

Manolis Sfakianakisin vuonna 2017 perustama Cyber Security International Institute (CSIi) on kreikkalainen voittoa tavoittelematon kansalaisjärjestö, joka on syntynyt halusta suojella kansalaisten turvallisuutta. CSIi tekee yhteistyötä muun muassa Kreikan kansalaistensuojeluministeriön (Υπουργείο Προστασίας του Πολίτη) kanssa. Järjestön tavoitteena on tarjota kansalaisille tietoa ja koulutusta uusista teknologioista ja internetistä, IT-järjestelmien ja -infrastruktuurien turvallisuudesta sekä internetin ja ohjelmistojen turvallisesta käytöstä. Se kannustaa kansalaisia ilmoittamaan havaitsemistaan verkkoturvallisuuden ongelmista ja tarjoaa kansalaisille käyttäjätukea. CSIi valmistelee koulutusohjelmia ja järjestää työpajoja, seminaareja ja konferensseja ympäri Kreikkaa ja on usein esillä mediassa. Kohderyhminä ovat erityisesti lapset, vanhemmat ja isovanhemmat. Oppilaille ja vanhemmille järjestetään ilmaisia "Digital Academy" -verkkokursseja, joihin on tähän mennessä osallistunut 7 000 oppilasta ja 10 000 vanhempaa. CSIi:n työryhmä, johon kuuluu eri alojen asiantuntijoita, tekee opetusmateriaalit itse. CSIi kehittää parhaillaan uudenlaista vuorovaikutteista opetusohjelmaa nimeltä "Super Internet". Ohjelman tavoitteena on opettaa 6–16-vuotiaille lapsille ja nuorille internetin käyttöä ja kertoa sen vaaroista ohjelman supersankareiden Lady Banin ja Mega Blockin johdolla. CSIi ja matkapuhelinoperaattori COSMOTE ovat tehneet yhdessä 20 videon #HowToVideos-kampanjan. Lyhyillä videoilla on helppoja vinkkejä siihen, miten internetin käyttäjät voivat suojautua verkkopetoksilta ja turvata henkilötietonsa.[332,333]

Kreikan kansallinen kyberturvallisuusviranomainen julkaisi kesäkuussa 2021 erityisesti julkiselle sektorille sekä pienille ja keskisuurille yrityksille suunnatun kyberturvallisuuden käsikirjan, jossa on verkon ja tietojärjestelmien suojaamisen ja häiriönsietokyvyn parhaita käytäntöjä. Käsikirjassa käsitellään myös työntekijöiden kyberturvallisuustaitojen ja -tietoisuuden parantamista.[334]

3.8.3. Kansalliset erityispiirteet

Kreikan Safer Internet Center (SIC) ja tutkimuskeskus FORTH toteuttivat vuosina 2018 ja 2019 laajan kyselytutkimuksen ”Understanding the online behavior and risks of children: results of a large-scale national survey on 10–18 year olds”. Tutkimuksen tavoitteena oli tarkastella lasten ja nuorten internetin käyttöä ja siihen liittyviä riskejä. Tutkimuksen ensimmäiseen osaan osallistui 14 000 oppilasta 400 koulusta ja toiseen osaan 13 000 oppilasta 500 koulusta. Tutkimukset toteutettiin anonyymeinä verkkokyselyinä opetus- ja uskontoasiainministeriön tuella. Tutkimustulosten perusteella lasten, nuorten ja vanhempien internetin turvallisen käytön osaamista tulisi parantaa. Lapset ja nuoret kertovat saavansa neuvoja lähinnä omilta vanhemmiltaan ja sisaruksiltaan. Tutkimuksessa suositellaan, että internetin turvallisuutta käsittelevät kurssit otettaisiin laajemmin ja systemaattisemmin osaksi peruskoulujen opetussuunnitelmaa ja ulotettaisiin myös pienempiin lapsiin. Tutkimuksen mukaan digitaalista lukutaitoa ja kyberturvallisuutta opetetaan tällä hetkellä jonkin verran osana peruskoulujen opetussuunnitelmaa, mutta määrä ei ole riittävä.[335]

Kreikka isännöi Euroopan unionin kyberturvallisuusvirasto ENISAa. Toimipisteet ovat Ateenassa ja Iraklionissa.[336] Kreikan kansallista kyberturvallisuusstrategiaa pidetään yhtenä kattavimmista koko EU:ssa. Kreikka on ollut ensimmäisellä sijalla NCSI-kyberturvallisuusindeksissä lokakuusta 2019 alkaen.[337]

3.8.4. Kyberkansalaistaitojen määrittäminen

National Academy for Digital Skillsin viiden kurssin Digitaalinen kansalainen -opintokokonaisuus perustuu DigComp-viitekehykseen, jonka yksi osa-alueista on turvallisuus. Kurssien aiheet ovat navigointi ja tiedonhaku verkossa, digitaalisen sisällön hallinta, tietosuoja ja yksityisyys, digitaalisen identiteetin luominen ja digitaalisena kansalaisena toimiminen. Kursseilla käsitellään muun muassa salasanoja, verkkohuijauksia, kalastelua, sosiaalisen median yksityisyys- ja tietoturva-asetuksia, valeprofiileja ja tietomurtoja.[338]

Viitteet

[314] National Cybersecurity Authority, Ministry of Digital Governance, Hellenic Republic, *National Cybersecurity Strategy 2020-2025* (2020).
[315] Digitaalisen hallinnon ministeriö, *Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025* (2021).
[316] European Commission, *Digital Economy and Society Index (DESI) 2022: Greece* (2022), 3-6.
[317] Henkilökohtainen tiedonanto tutkijalle, 1.8.2022 ja 26.11.2022.
[318] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 10-58.
[319] Henkilökohtainen tiedonanto tutkijalle, 22.6.2022, 1.8.2022 ja 9.8.2022.
[320] ”CYBERHEAD - Cybersecurity Higher Education Database,” *ENISA*, luettu 4.11.2022, https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/.
[321] Henkilökohtainen tiedonanto tutkijalle, 22.6.2022.
[322] ”SaferInternet4Kids.gr,” luettu 8.11.2022, https://www.saferinternet4kids.gr/.
[323] ”Greece, Cybersecurity Sources,” *European Cybersecurity Month*, luettu 8.11.2022, https://cybersecuritymonth.eu/countries/greece.
[324] “The European Cybersecurity Month 2022 Awards,” *ECSM*, luettu 8.11.2022, https://cybersecuritymonth.eu/awards.
[325] Henkilökohtainen tiedonanto tutkijalle, 23.6.2022.
[326] ”Media Kit,” *Grnet*, luettu 4.11.2022, https://grnet.gr/en/media-kit-2/.
[327] Henkilökohtainen tiedonanto tutkijalle, 23.6.2022.
[328] ”Cyber Crime Division,” *Hellenic Republic, Ministry of Citizen Protection*, luettu 30.8.2022, http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=EN.
[329] “Hellenic Republic, Ministry of Citizen Protection,” luettu 22.11.2022, http://www.astynomia.gr/index.php?option=ozo_content&lang=&perform=view&id=103304%20&Itemid=2646&lang=.
[330] Henkilökohtainen tiedonanto tutkijalle, 26.11.2022.
[331] ”Cyber Alert,” *Cyber Crime Division*, luettu 26.9.2022, https://cyberalert.gr/.
[332] Henkilökohtainen tiedonanto tutkijalle, 1.8.2022 ja 9.8.2022.
[333] ”CSIi Cyber Security International Institute,” luettu 8.11.2022, https://www.csii.gr/.
[334] Ministry of Digital Governance, National Cybersecurity Authority, *Cybersecurity Handbook* (2021), 6-52.
[335] Evangelia Daskalaki, Katerina Psaroudaki, Marieva Karkanaki & Paraskevi Fragopoulou, *Understanding the online behavior and risks of children: results of a large-scale national survey on 10-18 year olds*, Iraklion: Institute of Computer Science, Foundation for Research and Technology - Hellas (FORTH) (2020).
[336]”Contact,” *ENISA*, luettu 21.11.2022, https://www.enisa.europa.eu/about-enisa/contact.
[337] George Drivas, *CYBERSECURITY IN GREECE: Facts, Current Needs & Future Perspectives*, luettu 21.11.2022, https://www.sev.org.gr/Uploads/Documents/53423/Cybersecurity_in_Greece_Drivas_SEV.pdf.
[338] ”Ψηφιακός Πολίτης,” *govgr*, luettu 18.11.2022, https://nadia.gov.gr/.

3.9. Kroatia

ITU, Global Cybersecurity Index (GCI) 2020	33/182 (Global), 20/46 (Europe)
National Cyber Security Index (NCSI) 2022	16/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	21/27

3.9.1. Strategiset kyberkoulutuslinjaukset

Kroatian kyberturvastrategia on vuodelta 2015. Strategiassa linjataan tavoitteeksi kaikkien "kyberavaruuden" käyttäjien tietoturvatietoisuuden lisääminen. Erityisesti kaikkien kouluasteiden oppilaiden ja opiskelijoiden tulee saada tietoa digimaailman uhista ja osata toimia tietojensa turvaamiseksi sekä käyttää teknologiaa turvallisesti. Kouluissa kyberturvallisuuden opiskelu integroidaan muihin aineisiin. Koulutusta lisätään sekä koulun säännölliseen että koulun ulkopuoliseen toimintaan. Elinikäinen oppiminen huomioidaan siten, että kyberturvallisuuden opetusta tarjotaan eri väestöryhmille. Tavoitteena on myös lisätä tiedotusta suurelle yleisölle erilaisten kampanjoiden avulla.[339]

3.9.2. Kyberkansalaistaitojen opettamisen nykytila

Kyberturvallisuuden opetukseen osallistuvat Kroatiassa opetusministeriö (Ministarstvo znanosti i obrazovanja), joka hallinnoi opetusta kouluissa, Kansallinen CERT (Nacionalni CERT) sekä yksityisen sektorin toimijat.[340] Kroatian yleissivistävässä koulutuksessa, eli 7–14-vuotiaiden alakoulun oppilaiden ja 15–18-vuotiaiden lukion oppilaiden opetuksessa, otettiin vuonna 2018 käyttöön uusi opetussuunnitelma oppiaineelle ”Informatics” (computer science). Oppiaineen osa-alue E-society kattaa myös kyberturvallisuuden.[341] ”Informatics”-aineen opiskelu aloitetaan valinnaisena aineena seitsemänvuotiaana, ja opiskelu jatkuu neljännen luokan loppuun saakka. Peruskoulun ylemmillä luokilla (lower secondary school) ja lukiossa se on pakollinen aine.[342, 343] ”Informatics”-aineen opetussuunnitelman mukaan peruskoulun ja lukion jälkeen oppilaiden tulisi hallita tietokoneen käyttöä niin, että he voivat itsenäisesti, vastuullisesti, asianmukaisesti ja tehokkaasti hyödyntää digitaalitekniikkaa ja valmistautua toimimaan kaikilla elämänaloilla digitaalisessa ympäristössä. Heidän tulisi myös kehittää kriittistä ajattelua, luovuutta ja innovaatioita tieto- ja viestintätekniikan avulla ja kommunikoida ja tehdä yhteistyötä tehokkaasti ja vastuullisesti digitaalisessa ympäristössä. Tavoitteena on myös, että opiskelija ymmärtää ja soveltaa vastuullisesti turvallisuussuosituksia terveytensä suojelemiseksi ja noudattaa lakeja ja normeja käyttäessään digitaalitekniikkaa jokapäiväisessä elämässä.[344,345]

E-society-opinnot perustuvat ajatukseen, että verkkoturvallisuuden, tietosuojan ja verkkokiusaamisen kaltaisten aiheiden opiskelu kehittää taitoja ja asenteita, joita vastuullinen toimiminen digitaalisessa yhteiskunnassa edellyttää.[346] Alakoulun ensimmäisillä luokilla oppilas oppii käyttämään tieto- ja viestintälaitteita huolellisesti ja vastuullisesti ja suojaamaan henkilötietojaan. Hän analysoi riskejä, joita voi esiintyä tietokonetta ja internetiä käytettäessä ja reagoi niihin asianmukaisesti. Käyttäessään internetin sisältöä ja palveluja hän suojelee henkilötietojaan ja digitaalista mainettaan. Isommat koululaiset perehtyvät digitaaliseen jalanjälkeen ja verkkokiusaamiseen liittyviin kysymyksiin, sähköisen identiteetin ja käyttäjätilien turvaamiseen sekä vihapuheen ehkäisyyn. Lukion ensimmäisellä luokalla opiskellaan haittaohjelmien, verkkohyökkäysten ja identiteettivarkauksien seurauksia ja turvallisuussääntöjä.[347]

Korkea-asteella ei Kroatiassa ole varsinaista kyberturvallisuuden maisterikoulutusta, mutta Zagrebin yliopiston sähkötekniikan ja tietojenkäsittelyn tiedekunnassa (Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva) voi osallistua tietoturvan jatko-opintoihin Postgraduate specialist study Information security.[348] Samassa

tiedekunnassa pidetään yksittäisiä Computer security -kursseja opiskelijoille.[349] Myös Zagrebin yliopiston organisaatio- ja informaatiotieteen tiedekunta (Fakultet organizacije *i* informatike Sveučilišta u Zagrebu) järjestää jatko-opintoja nimeltään Safety Management and Information Systems Audit.[350] Zagrebin ammattikorkeakoulu (Tehničko veleučilište u Zagrebu) toteuttaa ”Specialist graduate professional study program Information Security on digital forensics -opiskeluohjelmia.[351] Algebra-yliopiston Kyberturvallisuuden laitos (Visoko učilište Algebra, Katedra za kibernetičku sigurnost) järjestää kyberturvallisuuden kursseja, joissa käsitellään laajasti kyberturvallisuuden eri osa-alueita.[352]

CERT tarjoaa kansalaisille kyberturvallisuuskoulutusta, johon myös aikuiset voivat osallistua. Se järjestää esimerkiksi verkkoseminaareja, konferensseja ja koulutuksia eri aiheista ja opettaa paitsi tunnistamaan kyberuhkia, myös reagoimaan niihin. Kansalaisia pyritään kouluttamaan esimerkiksi sosiaalisen median viesteillä, verkkosisällöillä, radio- ja televisio-ohjelmissa ja sanomalehtiartikkeleilla. Ajankohtaisista uhista varoitetaan myös infografiikalla ja tietokilpailuilla.[353]

CERTin ylläpitämässä portaalissa[354] on kansalaisille monipuolisesti kyberturvallisuuteen liittyvää informaatiota ja interaktiivista sisältöä, kuten pelejä, tietokilpailuja ja testejä. Materiaalia on kymmeneltä erilaiselta aihealueelta digitaalisesta jalanjäljestä tietojenkalasteluun.[355]

Ensimmäisen kansallisen kyberturvallisuuskampanjan ”Naivci” CERT järjesti vuonna 2019.[356] TV:ssä esitetyn kampanjan tavoitteena oli valistaa kansalaisia yleisimmistä verkkopetoksista ja kyberturvallisuusuhista, ja se perustui liian itsevarmaan ja naiiviin käyttäjään, joka ei välitä liikaa verkkoturvallisuudesta. Kampanjan jatko-osassa vuonna 2021 hyödynnettiin muun muassa TV:tä, Facebookia, Twitteriä ja YouTubea.[357]

Kroatia on osallistunut ENISAn (European Union Agency for Cybersecurity) organisoimiin ECSM (European cybersecurity month) -kampanjoihin esimerkiksi julkaisemalla sosiaalisessa mediassa postauksia, jotka liittyvät digitaaliseen jalanjälkeen ja huijauksiin, sekä järjestämällä Hacknite-kilpailuja koululaisille.[358] Vuonna 2021 pidettiin asiantuntijoiden paneelikeskustelu, jonka aiheina olivat social engineering, kyberhygienia ja turvallisuustietoisuuden lisääminen.[359] Kroatian Cybersecurity Month -kampanjan portaalissa[360] on kansalaisille saatavilla muun muassa tiedotusmateriaalia, videoita ja infograafeja.

Kampanjoiden lisäksi Kroatia yhdistää tiedottamista tiettyjen päivien yhteyteen. Kroatian Safer Internet Centre (SIC) osallistuu Safer Internet Day (SID) -päivään valmistelemalla muun muassa koulutuspaketteja kouluille ja organisaatioille, laatimalla lapsille ja nuorille verkkomateriaalia ja järjestämällä asiantuntijawebinaareja ja podcasteja vanhemmille.[361,362]

Ukrainan sodan alettua vuonna 2022 the Central State Office for the Development of the Digital Society on tehostanut yleistä tiedotustoimintaansa kansalaisille kyberturvallisuustyöpajoissa, joissa käsitellään kaikkia keskeisiä aiheita, myös disinformaatiota.[363] Yksityisellä sektorilla *Learning web skills -yritys*[364] järjestää esimerkiksi *"Information and data literacy"*- ja *"Safety"-kursseja.* Koulutukset on suunnattu lähinnä yrityksille sekä henkilöille, jotka haluavat vaihtaa ammattia IT-alalle.

Digitaalisista opetussisällöistä laajimpia on Netica.hr.[365] Se on Kroatian Safer Internet Centren tuottama värikäs lapsille ja aikuisille suunnattu sivusto, jossa on hyödyllisiä materiaaleja verkkoturvallisuudesta. Sivustolla voi myös esittää asiantuntijoille kysymyksiä. ”Safe with Netica” -kuvakirja ja työkirja sisältävät käytännön tilanteita ja neuvoja verkkoturvallisuuteen. Niiden sisältö on erityisesti tehty esikoululaisille ja alakouluikäisille.[366,367] Pienille lapsille on tarkoitettu myös interaktiivinen kirja ”Think and click”.[368] Sen on tuottanut Roda-yhdistys osana väestö-, perhe-, nuoriso- ja sosiaaliministeriön (Ministarstvo demografije, obitelji, mladih i socijalne politike) projektia. Safer Internet Centren YouTube-kanavalle on koottu videoita, joissa kuvataan verkkoturvallisuuden perusongelmia. Videot tarjoavat lapsille ja nuorille esimerkkejä seurauksista, joita heidän toimillaan voi olla.[369] Safer Internet Centre on tuottanut myös lautapelin sekä lasten ja vanhempien koulutusoppaan sosiaalisten verkostojen turvallisuus- ja yksityisyysasetuksista.[370]

*Kroatian akateeminen tutkimusverkosto (*Hrvatska akademska i istraživačka mreža) *CARNET* on tuottanut monipuolisen, interaktiivisia oppimisresursseja sisältävän portaalin kyberturvallisuudesta, ja se on kaikkien saatavilla internetissä. Kohderyhmänä ovat erityisesti peruskoululaiset ja lukiolaiset. Aiheita ovat muun muassa yksityisyyden ja tietokoneen suojaaminen ja tietokoneen turvallinen käyttö.[371,372,373]

Yksi kroatialaisista oppimispeleistä on *Learning associates* -yhdistyksen laatima *"Dabrica Darka - Growing up on a Safer Internet"*[374], joka sisältää neljä verkkopeliä verkkoturvallisuudesta peruskoulun 1.–8. luokan oppilaille. Lisäksi oppilaiden opettajille ja vanhemmille on tehty neljä käsikirjaa, joissa on muun muassa tietoa siitä, kuinka parantaa vanhempien tietämystä internetin mahdollisuuksista ja keinoista turvata lasten turvallinen internetin käyttö. *No to E-violence* on Safer Internet Centren ja Microsoftin pienille lapsille suunnittelema tietokilpailusovellus[375], jonka avulla voi oppia perustiedot verkkoturvallisuudesta hauskalla tavalla.

3.9.3. Kansalliset erityispiirteet

Kroatialla on vahvat perinteet IT-asiantuntijoista ja IT-alan yrityksistä[376], ja maassa on teknologiaosaamista varsinkin nuorten ja nuorten aikuisten keskuudessa[377]. Kansalaistaidot ja digi- ja kyberosaaminen ovat osa peruskoulujen opetusohjelmaa.[378] Suuri osa väestöstä on ikääntynyttä, ja heidän kohdallaan voidaan havaita haasteita tieto- ja viestintätekniikan tuntemuksessa. Iäkkäät ovat alttiita yksinkertaisille petoksille. Nuoremmilla sukupolvilla on verrattain lyhyt aika soveltaa nopeasti kehittyvää tekniikkaa erilaisiin reaalimaailman tarpeisiin. Kroatiassa tunnistetaan tarve lisätä tietoisuutta erityisesti tietosuojasta ja siitä, että pitää olla varovainen jaettaessa henkilötietoja verkkoympäristössä.[379] Kyberturvallisuus nähdään Euroopalle yhteisenä asiana, joten olisi hyvä yhdistää voimat sen edistämiseksi. Kyberturvallisuuteen liittyvän opetusmateriaalin tulisi olla ajankohtaista ja sisältää tämänhetkiset uhat ja mahdollisuudet. Toteutuksen pitäisi ottaa huomioon opiskelijan ikä, ja siinä olisi hyvä olla yhdistettynä sekä teoriaa ja käytäntöä. Jos toteutus olisi niin sanotusti HyFlex, sitä voitaisiin käyttää eri opetusympäristöissä.[380]

Tutkimuksen tekohetkellä Kroatiassa on työn alla strategia nimeltään *Digital Croatia 2032,* joka sisältää myös kyberturvallisuusasiaa ja kansalaistaitojen kehittämistä, niin yksilöiden kuin yritystenkin näkökulmasta.[381]

3.9.4. Kyberkansalaistaitojen määrittäminen

Kroatialla ei ole kansallisia kehyksiä kyberturvallisuustaidoille, ja maassa noudatetaan joko EU:n tai kansainvälisiä kehyksiä ja sertifikaatteja, kuten EU:n Digital comptences framework for citizens (*DigComp* 2.2) ja SELFIE for TEACHERS, joka on Euroopan komission hallinnoima peruskoulun ja lukion opettajille tarkoitettu ilmainen itsearviointityökalu. Sen avulla opettajien on mahdollista arvioida muun muassa omia kyberturvallisuuteen liittyviä taitoja.[382,383] Opetussuunnitelmasta on löydettävissä joitakin kyberturvallisuuteen liittyviä taitojen määritelmiä. Siinä mainitaan, että jokaisen sähköisiä palveluita käyttävän kansalaisen (e-Citizen) tulisi ymmärtää, mitä tarkoitetaan henkilötiedoilla ja miten niitä suojellaan. Heidän tulisi myös osata suojautua petoksilta, uhilta ja nettikiusaamiselta ja tietää, miten reagoida epäasialliseen käytökseen, miten kunnioittaa muiden ihmisten yksityisyyttä tai mistä etsiä apua, jos törmää sopimattomaan sisältöön tai henkilöihin.[384,385]

Viitteet

[339] Government of Croatia, *The National Cyber Security Strategy of Republic of Croatia* (2015), 7, 24–25.
[340] Henkilökohtainen tiedonanto tutkijalle, 27.9.2022.
[341] Henkilökohtainen tiedonanto tutkijalle, 14.9.2022.
[342] Henkilökohtainen tiedonanto tutkijalle, 27.9.2022.
[343] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 119.
[344] Lidija Kralj, *New Informatics curriculum—Croatian tradition with world trends*. *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, IEEE (2016), 1.
[345] Ministry of Science and education of Croatia. *Curriculum of the Teaching Object Informatica for Primary Schools and Gymnasiums* (2018).
[346] Henkilökohtainen tiedonanto tutkijalle 14.9.2022.
[347] Ministry of Science and education of Croatia, *Curriculum of the Teaching Object Informatica for Primary Schools and Gymnasiums*, (2018).
[348] "Information security," *University of Zagreb*, luettu 9.12.2022, https://www.fer.unizg.hr/studiji/specijalisticki_studiji/is.
[349] "Computer security," *University of Zagreb Faculty of Electrical Engineering and Computing*, luettu 9.12.2022, https://www.fer.unizg.hr/predmet/comsec.
[350] "Specijalist Informacijske Sigurnosti," *University of Zagreb Fakultet organizacije i informatike*, luettu 9.12.2022, https://usris.foi.hr/pocetna.
[351] "Graduate Professional Study in Information Security and Digital Forensics," *Zagreb university of applied sciences*, luettu 9.12.2022, https://www.tvz.hr/studiji/diplomski/spec-isecen/.
[352] "Department courses," *Algebra University College*, luettu 9.12.2022, https://www.algebra.hr/visoko-uciliste/en/for-students/departments-and-teachers/department-of-cyber-security/5.
[353] Henkilökohtainen tiedonanto tutkijalle, 3.5.2022.
[354] "Ne Budi i Ti Hrvatski Naivac," *National CERT Croatia*, luettu 26.11.2022, https://www.naivci.hr/#Uvod.
[355] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 95.
[356] "Ne Budi i Ti Hrvatski Naivac," *National CERT Croatia,* luettu 24.10.2022, https://www.naivci.hr/#Uvod.
[357] ENISA, *Raising Awareness of Cybersecurity as a Key Element of National Cybersecurity Strategies* (2021), 27, 39.
[358] ENISA, *European Cybersecurity Month (ECSM) 2020* (2021), 46.
[359] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 96.
[360]"Cybersecurity Material," *ENISA,* luettu 24.10.2022, https://cybersecuritymonth.eu/resources?country[]=HR&perPage=24&reqPage=1&searchText=&sortOrder=descending.
[361] ENISA, *Raising Awareness of Cybersecurity as a Key Element of National Cybersecurity Strategies* (2021), 27.
[362] "About Our SID Activities," *European schoolnet*, luettu 24.10.2022, https://www.saferinternetday.org/in-your-country/croatia.
[363] Henkilökohtainen tiedonanto tutkijalle 9.8.2022.
[364] "Areas and Modules," *Learning Web Skills*, luettu 24.10.2022, https://learningwebskills.com/index.php/areas-and-modules/.
[365] "I'm Netica!," *Croatian Safer Internet centre*, luettu 25.10.2022, http://www.netica.hr/.
[366] "Sigurni s Neticum," *Croatian Safer Internet centre*, luettu 26.10.2022, http://netica.hr/materijali/Slikovnica_web.pdf.
[367] "Sigurni s Neticum Radna Biležnica Sigurnosti Na Interneta," *Croatian Safer Internet Centre,* luettu 26.10.2022, http://netica.hr/materijali/Netica_rb_web.pdf.
[368] "Interaktivna Slikovnica Razmisli Pa Klikni Za Lakši Razgovor o Izazovima Interneta," *Roda -association,* luettu 26.10.2022, https://www.roda.hr/udruga/projekti/razmisli-pa-klikni/interaktivna-slikovnica-razmisli-pa-klikni-za-laksi-razgovor-o-izazovima-interneta.html.
[369] "Prijavi i Zaustavi,"*Croatian Safer Internet centre*, katsottu 26.10.2022, https://www.youtube.com/channel/UCOGImLmHlBh2wwE7eWPyj6Q.
[370] "Dan Sigurnijeg Interneta," *Croatian Safer Internet centre*, luettu 26.10.2022, https://csi.hr/dan-sigurnijeg-interneta/.
[371] "6. Ispravno i Odgovorno Koristenje Racunala," *Croatian Academic and Research Network – CARNET*, luettu 26.10.2022, https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/c4e1aebf-48e0-4d92-b6a9-0716a4e1c740/html/430_ispravno_i_odgovorno_koristenje_racunala.html.
[372] "5. Internet," *Croatian Academic and Research Network – CARNET*, luettu 26.10.2022, https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/c9d3bbb7-0fb8-45a8-ba91-4175fca0fc8a/html/538_internet.html.
[373] "1. Racunalo i Mreza," *Croatian Academic and Research Network CARNET*, luettu 26.10.2022, https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/c9d3bbb7-0fb8-45a8-ba91-4175fca0fc8a/html/538_internet.html.
[374] "Dabrica Darka – Growing up on a Safer Internet," *The association Learning Associates*, luettu 26.10.2022, https://ucitelji.hr/dabrica-darka-growing-up-on-a-safer-internet/.
[375] "Što Je e-Nasilje?," *Croatian Safer Internet centre,* luettu 26.10.2022, http://www.netica.hr/upoznajmo-i-prepoznajmo-e-nasilje/.
[376] Henkilökohtainen tiedonanto tutkijalle, 14.9. 2022.
[377] Henkilökohtainen tiedonanto tutkijalle, 9.8.2022.
[378] "Young Croats Have The Best Digital Skills In Europe," *Total Croatia news,* luettu 26.10.2022, https://www.total-croatia-news.com/news/45053-young-croats-have-the-best-digital-skills-in-europe.
[379] Henkilökohtainen tiedonanto tutkijalle, 3.5.2022.
[380] Henkilökohtainen tiedonanto tutkijalle, 14.9.2022.

[381] Henkilökohtainen tiedonanto tutkijalle, 9.8.2022.
[382] Henkilökohtainen tiedonanto tutkijalle, 14.9.2022.
[383] ”SELFIE for TEACHERS,” *The European commission*, luettu 9.12.2022, https://education.ec.europa.eu/selfie-for-teachers.
[384] Kralj, *New Informatics curriculum*, 3.
[385] Ministry of Science and education of Croatia, *Curriculum of the Teaching Object Informatica for Primary Schools and Gymnasiums* (2018).

3.10. Kypros

ITU, Global Cybersecurity Index (GCI) 2020	41/182 (Global), 26/46 (Europe)
National Cyber Security Index (NCSI) 2022	37/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	20/27

3.10.1. Strategiset kyberkoulutuslinjaukset

Kyproksen kyberturvallisuusstrategia on julkaistu vuonna 2020. Siinä korostetaan koko yhteiskunnan vastuuta turvallisemmasta internetin käytöstä. Kyberturvatietoisuuden kehittämiseen ja turvallisuuskulttuuriin on panostettava kaikissa yhteiskunnan kerroksissa. Eri sidosryhmien ja viranomaisten (esimerkiksi CSIRT-CY (Computer Security Incident Response Team), poliisi (Αστυνομία Κύπρου), Kyproksen pedagoginen instituutti CPI (Παιδαγωγικό Ινστιτούτο Κύπρου)) aktiivinen sitoutuminen tiedottamistoimenpiteisiin on tärkeää. Kansalaisia tulisi tiedottaa riskeistä ja varotoimenpiteistä, erityisesti internetpalveluihin liittyvistä. Tavoitteena on myös helpottaa kyberturvallisuustaitojen kehittämistä koko koulutusjärjestelmän alueella. Tärkeänä pidetään lisäksi tiedotusmateriaalin luomista sekä käytettävissä olevan materiaalin hyödyntämistä ulkoisista lähteistä, esimerkiksi ENISA (The European Union Agency for Cybersecurity) ja Safer Internet for Kids. Tiedottamisen on oltava jatkuvaa ja erilaisia tiedottamistapoja tulee käyttää suuren yleisön tavoittamiseksi. Tavoitteena on luoda kulttuuri internetin luovalle ja turvalliselle käytölle.[386]

3.10.2. Kyberkansalaistaitojen opettamisen nykytila

Kyberturvaosaamista ja -koulutusta edistävät Kyproksella pääasiassa Digitaalisen turvallisuuden viranomainen DSA (Αρχή Ψηφιακής Ασφάλειας), johon kuuluu myös CSIRT-CY, Kyproksen opetus-, urheilu- ja nuorisoministeriö (Υπουργείου Παιδείας, Αθλητισμού και Νεολαίας) sekä paikalliset julkiset ja yksityiset yliopistot.[387]

Perus- ja keskiasteen koulutuksessa internetin turvallisesta käytöstä vastaava osasto on CPI. Se myös vastaa ohjeista ja käytännöistä, jotka liittyvät internetin vastuulliseen käyttöön. Internetin turvallisuusasioiden sisällyttäminen koulun opetussuunnitelmaan, työpajojen järjestäminen oppilaille, opettajille ja vanhemmille sekä esitelmät konferensseissa ja tapahtumissa ovat CPI:n ydintehtäviä.[388] Digitaitojen opetus integroidaan peruskoulun alaluokilla (primary education) muihin pakollisiin oppiaineisiin, ja joissakin kouluissa on erillinen aine Informatics, joka on koulun mukaan joka pakollinen tai valinnainen. Peruskoulun ylemmillä luokilla (lower secondary education) on määritelty osaamistavoitteet DigCompin Safety-osa-alueelle, jota opetetaan Informatics/Computer science -aineen tunneilla.[389]

Peruskoulun viides- ja kuudesluokkalaisille on vuonna 2019 laadittu opetussuunnitelma, joka koskee uutta teknologiaa. Se koostuu erillisestä aiheesta, johon kuuluu "Health Education – Home Economics / Design and Technology – New Technologies". Tämän lisäyksen odotetaan vahvistavan digitaalisten taitojen ja digitaalisen/medialukutaidon valtavirtaistamista kaikissa kouluaineissa. Uudessa opetussuunnitelmassa kyberturvallisuuteen liittyviä aiheita ovat Cyberbullying / Video – Online Games (viidesluokkalaisille) ja Information – Misinformation / Personal Data and Digital Identity (kuudesluokkalaisille).[390,391] Peruskoulun ylempien luokkien oppilaat ovat perinteisesti myös opiskelleet ECDL (European computer driving licence) -moduulit, jotka sisältävät eSafety-kysymyksiä.[392]

Toisella asteella (upper secondary education) Informatics/computer science on pakollinen yhden vuoden ajan ja oppitunneilla käsitellään Safety-kysymyksiä. DigCompin osaamisaloille Protecting personal data and privacy ja Protecting health and well-being on määritelty osaamistavoitteet.[393]

Kyberturvallisuudesta on mahdollisuus suorittaa maisterin tutkinto seuraavissa yliopistoissa: Kyproksen avoin yliopisto (Ανοικτό Πανεπιστήμιο Κύπρου): MSc programme Computer and Network Security, Keski-Lancashiren yliopisto (University of Central Lancashire Cyprus (UCLan Cyprus)): MSc Cybersecurity ja Kyproksen Eurooppa-yliopisto (Ευρωπαϊκό Πανεπιστήμιο Κύπρου): The MSc in Cybersecurity at EUC.[394]

Lähtökohtana kansalaisten kyberturvakoulutuksessa on, että eri ikäryhmille valmistetaan erilaista koulutusmateriaalia, kullekin ryhmälle merkityksellisten uhkien mukaan. Esimerkiksi Internet Safety Awareness Centren sivuilta voi nähdä tarkemmin koulutuksessa huomioitavia ikäryhmiä (lapset, nuoret, aikuiset).[395] EU:n positiivinen vaikutus on selvästi havaittavissa Kyproksen kyberturvakoulutuksessa. Seuraavissa kappaleissa on eritelty opetus-, urheilu- ja nuorisoministeriön hankkeita Cyprus safer Internet centre – CyberSafety ja Helpline and Complaints Hotline 1480, joiden tarkoituksena on tarjota lapsille, nuorille, vanhemmille, opettajille ja laajemmallekin yhteisölle internetin ja digitaalitekniikan turvallista, vastuullista ja eettistä käyttöä koskevia neuvonta- ja tukipalveluita.[396]

Kyproksen Safer Internet Centre — CyberSafety[397] toimii EU-rahoituksella osana Better Internet for Kids -hanketta. Se edistää tärkeimpien kansallisten sidosryhmien välistä yhteistyötä turvallisen internetkulttuurin edistämiseksi. Tavoitteena on tukea ja vahvistaa kansalaisten toimintaa digitaalisessa yhteiskunnassa. Awareness Centre[398] tukee Safer Internet Centren työtä kehittämällä monipuolista koulutus- ja tiedotusmateriaalia, resursseja ja välineitä sekä järjestämällä kampanjoita, joissa lapsille, nuorille, vanhemmille, hoitajille ja opettajille tiedotetaan siitä, kuinka toimia turvallisesti internetissä. Awareness Centre tekee tiivistä yhteistyötä lasten ja nuorten kanssa ja motivoi heitä kertomaan ideoitaan, ehdotuksiaan ja näkemyksiään digitaalitekniikan ja internetin luovasta ja turvallisesta käytöstä. Myös Helpline/Hotline-palvelut tukevat Safer Internet Centerin toimintaa. Helplinen[399] tarkoitus on pyrkiä varmistamaan, että kaikilla on mahdollista saada asiantuntija-apua digitaalitekniikan ja internetin käyttöön liittyvissä kysymyksissä. Kyproksen CyberSafety-youth panelin[400] jäsenet toimivat parhaiden käytäntöjen ja toimien lähettiläinä, ja heidän tavoitteenaan on luoda innovatiivisia resursseja ja levittää tietoa internetin turvallisesta käytöstä nuorille ja myös muille toimintaan osallistuville ryhmille.

”Young coaches for the internet”[401] on vuosittainen ohjelma, jonka tarkoituksena on kouluttaa opiskelijoita internetin turvalliseen käyttöön ja auttaa heitä tukemaan kouluaan ja myös laajempaa yhteisöä kyberturva-asioissa. Myös ”eSafe schools”[402] on Kyproksella vuosittainen ohjelma, jonka tarkoituksena on kouluttaa opettajia vahvistamaan yhteisössään ja kouluyksikössään kyberturvallisuuskulttuuria. Ohjelman kautta koulut voivat saada Safety-labelin perustuen omaan tasoonsa digiturvallisuudessa.[403,404]

CPI:n koulutusteknologiaosasto tarjoaa vuosittain useita ohjelmia ja aktiviteetteja, joissa peruskoulun, keskiasteen ja teknisen alan kouluilla, opettajilla ja opiskelijoilla on mahdollisuus osallistua internetin turvallisuuden suunnitteluun ja toteuttamiseen, vahvistaa digitaalisia taitojaan ja edistää internetin luovan ja turvallisen käytön kouluttamista omassa koulussaan ja sen ulkopuolella.[405]

Yksityisellä sektorilla lapsille ja nuorille kohdennettuja, kyberturvallisuuteen ja digitaaliseen lukutaitoon liittyviä kursseja järjestää esimerkiksi Logischool. ”*Digital discovery 113*” -kurssilla käsiteltäviä aiheita ovat internetin käytön turvallisuus, netiketti ja kommunikointi verkossa.[406] Aikuisille yksityisen sektorin kyberturvallisuuteen liittyviä opiskelumahdollisuuksia tarjoaa esimerkiksi *Emphasys centre*, jossa voi suorittaa ECDL-koulutuksen.[407] *Myös School of certified professionals (SCP)* järjestää kyberturvallisuuskursseja ja -sertifikaatteja sekä kaikille kansalaisille avoimen *”Introduction to cybersecurity*” -verkkokurssin.[408]

Yliopistot järjestävät myös muille kuin asiantuntijoille seminaareja ja luentoja kyberturvallisuudesta ja osallistuvat kampanjoihin.[409] Esimerkiksi vuonna 2021 ECSM (European cybersecurity month) -kampanjan ohjelmaan sisältyi Kyproksen Eurooppa-yliopiston senioreille toteuttama webinaari. Nuorille kohdennetun verkkokiusaamista ja vihapuhetta käsittelevän tapahtuman järjestäjänä toimi Sosiaalisen innovaation keskus Center for social Innovation (CSI). ECSM-kampanjassa julkaistiin infograafeja, videoita ja materiaalia organisaation sosiaalisen median kanavissa.[410,411] Kyproksen Safer Internet Centre järjestää Safer Internet Day -

kampanjan aikana muun muassa kursseja, työpajoja, esityksiä ja tapahtumia oppilaille, opettajille ja vanhemmille. Internettietoisuutta edistetään eri mediakanavien, kuten radio-ohjelmien ja lehtien, kautta.[412,413,414]

Kyproksen keskuspankki (Κεντρική Τράπεζα της Κύπρου), Kyproksen pankkiyhdistys (Σύνδεσμος Τραπεζών Κύπρου), poliisi ja DSA järjestävät kampanjoita yhteistyössä. Esimerkiksi vuonna 2021 toteutetussa Aspis (Information Safety and Information Security) -kampanjassa tarkoituksena oli tiedottaa suurelle yleisölle yleisistä menetelmistä, joita huijarit käyttävät yrittäessään varastaa henkilötietoja ja pankkitietoja.[415]

Erilaisia koulutuspelejä integroidaan koulujen toimintaan oppimistavoitteiden tukemiseksi.[416] Esimerkiksi kreikankielisen 3D-pelin ”*eFollowMe*” kohderyhmänä ovat yläkoululaiset ja lukiolaiset. Pelin tavoitteena on tietoisuuden lisääminen digitaalisesta jalanjäljestä kiinnittämällä pelaajan huomiota esimerkiksi evästeiden käyttöön ja sosiaalisten verkostojen viestinnän menettelytapoihin. Peli on ladattavissa Windows- ja Mac-käyttöjärjestelmille.[417]

3.10.3. Kansalliset erityispiirteet

EU:n positiivinen vaikutus näkyy Kyproksella Cyprus Safe Internet Center – CYberSafety[418] -projektin lisäksi muun muassa Erasmus-kurssien määrässä. Emphasys centre[419], Dora education institute[420] ja Civic computing[421] järjestävät muun muassa opettajille ja nuorten kanssa työskenteleville kyberturvallisuuskoulutusta.

DSA:n perustaminen on ollut ratkaisevan tärkeää Kyproksen kyberturvallisuuden valmiuksien merkittävälle kohottamiselle ja yhteiskunnan turvaamiselle. DSA:han kuuluvan CSIRT:n ja yliopistojen edustajat kokoontuvat tarvittaessa ja osallistuvat tapahtumien valmisteluun tarkoituksenaan lisätä kansalaisten tietoisuutta kyberturvallisuudesta.[422]

Cyprus cyber security challenge[423] on merkittävä tapahtuma Kyproksella. Sen kautta valitaan ja koulutetaan Kyproksen maajoukkue kilpailemaan vuosittain järjestettävässä European Cyber Security Challenge -tapahtumassa. The CYberSafety summer camps -leirit tarjoavat hyviin verkkoturvallisuuskäytäntöihin liittyvää kokemuksellista toimintaa nuorille. CPI puolestaan järjestää vuosittain kilpailun, jossa opiskelijat tuottavat lyhyitä videoita mukaillen Safer Internet Day -kampanjan tunnuslausetta.[424]

Kyberturvallisuustaitojen koulutusmateriaalista Kyproksen asiantuntijakontakti esitti toiveen, että opetusaineiston tulisi olla mukaansatempaava, kattaa kaikki oppimistyylit ja sen tulisi keskittyä kansalaisten kannalta keskeisiin uhkiin.[425]

3.10.4. Kyberkansalaistaitojen määrittäminen

Kyproksella perusasteen ylemmillä luokilla ja toisella asteella hyödynnetään DigCompin viitekehystä kyberturvallisuuden opetuksen järjestämisessä.[426] Kyberturvastrategia määrittelee tärkeiksi kyberturvallisuustaidoiksi internetin turvallisen käytön, henkilötietojen suojaamisen, asianmukaisen käyttäytymisen kyberavaruudessa ja lasten suojelun internetissä. Tietoisuus kyberturvallisuusuhkista ja riskeistä ja niiden vaikutuksista yhteiskuntaan on elintärkeää. Tietoisuuden kautta kansalaiset ja yritykset voivat oppia käyttäytymään verkkomaailmassa ja suojautumaan tyypillisiltä riskeiltä.[427] Kyproksen asiantuntijakontaktit pohtivat kyberkansalaistaitojen määritelmää seuraavasti: 1) kansalaisten olisi tärkeää ymmärtää heidän kannaltaan merkityksellisten kyberuhkien perusteet ja heillä tulisi olla kyky soveltaa parhaita käytäntöjä tietojensa ja järjestelmiensä suojaamiseksi[428], 2) kyberkansalaistaito ja digitaaliset taidot määritellään taidoiksi, jotka kansalaisilla on oltava internetin asianmukaiseen käyttöön sekä internetin vaarojen havaitsemiseen.[429]

Viitteet

[386] Republic of Cyprus, State department of research innovation and digital politics, *Cyber Security Strategy of the Republic of Cyprus 2020*, 17, 38-40, 47.
[387]Jason R.C. Nurse , Konstantinos Adamos, Athanasios Grammatopoulos ja Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 45.
[388] Maria Bada ja Ioannis Agrafiotis, *Cybersecurity Capacity Review of the Republic of Cyprus*, Global Cyber Security Capacity Centre (2017), 54.
[389]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 119.
[390] Henkilökohtainen tiedonanto tutkijalle, 17.10.2022.
[391] Department of educational technology Cyprus pedagogical institute, *Αξιοποίηση των Ψηφιακών Τεχνολογιών για τη Μάθηση - Ψηφιακή Ικανότητα* (2019), 119.
[392] Emphasys Centre and ANT Limited, *Media and digital literacy report template* (2018), 4.
[393] European Commission, *Digital Education at School in Europe,* 119.
[394] ”Cyberhead-Cybersecurity higher education database,” *ENISA*, *luettu 7.12.2022, https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?search=cyprus.*
[395] Henkilökohtainen tiedonanto tutkijalle, 22.9.2022.
[396] Henkilökohtainen tiedonanto tutkijalle, 17.10.2022.
[397] ”Cyprus Safer Internet Centre,” luettu 7.11.2022, https://www.betterinternetforkids.eu/sic/cyprus.
[398] ”Internet Safety Awareness Centre,” *Cyprus Pedagogical institute*, luettu 7.11.2022, http://internetsafety.pi.ac.cy.
[399] ”The CyberSafety project. Helpline 1480,” *Cyprus pedagogical institute*, luettu 10.11.2022, https://www.cybersafety.cy/helpline.
[400] ”The CyberSafety project. Cyber Safety Youth Panel,” *Cyprus pedagogical institute*, luettu 27.11.2022, http://www.cybersafety.cy/youth-panel.
[401] ”Young Coaches for the Internet,” *Department of Educational Technology of the Cyprus Pedagogical Institute*, luettu 10.11.2022, https://youngcoaches.pi.ac.cy/.
[402] ”Safe School for the Internet Programme,” *Department of Educational Technology Cyprus Pedagogical Institute*, luettu 11.11.2022, https://esafeschools.pi.ac.cy/.
[403] ”eSafetyLabel,” *European schoolnet,* luettu 8.11.2022, https://www.esafetylabel.eu/.
[404] Henkilökohtainen tiedonanto tutkijalle, 17.10.2022.
[405] Henkilökohtainen tiedonanto tutkijalle, 17.10.2022.
[406] ”DIGITAL DISCOVERY 113 COURSE,” *Logischool*, luettu 29.9.2022, https://www.logiscool.com/en-cy/programs/digital-discovery-113.
[407] ”ECDL - European Computer Driving Licence,” *Emphasys centre*, luettu 10.11.2022, https://emphasyscentre.com/education/ecdl-european-computer-driving-licence/.
[408] ”Security,”*School of certified professionels*, luettu 10.11.2022, https://scp.ac.cy/.
[409] Henkilökohtainen tiedonanto tutkijalle 2.6.2022.
[410] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 97, 99.
[411] ”European Cybersecurity Month Cyprus,” *ENISA*, luettu 21.10.2022, https://cybersecuritymonth.eu/countries/cyprus.
[412] ”Safer Internet Day 2022,” *Cyprus pedagogical Institute*, luettu 10.11.2022, https://internetsafety.pi.ac.cy/safer-internet-day/SID2022/.
[413] ”Cyprus Safer Internet Centre CYberSafety About Our SID Activities,” *European Schoolnet*, luettu 21.10.2022, https://www.saferinternetday.org/in-your-country/cyprus.
[414] Henkilökohtainen tiedonanto tutkijalle, 17.10.2022.
[415] ”Campaign Launched to Boost Cyber Security,” *The CyprusMail*, luettu 21.10.2022, https://cyprus-mail.com/2021/07/30/campaign-launched-to-boost-cyber-security/.
[416] Henkilökohtainen tiedonanto tutkijalle, 22.9.2022.
[417] ”eFollowMe About the Game,” *University of Cyprus*, luettu 21.10.2022, http://efollowme.cs.ucy.ac.cy/.
[418] ”CYberSafety,” *Cyprus pedagogical institute*, https://cybersafety.cy/.
[419] ”Online Safety and Internet Addiction – Think before You Click!,” *Emphasys Centre*, luettu 11.10.2022, https://erasmuscoursescyprus.com/courses/online-safety-and-internet-addiction/.
[420] ”*Cybersecurity Education for Online Safety,” Dorea educational institute*, luettu 10.8.2022, https://dorea.org/erasmuscourses/cybersecurity-education-online-safety/.
[421] ”eSkills 4All,” *Civic computing*, luettu 29.9.2022, https://eskills4all.eu/index.php/about.
[422] Henkilökohtainen tiedonanto tutkijalle, 2.6.2022.
[423] ”Cyprus Cyber Security Challenge,” *The Cyprus Computer Society (CCS)*, luettu 21.10.2022, https://ccsc.org.cy/#home.
[424] Henkilökohtainen tiedonanto tutkijalle, 17.10.2022.
[425] Henkilökohtainen tiedonanto tutkijalle, 22.9.2022.
[426]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 125.
[427] Republic of Cyprus, State department of research innovation and digital politics, *Cyber Security Strategy of the Republic of Cyprus* 2020, 38-39, 45-46.
[428] Henkilökohtainen tiedonanto tutkijalle, 22.9.2022.
[429] Henkilökohtainen tiedonanto tutkijalle, 17.10.2022.

3.11. Latvia

ITU, Global Cybersecurity Index (GCI) 2020	15/182 (Global), 37/46 (Europe)
National Cyber Security Index (NCSI) 2022	25/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	17/27

3.11.1. Strategiset kyberkoulutuslinjaukset

Latvian kyberturvallisuusstrategia on vuodelta 2019. Siinä korostetaan, että kaikkien kansalaisten tulisi olla tietoisia riskeistä, joille he altistuvat verkkoympäristössä, ja toimista, jotka voivat estää altistumisen. Kyberturvallisuuden varmistamisen kannalta on ratkaisevan tärkeää, että jokainen henkilö on tietoinen turvallisuusasioista omassa arjessaan ja on näissä valpas. Tavoitteena on yleisen tietoisuuden parantaminen verkkoturvallisuudesta laatimalla ikäryhmäkohtaisia ohjeita ja opetusmateriaaleja sekä toteuttamalla kampanjoita sosiaalisen median turvallisuudesta. Myös haastavampaa ja syvällisempää koulutusta kyberturvallisuuskysymyksistä tarjotaan tietyille kohderyhmille. Lisätään myös opiskelijoiden ja opettajien tietoisuutta tietoturvasta, yksityisyyden suojasta ja luotettavista verkkopalveluista. Tuetaan aktiivisemmin latvialaisten lasten ja nuorten tietoisuuden lisäämistä kyberturvallisuudesta, esimerkiksi osallistumista epäviralliseen koulutukseen, peleihin ja kilpailuihin.[430]

3.11.2. Kyberkansalaistaitojen opettamisen nykytila

Latviassa tietotekniikan perusopetus alkaa peruskoulussa ja jatkuu toisen asteen kouluissa.[431] Peruskoulun ylemmillä luokilla (lower secondary school) ”Informatics” on yksi pakollisista aineista. Toisella asteella (upper secondary education) tietotekniikan opetus on integroitu muihin pakollisiin oppiaineisiin. DigCompin Safety-osaamisalueen ”Protecting personal data and privacy” osalta on peruskoulun ja toisen asteen opetussuunnitelmiin määritelty oppimistavoitteet.[432]

Kansallinen koulutuskeskus (Valsts izglītības satura centrs) aloitti uuden opetussuunnitelman kehittämisen yleissivistävässä koulutuksessa lokakuussa 2016 osana European Social Fund -hanketta ”Competence Approach to Curriculum” (School2030). Digitaalisen sisällön ja sen kulutuksen nopea kehitys oli yhtenä lähtökohtana kehittämistyölle. Uudet viestintäalustat, informaatioympäristön tietoturvan heikkeneminen ja epäluotettavan tiedon riskit ovat lisänneet tarvetta keskittyä tähän saakka vähemmän korostettuihin tietoihin, taitoihin ja asenteisiin, kuten digitaaliseen lukutaitoon ja medialukutaitoon.[433] Kriittinen ajattelu, kyberturvallisuus ja medialukutaito ovatkin olennainen osa opetussuunnitelmaa kaikilla koulutustasoilla: oppilaiden on tärkeää ymmärtää tietoturvan ja yksityisyyden suojan merkitys sekä hallita luotettavien sähköisten palvelujen käyttö. Nämä asiat sisältyvät eri oppiaineiden sisältöihin ja yleisopetuksen niin sanottuihin poikittaistaitoihin. Esimerkkiaiheita ovat se, kuinka luoda vastuullisesti digitaalista identiteettiä ja miten sosiaalista mediaa käytetään vastuullisesti.[434,435,436]

Esimerkiksi Social and civic learning -opinnoissa oppilas kolmannen luokan lopussa osaa tunnistaa eri tiedotusvälineiden tarjoamista tiedoista tosiasiat. kuudennen luokan lopussa oppilas arvioi ja käyttää kriittisesti eri medioiden ja historiallisten lähteiden tarjoamia tietoja. Hän tutkii, miten organisaatiot ja ihmiset muokkaavat digitaalista identiteettiään, ja päättelee, mistä se koostuu. Hän käyttää sosiaalista mediaa vastuullisesti. Yhdeksännen luokan lopussa opiskelija analysoi ja selittää median mahdollisuuksia heijastaa ja vaikuttaa ihmisten poliittisiin, sosiaalisiin, esteettisiin käsityksiin ja uskomuksiin. Hän etsii eri lähteistä sekä omasta ja muiden kokemuksista hyvin harkitun digitaalisen identiteetin kriteereitä ja luo vastuullisesti digitaalista identiteettiä.[437]

Kyberturvallisuudessa voi opiskella maisterin tutkinnon kolmessa yliopistossa: BA Liiketalouden ja rahoituksen korkeakoulussa (Banku augstskola) on ohjelma Professional Master's Degree in Cybersecurity Management[438], Riian teknillisessä yliopistossa (Rīgas Tehniskā universitāte) ohjelma Study programme Cybersecurity Engineering[439] ja Vidzemen ammattikorkeakoulussa (Vidzemes Augstskola) ohjelma Masters degree programme in Cybersecurity Engineering[440].

CERT.LV on Latvian keskeinen kyberturvallisuuden instituutio, joka toimii puolustusministeriön (Latvijas Republikas Aizsardzības ministrija) alaisuudessa. Se järjestää tiedotusta ja koulutusta suurelle yleisölle.[441] Esimerkiksi ennen merkittäviä tapahtumia, kuten vaaleja, se toteuttaa tiedotuskampanjoita. Se myös julkaisee sosiaalisessa mediassa kybersäätiedotteita Latvian kybertapahtumista.[442]

Zemgalen alueen henkilöstö- ja osaamiskehityskeskus ZRKAC (Zemgales reģiona kompetenču attīstības centrs) on kunnallinen oppilaitos, jonka tavoitteena on tarjota kansalaisille elinikäistä koulutusta. Oppilaitos järjestää omalla alueellaan kursseja aiheesta "Cybersecurity, computer systems and software".[443] Latvian työvoimatoimisto (Nodarbinātības valsts aģentūras) puolestaan tarjoaa työnhakijoille IT-alan koulutusta.[444] Yksityisellä puolella Baltic Computer Academy[445] -yrityksellä on valikoimassaan myös tavallisille tietokoneenkäyttäjille sopivia kyberturvallisuusaiheisia kursseja. NIC (Network Information Centre) on kehittänyt ilmaisen verkkokurssin *"The Cybersecurity Basics".*[446] Sen tarkoitus on toimia perehdytyksenä henkilöille, joilla ei ole aiempaa teknistä taustaa. Latvialaiset voivat osallistua myös CCDCOE:n (The NATO Cooperative Cyber Defence Centre of Excellence) Cyber Defence Awareness -verkkokurssille[447], jonka tavoitteena on lisätä tietoisuutta kyberturvallisuusriskeistä ja toimenpiteistä näiden riskien lieventämiseksi.

Koulutusportaali macibas.mana.latvija.lv[448] on kehitetty "Do it digitally" -hankkeessa (2018–2022). Hanketta hallinnoi ympäristönsuojelu- ja aluekehitysministeriö VARAM (Vides aizsardzības un reģionālās attīstības ministrija). Sivuston kautta kansalaiset voivat ilmoittautua ilmaiselle verkkokurssille "Distance learning programme for the development of digital skills in society"[449], jossa perehdytään muun muassa digitaaliseen identiteettiin, internetin turvallisuuteen sekä kriittiseen lukutaitoon. "Distance learning program for digital agents"[450] -kurssilla voi kouluttautua "digitaaliseksi agentiksi", joka neuvoo sähköisten palvelujen käytössä. Koulutukseen sisältyy aiheita myös turvallisuudesta ja kriittisestä ajattelusta ja lukutaidosta.

Latviassa on viime vuosina kohdennettu kansalaisille useita verkkoturvallisuuteen liittyviä kampanjoita. Esimerkiksi Latvian rahoitusyhdistys (Finanšu nozares asociācija) ja Mastercard ovat järjestäneet verkko-ostosten tekemiseen liittyviä kampanjoita "Viedpircējs" (Smart shopper)[451]. Myös "Neuzķeries! Esi gudrāks par krāpniekiem!" (Don't get caught! Be smarter than fraudster) -kampanjan yhtenä järjestäjänä toimi Latvian rahoitusyhdistys.[452] "Esi reāls" (Be real) -kampanjassa keskityttiin kriittisen ajattelun edistämiseen sosiaalisessa mediassa, järjestäjänä toimi Kuluttajansuojakeskus (Patērētāju tiesību aizsardzības centrs).[453] "Digitālās drošības ceļvedis" (Digital security roadmap) -kampanjan[454] toteutti televiestintä- ja internetpalveluntarjoaja TET. Kampanjan tuotoksena syntyi kaikille internetissä saatavilla oleva Digital Security Guide -opas, jossa neuvotaan digitaalisen identiteetin, laitteiden ja omien tietojen suojaamista. Portaalista löytyy sekä yleistä että enemmän nuorille kohdennettua tietoa sekä mahdollisuus testata kyberturvallisuustaitonsa kyselyn avulla.[455]

"Superheroes do not get lost" ja "Superheroes on the Internet" ovat Latvian valtiollisen poliisin (Valsts policija) ja yhteistyökumppaneiden kohdentamia kampanjoita lapsille, vanhemmille ja opettajille. Tarkoituksena on kiinnittää huomiota lasten turvallisuuteen internetissä.[456] Poliisin hallinnoimassa portaalissa on opetusmateriaaleja eri-ikäisille lapsille. Kampanjan yhteydessä suunniteltiin alakoululaisille lautapeli "Vaifija spēle", jota voi tilata rajoitetun määrän kouluihin veloituksetta.[457]

Latvian hallitus on järjestänyt digitaalista turvallisuutta koskevia aloitteita tietoisuuden ja hyvien käytäntöjen jakamiseksi, kuten Safer Internet Dayn ja ECSM:n (European cybersecurity month)[458.] Safer Internet Dayn aikana kouluille on esimerkiksi jaettu kampanjaan liittyviä materiaalipaketteja, joita opettajat ovat välittäneet oppilaille.[459] Digital Week[460] on Latviassa vuosittain järjestettävä kansallinen tiedotus- ja valistuskampanja, jossa edistetään digitaalista osaamista. Sitä koordinoi Latvian tieto- ja viestintätekniikan yhdistys LIKTA (Latvijas

Informācijas un komunikācijas tehnoloģijas asociācija) yhteistyössä VARAMin kanssa. Kampanjoissa on käsitelty myös digitaalinen identiteettiin, turvallisuuteen ja kriittiseen ajatteluun liittyviä asioita.[461]

CERT.LV:n ylläpitämä Esidross.lv-portaali [462] sisältää hyödyllisiä neuvoja kyberturvallisuudesta ja ohjeita digitaalisten laitteiden turvalliseen käyttöön. Aiheita ovat muun muassa omien tietojen hallinta ja yksityisyys ja laitteiden ja ohjelmistojen sekä sosiaalisten verkostojen turvallisuus. Lisäksi portaalissa on neuvoja siitä, kuinka puhua lapsille internetin turvallisuuskysymyksistä. Yleisimmät uhkatyypit ja suositukset niiden välttämiseksi ja ongelmatilanteiden ratkaisemiseksi toimivat konkreettisena apuna kyberturvallisuuden hallinnassa. Mana.Latvija.lv-portaaliin on koottu kansalaisille ohjeita e-asioinnista. Sivustoa hallinnoi VARAM. Sivustolla on oma osio ”Internet safety” (Drošība internetā), joka sisältää vinkkejä turvalliseen internetin ja mobiililaitteiden käyttöön, henkilötietojen suojaamiseen sekä neuvoja siihen, mistä hakea apua, jos joutuu esimerkiksi petoksen uhriksi.[463]

Latviassa kiinnitetään erityistä huomiota kriittisen lukutaidon kehittämiseen, mistä yhtenä esimerkkinä on Latvian keskusteluyhdistyksen ”Quotu domā?”:n kääntämä, kaikille saatavilla oleva vuorovaikutteinen peli, joka liittyy logiikkavirheisiin.[464] Peli auttaa tunnistamaan logiikkavirheitä sisältäviä huijausviestejä mediasta.

3.11.3. Kansalliset erityispiirteet

Latviassa kyberkansalaistaitoja opetetaan jonkin verran jo kouluissa, minkä lisäksi laajemmin eri ikäluokkia otetaan huomioon yleissivistyksen opetussuunnitelmassa, johon sisältyy erillinen digitaalinen osaamiskokonaisuus. Kyberturvallisuustaitojen päivittämiselle on kuitenkin tarvetta. [465] Haasteeksi koetaan tietämättömyys siitä, mikä olisi paras tapa tavoittaa kansalaiset ja järjestää hyvä valistuskampanja. [466] Henkilöstön ja rahoituksen puute hidastavat tietoisuuden lisäämistä.[467] Tulevaisuudessa tavoitteena on liittää koulujen kyberturvallisuuskoulutus maanpuolustuksen opetukseen. *State defence concept* -dokumentissa [468] todetaan, että kyberturvallisuuden tulisi olla osa koulujen opetussuunnitelmaa ja yksi maanpuolustustuntien aiheista. Maanpuolustustunnit tulevat Latviassa pakollisiksi yläkouluissa vuonna 2024.

Tammikuussa 2023 Latviaan perustetaan uusi kansallinen kyberturvakeskus, joka toimii puolustusministeriön (Aizsardzības ministrija) alaisuudessa. Keskuksen tehtäviin kuuluu muun muassa julkishallinnon ja suuren yleisön neuvonta ja tiedottaminen kyberturvallisuusasioissa.[469]

3.11.4. Kyberkansalaistaitojen määrittäminen

Kyberturvastrategia määrittelee jossain määrin kyberturvallisuuteen liittyviä taitoja. Sen mukaan ensiarvoisen tärkeää on varmistaa, että kaikki, jotka saattavat altistua tietojenkalastelusähköpostihuijauksille tai social engineeringille, ymmärtävät kyberturvallisuusasioita. Kaikki sidosryhmät ovat yhtä tärkeitä verkostojen ja tietojärjestelmien turvaamisen kannalta. Tämä tarkoittaa sitä, että kaikkien tulisi olla yhtä tietoisia riskeistä, joille he altistuvat online-tilassa, ja toimista, jotka voivat estää tällaisen altistumisen. Yksityisyyden suojaaminen ja luotettavien verkkopalvelujen tunnistaminen koetaan myös tärkeiksi taidoiksi.[470] Going digital in Latvia -dokumentissa[471] yhtenä tärkeänä taitona mainitaan verkkokiusaamisen tunnistaminen ja siihen puuttuminen. Kouluopetuksessa kyberturvallisuustaidot määrittyvät DigCompin Safety-osa-alueen kautta kaikilla luokka-asteilla peruskoulusta toiselle asteelle.[472]

Viitteet

[430] Ministry of Defence of Latvia, *Cybersecurity Strategy of Latvia 2019–2022,* 2019, 19-20.
[431] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.
[432] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45, 120.
[433] Henkilökohtainen tiedonanto tutkijalle, 21.6.2022.
[434] Henkilökohtainen tiedonanto tutkijalle, 21.6.2022.
[435] "Skola 2030," *National Centre for Education*, luettu 15.11.2022, https://www.skola2030.lv/lv.
[436] OECD, *Going Digital in Latvia*, OECD Reviews of Digital Transformation, (Paris: OECD Publishing, 2021), 101.
[437] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.
[438] "Professional Master's Degree in Cybersecurity Management," Banku augstskola, luettu 1.12.2022, https://www.ba.lv/studies/program/cybersecurity-management/.
[439] "Cybersecurity Engineering," *Riga technical university*, luettu 1.12.2022, https://international.rtu.lv/masters-studies/cybersecurity-engineering/.
[440] "Professional Master's in cybersecurity engineering," *Vidzeme University of Applied Sciences,* luettu 1.12.2022, https://va.lv/en/study-here/masters-degree/cybersecurity-engineering/about-programme.
[441] "CERT.LV lectures in schools and state and municipal institutions in 2022," *CERT.LV*, luettu 16.11.2022, https://cert.lv/lv/2022/01/cert-lv-lekcijas-skolas-un-valsts-un-pasvaldibu-iestades-2022.
[442] ENISA, *Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 18-20.
[443] "Courses," *Zemgale Region Human Resource and Competences Development Centre*, luettu 15.11.2022, https://www.zrkac.lv/en/index.php?view=en&id=64.
[444] Henkilökohtainen tiedonanto tutkijalle, 21.6.2022.
[445] "Course catalogue," *BDA*, luettu 16.11.2022, https://www.bda.lv/bda4/en/Catalog.
[446] "Free online course "Cybersecurity Basics"," *NIC*, luettu 15.11.2022, https://www.nic.lv/en/free-online-course-cybersecurity-basics.
[447] "Cyber Defence Awareness," CCDCOE, luettu 16.11.2022, https://ccdcoe.org/training/cyber-defence-awareness-e-course/.
[448] "Welcome to the e-learning environment!," *Ministry of Environmental Protection and Regional Development*, luettu 17.11.2022, macibas.mana.latvija.lv.
[449] "Distance learning programme for the development of digital skills in society," *Ministry of Environmental Protection and Regional Development*, luettu 17.11.2022, https://macibas.mana.latvija.lv/courses/course-v1:VARAM+SAB101+2022_02/about.
[450] "Distance learning program for digital agents," *Ministry of Environmental Protection and Regional Development*, luettu 16.11.2022, https://macibas.mana.latvija.lv/courses/course-v1:VARAM+DAT101+2022_02/about.
[451] "Education," *Latvian Finance Latvia Association*, luettu 28.11.2022, https://www.financelatvia.eu/viedpircejs/.
[452] "Neuzķeries! Esi gudrāks par krāpniekiem!," *Finanšu nozares asociācija*, luettu 16.11.2022, https://neuzkeries.lv/.
[453] "Esireals,"*Patērētāju tiesību aizsardzības centrs*, luettu 16.11.2022, https://www.esireals.lv/.
[454] "Sociālajā iniciatīvā "Digitālās drošības ceļvedis" aicina aizsargāties pret digitālajiem uzbrucējiem," *LIKTA*, luettu 16.11.2022, https://likta.lv/socialaja-iniciativa-digitalas-drosibas-celvedis-aicina-aizsargaties-pret-digitalajiem-uzbrucejiem/.
[455] "Digitālās drošības ceļvedis," *Tet*, luettu 16.11.2022, https://www.tet.lv/vairak/digitala-drosiba.
[456] "State Police Superheroes," *Valsts policija*, luettu 16.11.2022, https://www.vp.gov.lv/lv/valsts-policija-supervaroni.
[457]"Play the WAIFY GAME and get five SUPER POWERS!," *Latvian Safer Internet Centre*, luettu 16.11.2022, https://drossinternets.lv/lv/posts/view/spele-vaifija-speli-un-iegusti-piecas-superspejas.
[458]OECD, *Going Digital in Latvia*, OECD Reviews of Digital Transformation, (Paris: OECD Publishing, 2021), 135.
[459] "About our SID activities," *European Schoolnet*, luettu 17.11.2022, https://www.saferinternetday.org/in-your-country/latvia.
[460] "Digital Week in Latvia," *Digital skills & jobs platform*, luettu 17.11.2022, https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/digital-week-latvia.
[461] "We invite you to participate in Digital Week 2022!," *LIKTA*, luettu 17.11.2022, https://digitalanedela.lv/.
[462] "Esidrošs," *CERT.LV,* luettu 17.11.2022, Esidross.lv.
[463] "Drošība internet," *Ministry of Environmental Protection and Regional Development*, luettu 15.11.2022, https://mana.latvija.lv/drosiba/.
[464] "Thou shalt not commit logic fallacies," *The school of thought*, luettu 17.11.2022, https://yourlogicalfallacyis.com/lv.
[465] Henkilökohtainen tiedonanto tutkijalle, 27.7.2022.
[466] ENISA, *Raising Awareness of Cybersecurity*, 45.
[467] Jason R.C. Nurse , Konstantinos Adamos, Athanasios Grammatopoulos ja Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 55.
[468] Ministry of Defence of the Republic of Latvia, *State defence concept* (2020), 1, 17.
[469] "New National Cyber Security Center set to launch next year," *LSM.lv*, luettu 28.8.2022, https://eng.lsm.lv/article/society/defense/new-national-cyber-security-center-set-to-launch-next-year.a460484/.
[470] Ministry of Defence of Latvia, *Cybersecurity Strategy of Latvia 2019–2022, 17, 19.*
[471] OECD, *Going Digital in Latvia*, OECD Reviews of Digital Transformation, (Paris: OECD Publishing, 2021), 101.
[472] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45, 120.

3.12. Liettua

ITU, Global Cybersecurity Index (GCI) 2020	6/182 (Global), 4/46 (Europe)
National Cyber Security Index (NCSI) 2022	2/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	14/27

3.12.1. Strategiset kyberkoulutuslinjaukset

Liettuan kyberturvallisuusstrategiassa (2018) todetaan, että kyberturvallisuuskulttuurin vahvistamiseksi lapsille ja nuorille olisi annettava perustavanlaatuinen tietoverkkoturvallisuuden tuntemus eri luokka-asteilla alkaen lastentarhasta. Olisi pyrittävä myös parantamaan opettajien pätevyyttä kyberturvallisuudessa. Näin he voisivat paitsi kouluttaa nuoria paremmin, myös edistää yhteiskunnan kehittymistä ja lisätä yleistä kyberturvallisuustietoisuutta. Tutkimusten mukaan suuri osa liettualaisista ei ymmärrä kyberrikosten riskejä, ja siksi tietoisuutta tulee lisätä tavallisten kansalaisten keskuudessa. Verkkoturvallisuuskulttuurin vahvistamisen kannalta on tärkeää levittää tehokkaasti ja säännöllisesti tietoa uusimmista uhista ja muista tekijöistä, jotka saattavat uhata henkilötietojen turvallisuutta tai tehdä ihmisistä rikosten uhreja kyberavaruudessa.[473]

3.12.2. Kyberkansalaistaitojen opettamisen nykytila

Liettuassa kyberturvallisuustaitojen kehittämistä edistävät pääasiassa koulut, korkeakoulut, yksityinen sektori, valtion laitokset sekä hallitus. [474] Koulujen kyberturvallisuuskoulutus kuuluu Kansallisen opetusviraston (Nacionalinės švietimo agentūros, NŠA) vastuulle. Se kehittää perus-, keski- ja toisen asteen koulutusohjelmia. Perusopetuksen yleinen opetussuunnitelma korostaa vahvasti turvallista internetiä ja viestintää, ja peruskoulussa opiskellaan internetturvallisuuteen liittyviä asioita. [475] Digitaalinen osaaminen sisältyy opetussuunnitelmaan ja digitaalinen lukutaito on kaikille yleinen osaamisalue. DigCompin Safety-osaamisalueet löytyvät peruskoulun opetussuunnitelmasta ja osa-alue ”Protection personal data and privacy” myös toisen asteen opetussuunnitelmasta.[476]

1.–4. luokkien (primary education) opetussuunnitelmassa korostetaan, että opettaja on velvollinen puhumaan oppilaille internetin vaaroista, selittämään henkilötietojen paljastamisen vaarat sekä neuvomaan, miten välttää joutumasta vaarallisiin tilanteisiin internetiä käyttäessään. [477] Perusasteen alaluokilla opetettavassa valinnaisessa Informatics-oppiaineessa käsitellään aihetta Turvallisuus ja oikeudenmukaisuus.[478] Viidennen ja kuudennen. luokkien opetussuunnitelmassa Internet ja sen palvelut -aiheen yhteydessä käsitellään internetin turvallisuuteen liittyviä kysymyksiä.[479]

Keski- ja toisen asteen koulujen kyberturvallisuuden opetussuunnitelma sisältää Information technology -oppiaineen, jonka tavoitteena on, että opiskelijat oppivat käyttämään internetresursseja ja palveluja laillisesti ja turvallisesti.[480] Esimerkiksi osa-alueella Technologies: Safe and lawful use of information and the Internet (8.2.4.) opiskellaan tietokoneen ja henkilötietojen suojaamista, tekijänoikeuksia, viestintää sosiaalisissa verkostoissa sekä sähköiseen allekirjoitukseen ja elektronisiin palveluihin liittyviä asioita.[481] Valinnaisten ICT (Information Communication Technology)- ja Engineering-oppiaineiden lukio-opetukseen kuuluu turvallisten tietojärjestelmien kehittäminen, konfigurointi ja turvallinen toiminta digitaalisia laitteita käytettäessä.[482]

Neljä yliopistoa tarjoaa Liettuassa mahdollisuuden suorittaa maisterin tutkinnon kyberturvallisuudesta: Vilna Gediminasin teknillinen yliopisto (Vilniaus Gedimino Technikos Universitetas): Master's degree studies ”Information and Information Technology Security”[483], Vilnan yliopisto (Vilniaus universitetas): Master's degree studies ”Computer Modelling”[484], Kaunasin teknillinen yliopisto (Kauno technologijos universitetas): Master's

degree studies ”Information and Information Technology Security”[485], Mykolas Romeriksen yliopisto (Mykolo Romerio universitetas, MRU): Master's degree studies ”Cybersecurity Management”[486].

Yksityinen ja kolmas sektori tarjoavat aikuisväestölle erilaisia kursseja ja materiaaleja kyberturvallisuudesta.[487] Osa kursseista on yrityksille, mutta esimerkiksi CSA (Cyber Security Academy) järjestää Security awareness training -kursseja, jotka sopivat myös tavallisille kansalaisille.[488] Yritykset toteuttavat yksittäisiä koulutusaloitteita myös kouluissa ja päiväkodeissa.[489] Yksi mahdollisuus taitojen päivittämiseen on LCC International Universityn järjestämä LCC Cybersecurity Bootcamp -kyberturvallisuuskoulutusohjelma. Se on suunnattu erityisesti henkilöille, joilla on vain vähän tietotekniikkaosaamista ja jotka haluaisivat kouluttautua kyberturva-alalle.[490]

Liettuan pankit, poliisi ja kirjastot ovat aktiivisia kyberturvallisuuskoulutuksen saralla. Poliisit ovat järjestäneet kansalaisille tapaamisia, joissa opetettiin tunnistamaan kybermaailman rikoksia ja suojautumaan niiltä.[491] Liettuan pankit ja Liettuan pankkiyhdistys (Lietuvos bankų asociacija) ovat toteuttaneet tiedotuskampanjoita tietojenkalastelusta.[492] Kirjastot puolestaan ovat osallistuneet Safer Internet Dayn toteutuksiin esimerkiksi järjestämällä interaktiivisia luentoja Zoomissa ja lapsille ja aikuisille kyselyitä Quizziz-alustalla.[493] Women4cyber-yhteisön jäsenet luennoivat yliopisto-opiskelijoille ja käyvät myös kouluttamassa päiväkodeissa.[494]

Liettuan Safer Internet Centre edistää internetin ja mobiiliteknologian turvallisempaa käyttöä. Resursseja kehitetään eri kohderyhmille: lapsille ja nuorille, vanhemmille ja hoitajille, opettajille, sosiaalityöntekijöille ja kouluttajille. Kansallisista kampanjoista tärkeimpiä ovat Safer Internet Day (SID) ja viikko sekä All Digital Week. Safer Internet Centre osallistuu paikallisiin ja kansallisiin tapahtumiin, järjestää opettajille koulutuksia ja opiskelijoille tapaamisia. Verkkoturvallisuutta edistetään myös perinteisen ja sosiaalisen median avulla.[495] Yksi tärkeimmistä tiedotusvälineistä on kansallinen Safer Internet Centren portaali[496], joka on tarkoitettu turvalliseen internetin käyttöön liittyvien resurssien ja tapahtumien levittämiseen kansalaisille.

Joitakin kyberturvallisuuskampanjoita toteutetaan säännöllisesti, kuten Local Hack Day. Lisäksi kampanjoidaan silloin, jos kyberturvallisuustapahtumia on näyttävästi esillä mediassa.[497] Liettuan hallitus toteutti vuosina 2019 ja 2020 kampanjan ”Sustiprink imunitetą” (Strengthen Immunity)[498], jonka tarkoituksena oli opettaa tunnistamaan ja torjumaan uhkia internetissä. Portaalin ”Naršyk saugiai” (Browse safely) -osion tavoitteena on tiedottaa kaikenikäisille internetissä piilevistä uhista. ”Atpažink melagienas” (Recognize Liars) opettaa tunnistamaan valeuutiset. Portaalissa on myös testejä, jotka liittyvät valeuutisiin ja tietokoneen ja puhelimen suojaukseen.

”Langas į ateitį” -yhdistys koordinoi Liettuassa vuosittaisia All digital weeks -tapahtumia. Tavoitteena on auttaa kaikenikäisiä ihmisiä digitaitoihin liittyvissä kysymyksissä. Vuonna 2022 aiheena olivat myös kyberturva-asiat: turvallisempi verkkokäyttäytyminen, salasanahallinta, turvallinen verkkomaksaminen ja toiminta epäilyttävässä tilanteessa. Asiantuntijoina toimivat muun muassa talousrikosten ehkäisyn asiantuntijat.[499,500]

Vuosina 2018–2021 toteutettu projekti Connected Lithuania: effective, secure and responsible digital society in Lithuania oli suunnattu kansalaisille, joilla on puutteita digitaidoissa, sekä nuorelle väestölle. Projektin toteuttajina oli useita valtiollisia tahoja ja toimijoita, muun muassa Liettuan sisäministeriö (Lietuvos Respublikos vidaus reikalų ministerija) ja Liettuan viestinnän sääntelyviranomainen RRT (Lietuvos Respublikos ryšių reguliavimo tarnyba). Hankkeessa järjestettiin nuorten tapahtumia, kyberturvallisuusaiheita sisältäviä kursseja sekä digitaalisen lukutaidon oppitunteja kirjastoissa.[501] Projektin portaalin itseopiskelumateriaalissa on aiheita yksityisyydensuojasta kriittiseen ajatteluun ja uhkien tunnistamiseen sekä lapsille ja vanhemmille suunnattu kysely Kid online quiz[502], jonka avulla voi oppia tunnistamaan epäilyttävät online-pelit ja social engineeringin.

Esaugumas (Security) -portaalia ylläpitää RRT. Portaalissa on teemoja kyberturvallisuuden opetukseen, aina teknisemmistä aiheista (virustorjunta, vakoilu- ja haittaohjelmat) enemmän yksityisyyden suojaan painottuviin aiheisiin ja sähköiseen kaupankäyntiin. Portaalissa voi tehdä kysymyksiä kyberturvallisuuden asiantuntijoille.[503] Kriittisen ajattelun kehittämiseen liittyvä oppimispeli älylaitteille ”Editorial office 2030” löytyy Connected Lithuania -projektin portaalista.[504] Portaalissa on myös älypuhelimille ja tableteille ”Safer Internet”-sovellus, jolla

voi testata tietonsa turvallisesta verkkokäyttäytymisestä. Vilnan yliopiston Kaunasin tiedekunta (Vilniaus universitetas Kauno fakultetas) on kehittänyt pelin ”CTF @KnF”. Isommille koululaisille on peli ”TableTop”.[505]

3.12.3. Kansalliset erityispiirteet

Kyberturvahyökkäyksistä on tulossa yhä hienostuneempia, ja Liettuassa pohditaankin sitä, kasvaako yleinen kyberturvallisuusosaaminen riittävän nopeasti, jotta voidaan kuroa umpeen yhteiskunnan kyberpuolustustaitojen ja pahantahtoisten henkilöiden kyberhyökkäystaitojen välistä kuilua. [506] Kyberturvallisuustaidot erityisesti nuoremman sukupolven ja IT-asiantuntijoiden keskuudessa on paremmat, mutta on myös paljon käyttäjiä, joilla ei ole perustietoa kyberturvallisuudesta, sekä myös erittäin naiiveja käyttäjiä, jotka ovat helppoja huijauksen kohteita. Liettualaiset kokevat myös tarvetta tiedottamiselle valeuutisten torjumisessa.[507]

Julkisen sektorin kouluissa on haasteita opiskelijoiden kyberturvallisuuskoulutuksen järjestämisessä. Opettajien taidoissa on puutteita, minkä lisäksi kouluilta näyttää puuttuvan yhtenäinen järjestelmä opiskelijoiden kyberturvallisuustaitojen vahvistamiseksi. [508] Esimerkiksi lukioissa kyberturvallisuuden perusteita suositellaan opetettavaksi, mutta koska opettajilla on käytännössä laaja vapaus valita, mitä opettaa, kaikki koululaiset eivät välttämättä opi aiheesta perustietoja. Positiivista on se, että periaatteessa tilanne kyberturvallisuustaitojen suhteen paranee vuosittain.[509] Tänä vuonna puolustusministeriön tavoitteena on tunnistaa kyberturvallisuuteen liittyvät tarpeet ja puutteet ja valmistella kansallinen kyberturvallisuuden kehittämisohjelma, johon sisältyy ehdotus kyberturvallisuuskoulutuksen parantamiseksi. Opetus-, tiede- ja urheiluministeriö (Švietimo, mokslo ir sporto ministerija), NŠA sekä yliopistot tekevät yhteistyötä tutkiakseen kyberturvallisuuskysymyksiä, ja tavoitteena on ehdottaa toimivia ja selkeitä ratkaisuja tulevaisuutta ajatellen. [510] Liettuassa edistetään aktiivisesti tutkimusta, joka liittyy pelillistämisen soveltamiseen kyberturvakoulutuksessa. TableTop-tyyppisissä toteutuksissa pelillistämistä käytetään simuloimaan erilaisia kyberturvallisuuteen liittyviä skenaarioita, esimerkiksi kriittisiä kyberturvallisuuteen liittyvä tapauksia, joita pelaajat ratkaisevat.[511]

3.12.4. Kyberkansalaistaitojen määrittäminen

Liettuassa on käytetty DigCompia perustana tieto- ja viestintätekniikan opetuksen kehittämiselle. peruskouluissa. ”Connected Lithuania” -hankkeessa kaikki koulutusohjelmat laadittiin DigComp-ohjelman tasojen 1–2 mukaisesti. DigComp oli myös digitaalisten taitojen suosituksena Digital Agenda 2014–2020:ssa.[512]

Liettuassa ei vielä ole virallisesti muotoiltu kansallisia kyberturvallisuustaitoja koskevia vaatimuksia suurelle yleisölle, ja tarve tällaisten taitojen selkeälle määrittelylle lainsäädäntöasiakirjoihin tiedostetaan. [513, 514] Tarkasteltaessa kyberturvallisuuskurssien opetussuunnitelmia voidaan nähdä, että päähuomio niissä kiinnitetään kyberturvallisuuden toteuttamiseen käytettäviin teknologioihin, salasanojen hallintaan ja tapoihin tunnistaa kalastelu sekä muita verkossa ilmeneviä huijaustapoja. Koska suurin osa onnistuneista kyberhyökkäyksistä tehdään ihmisten heikkouksia hyödyntäen, näihin näkökohtiin on kiinnitettävä paljon huomiota. Siksi tietojenkalastelun ja muiden huijaustapojen tunnistaminen on ratkaisevan tärkeää. Olennaista on myös osata turvallisuuden hallintaprosessit, kuten ohjelmistojen päivitys sekä salasanojen säännöllinen vaihtaminen.[515]

Viitteet

[473] Ministry of National Defence Republic of Lithuania, *National Cyber Security Strategy* (2018), 12-13.
[474]Jason R.C. Nurse , Konstantinos Adamos, Athanasios Grammatopoulos ja Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 56.
[475] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[476] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45.
[477] Nacionalinė švietimo agentūra, *Pradinio ugdymo bendroji programa (1 priedas)* (2008), luettu 3.11.2022, https://duomenys.ugdome.lt/saugykla/bp/2016/pradinis/1_pradinio%20ugdymo%20bendroji%20programa.pdf.
[478] European Commission, *Digital Education*, 120.
[479] Nacionalinė švietimo agentūra, *Informacinės technologijos* (2008), luettu 3.11.2022, https://duomenys.ugdome.lt/saugykla/bp/2016/pagrindinis/8_Informacines_technologijos.pdf, 17-19.
[480] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[481] Nacionalinė švietimo agentūra, *Informacinių technologijų ugdymo bendroji programa* (2011), luettu 3.11.2022, https://duomenys.ugdome.lt/saugykla/bp/2016/vidurinis/IT_7_priedas.pdf, 14-15.
[482] European Commission, *Digital Education*, 120.
[483] "Information and Information Technologies Security," *Vilnius Gediminas Technical University*, luettu 1.12.2022, https://vilniustech.lt/for-international-students/degree-programmes-in-english-language-20222023/graduate-studies/information-and-information-technologies-security/102373?lang=2.
[484] "Computer Modelling," *Vilnius University*, luettu 1.12.2022, https://www.vu.lt/en/studies/master-studies/computer-modelling#programme-structure.
[485] "Information and Information Technology Security," *Kaunas University of Technology*, luettu 1.12.2022, https://admissions.ktu.edu/programme/m-information-and-information-technology-security/.
[486] "Cybersecurity Management," *Mykolas Romeris University*, luettu 1.12.2022, https://www.mruni.eu/en/study_program/cybersecurity-management/.
[487] Henkilökohtainen tiedonanto tutkijalle, 6.11.2022.
[488] "Security awareness training," *Cyber security academy*, luettu 31.10.2022, https://www.cybersecurityacademy.lt/en-security-awareness.
[489] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[490] "Cybersecurity bootcamp," *LCC International university*, luettu 31.10.2022, https://lcc.lt/cybersecurity-bootcamp.
[491] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[492] Maria Bada ja Carolin Weisser, *Cybersecurity Capacity Review Republic of Lithuania*, Global Cyber Security Capacity Centre 2017, 36.
[493] "Safer Internet day in Lithuanian libraries," *International Federation of Library Associations and Institutions,* luettu 31.10.2022, https://www.ifla.org/news/safer-internet-day-in-lithuanian-libraries/.
[494] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[495] "Lithuan Safer Internet Centre," *European schoolnet*, luettu 31.10.2022, https://www.betterinternetforkids.eu/sic/lithuania.
[496] "Kurkime *saugesnį* internetą kartu," *Draugiškas Internetas*, luettu 31.10.2022, www.draugiskasinternetas.lt.
[497] Henkilökohtainen tiedonanto tutkijalle, 6.11.2022.
[498] "Atpažink ir atremk grėsmes internete," *Government of the Republic of Lithuania,* luettu 31.10.2022*,* https://sustiprinkimuniteta.lt/.
[499] "Digital Week events 2022 in Lithuania," *Digital Skills and Jobs Platform*, luettu 31.10.2022, https://digital-skills-jobs.europa.eu/en/latest/events/digital-week-2022-events-lithuania.
[500] "All digital weeks event in Lithuania-Invited all ages," *All digital week*, luettu 31.10.2022, https://www.alldigitalweek.eu/all-digital-week-2022-events-in-lithuania-invited-all-ages/.
[501] "Connected Lithuania," *Digital Skills and jobs Platform*, luettu 1.11.2022, https://digital-skills-jobs.europa.eu/en/inspiration/good-practices/connected-lithuania.
[502] "Safer Internet for Kids (quiz)," *Langas į ateitį,* https://www.prisijungusi.lt/savarankiskas-mokymasis/saugesnis-internetas-vaikams-viktorina/.
[503] "Be safe in cyberspace," *Communications Regulatory Authority of the Republic of Lithuania*, luettu 31.10.2022, https://www.esaugumas.lt/.
[504] "A safer Internet," *Langas į ateitį*, luettu 1.11.2022, https://www.prisijungusi.lt/savarankiskas-mokymasis/saugesnis-internetas/.
[505] Henkilökohtainen tiedonanto tutkijalle, 6.11.2022.
[506] Henkilökohtainen tiedonanto tutkijalle, 6.11.2022.
[507] Aelita Skaržauskienė, Monika Mačiulienė ja Ornela Ramašauskaitė, *The digital media in Lithuania: Combating disinformation and fake news, Acta Informatica Pragensia* 9.2 (2020), 1, 13-15.
[508] Rūta Valavičiūtė, *Kibernetinio saugumo kultūros vystymas Lietuvos bendrojo ugdymo mokyklose*, PhD Thesis, Mykolo Romerio universitetas (2022), 89.
[509] Henkilökohtainen tiedonanto tutkijalle, 6.11.2022.
[510] Henkilökohtainen tiedonanto tutkijalle, 14.6.2022.
[511] Agnė Brilingaitė, Linas Bukauskas, Virgilijus Krinickij ja Eduardas Kutka, *Environment for cybersecurity tabletop exercises, ECGBL 2017 11th European Conference on Game-Based Learning*, Academic Conferences and publishing limited, 2017.
[512] "Awareness of the DigComp framework among the CEPIS community," *Council of European Professional Informatics Societies*, luettu 11.11.2022, https://cepis.org/digcomp-report-2021/.
[513] Henkilökohtainen tiedonanto tutkijalle, 6.11.2022.
[514] Henkilökohtainen tiedonanto tutkijalle, 22.11.2022.
[515] Henkilökohtainen tiedonanto tutkijalle, 6.11.2022.

3.13. Luxemburg

ITU, Global Cybersecurity Index (GCI) 2020	13/182 (Global), 7/46 (Europe)
National Cyber Security Index (NCSI) 2022	39/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	8/27

3.13.1. Strategiset kyberkoulutuslinjaukset

Luxemburgin hallitus julkaisi vuonna 2021 kansallisen kyberturvallisuusstrategian IV vuosille 2021–2025. Sen kolme strategista päätavoitetta ovat 1) luottamuksen rakentaminen digitaaliseen maailmaan ja ihmisoikeuksien suojeleminen verkossa, 2) Luxemburgin digitaalisten infrastruktuurien turvallisuuden ja kestävyyden vahvistaminen ja 3) luotettavan, kestävän ja turvallisen digitaalitalouden kehittäminen. Kansalaisia suoraan koskettavat toimenpiteet kuuluvat erityisesti ensimmäisen päätavoitteen alle. Ponnisteluja lasten ja nuorten oikeuksien suojelemiseksi verkossa jatketaan lisäämällä kansalaisten tietoisuutta kyberturvallisuusuhkista. Tehtävä kuuluu erityisesti hallituksen vuonna 2010 käynnistämälle ja National Youth Servicen (SNJ, Service National de la Jeunesse) koordinoimalle BEE SECURE -hankkeelle. Kyberturvallisuusalalla aliedustettuina olevia väestöryhmiä, kuten naisia, tyttöjä ja maahanmuuttajataustaisia henkilöitä, kannustetaan hakeutumaan koulutukseen ja alalle. Kyberturvallisuusasioita käsitellään ministeriöiden välisessä työryhmässä, jonka tavoitteena on parantaa kansalaisten digitaalista osallisuutta. Kyberturvallisuuskoulutusta kehitetään vastaamaan paremmin yhteiskunnan tarpeita, ja tietoisuutta kyberturvallisuusalan ammateista lisätään.[516]

Digitalisaatioministeriö (Ministère de la Digitalisation) on laatinut kansallisen digitaalisen osallisuuden toimintasuunnitelman (National Action Plan for Digital Inclusion) vuosille 2021–2024. Sen tavoitteena on parantaa sosioekonomisen yhteenkuuluvuuden kannalta tärkeää digitaalista osallisuutta, torjua väestön digitaalista jakautumista ja tukea digitaalista kansalaisuutta. Toimintasuunnitelma keskittyy digitaalisen lukutaidon ja digitaalisen kansalaisuuden kehittämiseen, jotta kansalaiset voisivat käyttää digitaalisia väyliä itsenäisemmin ja turvallisemmin. Yksi keskeisistä toimenpiteistä on verkkoturvallisuustietoisuuden lisääminen. Digitaalisten taitojen kehitystä tuetaan nuoresta iästä lähtien, muun muassa opetus-, lapsi- ja nuorisoministeriön (Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse) digitaalisen koulutuksen Einfach Digital -strategian kautta. Digitaalista koulutusta tarjotaan eri taitotasoille ja ikäryhmille sekä useilla eri kielillä. Digitaalisen osallisuuden toimintasuunnitelmassa huomioidaan erityisesti ryhmät, joilla on tyypillisesti puutteita digitaalisessa osaamisessa, kuten seniorit ja toimintarajoitteiset.[517]

3.13.2. Kyberkansalaistaitojen opettamisen nykytila

Digitaalisen osallisuuden toimintasuunnitelmassa on useita aloitteita, jotka tähtäävät kansalaisten verkkoturvallisuustietoisuuden parantamiseen. Zesummen Digital -verkkoportaaliin on koottu digitaalista osallisuutta edistäviä toimijoita, koulutustarjontaa, materiaaleja ja julkaisuja. Osa niistä painottuu kyberturvallisuuteen. Talousministeriön (Ministère de l'Économie) CYBERSECURITY Luxembourg -verkkosivusto kokoaa yhteen julkisia ja yksityisiä kyberturvallisuuteen keskittyviä toimijoita. Sivustolla on lisäksi muun muassa kyberturvallisuuteen liittyviä uutisia, materiaaleja ja tapahtumia. Luxemburgin uudistettu kyberturvallisuusviranomainen Luxembourg House of Cybersecurity (LHC) (aiemmin SECURITYMADEIN.LU) julkistettiin lokakuussa 2022. Talousministeriön alla toimivan tahon tavoitteena on edistää avointa ja luotettavaa kyberturvallisuustietotaloutta. Toiminta perustuu kyberturvallisuustoimijoiden väliseen yhteistyöhön ja 20 vuoden aikana kertyneeseen asiantuntemukseen kyberturvallisuuden alalta. LHC tarjoaa tietoa erilaisista hankkeista, kuten kansalaisten kyberturvallisuusosaamisen kehittämiseen tähtäävästä BEE SECUREsta. Lisäksi se

toimii Luxemburgin kansallisena kyberturvallisuuden koordinaatiokeskuksena (NCC), jonka yksi tehtävistä on koordinoida kyberturvallisuuden koulutus- ja tietoisuusasioita. LHC:n alla toimii CERT-kyberturvallisuuskeskus CIRCL ja kyberturvallisuuden osaamiskeskus NC3. NC3 auttaa erityisesti yrityksiä testaamaan ja parantamaan henkilöstön kyberturvallisuusosaamista. Keskeinen koulutusmenetelmä on ROOM#42-simulaattori, jossa osallistujat harjoittelevat kyberturvallisuustaitoja realistisessa ja intensiivisessä kyberiskusimulaatiossa.[518,519]

Luxemburgin kansalaisten tietämystä digitaalisen turvallisuuden käytännöistä ja samalla luottamusta digitaaliseen toimintaympäristöön parannetaan erilaisten koulutusten, tietoisuuskampanjoiden ja materiaalien avulla. Tämä tehtävä kuuluu erityisesti BEE SECURE -hankkeelle. BEE SECURE toimii myös Luxemburgin Safer Internet Centerinä (SIC) ja on näin mukana kansainvälisissä Insafe-, INHOPE- ja Better Internet for Kids -verkostoissa. BEE SECUREn tavoitteena on edistää uusien informaatioteknologioiden turvallista, vastuullista ja positiivista käyttöä kansalaisten keskuudessa. Se neuvoo lapsia ja nuoria käyttämään uusia teknologioita turvallisesti, tukee vanhempia, opettajia ja kasvattajia hyvän roolimallin antamisessa lapsille ja nuorille ja vastaa senioreiden jatkuvasti kasvavaan tuen tarpeeseen kyberturvallisuusasioissa. Toiminnan pääalueet ovat opetussisältöjen kehittäminen, opettaminen, kouluttaminen, neuvominen, tietoisuuskampanjointi, seuranta ja laittoman sisällön raportointi.[520]

Verkkoturvallisuuden BEE SECURE -opetusohjelma lapsille ja nuorille käynnistettiin peruskouluissa vuonna 2011. Tämän maanlaajuisen ja jatkuvan hankkeen tavoitteena on tarjota koululaisille tarvittavat taidot digitaalisen toimintaympäristön turvalliseen ja vastuulliseen hyödyntämiseen. Opetus on pakollista seitsemäsluokkalaisille, mutta sitä on tarjolla myös muille ikäryhmille. Peruskoulujen BEE SECURE -opetus sisältää erityisesti verkkoturvallisuuteen ja jonkin verran myös medialukutaitoon liittyviä aiheita. Tunneilla keskustellaan muun muassa internetin rakenteesta ja toiminnasta, kyberkiusaamisesta, tietojenkalastelusta, haittaohjelmista, tietosuojasta, salasanoista ja tekijänoikeuksista. Opetus kiteytyy kolmeen pääviestiin: 1) internet perustuu tekniseen infrastruktuuriin, eikä se ole mikään ”maaginen juttu”, 2) internet ei unohda mitään ja 3) itsesi ja tietojesi suojaaminen on omissa käsissäsi. Lukuvuodesta 2021–2022 lähtien yläkouluissa on opetettu Digital Sciences -oppiainetta, jonka yksi oppimistavoitteista on digitaalitekniikan vastuullinen ja turvallinen käyttö.[521,522,523]

BEE SECUREn järjestämässä opetuksessa hyödynnetään erilaisia opetusmenetelmiä ja -välineitä. Opettajat käyttävät opetuksen tukena PowerPoint-esityksiä, jotka sisältävät teoriaa visuaalisessa muodossa, ja teoriaa tukevia aktiviteetteja, kuten pelejä, tietovisoja ja keskustelunaiheita. Opetus on interaktiivista ja osallistavaa. Pienten lasten opetuksessa käytetään apuna tarinankerrontaa. Erityisesti nuorten kanssa pyritään mahdollisimman vapaamuotoiseen keskusteluun. Opettajat nostavat esiin erilaisia verkkoturvallisuuden riskejä, mutta antavat nuorten viedä keskustelua eteenpäin. Opetuskerrat kestävät yleensä puolestatoista kahteen tuntiin. Opetusta on tarjolla saksan, ranskan, luxemburgin ja englannin kielillä.[524]

Muodollisen opetuksen lisäksi BEE SECURE järjestää epämuodollista koulutusta ja kampanjointia lapsille, nuorille, opettajille, kasvattajille, vanhemmille, senioreille ja yleisesti kaikille kansalaisille.[525] Alle kouluikäisille suunnatulla Bee.lu-sivustolla Bibi-mehiläinen ystävineen seikkailee kyberturvallisuuden teemoja käsittelevissä saduissa. Sivustolla on lapsille sopivia aktiviteetteja, kuten askartelua ja värittämistä.[526] Senioreille suunnatulla Silversurfer.lu-sivustolla on kyberturvallisuuteen liittyvää tietoa, uutisia ja tapahtumia. Silver Surfer järjestää senioreille tilaisuuksia, joissa käsitellään uusien teknologioiden turvallista käyttöä. Seniorit voivat hakea apua kyberturvallisuuspulmiin Silver Surferin auttavasta puhelimesta ja sähköpostitse.[527]

BEE SECURE ja voittoa tavoittelematon yhteisö GoldenMe ovat hiljattain tehneet sopimuksen senioreille järjestettävistä cyber-café-tilaisuuksista. Seniorit voivat tuoda tilaisuuksiin oman tabletin, tietokoneen tai kännykän ja saada käyttäjätukea vapaaehtoisilta.[528,529] Iltapäiväkerhoissa ja nuorisokeskuksissa ympäri maata järjestetään vapaamuotoista kyberturvallisuusopetusta. 9–12-vuotiaille suunnatut DigiRallye-tapahtumat ovat suosittuja. Koronaviruspandemian myötä tapahtumaa on alettu järjestää myös virtuaalisesti. Tapahtumatilaan, esimerkiksi koulurakennukseen, järjestetään tehtäväpisteitä, joissa lapset suorittavat kyberturvallisuuteen liittyviä aktiviteetteja. Kehitysvammaisille nuorille on tehty kyberkiusaamista käsittelevä opetuspaketti.

Vanhemmille järjestetään omia vanhempainiltoja, joissa vanhemmat voivat esittää lastensa digitaalisiin laitteisiin ja internetin käyttöön liittyviä kysymyksiä. Lisäksi BEE SECUREn verkkosivuilla on saatavilla runsaasti tietoa.[530,531]

BEE SECURE kouluttaa omat freelance-opettajansa, jotka opettavat esimerkiksi kouluissa ja nuorisokeskuksissa. Alkukoulutuksen lisäksi opettajat osallistuvat säännöllisiin opettajatapaamisiin. Muiden opettajien ja vanhempien antaman palautteen perusteella konsepti on toimiva. Opetus on kouluille ilmaista. Jokaisen opetuskerran jälkeen sekä oppilaat että opettajat täyttävät palautelomakkeen, jotta BEE SECUREn tarjoamaa opetusta voidaan jatkuvasti kehittää tehokkaammaksi. Vuosina 2011–2018 yli 28 000 oppilaalta ja yli 5 000 opettajalta kerättyjen palautteiden perusteella tällainen huolellisesti suunniteltu ja jatkuvasti arvioitava kyberturvallisuusopetus tukee hyvin lasten ja nuorten ymmärrystä aiheesta ja lisää opettajien halukkuutta ottaa kyberturvallisuus osaksi opetussuunnitelmaa. Suurin osa oppilaista piti opetusta hyödyllisenä.[532,533]

Lycée Guillaume Krollissa voi opiskella lukion jälkeen kaksivuotisen kyberturvallisuuskoulutuksen (Brevet de technicien supérieur en Cybersécurité).[534] Luxemburgin yliopistossa on puolestaan tarjolla Information System Security Management -maisteriohjelma.[535] Digital Learning Hub on tarjonnut vuodesta 2021 alkaen IT-opetusta, johon kuuluu myös kyberturvallisuuskursseja. Kurssit ovat ilmaisia työttömille, opiskelijoille ja valtion palveluksessa oleville. Digital Learning Hubissa on naisille räätälöityjä omia koulutusohjelmia, jotta he löytäisivät helpommin uusia mahdollisuuksia digitaalisuuden parissa. Myös Luxembourg Women Cyberforce, Women In Digital Empowerment ja Cyberwayfinder ovat hankkeita, joiden tavoitteena on houkutella erityisesti naisia digitaalisten tehtävien ja kyberturvallisuuden pariin.[536,537]

Kyberturvallisuustietoisuuden lisäämiseksi Luxemburgissa järjestetään paljon erilaisia kyberturvallisuuteen liittyviä tapahtumia sekä verkossa että fyysisesti, kuten kampanjoita, kilpailuja ja kokoontumisia. Luxemburgissa pidetään vuosittain kansan hyvin tuntema Cybersecurity Week Luxembourg, joka kokoaa yhteen kyberturvallisuuden ekosysteemin toimijoita. Konferenssi ja messualue ovat avoimia ja ilmaisia kaikille.[538,539]

3.13.3. Kansalliset erityispiirteet

Luxemburg on hyvin sitoutunut maan kyberturvallisuuden parantamiseen, ja kansalaisten kyberturvallisuustietoisuuden lisääminen otettiin tehtäväksi jo yli 20 vuotta sitten. Kansallinen kyberturvallisuuden ekosysteemi perustuu julkisten ja yksityisten sidosryhmien tiiviiseen yhteistyöhön. Talousministeriön keskeinen rooli tekee Luxemburgista ainutlaatuisen Euroopassa: kyberturvallisuutta ei pidetä vain puolustuskysymyksenä vaan myös taloudellisesti merkittävänä asiana.[540,541] Kyberturvallisuuskoulutusta annetaan pääasiassa kouluissa ja työpaikoilla. Kohderyhminä ovat erityisesti lapset, nuoret, opettajat, vanhemmat, seniorit ja työntekijät. Laadukasta opetusmateriaalia on tarjolla runsaasti. Haasteena on se, miten koko väestö saadaan osallistumaan koulutuksiin ja tutustumaan materiaaleihin.[542]

3.13.4. Kyberkansalaistaitojen määrittäminen

Medienkompass on kansallinen mediakasvatuksen viitekehys, jossa on sovellettu Euroopan komission Digital Competence Framework for Citizens -viitekehystä. Medienkompassiin sisältyy viisi osaamisaluetta: tiedot ja informaatio, viestintä ja yhteistyö, sisällön tuottaminen, tietosuoja ja tietoturva sekä digitaalinen maailma. Tietosuojaan ja tietoturvaan kuuluu laitteiden suojaaminen sekä tietojen ja yksityisyyden suojaaminen. Tavoitteena on tunnistaa ja ymmärtää digitaalisen ympäristön riskit ja uhat (esimerkiksi haittaohjelmat, sosiaalinen manipulointi, identiteettivarkaudet) ja tietää tarvittavat turvallisuustoimenpiteet (esimerkiksi virustorjuntaohjelman ja palomuurin käyttö). Lisäksi jokaisen tulisi osata suojata henkilötietonsa ja yksityisyytensä digitaalisessa toimintaympäristössä ja olla tietoinen tietosuojaan liittyvistä oikeuksistaan.[543]

Viitteet

[516] Le Gouvernement Du Grand-Duché De Luxembourg, *National Cybersecurity Strategy IV* (2021), 8-10.
[517] Ministry for Digitalisation, *National Action Plan for Digital Inclusion, For a digitally inclusive society* (2021).
[518] Ministry for Digitalisation, *National Action Plan for Digital Inclusion, For a digitally inclusive society* (2021).
[519] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[520] Le Gouvernement Du Grand-Duché De Luxembourg, *National Cybersecurity Strategy IV* (2021), 24.
[521] Aline Tiemann, André Melzer ja Georges Steffgen, *Nationwide Implementation of Media Literacy Trainings on Internet Safety* (2021), Communications, 46 (3), 394-418, https://doi.org/10.1515/commun-2021-0049.
[522] Henkilökohtainen tiedonanto tutkijalle, 10.6.2022.
[523] Ministry for Digitalisation, *National Action Plan for Digital Inclusion, For a digitally inclusive society* (2021), 29.
[524] Henkilökohtainen tiedonanto tutkijalle, 10.6.2022.
[525] ”BEE SECURE,” luettu 31.10.2022, https://www.bee-secure.lu/de/.
[526] ”BEE SECURE, bee.lu,” luettu 31.10.2022, https://www.bee.lu/.
[527] ”BEE SECURE, silversurfer.lu,” luettu 31.10.2022, https://silversurfer.lu/de/.
[528] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[529] ”GoldenMe,” luettu 1.11.2022, https://en.goldenme.me/.
[530] Henkilökohtainen tiedonanto tutkijalle, 10.6.2022.
[531] ”BEE SECURE,” luettu 31.10.2022, https://www.bee-secure.lu/de/.
[532] Aline Tiemann, André Melzer ja Georges Steffgen, *Nationwide Implementation of Media Literacy Trainings on Internet Safety* (2021).
[533] Henkilökohtainen tiedonanto tutkijalle, 10.6.2022.
[534] ”BTS Cybersecurity,” *Lycée Guillaume Kroll*, luettu 31.10.2022, https://www.lgk.lu/bts/cyb/.
[535] ”Master in Information System Security Management,” *Université Du Luxembourg*, luettu 31.10.2022, https://wwwen.uni.lu/studies/fstm/master_in_information_system_security_management.
[536] ”Digital Learning Hub,” *Le Gouvernement Du Grand-Duché De Luxembourg*, luettu 31.10.2022, https://dlh.lu/.
[537] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[538] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[539] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 111-114.
[540] Cybersecurity Luxembourg, *Luxembourg Cybersecurity Ecosystems, Key Insights* (2020), 4.
[541] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 111-114.
[542] Henkilökohtainen tiedonanto tutkijalle, 25.10.2022.
[543] Script, *Medienkompass Medienkompetent lehren und lernen*, Einfach Digital (2022).

3.14. Malta

ITU, Global Cybersecurity Index (GCI) 2020	49/182 (Global), 29/46 (Europe)
National Cyber Security Index (NCSI) 2022	72/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	6/27

3.14.1. Strategiset kyberkoulutuslinjaukset

Maltan kansallinen kyberturvallisuusstrategia vuosille 2023–2026 julkaistiin marraskuussa 2022. Se on osa Digital Malta -kattostrategiaa ja pohjautuu vuonna 2016 julkaistuun kyberturvallisuusstrategiaan. Strategian mukaan kaikilla, myös kansalaisilla, on vastuu suojata kybertoimintaympäristöä. Koko yhteiskunnan tulee toimia turvallisesti ja harkiten verkossa. Yksi strategian neljästä kulmakivestä on kyberosaaminen ja -kulttuuri, joita vahvistetaan eri toimenpiteillä. Kyberturvallisuuskapasiteettia parannetaan jatkuvilla ja kattavilla tietoisuusohjelmilla, jotka edistävät ”turvallisuus ensin” -kulttuuria. Kyberturvallisuuskoulutusta lisätään sekä perusopetuksessa että jatkokoulutuksissa, ja oppilaitosten välistä yhteistyötä vahvistetaan. Opettajille annetaan säännöllisesti digitaalisten taitojen ja kyberturvallisuusosaamisen koulutusta. Julkisen sektorin työntekijöille ja merkittäville sidosryhmille tarjotaan kyberturvallisuuskoulutusta, sillä julkisella sektorilla käsitellään runsaasti sensitiivistä tietoa. Sekä ICT-ammattilaisten että muiden alojen ammattilaisten ja johdon kyberturvallisuuskoulutus- ja sertifiointimahdollisuuksia lisätään. Naisia kannustetaan osallistumaan kyberturvallisuushankkeisiin. Kyberturvallisuuteen liittyvää tutkimus- ja innovaatiotyötä tuetaan riittävästi.[544,545]

Digital Malta -kattostrategian alle kuuluu myös marraskuussa 2022 julkaistu uusi National eSkills Strategy 2022–2025 -strategia, joka on jatkoa National eSkills Strategy 2019–2021 -strategialle. Strategian tavoitteena on edelleen kohentaa maltalaisten digitaalista osaamista. Jokaisen maltalaisen tulisi iästä, sukupuolesta, mahdollisista toimintarajoitteista, koulutuksesta, taloudellisesta asemasta tai etnisyydestä riippumatta kasvaa digitaaliseksi kansalaiseksi, jolla on oikeuksia, velvollisuuksia ja kykyjä käyttää tieto- ja viestintätekniikkaa. Digitaalisia taitoja ei omaksuta vain muodollisen opetuksen kautta, vaan jo varhaislapsuudessa ja myöhemmin työelämässä. Jokaisella maltalaisella tulee olla riittävät tiedot, taidot ja kyvyt, jotta he pystyvät käyttämään digitaalisia välineitä turvallisesti ja eettisesti. Tähän luetaan myös kyberturvallisuusosaaminen. Tällä osaamisella katsotaan olevan jopa merkittävä vaikutus kansalaisten hyvinvointiin ja sietokykyyn, ja se lisää myös luottamusta digitaalisiin teknologioihin. Oppilailla on oikeus saada digitaalisen lukutaidon opetusta varhaiskasvatuksesta peruskoulun loppuun asti. Digitaalinen lukutaito muutetaan omaksi oppiaineekseen. Työväestön digitaalisten taitojen tulee olla riittävät, jotta he pärjäävät työelämässä ja työnantajat pysyvät kilpailukykyisinä. Opettajien ja opiskelijoiden hyvät digitaaliset taidot edesauttavat menestymistä digitaalisissa oppimisympäristöissä. Kansalaisia kannustetaan ICT-alalle ja digitaalisen sektorin työtehtäviin.[546,547]

3.14.2. Kyberkansalaistaitojen opettamisen nykytila

Maltan tieto- ja teknologiavirasto MITA (Malta Information Technology Agency) koordinoi Maltan kyberturvallisuusasioita. Se sai vuonna 2016 tehtäväksi järjestää ja valvoa kyberturvallisuusstrategiassa suunniteltuja, kansalaisille tarkoitettuja kyberturvallisuuden kampanjoita ja koulutuksia. Myös muita viranomaisia, kuten opetusministeriö (Ministry for Education, Sport, Youth, Research and Innovation), osallistuu tavoitteen toteutukseen. Koulutus- ja tietoisuuskampanjatavoitteen täyttämiseksi lanseerattiin jatkuva Cyber Security Malta -kampanja. Kampanjassa nostetaan esiin ajankohtaisia kyberturvallisuusriskejä. Lokakuussa 2022 Maltalla avattiin kansallinen kyberturvallisuuden koordinointikeskus NCC (National Cybersecurity Coordination Centre) ja samalla Cyber Security Maltaan liittyvä sisältö siirtyi NCC:lle. Uuden keskuksen tehtävänä on tarttua

kyberturvallisuuden tarjoamiin mahdollisuuksiin, lisätä tietoisuutta, tukea koulutusohjelmia, kannustaa tiedonvaihtoon ja yhteistyöhön, edistää kyberammattilaisten kasvua, helpottaa kyberinvestointeja ja tarjota tukea paikalliselle ekosysteemille. Maltan NCC:n toiminnasta vastaa MITA. NCC:n uusilla verkkosivuilla on Maltan kyberturvallisuusstrategian lisäksi muun muassa kyberturvallisuuteen liittyviä artikkeleita, uutisia ja ohjeita sekä tietoa tapahtumista. NCC:n sosiaalisen median kanavilla nostetaan kansalaisten kyberturvallisuustietoisuutta säännöllisten julkaisujen avulla. YouTube-kanavalla julkaistaan erilaisia ohje- ja vinkkivideoita. Vuoden 2022 videokampanjassa maltalaiset muusikot jakavat kansalaisille erilaisia kyberturvallisuusvinkkejä. MITA järjestää vuosittain kansallisen Cyber ROOT -kyberturvallisuuskonferenssin.[548,549,550]

Tietojenkäsittelyä opetetaan omana erillisenä ja pakollisena aineena peruskoulussa yläkoulusta alkaen. Tietojenkäsittelyyn kuuluu turvallisuuteen liittyviä oppimistavoitteita, jotka ovat pakollisia kaikille. [551] Digitaalinen lukutaito on määritelty keskeiseksi oppiainerajat ylittäväksi teemaksi perusopetuksessa. Verkkoetiketti ja turvallisuuskäytännöt ovat osa digitaalista lukutaitoa. [552] Directorate for Learning and Assessment Programmes (DLAP) on vastuussa peruskoulujen opetussuunnitelmasta, opetuksesta, arvioinnista ja seurannasta. DLAP on mukana BeSmartOnline!-hankkeessa ja tuo kouluihin verkkoturvallisuuden opetusta Personal, Social and Career Development -oppiaineen (PSCD) kautta. PSCD on pakollinen oppiaine lukuvuosina 3–11, ja siihen kuuluu osana verkkoturvallisuus. Käsiteltäviä aiheita ovat muun muassa digitaalinen jalanjälki, digitaalinen kansalaisuus, internetin turvallisuus, kyberkiusaaminen, digitaaliset pelit ja kriittinen medialukutaito. Tunnit ovat interaktiivisia, ja niihin voi osallistua kerrallaan korkeintaan 16 oppilasta. Oppilaat istuvat piirissä, mikä edistää aktiivista keskustelua, reflektointia ja osallistumista. Opettajat hyödyntävät erilaisia opetusmenetelmiä, kuten pelejä, roolileikkejä ja pienryhmätyöskentelyä. Opetuksen tueksi on tuotettu erilaisia materiaaleja, kuten oppaita verkkoturvallisuudesta.[553]

Peruskoulun etiikan oppitunneilla opetetaan kyberturvallisuutta osana digitaalisen kansalaisuuden viitekehystä. Etiikkaa tarjotaan 5–16-vuotialle oppilaille, jotka eivät osallistu uskonnon opetukseen. Tunneilla painotetaan vastuullisen verkkokäyttäytymisen eettisiä arvoja. 5–10-vuotiaille lapsille opetetaan, miten internetissä viestitään vastuullisesti omaa ja muiden turvallisuutta ja hyvinvointia kunnioittaen ja millainen on hyvä salasanahygienia. Oppilaita neuvotaan, miten kyberkiusaamiselta ja verkkovaanijoilta voi suojautua. 11–16-vuotiaiden nuorten kanssa keskustellaan esimerkiksi verkkoelämän ja muun elämän tasapainosta, maineenhallinnasta, kyberkiusaamisesta, seksiviestittelystä, vihapuheesta ja verkossa radikalisoitumisesta.[554] Lisäksi kyberturvallisuusalan asiantuntijat vierailevat kouluissa puhumassa kyberturvallisuudesta.[555] American University of Maltassa voi suorittaa maisterintutkinnon kyberturvallisuudesta.[556] Useat maltalaiset yritykset tarjoavat aikuisille kyberturvallisuuskoulutusta.[557] B SECURE -hanke on järjestänyt kyberturvallisuuskursseja yrityksille ja CSIRT Malta kyberturvallisuuskoulutusta jäsenilleen.[558]

Maltan hallituksen vuonna 2014 perustaman eSkills Malta Foundationin tehtävänä on edistää maltalaisten digitaalisia taitoja ja kehittää Maltan IT-alaa. Se toteuttaa yhteistyökumppaneidensa kanssa erilaisia digitaalisen osaamisen vahvistamiseen tähtääviä hankkeita. Esimerkiksi naisille ja senioreille on tarjolla kohdennettuja koulutuksia digitaalisen osallisuuden parantamiseksi. eSkills Malta Foundation järjestää erilaisia tapahtumia, vierailee kouluissa, julkaisee tutkimuksia ja antaa suosituksia päättäjille. Agendalla on myös kyberturvallisuusasiat. Vuonna 2020 eSkills Malta Foundation ja talousportaali ĠEMMA aloittivat yhteistyön, jonka tuloksena syntyi petosten ja huijausten vaaroista kertovia materiaaleja. Vuonna 2021 eSkills Malta Foundation järjesti useita Digital Skills Bootcamps -koulutuksia eri kohderyhmille ja rahoitti erilaisia digitaalisen osaamisen kursseja.[559,560]

BeSmartOnline! on toiminut Maltan Safer Internet Centrenä (SIC) vuodesta 2010, ja se on osa Euroopan komission tukemia Insafe-, INHOPE- ja Better Internet for Kids -verkostoja. BeSmartOnline!-hanketta koordinoi Foundation for Social Welfare Services (FSWS), ja siinä on mukana Office of the Commissioner for Children, DLAP ja Maltan poliisin verkkorikollisuuden yksikkö (Cyber Crime Unit). Yhteenliittymällä on tukenaan useita strategisia kumppaneita, jotka ovat mukana hankkeen neuvottelukunnassa. BeSmartOnline!:n tarkoituksena on

edistää internetin ja teknologioiden turvallista käyttöä. Kohderyhminä ovat erityisesti lapset ja nuoret. Maltan SIC tuottaa erilaisia opetusmateriaaleja, artikkeleita ja uutisia. Sen Facebook-sivuilla jaetaan tietoa muun muassa ajankohtaisista tapahtumista ja kampanjoista. BeSmartOnline! on usein näkyvästi esillä erilaisissa tapahtumissa, kuten messuilla.[561,562]

Maltan poliisin verkkorikollisuuden yksikön tehtävänä on tutkia ja ehkäistä rikoksia, joissa kohteena tai välineenä on tietokone. Verkkorikollisuuden yksikkö vierailee säännöllisesti muun muassa kouluissa, nuorisojärjestöissä ja erilaisissa tapahtumissa. Tarkoituksena on edistää internetin vastuullista käyttöä ja neuvoa, miten verkkorikollisuudelta voi parhaiten suojautua. Poliisin verkkosivuilla on kansalaisille osoitettuja vinkkejä internetin turvalliseen käyttöön.[563]

Vuonna 2021 MITA toteutti senioreille suunnatun kampanjan digitaalisesta turvallisuudesta. Mediassa ja sosiaalisessa mediassa näkyvyyttä saaneen kampanjan kasvoina oli suosittu maltalainen näyttelijä Narcy Calamatta.[564] Senioreille on järjestetty ympäri Maltaa ja Gozoa kohdennettuja työpajoja, joissa keskustellaan kyberturvallisuudesta ja käydään läpi erilaisia tapoja toimia internetissä turvallisesti. Senioreille on tehty myös seitsenosainen Digital Age -videosarja, jonka tarkoituksena on auttaa senioreita huolehtimaan omasta digitaalisesta turvallisuudestaan.[565]

Malta on pärjännyt hyvin DESI-vertailussa, mutta kansalaisten kyberturvallisuusosaamista tulisi vielä parantaa. Osaamisen parantamiseksi tarvittaisiin keskitetty ja kaikkia ikäryhmiä palveleva hanke.[566] Farrugian (2020) mukaan lapsille voisi kehittää verkkoturvallisuuteen liittyviä VR-pelejä, joiden kautta he oppisivat hallitsemaan internetin riskejä turvallisessa ympäristössä. Medialukutaidon opettamiseen voitaisiin kehittää tekoälyä hyödyntäviä alustoja. Tekoälyn avulla tunnistettaisiin paremmin käyttäjän tarpeet ja pystyttäisiin tarjoamaan jokaiselle käyttäjälle parhaiten soveltuvia sisältöjä. Opetusmateriaalit tulisi julkaista sekä englannin että maltan kielillä.[567]

3.14.3. Kansalliset erityispiirteet

Lorleen Farrugia (2020) tutki väitöskirjassaan 9–12-vuotiaiden maltalaislasten käsityksiä verkon riskeistä ja näiden käsitysten vaikutusta lasten verkkokäyttäytymiseen. Neljä viidestä tutkimukseen osallistuneesta lapsesta ei pitänyt internetiä turvallisena paikkana. Vaarallisimpina riskeinä pidettiin tekniseen turvallisuuteen liittyviä riskejä eli hakkerointia ja viruksia. Kolme neljästä oli kohdannut verkossa riskejä. Niistä yleisimpiä olivat olleet virukset ja ponnahdusikkunat. Moni lapsista oli tällaisissa tilanteissa hakenut tukea esimerkiksi vanhemmiltaan. Yli 20 prosentilla tutkimuksen lapsista ei joko ollut minkäänlaista verkkoturvallisuuteen liittyvää osaamista tai he eivät olleet tehneet minkäänlaisia turvallisuuteen liittyviä toimenpiteitä. Tutkimustuloksissa todetaan, että lasten suojelemiseksi verkkoriskeiltä tarvitaan monitahoista ja monipuolista yhteistyötä. Maltan kouluissa annettavaa opetusta olisi uudistettava. Vanhempien ja erityisesti opettajien osaamistasoa olisi parannettava.[568]

3.14.4. Kyberkansalaistaitojen määrittäminen

Digitaalisten taitojen tulisi olla vähintään perustasoa, jotta kansalaiset pystyvät toimimaan digitaalisessa ympäristössä. Perustaitoihin kuuluvat laitteistojen ja ohjelmistojen käyttö ja perustoiminnot verkossa, mukaan lukien kyberturvallisuusosaaminen.[569] Maltan vuoden 2016 kansallisessa kyberturvallisuusstrategiassa kansalaisia kehotetaan noudattamaan vähintään perustason kyberturvallisuushygieniaa. Esimerkkeinä tähän liittyvistä taidoista annetaan henkilötietojen huolellinen käsittely ja jakaminen verkossa, ohjelmistopäivitysten ja virustorjuntaohjelmien asentaminen sekä perusturvatoimien, kuten vahvojen salasanojen käytön, omaksuminen. Lisäksi jokaisen tulisi mahdollisuuksien mukaan pysyä valppaana omiin verkkotileihin kohdistuvien epäilyttävien toimien varalta.[570]

Viitteet

[544] Government of Malta, MITA, *National Cyber Security Strategy 2023-2026* (2022).
[545] Ministry for Competitiveness and Digital Maritime and Services Economy, MITA, *Malta Cyber Security Strategy* (2016.)
[546] Government of Malta, eSkills Malta Foundation, *National eSkills Strategy 2022-2025* (2022).
[547] Government of Malta, eSkills Malta Foundation, *National eSkills Strategy 2019-2021* (2018).
[548] ENISA, *Raising Awareness of Cybersecurity. A Key Element of National Cybersecurity Strategies*, 2021.
[549] ”Launch of the NCC and Community,” *NCC*, luettu 10.11.2022, https://ncc-mita.gov.mt/news/launch-of-the-ncc-and-community/.
[550] ”NCC Cybersecurity National Coordination Centre Malta,” *NCC*, luettu 10.11.2022, https://ncc-mita.gov.mt/.
[551]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 23-58.
[552] Ministry of Education and Employment, *A National Curriculum Framework for All*, 2012, 37.
[553] Henkilökohtainen tiedonanto tutkijalle, 8.8.2022.
[554] Henkilökohtainen tiedonanto tutkijalle, 8.8.2022.
[555] Henkilökohtainen tiedonanto tutkijalle, 2.9.2022.
[556] ”Master of Science in Cyber Security,” *AUM American University of Malta*, luettu 10.11.2022, https://aum.edu.mt/programs/graduate-program-2/cyber-security/.
[557] Henkilökohtainen tiedonanto tutkijalle, 2.9.2022.
[558] Jason R.C. Nurse, Konstantinos Adamos, Athanasios Grammatopoulos ja Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 30.
[559] eSkills Malta Foundation, *Annual Report 2021* (2022).
[560] ”ĠEMMA, know, plan, act,” *eSkills Malta Foundation*, luettu 6.9.2022, https://eskills.org.mt/en/gemma/Pages/GEMMA.aspx.
[561] ”Maltese Safer Internet Centre,” *Better Internet for Kids*, luettu 22.11.2022. https://www.betterinternetforkids.eu/sic/malta.
[562] ”BeSmartOnline!,” luettu 6.9.2022, https://www.besmartonline.org.mt.
[563] ”Cyber Crime Unit,” *The Malta Police Force*, luettu 12.9.2022, https://pulizija.gov.mt/en/police-force/police-sections/Pages/Cyber-Crime-Unit.aspx.
[564] ”MITA announces a new initiative to help seniors in the digital world,” *NCC*, luettu 22.11.2022, https://ncc-mita.gov.mt/articles/mita-announces-a-new-initiative-to-help-seniors-in-the-digital-world/.
[565] ”Cyber Security Malta,” luettu 6.9.2022, https://cybersecurity.gov.mt/.
[566] Henkilökohtainen tiedonanto tutkijalle, 2.9.2022.
[567] Lorleen Farrugia, *Children and New Media. A Psychosocial Approach to Understanding how Preadolescents Make Sense of Online Risks*, University of Malta: Department of Psychology (2020), 292-293.
[568] Lorleen Farrugia, *Children and New Media. A Psychosocial Approach to Understanding how Preadolescents Make Sense of Online Risks*, University of Malta: Department of Psychology (2020).
[569] Government of Malta, eSkills Malta Foundation, *National eSkills Strategy 2022-2025* (2022), 32.
[570] Ministry for Competitiveness and Digital Maritime and Services Economy, MITA, *Malta Cyber Security Strategy* (2016), 26.

3.15. Portugali

ITU, Global Cybersecurity Index (GCI) 2020	14/182 (Global), 8/46 (Europe)
National Cyber Security Index (NCSI) 2022	8/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	15/27

3.15.1. Strategiset kyberkoulutuslinjaukset

Portugalin kyberturvallisuusstrategiassa 2019–2023, joka koskee myös autonomisia alueita Azoreita ja Madeiraa[571], painotetaan ennaltaehkäisyä, koulutusta ja tietoisuuden lisäämistä. Kansalaisten digitaalisia taitoja kehitetään ”National Digital Skills Initiative e.2030 — INCoDe.2030” -ohjelmalla. Lisätään tietoisuutta ja luodaan työkaluja digiteknologioiden turvalliseen ja vastuulliseen käyttöön; keskitytään erityisesti lapsiin, nuoriin, ikäihmisiin ja muihin riskiryhmiin. Edistetään vahvaa ja monialaista kyberturvallisuuskoulutusta organisaatioille ja tavallisille kansalaisille. Vahvistetaan kyberturvallisuustaitoja ja -tietämystä sisällyttämällä nämä perusopetuksen opetussuunnitelmaan, keski- ja korkea-asteen koulutukseen sekä opettajien täydennyskoulutukseen. Lisätään uusien sukupolvien (erityisesti haavoittuvat ryhmät) luottamusta ja digitaalisten laitteiden käyttökoulutusta sekä digilukutaitoa tietoisella ja vastuullisella tavalla. Identifioidaan nuoria talentteja ja kannustetaan heitä kyberturvallisuusalalle. Alan jatkokoulutusta lisätään sekä sertifioidaan kyberturvallisuuskoulutuksia ja pätevöitymiskursseja. Julkisten ja yksityisten instituutioiden avulla edistetään tietoisuutta tietoisuuskampanjoilla.[572] Strategian mukaan kyberturvallisuus on jaettua vastuuta eri toimijoiden kesken, olivatpa ne sitten julkisia tai yksityisiä, yhteisöjä tai yksilöitä.[573]

INCoDe.2030-ohjelma [574] on poliittinen aloite, joka pyrkii lisäämään digitaalisia taitoja ja sitä kautta vahvistamaan Portugalin asemaa ja kilpailukykyä. Elämä perustuu yhä enemmän digitaalitekniikkaan, joten on tärkeää, että kaikilla on valmiudet käsitellä tätä uutta todellisuutta. Portugalin INCoDe.2030-aloitteessa käsitellään digitaalisen osaamisen käsitettä laajasti. Osaamiseen sisältyy digitaalisen lukutaidon käsite (kyky käyttää digitaalista mediaa ja tekniikkaa, kriittinen sisällön arviointi ja tehokas viestintä) ja kyky tuottaa uutta tietoa tutkimuksen avulla. Tämä vaatii tiedon käsittelyä, viestintää, vuorovaikutusta ja digitaalisen sisällön tuottamista. Osaamista voidaan kehittää erilaisilla tasoilla ja tavoitteilla. Tasot heijastavat siihen, millaisia toimenpiteitä edistetään osallistavasti ja kattavasti koko yhteiskunnassa.[575]

3.15.2. Kyberkansalaistaitojen opettamisen nykytila

Kyberturvallisuuskoulutus (opintosuunnitelmiin kuuluva opetus sekä yhteiskunta ja kansalaiset) keskittyy enemmän verkon käyttöön ja etikettiin liittyvään turvallisuuteen *(”More security than defence”* -perspektiivi) kuin itse verkon turvallisuuteen. Tietoisuuskampanjoissa käsitellään yleisesti kyberturvallisuutta, mutta ne keskittyvät käyttäjäturvallisuuteen ja esimerkiksi siihen, kuinka reagoida verkkokiusaamiseen.[576] Portugalissa tietojenkäsittely (ICT) on aluksi osana muita oppiaineita yläkoulujen perusopetuksessa ja myöhemmin erillisenä oppiaineena. Opetus Portugalin alakouluissa keskittyy digitaalisiin taitoihin osana oppiaineita. Tietojenkäsittely on perusopetuksen yläkouluissa pakollisena ja integroituna muihin oppiaineisiin. Yhtenä osa-alueena on turvallisuus. Toisen asteen koulutuksessa se on vapaaehtoisena erillisenä oppiaineena. Yhtenä osa-alueena käsitellään tietoisuutta ja vaikutusmahdollisuuksia. Oppiaineessa korostetaan kehittyvää teknologiaa ja sen vaikutusta yhteiskuntaan ja jokapäiväiseen elämään.[577] Opetusministeriö ja Portugalin kyberturvallisuuskeskus koordinoivat perusopetuksen opetussuunnitelmaan kuuluvan ”turvallinen internet” -kokonaisuuden sisältöjä. Tavoitteena on sisällyttää opintokokonaisuus jo olemassa olevan oppiaineen sisältöihin. [578] Portugalin kansallinen opetussuunnitelma on päivitetty viimeksi 2018. Uudistuksen myötä ICT-opetusta laajennettiin 10–

15-vuotiaisiin, kun ainetta aiemmin opetettiin vain 12–14-vuotiaille oppilaille. Opintoihin kuuluu jo aiemmin mainittu (kyber)turvallisuuden osa-alue. Opetussisällöt vaihtelevat opintojen eri vaiheissa. Sisältöihin kuuluu muun muassa tekijänoikeudet, turvalliset digitaaliset käytännöt, harkitseva ja kunnioittava asenne, turvallinen verkkokäyttäytyminen, väärennetyt ja roskapostiviestit, kuvien ja videoiden epäasiallinen käyttö verkossa ja kriittinen asenne.[579] ENISAn CyberHEAD-tietokannan mukaan Portugalin korkeakouluissa kyberturvallisuutta opetetaan kahdeksassa eri ohjelmassa.[580]

Portugalin Safer Internet Centre (PT SIC) on osa EU:n Better Internet for Kids (BIK) -ohjelmaa, Insafe tietoisuuskeskus- ja INHOPE-hotline-verkostoa. PT SICin konsortioon kuuluu kuusi organisaatiota, esimerkiksi koulutuksen pääosasto (Directorate-General for Education, DGE), Portugalin urheilu- ja nuorisoinstituutti (IPDJ) ja Portugalin johtavan teleoperaattorin Alticen säätiö. Seitsemäntenä kansallinen kyberturvallisuuskeskus CNCS (Centro Nacional de Cibersegurança) koordinoi ja valvoo hankkeen toteutusta. PT SICillä on kaksi tietoisuuskeskusta. Ensimmäistä, Centro Internet Seguraa[581] (SIC), joka lisää tietoisuutta ja kouluttaa suurta yleisöä, hallinnoi CNCS. Toista, SeguraNet[582]-tietoisuuskeskusta koordinoi DGE. Sen tavoitteena on edistää digitaalista kansalaisuutta kouluyhteisössä ja lisätä (lapset, vanhemmat, opettajat) tietoisuutta verkkoturvallisuudesta. Keskus edistää opettajien koulutusta, jakaa tietoisuus- ja koulutusmateriaaleja sekä kampanjoi. DGE myös edistää kansallista suunnitelmaa, jolla ehkäistään kiusaamista ja verkkokiusaamista, sekä Digital Leaders -hanketta.[583,584,585] BIKin Safer Internet Day -päivää (SID), jota vietetään joka helmikuu, vietetään Portugalissa koko kuukausi.[586]

Portugalin kyberturvallisuuskeskus (NCSC) on kehittänyt neljä kansalaisille suunnattua verkkokurssia: 1) Kybersosiaalinen kansalainen; sosiaalisen median turvallinen käyttö (parhaat käytännöt), 2) Kybertietoinen kansalainen; valeuutiset ja kritiikittömän tiedonkäytön vaarat, 3) Kyberturvallinen kansalainen; hyvät kyberhygieniakäytännöt vapaa-ajalla ja työssä (verkkoselailu, laitteiden ja yksityisyyden suojaaminen, vastuullisuus) ja 4) Kyberturvallinen kuluttaja; turvallisten verkkokauppasivustojen tunnistaminen, turvallinen maksaminen ja asiakkaan oikeudet EU:ssa.[587,588] Kurssikokonaisuutta tarjotaan myös julkishallinnolle, organisaatioille ja IT-ammattilaisille.[589]

Digitaalinen akatemia vanhemmille -ohjelma on DGE:n ja E-REDESin yhteinen hanke, jossa vanhemmat ja huoltajat voivat osallistua lasten ja nuorten digitaalisten taitojen perusopetukseen.[590] Ohjelmalla pyritään tarjoamaan perheille digitaaliset perustaidot, mikä helpottaa lasten kouluseurantaa. Ohjelman ensimmäisessä osassa taitoja opetettiin ensisijaisesti interventioalueilla. Toinen osa käsittelee myös turvallisuusasioita (Digitaalinen turvallisuus ja kansalaisuus) ja kolmannessa osassa kokonaisuuteen kuuluu myös Digitaalinen kuluttaja -osio.[591,592] IDJP:llä on valtakunnallinen Naveg@s em Segurança -tietoisuuskampanja. Kampanjalla edistetään turvallista internetin käyttöä ja digitaalista kansalaisuutta. Kohderyhmänä ovat lapset ja nuoret, kouluttajat, koulut, seniorit ja kansalaiset yleisesti. Aihealueet käsittelevät disinformaatiota, verkkokiusaamista, IoT:tä, verkkoriippuvuutta, tiedonsuojausta, vihapuhetta ja sosiaalisia verkostoja.[593] PT SIC kehitti yhteistyössä Pato Lógico -kustantamon kanssa tietoisuuden lisäämiseen kuvasarjan, joka perustuu Zig Zaga na Net -podcastiin. Siihen kuuluu 30 erilaista lyhyttarinaa, jotka koottiin ja painettiin kirjaksi. Kirjat (9 500 kappaletta) lähetettiin päiväkoteihin, alakouluihin ja koulujen kirjastoihin Portugalissa ja saarilla.[594,595] CNCS:n ja Portugalin psykologien järjestön ”Mitä Internet kertoo sinusta!” -tietoisuuskampanja[596], jonka yksi iskulause on "Vahvat salasanat ja kanakeitto eivät koskaan vahingoita ketään", on suunnattu seniorikansalaisille. Kampanjan kasvoina toimivat suositut tv-juontajat Júlio Isidro ja Júlia Pinheiro.[597] DGE:n ”Cibersegurança nas Escolas” (Kyberturvallisuus kouluissa) on Portugalin vuoden 2022 ECSM:n laaja kampanja, joka haastaa kaikki koulut mukaan kampanjoimaan ja edistämään kyberturvallisuutta.[598] Kampanjan materiaalipankista löytyy eri-ikäisille suunnattua materiaalia ja myös Guía para uma Internet segura -kirja (Turvallisen internetin opas).[599]

”Sisällöt ja kurssitarjonta pääsääntöisesti portugaliksi. Peliteollisuus ei vielä ole tuottanut merkittävästi sisältöjä.”[600] Portugalin SIC kehitti yhdessä CICADin (Addiktoivan käytöksen ja riippuvuuksien interventiopalvelu) ”Eu e os Outros” -ohjelman kanssa videopelin, jossa aiheena on muun muassa ongelmallinen netin käyttö ja kyberseksi. Peliä pilotoidaan Odivelasin kunnan kouluissa.[601] Journalisti Paulo Penan kanssa yhteistyössä on

kehitetty mediakasvatuksellinen pedagoginen tietovisa ”Verdade ou Mentira” (Totuus vai valhe), jonka avulla edistetään kriittistä ajattelua.[602]

Vuoden 2021 Portugalin Euroopan kyberturvallisuuskauden kampanjassa haluttiin kiinnittää erityishuomio kyberhygienian parhaisiin käytäntöihin helposti lähestyttävällä sosiaalisen median ”Kyberturvallisuuskuukaudessa kansanviisaus auttaa aina” -kampanjalla. Kampanjassa luotiin yhteys sen välille, mitä ihmiset tietävät (kansanviisaus) ja mitä heidän on opittava (kyberhygieniakäytäntö). Graafisesti sisällön (kuten ”Laiskuus on kaikkien paheiden äiti”. OTA KÄYTTÖÖN KAKSIVAIHEINEN TUNNISTUS AINA KUN SE ON MAHDOLLISTA.) tausta on perinteinen portugalilainen laatta[603], jonka avulla tehostettiin viestin kansanomaisia ja perinteisiä elementtejä viestien kaikille sukupolville. Osa sananlaskuista kaiverrettiin fyysisisille laatoille ja niitä jaettiin CNCS:n vuosittaisessa C-Days-konferenssissa.[604]

3.15.3. Kansalliset erityispiirteet

Portugalin kyberturvallisuuden kulttuuria kehystävät eettiset periaatteet, joiden mukaisesti huolehditaan, että kaikilla on riittävästi tarvittavaa tietoa ja tietoisuutta sekä luottamusta käyttää tietoverkkoja ja -järjestelmiä.[605] Portugalissa kyberturvallisuus lähtee kansalaisnäkökulmasta. Jokaisella on rooli kyberturvallisuudessa ja myös vastuu suojella itseään ja muita.[606] Osallistuminen kyberturvallisuuteen ja sen edistämiseen koetaan tärkeäksi.[607] Kansalaisten digitaalisia taitoja kehittämällä luodaan Portugaliin resilienssiä ja sen avulla entistä kestävämpi yhteiskunta.[608]

Portugalissa digitaalista kansalaisuutta käsitellään myös kolmen kouluyhteisöihin liittyvän hankkeen kautta. Cidadania Digital (Digitaalinen kansalaisuus) -käsitteen alle kuuluu aiemmin mainittu SeguraNet-ohjelma ja siihen kuuluvat Líderes Digitais (Digitaaliset ”johtajat”) -hanke sekä Selo de Segurança Digital (eSafety-tunnus).[609] Digitaaliset johtajat -hankkeen tavoitteena on parantaa ikätovereiden ja kouluyhteisön medialukutaitoja sekä lisätä internetin turvallista ja tietoista käyttöä. Sen avulla halutaan myös edistää digitaalisen kansalaisuuden kehitystä. Oppilaat järjestävät epävirallisia koulutustilaisuuksia omassa kouluyhteisössään.[610, 611] Kaikille kouluille suunnatun eurooppalaisen eSafety-hankkeen tavoitteena on edistää ja sertifioida koulujen digiturvallisuuden käytäntöjä.[612]

3.15.4. Kyberkansalaistaitojen määrittäminen

Yksinkertaisimmillaan e-kansalaisuus on hyvää käytöstä digimaailmassa, mutta se on paljon muutakin. Siihen kuuluu digitaalinen etiketti, viestintä, turvallisuus ja lainsäädäntö, käyttömahdollisuus (access) ja osallisuus, digitaaliset taidot, oikeudet ja velvollisuudet sekä osallistuminen.[613] Portugalissa kyberkansalaistaidoissa painotetaan (*”More security than defense” -näkökulma*) verkon käytön turvallisuutta, etikettiin liittyviä turvallisuuskysymyksiä ja käyttäjäturvallisuutta (kuten kuinka reagoida kiusaamiseen verkossa).[614]

Portugalissa digitaalisen osaamisen dynaamiseen viitekehykseen (Quadro Dinâmico de Referência de Competência Digital, QDRCD), joka pohjautuu kansalaisten digitaalisen osaamisen viitekehykseen (the Digital Competence Framework for Citizens), kuuluu viisi osaamisaluetta: 1) informaatiolukutaito, 2) viestintä ja kansalaisuus, 3) sisällön luominen, 4) turvallisuus ja yksityisyys ja 5) ratkaisujen kehittäminen, joiden taitotasot vaihtelevat perustasosta erittäin erikoistuneeseen. Viestintä ja kansalaisuus -osa-alueeseen kuuluu muun muassa kansalaisuus digitaaliteknologioiden kautta, käyttäytymissäännöt digitaalisessa ympäristössä ja digitaalisen identiteetin hallinta. Turvallisuus ja yksityisyys -osa-alueeseen kuuluu laitteiden suojaus, henkilötietojen suojaaminen sekä terveyden ja ympäristön suojelu.[615] Portugalissa kyberkansalaistaitoja voidaan määritellä myös aiemmin mainitun NCSC:n verkkokurssikokonaisuuden neljän kurssin ja niiden sisältöjen kautta.[616] Myös koulumaailmassa halutaan kehittää digitaalista kansalaisuutta kasvattamalla luottavaisia kansalaisia, jotka pystyvät vastaamaan digitaalisiin haasteisiin turvallisella ja vastuullisella tavalla.[617]

Viitteet

[571] Henkilökohtainen tiedonanto tutkijalle, 3.10.2022.
[572] Resolution of the Council of Ministers No. 92/2019, *Portugal National Strategy for Cyberspace Security 2019-2023*, *Portuguese Official Journal*, Series 1 – No. 108 (5.6.2019), 2891-2892.
[573] Council of Ministers, *Strategy for Cyberspace Security*, 2889.
[574] "Portugal INCoDe.2030, The Programme," luettu 30.11.2022, https://www.incode2030.gov.pt/en/programme.
[575] "A INCoDe.2030," luettu 11.10.2022, https://www.incode2030.gov.pt/en/initiative.
[576] Henkilökohtainen tiedonanto tutkijalle, 3.10.2022.
[577] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 10-62.
[578] Henkilökohtainen tiedonanto tutkijalle, 3.10.2022.
[579] Global Forum on Cyber Expertise (GFCE), *Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people*, Krysia Emily Waldock, Vince Miller, Shujun Li and Virginia N.L. Franqueira Institute of Cyber Security for Society (iCSS) (UK: University of Kent, February 2022), 98.
[580] "CYBERHEAD – Cybersecurity Higher Education Database," *ENISA*, luettu 22.11.2022, https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=prt.
[581] "Centro Internet Segura," luettu 30.11.2022, https://www.internetsegura.pt/.
[582] "SeguraNet, Navegar em Segurança," luettu 30.11.2022, https://www.seguranet.pt/.
[583] Portuguese Safer Internet Centre V, Centro Internet Segura, *Final Public Report, January 1st, 2020 – December 31th* (2020), 13-14.
[584] "Portuguese Safer Internet Centre," luettu 21.11.2022, https://www.betterinternetforkids.eu/sic/portugal.
[585] "Portuguese Safer Internet Centre, About us," luettu 21.11.2022, https://www.saferinternetday.org/in-your-country/portugal.
[586] "Portuguese Safer Internet Centre, About our SID activities," luettu 21.11.2022, https://www.saferinternetday.org/in-your-country/portugal.
[587] Henkilökohtainen tiedonanto tutkijalle, 12.7.2022.
[588] E-learning Courses," luettu 22.11.2022, https://www.cncs.gov.pt/en/e-learning/.
[589] "E-learning Courses>Public Administration/ Organizations/ IT Professionals," luettu 22.11.2022, https://www.cncs.gov.pt/en/e-learning/.
[590] Henkilökohtainen tiedonanto tutkijalle, 12.7.2022.
[591] " Academia Digital para Pais (3.ª Edição)," luettu 23.11.2022, https://www.dge.mec.pt/academia-digital-para-pais-3a-edicao.
[592] " Investimento social, Conheça os nossos programas, Um projeto de literacia digita," luettu 23.11.2022, https://www.e-redes.pt/pt-pt/sustentabilidade/nos-e-as-comunidades/investimento-social/academia-digital-para-pais.
[593] "Programa «Naveg@s em Segurança?» - sessões de sensibilização de Cidadania Digital," luettu 23.11.2022, https://erte.dge.mec.pt/noticias/programa-navegs-em-seguranca-sessoes-de-sensibilizacao-de-cidadania-digital-0.
[594] "ZigZaga on the Internet," luettu 30.11.2022, https://cybersecuritymonth.eu/countries/portugal/zigzaga-on-the-internet.
[595] Henkilökohtainen tiedonanto tutkijalle, 12.7.2022.
[596] "O que a Internet diz de si!," luettu 30.11.2022, https://www.internetsegura.pt/o-que-internet-diz-de-si.
[597] "New awareness-raising campaign for senior users," luettu 23.11.2022, https://www.betterinternetforkids.eu/practice/articles/article?id=6918638.
[598] "Cibersegurança nas Escolas," luettu 23.11.2022, https://cybersecuritymonth.eu/countries/portugal/ciberseguranca-nas-escolas.
[599] "CIBERSEGURANçA NAS ESCOLAS, Recursos de Apoio," luettu 24.11.2022, https://www.seguranet.pt/mes-ciberseguranca-2022/recursos-de-apoio.
[600] Henkilökohtainen tiedonanto tutkijalle, 3.10.2022.
[601] Henkilökohtainen tiedonanto tutkijalle, 12.7.2022 ja 18.7.2022.
[602] "Jogo Pedagógico Verdade ou Mentira," luettu 24.11.2022, https://www.seguranet.pt/pt/jogo-pedagogico-verdade-ou-mentira.
[603] "MÊS EUROPEU DA CIBERSEGURANÇA, A SABEDORIA POPULAR PODE AJUDAR," luettu 30.11.2022, https://www.cncs.gov.pt/docs/1626333366.pdf.
[604] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 121-126.
[605] Council of Ministers, *Strategy for Cyberspace Security*, 2891.
[606] "Citizen," luettu 20.11.2022, https://www.cncs.gov.pt/en/citizen/?persona=citizen.
[607] Portuguese Safer Internet Centre V, Centro Internet Segura, *Final Public Report, January 1st, 2020 – December 31th* (2020), 2.
[608] Council of Ministers, *Strategy for Cyberspace Security*, 2891.
[609] "Equipa de Recursos e Tecnologias Educativas >CIDADANIA DIGITAL," luettu 21.11.2022, https://erte.dge.mec.pt/noticias/programa-navegs-em-seguranca-sessoes-de-sensibilizacao-de-cidadania-digital-0.
[610] Henkilökohtainen tiedonanto tutkijalle, 12.7.2022.
[611] " Líderes Digitais SeguraNet," luettu 21.11.2022, https://www.seguranet.pt/pt/lideres-digitais-seguranet.
[612] "eSafety Label (Selo de Segurança Digital)," luettu 22.11.2022, https://erte.dge.mec.pt/esafety-label.
[613] "A Internet pode favorecer a cidadania?," luettu 18.11.2022, https://mild.rbe.mec.pt/a-internet-pode-favorecer-a-cidadania/.
[614] Henkilökohtainen tiedonanto tutkijalle, 3.10.2022.
[615] "INCODE.2030 Digital Competence Reference Framework," luettu 20.10.2022, https://www.incode2030.gov.pt/en/featured/incode2030-releases-digital-competence-dynamic-reference-framework.
[616] "E-learning Courses," luettu 24.11.2022, https://www.cncs.gov.pt/en/e-learning/.
[617] "O que fazemos?," luettu 21.11.2022, https://www.seguranet.pt/pt/o-que-fazemos.

3.16. Puola

ITU, Global Cybersecurity Index (GCI) 2020	30/182 (Global), 18/46 (Europe)
National Cyber Security Index (NCSI) 24.10.2022	10/160 (24.10.2022)
The Digital Economy and Society Index (DESI, 2022)	24/26

3.16.1. Strategiset kyberkoulutuslinjaukset

Puolan presidentti Andrzej Duda hyväksyi toukokuussa 2020 uuden kansallisen turvallisuusstrategian. Yksi strategian olennaisista elementeistä on kyberturvallisuus. Strategia on Puolan tärkein kansallinen asiakirja. Yksi lain alakohtaisista strategioista on Puolan kansallinen kyberturvallisuusstrategia vuosille 2019–2024. Tärkeänä tavoitteena on muun muassa lisätä toimia, joilla kansalaiset voivat paremmin suojata tietonsa. Strategiassa mainitaan myös, että kyberturvallisuuskoulutusta tulisi järjestää mahdollisimman aikaisessa vaiheessa, jopa ennen digitaalisiin palveluihin pääsyä. Käytännössä koulutusta tulisi antaa jo varhaiskasvatuksessa. Korkeakouluja kannustetaan kehittämään monialaisia opetusaloja, jotka kattavat tietoturvallisuuden. Strategia huomioi myös kansalaisia koskevat koulutustoimet ja kampanjat, jotka tähtäävät yleisen tietoisuuden lisäämiseen. Tätä toteutetaan erilaisille kohderyhmille, kuten lapsille, aikuisille ja vanhuksille.[618]

Puolan tasavallan kansallinen kyberturvallisuuspoliittinen viitekehys sisältää ehdotuksia koulutusalan erityistoimiksi. Viitekehys on laadittu vuosille 2017–2022. Kansallinen viitekehys painottaa kyberturvallisuuteen liittyvien tieteidenvälisten erikoisalojen kehittämistä, uuden teknologian kehittämistä Puolan yliopistoissa sekä IT-opettajien pätevyyden parantamista. Viitekehyksen mukaan kyberavaruuden turvallisen käytön tulee olla osa opetussuunnitelmaa ja varhaiskasvatuksen tasolla. Kansallisesti viitekehyksessä halutaan kohdistaa myös eri kohderyhmille (lapset, vanhemmat, eläkeläiset) kyberturvallisuuskampanjoita.[619]

3.16.2. Kyberkansalaistaitojen opettamisen nykytila

Vuonna 2017 voimaan tulleessa perusopetussuunnitelmassa ja yleisopetuksen perusopetussuunnitelmasta peruskouluissa kyberturvallisuus mainitaan osana turvallisuusalan koulutusta. Peruskoulun ja lukion opiskelijoille on tarkoitus käynnistää toimia, joilla jaetaan tietoa kyberturvallisuudesta, luodaan kriittistä asennetta internetin sisältöön ja edistetään turvallista verkkokäyttäytymistä. Eräissä lukioissa on tarjolla myös kyberturvallisuuteen liittyviä erikoislinjoja. Tarkoituksena olisi myös käynnistää yhteistyötä opetuksen ja yksityisten toimijoiden kesken erilaisissa koulutusprojekteissa, yhteishankkeissa tai työpajoissa. Yleisesti Puolassa on todettu, että pienten päiväkoti-ikäisten lasten digitaalisia taitoja kehittävää toimintaa tulisi suunnata erityisesti lasten vanhemmille. Digitaalisesti osaava vanhempi pystyy tukemaan kehittymistä yhteistyössä varhaiskasvatuksen kanssa. Kasvatuksessa tulisi lähtökohtaisesti huomioida laskennallisen ajattelun kehittäminen, mediakasvatus, erilaiset luokkaskenaariot sekä didaktisia työkaluja sovellettuina esikouluikään.[620]

Korkeakouluopiskelijoille tarjotaan Legia Akademicka -koulutusta, jossa on kyberturvallisuuden opintoja, mutta ylipäänsä Legia Akademicka valmentaa sotilasvalaan. Tarkoituksena on pyrkiä kouluttamaan ja rekrytoimaan enemmän ammattilaisia. Kansalaisille tarjotaan myös mahdollisuutta palvella alueellisissa puolustusjoukoissa, mikä voidaan rinnastaa Suomessa olevaan Maanpuolustuskoulutukseen (MPK). Toimintaa kutsutaan WOT-joukoiksi. WOT-joukoilla on myös kyberyksikkö. Joukkoihin kuuluville tarjotaan säännöllisesti koulutusta ja harjoituksia muun työelämän ohella. Tämän lisäksi joskus järjestetään myös Sotataidon akatemiassa kyber- ja informaatioturvallisuuteen liittyviä tilaisuuksia, joihin myös kansalaiset voivat osallistua.[621]

Puolan yliopistoissa järjestetään kyberturvallisuuteen liittyvää koulutusta. Koulutusohjelmia on tarjolla maksullisina sekä ilmaisina tutkinto-ohjelmina. Yleisesti sisällöt painottuvat teknisen osaamisen lisäämiseen. Seuraavien tutkinto-ohjelmien nimessä esiintyy kyberturvallisuus: Cybersecurity - Akademia Ignatianum in Krakow, Cybersecurity – AGH University of Science and Technology, Cybersecurity (IT Cyber Security) - Maria Curie-Skłodowska University in Lublin, Information security and cybersecurity - Academy of War Arts in Warsaw, Cybersecurity - Wroclaw University of Science and Technology ja Cryptology and cybersecurity - Military University of Technology Jarosław Dąbrowski in Warsaw.[622]

Puolan perusasteen koulut järjestävät yhteistyössä Class Foundation -järjestön kanssa Asa Internet -koulutusohjelmaa, jonka tarkoituksena on opettaa kansalaisia olemaan hyviä ihmisiä internetissä. Koulutusohjelma nojaa yleismaailmallisten periaatteiden noudattamiseen niin todellisessa kuin digitaalisessa maailmassa. Tällaisia periaatteita ovat järkevyys, tietoisuus, vahvuus, ystävällisyys sekä rohkeus. Osana ohjelmaa on laadittu kymmeniä tuntiskenaarioita hyödynnettäväksi sekä luokkahuoneessa että etäopiskelussa. Opit kohdistuvat tiedon jakamiseen ja sen arvioimiseen, erilaisten verkkohuijauksien tunnistamiseen sekä itsensä suojaamiseen muun muassa käyttämällä vahvoja tunnistautumisen keinoja.[623]

Puolassa toimii valtionhallinnon ohella useita toimijoita, jotka osaltaan edistävät kansalaisten kybertietoisuuden ja taitojen lisäämistä. Keskeisin toimija on Kansallinen tutkimuslaitos (National Research Institute, NASK), joka toimii pääministerin kanslian alaisena. NASKin päätehtäviin kuuluu hallinnoida Puolan kansallista koulutusverkostoa, vastata kansallisesta verkkotunnusrekisteristä sekä tutkia digitalisaation vaikutuksia yhteiskunnallisesti. NASK järjestää kansalaisille suunnattua kyberturvallisuuden koulutusta sekä vuosittain erilaisia tiedotuskampanjoita. Yhtenä esimerkkinä tästä on kouluille suunnattu ohjeistus ”Online safety in the schools of the Polish educational Network”. Osana Puolan kansallista koulutusverkostoa koulutusverkosto on myös luonut ilmaisen mochrona-sovelluksen, joka tukee vanhempia pitämään lapsensa turvassa verkossa. NASK on luonut myös kansallisia sopimuksia keskeisten kansalaisjärjestöjen kanssa, millä vahvistetaan yhteistyötä kyberturvallisuuden tietoisuuden lisäämiseksi.[624] Kansalaisille suunnattuja alustoja kybertaitojen harjoitteluun on kehitetty muutamia, mutta ne on tarkoitettu enemmänkin käyttäjille, jotka haluavat syventää tietojaan, sekä yrityksille, jotka voivat ostaa koulutusta työntekijöilleen. Tarjottavat koulutukset ovat maksullisia. Tällaisia sivustoja ovat esimerkiksi ZaufanaTrzeciaStrona.pl, Niebezpiecznik.pl, Sekurak.pl sekä CyberDefence24.pl.[625]

OSE IT School on koulutusalusta, josta pääsee ilmaisiin verkko-opetusmateriaaleihin ja -kursseihin. Alusta on suunnattu erityisesti opiskelijoille, mutta myös opettajille. Alusta tarjoaa yli 200 ilmaista kurssia ja siinä voi suunnitella oman koulutuspolkunsa. Alusta huomioi myös eri ikäryhmät.[626] NASK ylläpitää sivustoa, joka tunnetaan nimellä European Cybersecurity Month, ECSM. Puolassa kampanja on toteutettu vuonna 2022 jo kahdeksatta kertaa. Sivusto toimii kuukauden pituisen kampanjan kotisivuna, mutta sieltä löytyy myös merkittävä määrä erilaista aiheeseen liittyvää materiaalia tietoisuuden ja oppimisen lisäämiseksi.[627] Hallinto- ja digitalisaatioministeriön ja Cities on Internet -yhdistyksen yhteistyönä toteutettu Digital Poland of Equal Opportunities -ohjelma (PCRS-ohjelma) on aloite, jonka tarkoituksena on rohkaista yli 50-vuotiaita ihmisiä ottamaan tämä ensimmäinen askel digitaaliseen maailmaan.[628] ”Kaupungit Internetissä” -projekti oli suunnattu yli 50-vuotiaille ja toteutettiin 2016–2018. Hankkeen tarkoituksena oli kehittää digitaalista osaamista, ja siinä osallistujat päättivät, millaisia aiheita käsiteltiin. Hanke on saanut jatkoa, nyt vastaava toteutetaan yli 18-vuotiaiden kohderyhmälle kybertaitojen osalta.[629] Puolan Safer Internet Center (PCPSI) perustettiin vuonna 2005 Euroopan komission Safer Internet -ohjelmassa, ja se toimii nyt Digital Europe -ohjelman alaisuudessa. Keskuksen muodostavat kansallinen tutkimuslaitos NASK (PSIC:n koordinaattori) ja Empowering Children Foundation (ECF). Keskus toteuttaa kattavia toimia lasten ja nuorten turvallisuuden takaamiseksi internetiä ja uutta teknologiaa hyödyntäen. Kohderyhmiä ovat lapset, nuoret, vanhemmat, opettajat sekä muut lasten verkkohaittoja vastaan työskentelevät ammattilaiset. Keskus järjestää konferensseja, tuottaa koulutusmateriaalia sekä sosiaalisia kampanjoita. Osana keskuksen toimintaa järjestetään vuosittain Safer Internet Day, joka on toteutettu vuodesta 2005 lähtien.[630]

Sieciaki.pl ”get to know safe internet” -sivusto on tarkoitettu 6–12-vuotiaille lapsille ja käsittelee turvallista internetin käyttöä pelien, sarjakuvien kuin kirjojenkin välityksellä.[631] Necio-sivusto on tarkoitettu 4–6-vuotiaille lapsille ja heidän vanhemmilleen. Sivustolla käsitellään internetiä ja siellä tapahtuvia asioita videoiden, tehtävien ja sarjakuvan avulla interaktiivisesti.[632] Protect your child online -kampanjan tavoitteena on varoittaa vanhempia internetin haitallisista seurauksista esikoulu- ja varhaiskouluikäisille lapsille ja kertoa heille, miten näitä riskejä voidaan vähentää. Kampanjan järjestävät Empowering Children Foundation (entinen Nobody's Children Foundation) ja NASK osana Puolan Safer Internet Centerin toimintaa.[633]

Opetuspeli Rufus in peril näyttää, millaisia vaaroja nuori nykyteknologian käyttäjä kohtaa ja kuinka hänen kannattaa reagoida vaikeissa tilanteissa. Graafinen muoto ja kieli on mukautettu ala- ja yläkoulujen vanhempien luokkien pelaajille, mutta se sopii myös muille.[634]

Paikallisella tasolla myös opettajille ja rehtoreille järjestetään kyberturvallisuutta käsitteleviä konferensseja. Näitä järjestävät erityisesti koulujen opetuslautakunnat ja koulutuskeskukset. Yksi tällainen esimerkki on Rzeszowin opetuslautakunnan (Board of Education in Rzeszow) järjestämä Online Konference: Cybersecurity at School. [635] NASK järjestää kurssimuotoista opetusta opettajille kyberturvallisuudesta. NASK:n järjestämä koulutussarja opettajille kyberuhista ”Safe in the Web with OSE” on alkamassa. Osana ohjelmaa kouluttajat voivat saada tietoa sellaisista ilmiöistä kuin seksiviestittely, kyberkiusaaminen tai FOMO, minkä ansiosta he voivat paremmin tukea oppilaita selviytymään etäoppimisen aiheuttamista kyberuhkista ja haasteista.

E-oppimisportaali on digitaalinen opettajille ja opiskelijoille suunnattu alustaratkaisu, joka esittelee eri kyberturvallisuuden osa-alueita ja teknologioita, kuten tekoälyä, algoritmeja, ohjelmointia, tietokantoja, kemiaa, fysiikkaa ja multimediaa. Alustalla voidaan tuottaa kampanjoita ja kilpailuja eri tarkoituksiin.[636]

3.16.3. Kansalliset erityispiirteet

TrendMicro Poland on luonut Kyberturvallisuuskoulutus yliopistoille -ohjelman, jonka tarkoituksena on tukea yliopistoja maksutta kyberturvallisuuskoulutuksen järjestämisessä. Yhteistyössä koulujen kanssa TrendMicro keskittyy muun muassa järjestämään seminaareja ja webinaareja opiskelijoille tarjoamalla uusinta asiantuntijatietoa. Tämän lisäksi TrendMicro osallistuu konsultointiin opetusohjelmien osalta, millä pyritään varmistamaan, että opetussuunnitelmien aineet vastaavat todellisia tarpeita ja mahdollistavat asiankuuluvan tiedon saamisen nopeasti muuttuvassa teknologian ja tietoverkkorikollisuuden maailmassa.[637]

3.16.4. Kyberkansalaistaitojen määrittäminen

Puolassa ei ole kansallisella tasolla määritelty kansalaisten osalta kyberturvallisuuden osaamista. Saatujen vastausten perusteella kansalaisia lähinnä ohjeistetaan suhtautumaan kriittisesti verkossa oleviin tietoihin. Asiantuntijoiden mukaan näiden taitojen määrittely on vielä lapsenkengissä. Tätä kuvaa myös vuonna 2018 säädetty laki kyberturvajärjestelmistä. Lain mukaan kyberturvallisuus voidaan nähdä ennen kaikkea eräänlaisena vastustuksena sellaisille toimille, jotka loukkaavat kyberturvajärjestelmien tarjoamien tietojen tai niihin liittyvien palvelujen luottamuksellisuutta, eheyttä, saatavuutta ja aitoutta. Määritelmästä voidaan tulkita, että se suuntautuu vahvasti tietoturvallisuuden kenttään. Hallitukseen on nimitetty erityisvaltuutettu, joka vastaa informaatioturvallisuudesta.[638]

Viitteet

[618] Ministry of Digital Affairs, *Cybersecurity strategy of the Republic of Poland for 2019-2024* (2019), 10, 26; Henkilökohtainen tiedonanto tutkijalle, 23.8.2022.
[619] Henkilökohtainen tiedonanto tutkijalle, 25.8.2022.
[620] Chancellery of the Prime Minister, *Digital Competences development program* (2022), 24-26, 57-59, 60-64; Henkilökohtainen tiedonanto tutkijalle, 21.10.2022.
[621] Henkilökohtainen tiedonanto tutkijalle 21.10.2022; "Dowództwo Wojsk Obrony Terytorialnej," luettu 12.10.2022, https://terytorialsi.wp.mil.pl/.
[622] "Studia cyberbezpieczeństwa," *Studia.pl*, luettu 20.10.2022, https://studia.pl/kierunki/cyberbezpieczenstwo/; "Education," *AGH*, luettu 12.9.2022, https://iet.agh.edu.pl/en/education/.
[623] "Asy Internetu," luettu 16.10.2022, https://asyinternetu.szkolazklasa.org.pl/wez-udzial/.
[624] "NASK," luettu 23.9.2022, https://www.nask.pl/; "NASK," luettu 11.8.2022, https://www.nask.pl/pl/aktualnosci/3795,Cyberbezpieczny-uczen-cyberbezpieczna-szkolaporadniki-dla-szkol-o-bezpieczenstw.html?search=60470; Henkilökohtainen tiedonanto tutkijalle, 10.8.2022.
[625] Henkilökohtainen tiedonanto tutkijalle, 15.8.2022 ja 20.8.2022.
[626] "OSE IT Szkoła," luettu 10.11.2022, https://it-szkola.edu.pl/.
[627] "Europejski Miesiąc Cyberbezpieczeństwa," *NASK*, luettu 18.9.2022, https://bezpiecznymiesiac.pl/.
[628] "National Digital Literacy Campaign," *Polska Cyfrowa Rownych Szans*, luettu 2.9.2022, https://latarnicy.pl/english/.
[629] Henkilökohtainen tiedonanto tutkijalle, 24.8.2022.
[630] Henkilökohtainen tiedonanto tutkijalle, 9.8.2022.
[631] "Sieciaki.pl," luettu 2.10.2022, https://sieciaki.pl/.
[632] "Necio.pl," luettu 20.9.2022, https://www.necio.pl/.
[633] "Chroń dziecko w sieci," luettu 13.9.2022, http://www.dzieckowsieci.pl/kampania/; Joanna Świątkowska, Izabela Albrycht ja Dominik Skokowski, *National Cyber Security Organization: POLAND* (Tallinn: CCDCOE, 2017).
[634] "Rufus w opałach," *Safer Internet.pl*, luettu 18.7.2022, https://sites.google.com/a/zspkowalew.pl/bezpieczenstwo-w-sieci1/home/dla-uczniow-1/rufus-w-opalach.
[635] "Konferencja on-line: Cyberbezpieczeństwo w szkole," *Kuratorium Oświaty w Rzeszowie*, luettu 22.6.2022, https://www.ko.rzeszow.pl/dla-dyrektora-i-nauczyciela/dla-dyrektora-i-nauczyciela-komunikaty/konferencja-on-line-cyberbezpieczenstwo-w-szkole/.
[636] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022).
[637] Kancelaria Sejmu, *O krajowym systemie cyberbezpieczeństwa*, *Dz. U. 2018 poz. 1560*, luettu 21.8.2022, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf; Henkilökohtainen tiedonanto tutkijalle, 21.11.2022.
[638] "Edukacja z zakresu cyberbezpieczeństwa dla uniwersytetów," *TrendMicro*. luettu 8.10.2022, https://www.trendmicro.com/pl_pl/initiative-education/cybersecurity-education-universities.html.

3.17. Ranska

ITU, Global Cybersecurity Index (GCI) 2020	9/182 (Global), 5/46 (Europe)
National Cyber Security Index (NCSI) 2022	13/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	12/27

3.17.1. Strategiset kyberkoulutuslinjaukset

Vuonna 2008 Ranskan presidentti Nicolas Sarkozy päätti, että muuttuneen turvallisuustilanteen vuoksi Ranskaan tulisi laatia kansallisen puolustuksen ja turvallisuuden valkoinen kirja. Valkoisen kirjan tarkoituksena oli määritellä kansakuntaan kohdistuvat uhka- ja riskitekijät sekä toimenpiteet niiden hallitsemiseksi. [639] Kyberpuolustuksen kannalta kirjaa on luonnehdittu jopa käänteentekeväksi sekä ensimmäiseksi valtiotason strategiaksi, joka tunnustaa kyberuhkien merkittävyyden. Vuonna 2013 laadittiin uusi kansallisen puolustuksen ja turvallisuuden valkoinen kirja presidentti François Hollanden vaatimuksesta. Valkoisessa kirjassa kuvatut strategiset tavoitteet johtivat myös tietojärjestelmien turvallisuudesta vastaavan kansallisen viraston, ANSSIn (Agence nationale de la sécurité des systèmes d'information) syntymiseen. ANSSI toimii Ranskan pääministerin alaisuudessa toimivan Puolustuksen ja kansallisen turvallisuuden pääsihteeristön SGDSN:n (Secrétariat général de la défense et de la sécurité nationale) alaisuudessa.[640]

Yksi ANSSIlle valtuutetuista tehtävistä oli laatia kansallinen kyberturvallisuusstrategia, joka julkaistiin vuonna 2011 ja jota päivitettiin vuonna 2015. Päivitetyn kansallisen kyberturvallisuusstrategian tarkoitus oli ohjata Ranskan siirtymistä kohti digitalisoituvaa yhteiskuntaa, ja se sisälsi viisi eri strategista tavoitetta. Näistä kolmantena strategisena tavoitteena oli lisätä kouluikäisten lasten tietoisuutta digitaalisesta turvallisuudesta sekä vastuullisesta käyttäytymisestä kybermaailmassa. Lisäksi korkea-asteen koulutuksiin sekä jatkokoulutuksiin tulisi strategian mukaan myös digitaaliselle turvallisuudelle omistettu koulutuskokonaisuus. Sen tavoitteena on lisätä kansalaisten osaamista integroimalla kyberturvallisuuskoulutus kaikkiin korkea-asteen koulutuksiin sekä täydennyskoulutusohjelmiin.[641]

Kansallisen kyberturvallisuusstrategian tavoite, jonka mukaisesti Ranska pyrkii suojelemaan kansalaisten digitaalisten palvelujen käyttöä sekä tehostaa tietoverkkorikollisuuden torjuntaa ja avun tarjoamista sen uhreille, sai aikaan GIP ACYMA -nimisen avustusjärjestelmän (Le Groupement d'Intérêt Public Action contre la Cybermalveillance) perustamisen maaliskuussa 2017. Järjestelmän tarkoituksena on avustaa ja tukea kyberhyökkäysten kohteeksi joutuneita kansalaisia, kuten yksityisiä henkilöitä, yrityksiä ja julkisen sektorin toimijoita, sekä pyrkiä ennaltaehkäisemään ikäviä tapahtumia lisäämällä aiheeseen liittyvää tietoisuutta. Vuonna 2022 ACYMA koostuu noin viidestäkymmenestä yksityisen ja julkisen sektorin jäsentoimijasta.[642]

Huhtikuussa 2013 julkaistussa Kansallisen puolustuksen ja turvallisuuden valkoisessa kirjassa nostetaan esille Ranskassa koulutettujen tieto- ja kyberturva-asiantuntijoiden määrän lisäämisen vaikutus kansalliselle turvallisuudelle. Lisäksi kirjan mukaan tulee varmistaa, että tieto- ja kyberturvallisuus on integroitu osaltaan tietojenkäsittelytieteiden korkeakoulututkintoihin, millä halutaan estää tietojärjestelmien haavoittuvuuksien syntymistä ja edistää valppautta sekä reagointia kyberuhkia vastaan. Tavoitteiden saavuttamiseksi ANSSI oli luomassa CyberEdu-ohjelmaa, jonka tarkoituksena on tarjota resursseja edellä mainittua koulutusta järjestäville oppilaitoksille. Toiminta johti CyberEdu-yhdistyksen luomiseen. Yhdistyksen tehtävänä on alkuperäisen ohjelman kehittäminen ja ylläpito sekä myöntää hyväksyntä oppilaitosten järjestämille kursseille, jotka täyttävät ohjelman vaatimukset. Syksyllä 2019 CyberEdu julkaisi 78 sertifioitua koulutusta. Ranskassa koulutettujen tieto- ja kyberturva-asiantuntijoiden määrän kasvu sai aikaan erinäisiä ANSSIn käynnistämiä toimintoja, kuten koulutuksen tunnistamista ja edistämistä koskevan SecNumedu-sertifiointimerkinnän.[643]

3.17.2. Kyberkansalaistaitojen opettamisen nykytila

Jotta kyberturvallisuuteen liittyvää koulutusta olisi mahdollista tarjota myös Ranskan kansalaisille, kuten kouluikäisille lapsille (strategian mukaisesti), lanseerattiin ANSSI MOOC maaliskuussa 2017. MOOCIn tavoitteena on opettaa ja lisätä kansalaisten tietoisuutta digitaaliseen turvallisuuteen liittyvistä haasteista. Selainpohjainen ja käyttäjilleen ilmainen MOOC-oppimisympäristö on kohdistettu työelämässä toimiville käyttäjille ja sen harjoitukset vahvistavat osaamista ja keskittyvät työpaikan ja kodin kyberturvallisuuteen. MOOCin kohderyhmänä ovatkin kansalaiset, jotka haluavat oppia perusasioita digitaalisesta turvallisuudesta ja kyberturvallisuudesta. Koulutus on CFSSI:n määrittelemä ja viraston teknisten asiantuntijoiden toteuttama. ANSSI MOOC tarjoaa hauskaa koulutussisältöä, joka on kaikkien saatavilla, milloin tahansa.[644] Koulutus on jaettu neljään opetusmoduuliin, joissa koulutettava oppii perusasioita tieto- ja digitaalisesta turvallisuudesta sekä kyberturvallisuudesta, jotka ovat hyödyllisiä perusarjessa, kotona ja työpaikalla.

MOOCin lisäksi Ranskassa on pyritty kehittämään kansalaisten kyberturvallisuusosaamista ja etenkin lasten ja nuorten aiheeseen liittyvää osaamista muun muassa Pix:n avulla. Pix on voittoa tavoittelematon ranskalainen julkinen organisaatio, jonka tavoitteena on kehittää ihmisten digitaalisia taitoja kaikkialla maailmassa. Pix perustettiin vuonna 2016, ja sen taustalla on noin 70 eri alojen asiantuntijaa, joiden tavoite on auttaa ihmisiä parantamaan digitaalista osaamistaan. Pix tekee yhteistyötä myös Unescon kanssa tavoitteenaan kehittää nuorten digitaalisia taitoja ympäri maailmaa. Kansainvälinen sivusto pix.org on kehitetty osana Euroopan unionin rahoittamaa Unescon Youth employment in the mediterranean (YEM) -projektia. Pix.org-sivustolla on verkko-oppimisalusta, joka on luotu digitaalisten taitojen arvioimista ja kehittämistä varten.[645]

Oppimisalustalla oleva peli sisältää erilaisia digitaaliseen maailmaan liittyviä oppimistehtäviä. Peli on suoritettavissa ranskan kielen lisäksi myös englanniksi. Pelin tehtävät ovat erilaisia kysymyksiä ja käytännöllisiä tehtäviä, jotka liittyvät muun muassa salasanojen muodostamiseen, tekstinkäsittelyyn, tiedonhakuun ja yleiseen tietouteen. Peli sisältää viisi tehtäväaluetta: tiedot ja taidot, viestintä ja yhteistyö, sisällön luominen, suojaus ja turvallisuus sekä digitaalinen ympäristö. Tilastojen mukaan peliä pelaa päivittäin noin 63 000 käyttäjää.

Keskeisessä osassa kyberturvallisuuteen liittyvän koulutuksen lisäämisessä on myös ANSSIn Kyberturvallisuuden harjoituskeskus (Cybersecurity training center, CFSSI). CFSSI:llä on tärkeä osa kansallisen tietojärjestelmien turvallisuuden koulutuspolitiikan määrittelyssä ja toteuttamisessa. CFSSI koordinoi myös ohjelmaa nimeltä SecNumedu, jonka tehtävänä on varmistaa, että muun muassa opiskelijoille ja työntekijöille tarjottava kyberturvallisuuskoulutus vastaa ANSSIn ja alan toimijoiden yhteistyössä määrittelemiä sopimuksia ja kriteeristön vaatimuksia.[646]

SecNumedun toteuttamalla prosessilla on mahdollista varmistaa eri koulutusohjelmien sisällön kattavuus ja tarkoituksenmukaisuus suhteessa sen oppimistavoitteisiin. SecNumedu-sertifiointi on kehitetty yhteistyössä yritysten, korkeakoulujen, yhdistysten ja Ranskan opetusministeriön (Ministère de l'éducation nationale) kanssa ja se myönnetään aina kolmeksi vuodeksi kerrallaan. Sertifioinnista vastaa ANSSI, joka ylläpitää myös luetteloa sertifioinnin suorittaneista koulutusohjelmista. Vuonna 2022 ANSSIn mukaan eri oppilaitosten järjestämiä SecNumedu-sertifioituja koulutuksia oli 72. Koulutukset olivat pääosin ammatillisia tutkintoja, insinööritutkintoja sekä maisterikoulutuksia.[647] ENISAn (The European Union Agency for Cybersecurity) mukaan Ranskassa on vuonna 2022 yksitoista kyberturvallisuuteen keskittyvää korkeakouluohjelmaa.[648]

Vuonna 2017 ACYMA lanseerasi Cybermalveillance.gouv.fr-alustan. Alustan tarkoituksena on auttaa kyberhyökkäysten ja kyberrikollisuuden uhreiksi joutuneita tarjoamalla neuvoja ja apua. Lisäksi sen tarkoituksena on kasvattaa ihmisten tietoisuutta digitaalisesta turvallisuudesta alustalla olevien tietopakettien avulla. Tietopaketit koostuvat yhdeksästä teemasta, jotka ovat saatavilla useassa eri muodossa, esimerkiksi julisteina, videoina tai sarjakuvina. Tietopakettien sisältöön voi tutustua myös tietokilpailupelin muodossa. Paketit sisältävät perustietoja hyvistä käytännöistä toimittaessa digitaalisessa maailmassa, kuten vahvoista salasanoista, varmuuskopioinnista, sosiaalisen median turvallisuudesta ja päivitysten tärkeydestä. Lisäksi

paketeissa on paljon ajankohtaista tietoa erilaisista riskeistä ja uhkista, kuten tietojen kalastelusta sekä erilaisista haittaohjelmista. Tietopaketit on luotu yhteistyössä ACYMA:n jäsentoimijoiden kesken.[649]

Safer Internet France on ranskalainen osa eurooppalaista Better Internet For Kids -ohjelmaa, jonka Euroopan komissio käynnisti vuonna 2008. Ranskan Safer Internet -ohjelma perustuu kolmeen toimintalinjaan: palvelevaan avustusnumeroon, tietoisuutta lisäävään internetsivustoon (Internet Without Fear) ja foorumiin, jossa voi ilmoittaa internetissä olevasta laittomasta sisällöstä. Safer Internet -keskukset (SIC) järjestävät myös vuosittain kansainvälisen Safer Internet -päivän, johon liittyy kansallisia tapahtumia ja kampanjoita. Ranskan SIC on toteuttanut myös FamiNum-ohjelman, joka tarjoaa oppeja perheille hyvistä ja turvallisista käytännöistä digitaalisessa maailmassa.[650]

3.17.3. Kansalliset erityispiirteet

Vaikka Ranska on vuosien ajan nostanut esille kybersodankäynnin puolustuksellisen ja hyökkäävän vaikuttavuuden tärkeyden, on se tuonut esille myös inhimillisten tekijöiden tärkeyttä osana kokonaisvaltaista kyberturvallisuutta ja pyrkii vaikuttamaan tähän tarjoamalla monipuolisesti kyberturvallisuuteen liittyvää koulutusta. Useiden maiden tapaan Ranska pyrkii integroimaan kyberturvallisuuskoulutusta kaikille oppiasteille, mutta se tarjoaa myös kyberturvallisuuden perustaitoihin keskittyvää koulutusta kansalaisille. Koulutuksen lisäksi Ranska pyrkii monin keinoin lisäämään kansalaisten tietoisuutta kyberturvallisuudesta ja tarjoaa tukea kyberrikollisuuden uhreille kyberstrategiansa mukaisesti.

Ranskan valtion tieto- ja kyberturvallisuusviranomainen ANSSI toimii Pariisissa La Défensen alueella sijaitsevassa vuonna 2022 toimintansa aloittaneessa kolmetoistakerroksisessa Cyber Campus -rakennuksessa. Kampus on osa presidentti Emmanuel Macronin kyberturvallisuushanketta, jonka tarkoituksena on kehittää Ranskan kyberturvallisuutta ja mahdollistaa valtion eri toimijoiden, kuten yritysten, koulutusorganisaatioiden, tutkijoiden ja yhdistysten, toimiminen yhteisissä tiloissa. Cyber Campus pyrkii myös vastaamaan koulutuksen tarpeen jatkuvaan lisääntymiseen kehittäen koulutustoimintaa. Cyber Campuksen tiloissa sijaitsee myös ANSSIn kyberturvallisuuteen keskittynyt koulutus- ja harjoittelukeskus, CFSSI.[651]

Ranskalla on myös tärkeä rooli kyberturvallisuuteen liittyvien kansallisten ja kansainvälisten verkostojen rakentajana. Pariisin rauhanfoorumin aikana 12. marraskuuta 2018 Ranska käynnisti Pariisin vetoomuspyynnön luottamuksesta ja turvallisuudesta kyberavaruudessa. Paris Call For Trust -vetoomuspyynnössä kehotetaan kaikkia kyberavaruudessa toimivia tahoja sitoutumaan yhteistyöhön turvaamaan yhteistä kybertoimintaympäristöä. Vetoomuspyyntö on ensimmäinen merkittävä aloite, joka tuo yhteen valtiot, yritykset ja järjestöt Euroopassa ja maailmanlaajuisesti.[652]

3.17.4. Kyberkansalaistaitojen määrittäminen

Ranska ei ole tarkasti määrittänyt kyberkansalaistaitojaan, mutta kansalaistaitojen voidaan katsoa perustuvan kansalaisille suunnatuissa koulutuskokonaisuuksissa esiintyviin sisältöihin, jotka usein keskittyvät digitaalisessa maailmassa tarvittaviin perustietoihin ja -taitoihin. Nämä tiedot ja taidot ovat digitaalisessa toimintaympäristössä vastuullista käyttäytymistä, jolla voidaan vaikuttaa omaan ja muiden turvallisuuteen. Kyberkansalaistaitojen opettaminen Ranskassa on kohdistettu kaikille kansalaisille ja kaikille ikäluokille.

Viitteet

[639] Philippe Baumard, *Cybersecurity in France* (SpringerLink, 2017), 56; Pascal Brangetto, *National Cyber Security Organisation: France* (Tallinn: CCDCOE, 2015), 8.
[640] ”SGDSN in English,” *Secrétariat général de la défense et de la sécurité nationale*, luettu 30.11.2022, http://www.sgdsn.gouv.fr/accueil/sgdsn-in-english/.
[641] République Française, Premier Ministre, *Estrategia Nacional Francesa para la seguridad del ambito digital*.
[642] ”Arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance. Arrêté du 3 mars 2017 portant approbation de la convention constitu-tive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance – Légifrance,” *Legifrance*, luettu 25.9.2022, www.legifrance.gouv.fr.
[643] Guillaume Poupard, *PROCESSUS POUR L'OBTENTION DU LABEL SECNUMEDU*, Premier Ministre (2016).
[644] ”SECNUMACADÉMIE,” *Agence nationale de la sécurité des systèmes d'informatio*, luettu 15.9.2022, https://www.ssi.gouv.fr/entreprise/formations/secnumacademie/.
[645] ”Cultivez vos compétences numériques,” *Pix*, luettu 12.9.2022, https://pix.org/fr/.
[646] Borka Jerman Blažič, *Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?* (Springer, 2021), 3025.
[647] ”FORMATIONS LABELLISÉES SECNUMEDU,” *Agence nationale de la sécurité des systèmes d'information*, luettu 2.10.2022. https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/.
[648] ”CYBERHEAD - Cybersecurity Higher Education Database,” *ENISA*, luettu 30.11.2022, https://www.enisa.europa.eu/topics/education/cyberhead#/.
[649] ”Assistance aux victimes de cybermalveillance,” *Cybermalveillance*, luettu 20.10.2022, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/qui-sommes-nous.
[650] ”Safer Internet France, Programme national de prévention et d’éducation aux bons usages d’Internet,” luettu 5.11.2022, https://www.saferinternet.fr.
[651] Michel Van Den Berghe, Yann Bonnet, Charly Berthet, Christian Daviot, Jean-Baptiste Demaison ja Faustine Saunier, *Cyber Campus, Uniting and expanding the cybersecurity ecosystem* (2021).
[652] ”Appel de Paris Pour la confiance et la sécurité dans le cyberspace,” *Appel de Paris 12.11.2018*, luettu 30.11.2022, https://pariscall.international/fr/.

3.18. Romania

ITU, Global Security Index (GCI) 2020	62/182 (Global), 32/46 (Europe)
National Cyber Security Index (NCSI) 2022	7/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	27/27

3.18.1. Strategiset kyberkoulutuslinjaukset

Romanian hallitus julkaisi 2021 uuden kyberturvallisuusstrategian ja tämän toimeenpano-ohjelman vuosille 2022–2027. Päivitetyssä strategiassa on määritetty uusia tavoitteita sekä tunnistettu osatekijöitä, jotka ovat merkityksellisiä digitaalisten palveluiden toiminnallisuuden sekä näiden turvallisen hyödyntämisen kannalta. Romanian kansallisen kyberturvallisuusstrategian tavoitteena on luoda tarvittavat puitteet valtionhallinnon, elinkeinoympäristön, kansantalouden sekä koulutus- ja tutkimusalan tulevaisuuden kehitykselle.[653]

Strategiassa korostuu yhtenäisen kyberturvallisuuskulttuurin systemaattinen rakentaminen ja tämän edelleen kehittäminen. Kulttuurin osalta keskeisiksi vaikutuskeinoiksi on tunnistettu muun muassa kansalaisten yleisen tietoisuuden lisääminen kybertoimintaympäristön, toiminnallisuuden, haavoittuvuuksien, riskien sekä tietojärjestelmien suojaamisen suhteen. Strategiassa määriteltyjen toimenpiteiden tarkoituksena on täyttää Romanian osalta Naton ja Euroopan unionin turvallisuustavoitteet ja sitoumukset. Romaniassa nähdään erittäin tärkeänä aktiivinen osallistuminen kansainväliseen kyberturvallisuuteen liittyvään tutkimusyhteistyöhön, yhteistoimintaan, tapahtumiin ja tiedonvaihtoon.[654]

Romaniassa toimintaa ohjaa lisäksi vuonna 2015 laadittu kansallinen digitaalistrategia (National Strategy on the Digital Agenda for Romania 2020), joka asettaa yhteiskunnan tavoitteet tieto- ja viestintäteknologian (ICT) taitojen kehittämiselle. Tavoitteena on luoda vankka tietopohja ja kouluttaa ammattitaitoista työvoimaa kyberturvallisuuden, pilvipalveluiden, avoimen datan, massadatan ja sosiaalisen median alojen tarpeisiin. Romanian yhteiskunnalle keskeiset arvot ja tavoitteet, kuten ilmastonmuutoksen ja energiavajeen sekä köyhyyden ja sosiaalisen syrjäytymisen torjunta, saavat erityistä painoarvoa eri toimialojen kuten valmistavaan tuotantoon, tutkimukseen ja kehittämiseen liittyvässä määrittely- ja sääntelytyössä.[655]

Romanian pääministerin kanslian alaisuuteen perustettiin vuonna 2022 kyberturvallisuusosasto (Directoral National De Securitate Cibernetică, DNSC), joka vastaa kyberturvallisuusasioiden koordinoinnista valtionhallinnossa. Romania käyttää osan tarkoitukseen suunnatuista EU:n elpymisvaroista osaston perustamiseen ja tämän tunnistettuihin kyberturvallisuushankkeisiin. Perustettu osasto toimii julkishallinnon, liike-elämän ja tiedemaailman välisenä yhdyssiteenä, jonka tavoitteena on luoda johdonmukainen ja häiriönsietokykyinen kybertoimintaympäristö kansallisella tasolla. DNSC järjestää tietoisuuskampanjoita ajankohtaisista aiheista, kuten roskapostien, haittaohjelmien ja verkkorikollisuuden ehkäisystä, sekä tiedottaa kansalaisille vallitsevasta kybertilanteesta ja sen uhkakentän muutoksista (CERT-RO). DNSC:llä on keskeinen rooli uuden kansallisen kyberturvallisuusstrategian täytäntöönpanossa ja tämän varmistamisessa. [656,657]

3.18.2. Kyberkansalaistaitojen opettamisen nykytila

Kyberkansalaistaitojen kehittämisen näkökulmasta Romaniassa on uudessa opetussuunnitelmassa huomioitu kyberturvallisuutta käsittelevien pakollisten koulutusohjelmien luominen ja toteuttaminen eri opintoasteilla. Romanian hallitus investoi koulutusteknologian kehittämiseen osana Euroopan komission 2021–2027 julkaisemaa, digitaalisen koulutuksen toimintasuunnitelmaohjelman toteutusta. Romaniassa on kohdennettu 881 miljoonaa euroa koulutuksien digitalisointiin, osana maan elvytys- ja selviytymissuunnitelmaa. Varat

käytetään digitaalisten pedagogisten taitojen, koulutussisältöjen sekä fyysisien laitteiden ja muiden resurssien parantamiseen kolmen periaatteen mukaisesti: i) koulutusjärjestelmien parantaminen data-analyysin ja ennakoinnin avulla, ii) digitaalisen teknologian parempi hyödyntäminen opetuksessa ja oppimisessa ja iii) digitaalisten taitojen ja osaamisen kehittäminen digitaaliseen toimintaympäristöön. Toimet tähtäävät muun muassa julkisen sektorin ja julkisten palvelujen käyttöön liittyvien kustannusten vähentämiseen sekä koulutusrakenteiden nykyaikaistamiseen. Romanian korkeakoulut pystyivät Covid-19-pandemian aikana mukautumaan uusiin opetusmalleihin, mutta ne vaativat selvästi lisäresursseja ja erityiskoulutuksien toteutumista tukeakseen digitaalisia mahdollisuuksia täysimääräisesti.[658]

Kuten DESI-indeksi osoittaa, Romanian aiempi panostus kansalaisten digitaalisten perustaitojen koulutukseen on ollut vähäistä. Tämän johdosta Romanian hallitus ryhtyi toimenpiteisiin osaamis- ja koulutustilanteen parantamiseksi. Helmikuussa 2017 käynnistettiin kolme hanketta: Cyber_Education, Cloud_Education ja K5-K8 Curricular Reform.[659]

Euroopan unionin rahoittamassa Cyber_Education-hankkeessa Romanian yhdeksän suurinta yliopistoa kutsuttiin luomaan yhteiset ja nykyaikaiset kyberturvallisuus- ja koulutuslaboratorioiden opetussuunnitelmat. Hankkeen käynnisti Bukarestin taloustieteellinen yliopisto, joka kouluttaa erityisesti kyberturvallisuuden erityisasiantuntijoita.[660] Cyber_Education-hankkeeseen liittyi kiinteänä osana Cloud_Education-ohjelma, joka keskittyy erityisesti uusien teknologioiden kuten pilvipalveluiden, massadatan, sosiaalisen median ja mobiiliohjelmoinnin ja näihin liittyvän osaamisen kehittämiseen. K5-K8 Curricular Reform -hankkeessa nykyaikaistettiin Romanian peruskoulujen opetussuunnitelmat 5.–8. luokkien (11–14-vuotiaiden) tietotekniikan ja tietojenkäsittelytieteen osalta. Hankkeen seurauksena kyberturvallisuustietoisuutta sisällytettiin ohjelmistosuunnitteluun ja koodaamiseen sekä 3D-suunnitteluun ja virtuaalitodellisuuteen liittyviin koulutusohjelmiin ja opintokokonaisuuksiin. Uudistettu opetussuunnitelma noudattaa MIT:n (Massachusetts Institute of Technology) professori Seymour Papertin periaatteita. Käynnissä on myös kyberturvallisuus- ja digitaitoja kehittävien valmennuksien ja koulutuksien toteuttaminen opettajille.[661]

Romaniassa on 54 julkista ja 35 yksityistä yliopistoa, jotka sijaitsevat 24 kaupungissa ja palvelevat yli 550 000:ta opiskelijaa. Kyberturvallisuuden koulutukseen erikoistuneita yliopistoja Romaniassa ovat Technical University of Cluj-Napoca, Information and Computing System Security ja University Politehnica of Bukharest-Faculty of Applied Sciences, Coding and Storage Theory of Information Master. [662,663,664]

Vuodesta 2012 alkaen Romaniassa on toiminut ammattimainen, riippumaton, puolueeton ja voittoa tavoittelematon yhdistys, Romanian tietoturvayhdistys RAISA (Romanian Association for Information Security Assurance), joka muodostui hankkeen kautta. Sen tavoitteena on edistää ja tukea yhteiskunnan toimintaa lisäämällä Romanian julkisten, yksityisten ja akateemisten toimijoiden välistä tiedonvaihtoa. Osapuolien tulee noudattaa seuraavia arvoja: jatkuvat investoinnit koulutukseen, avoimuus uusille menetelmille tiedon turvaamiseksi, osallistuminen tietoverkkorikollisuuden torjuntaan, faktoihin keskittyminen ja huippuosaamisesta huolehtiminen. Yhdistyksen visiona on edistää tietoturva-alan tutkimusta ja koulutusta sekä myötävaikuttaa alan tiedon ja teknologian luomiseen ja levittämiseen. RAISAlla on vahva edustus kansallisella tasolla. Se kokoaa yhteen professoreita ja tutkijoita huippuyliopistoista ja Romanian instituutioista, tohtorintutkintoja, maisteri- ja lisenssiopiskelijoita sekä IT-segmentin yrityksiä. Motivaationa on, että mikä tahansa yritys, organisaatio tai yhteisö hyötyy investoimalla järjestelmäturvallisuuteen parantaakseen tietoturvariskejä, kun järjestelmät ovat yhteydessä internetiin.[665]

Cyber4Kids-kampanja on hanke, jonka tavoitteena on kertoa vanhemmille ja heidän lapsilleen riskeistä, joille lapset altistuvat verkossa, ja siitä, miten niiltä voi suojautua. Kampanjan piirroselokuvien sarjassa esitetään, mitä kyberturvallisuus tarkoittaa. Jokaiseen jaksoon liittyy opas, jossa on verkkoturvallisuusvinkkejä. Yksi osio on vanhemmille ja yksi lapsille.[666]

MyDigiSkills auttaa ymmärtämään paremmin digitaalisten taitojen tasoa, joka perustuu tietoihin, taitoihin ja asenteisiin jokaisella Digital Competence Framework for Citizens -viitekehyksen (DigComp) viidellä osa-alueella. Sivustolla on 82 digitaalisiin taitoihin liittyvää kysymystä, joiden perusteella saa raportin digitaalisten taitojen tasosta. Foorumi on yleiseurooppalainen, mutta se on saatavilla myös romanian kielellä.[667]

Ora de Net on ohjelma, joka edistää lasten ja nuorten internetin käyttöä luovalla, hyödyllisellä ja turvallisella tavalla. Ohjelmassa järjestetään koulutustoimintaa ja kehitetään vanhemmille, opettajille ja asiantuntijoille suunnattuja koulutusresursseja. Ora de Netistä voi saada neuvoja mihin tahansa internetiin tai verkkoprofiileihin liittyviin kysymyksiin. Ora de Netiin voi raportoida Romanian verkkosivuilta löytyvää laitonta sisältöä ja auttaa näin rakentamaan turvallisempaa internetiä. Ohjelma koordinoi myös laajaa vapaaehtoisten opettajien ja asiantuntijoiden verkostoa. Vapaaehtoiset työskentelevät lasten kanssa ja toteuttavat koulutustoimintaa kansallisella tasolla.[668]

Fundația EOS – Koulutusta avoimelle yhteiskunnalle (EOS Romania – www.eos.ro) on yksityinen voittoa tavoittelematon organisaatio. Sen päätavoite on kaventaa digitaalista kuilua Romaniassa auttamalla ihmisiä tavoittamaan ja hyödyntämään koko potentiaalinsa teknologioiden avulla. Organisaatiolla on hankkeita kahdella osa-alueella: i) esikoulutusjärjestelmä (opettajien kouluttaminen tieto- ja viestintätekniikan käytössä ja heikommassa asemassa olevien nuorten kanssa työskentely) ja ii) laajempi yhteisö (työskentely IT- ja tietoyhteiskunnan heikommassa asemassa olevien yhteisöjen kanssa, niiden saattamiseksi osaksi tietoyhteiskuntaa).[669]

3.18.3. Kansalliset erityispiirteet

Tarkkaa kuvaa romanialaisten kyberkansalaistaidoista on vaikea muodostaa, koska asiasta ei kirjoiteta kovinkaan paljon eikä Romaniassa aiemmin ole ollut ajatushautomoita, jotka olisivat asiaa tutkineet. Yleisesti ottaen on syntynyt käsitys, että kansalaiset eivät ole kovin hyvin varautuneita kyberuhkiin Romaniassa, sillä kyberturvallisuudesta on alettu laajemmin puhua mediassa vasta parin viime vuoden aikana. Yhtenä syynä varautumattomuuteen kybertoimintaympäristössä ja ylipäätään digitalisaation tilaan on ollut Romanian aiempi koulutusjärjestelmä, joka ei ole panostanut medialukutaidon saatikka digi- tai kybertaitojen kehittämiseen. Muun muassa COVID-19-pandemian aikana huomattiin, että romanialaiset uskovat helposti valeuutisiin ja salaliittoteorioihin.[670]

Bukarest valittiin isännöimään Euroopan kyberturvallisuuden osaamiskeskusta (ECCC) vuonna 2020. Se on uusi Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, joka yhdistää keskeiset julkiset toimijat, teollisuuden toimijat ja alan tutkimuksen. Keskus hallinnoi Euroopan unionin miljardien eurojen kyberturvallisuuden tutkimus- ja kehitysrahoitusta, esimerkiksi salauksen ja tietoverkkoturvallisuuden alalla.[671]

3.18.4. Kyberkansalaistaitojen määrittäminen

Romaniassa ei ole määritelty selkeästi kyberkansalaistaitoja, mutta ne katsotaan liittyvän tiiviisti yleisiin digitaalisiin taitoihin verkossa liikkumisessa ja sovellusten käytössä. Viestinnässä painotetaan tietoisuutta omien toimien vaikutuksesta ja sosiaalisesta vastuusta, koska sillä on suuri merkitys myös muiden turvallisuuteen. Tarkoituksena on kehittää koulutusta ja vaikuttaa sitä kautta kansalaisten taitoihin, kuten ymmärtämään henkilötietojensa ja laitteidensa suojaamisen perusperiaatteet. Tavoitteena on ymmärtää digitaalisen ympäristön riskit ja uhat (esimerkiksi haittaohjelmat, sosiaalinen manipulointi, identiteettivarkaudet) ja tiedostaa tarvittavat toimenpiteet (esimerkiksi virustorjuntaohjelman ja verkon palomuurin käyttö).[672]

Viitteet

[653] GUVERNUL ROMÂNIEI, *Strategia de Securitate Cibernetica a României, pentru perioada 2022-2027* (2022).
[654] GUVERNUL ROMÂNIEI, Strategia de Securitate Cibernetica a României, pentru perioada 2022-2027 (2022).
[655] "National Strategy on the Digital Agenda for Romania 2020," *GUVERNUL ROMÂNIEI,* luettu 4.1.2023, https://www.gov.ro/en/government/cabinet-meeting/national-strategy-on-the-digital-agenda-for-romania-2020.
[656] "Press release," *Directoratul National De Securitate Cibernetică*, luettu 26.11.2022, https://dnsc.ro/vezi/document/dnsc-romanian-national-cyber-security-directorate-approved-by-government.
[657] Henkilökohtainen tiedonanto tutkijalle, 8.6.2022.
[658] "Romania Digilization of Education," *International Trade Administration*, luettu 5.12.2022, https://www.trade.gov/market-intelligence/romania-digitalization-education.
[659] "Cyber_Education, Cloud_Education and K5-K8 Curricular Reform," *CyberKnowledge Club*, luettu 4.1.2023, https://cyberknowledgeclub.org/projects/cyber_education-cloud_education-and-k5-k8-curricular-reform/.
[660] "TEORIA CODĂRII ŞI STOCĂRII INFORMAŢIEI," *FSA*, luettu 30.11.2022, https://www.tcsi.ro/.
[661] "Cyber_Education, Cloud_Education and K5-K8 Curricular Reform," *CyberKnowledge Club*, luettu 4.1.2023, https://cyberknowledgeclub.org/projects/cyber_education-cloud_education-and-k5-k8-curricular-reform/.
[662] "Information and Computing System Security," *Technical University of Cluj-Napoca*, luettu 27.11.2022, https://os.cs.utcluj.ro/sisc/.
[663] "Information and Computing System Security," Technical University of Cluj-Napoca, luettu 27.11.2022, https://os.cs.utcluj.ro/sisc/.
[664] "TEORIA CODĂRII ŞI STOCĂRII INFORMAŢIEI," *FSA*, luettu 30.11.2022, https://www.tcsi.ro/.
[665] "Romanian Association for Information Security Assurance," luettu 24.10.2022, https://www.raisa.org/.
[666] "Cyber4kids," luettu 26.11.2022. https://www.certsign.ro/en/cyber4kids/.
[667] "Mydigiskills," luettu 24.11.2022. https://mydigiskills.eu/index.php.
[668] "Ora De Net," luettu 28.10.2022. https://oradenet.ro/public/.
[669] "EOS Romania," luettu 4.1.2023, www.eos.ro.
[670] Henkilökohtainen tiedonanto tutkijalle, 19.7.2022.
[671] "Bucharest to host new EU cyber research hub," *Politico*, luettu 24.11.2022, https://www.politico.eu/article/bucharest-to-host-eus-new-cyber-research-hub/.
[672] "Strategia privind digitalizarea educatiei din Romania 2021-2027," *SMART-Edu*, luettu 3.12.2022, https://www.smart.edu.ro/#h.xck2kklw9ox5.

3.19. Ruotsi

ITU, Global Cybersecurity Index (GCI) 2020	26/182 (Global), 15/46 (Europe)
National Cyber Security Index (NCSI) 2022	14/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	4/27

3.19.1. Strategiset kyberkoulutuslinjaukset

Ruotsin vuonna 2017 käyttöön otettu kyberturvallisuusstrategia (Nationell strategi för samhällets informations- och cybersäkerhet) linjaa Ruotsin valtion kyberturvallisuuden prioriteetit ja tavoitteet. Sen päätavoite on taata yhteiskunnan toimivuuden kannalta tärkeiden osapuolten toimintakyky ja koko yhteiskunnan kokonaisturvallisuus. Julkisen sektorin, yksityisen sektorin ja kolmannen sektorin toimijoiden lisäksi tavoitteena on parantaa myös yksityishenkilöiden tietotaitoja arjen kyberturvallisuudessa.[673]

Strategiassa on kuusi osa-aluetta: systemaattinen ja yhteisesti johdettu kyberturvallisuustoiminta, tietoverkkojen, tuotteiden ja järjestelmien tietoturvallisuus, kyberhyökkäyksien ja muiden digitaalisten uhkien havainnointi ja käsittely, kyberrikosten vastainen taistelu ja ennaltaehkäisy, yleinen tietotason nostaminen digitaalisesta turvallisuudesta sekä kansainvälisen yhteistyön rakentaminen. Se painottaa tavallisen käyttäjän vastuuta ja korostaa inhimillisen tekijän tärkeyttä kybermaailman riskienhallinnassa. Ensimmäinen osa-alue koskee tiedon keskittämistä ja jakamista kaikille yhteiskunnan toimijoille, myös kansalaisille. Toiseen osa-alueeseen kuuluvat tietoturvalliset tuotteet, myös kuluttajamarkkinoilta. Kolmanteen osa-alueeseen sisältyy yhteiskunnan toimivuuden kannalta keskeiset palvelut, jotka sivuavat kansalaisen arkea. Neljäs osa-alue käsittelee verkkorikollisuutta ja ottaa huomioon myös kuluttajat. Viides osa-alue keskittyy yleisen tietoturvaosaamisen tason nostamiseen, mikä tarkoittaa myös tavallisten kansalaisten osaamistasoa. Kuudes osa-alue on suunnattu kansainväliseen yhteistyöhön, mutta silläkin on kytkös kuluttajiin ja kansalaisiin, sillä sen myötä muovautuu muun muassa kansainvälinen säätely esimerkiksi erilaisiin kuluttajien käyttämiin palveluihin.[674]

Strategian pohjalta on laadittu kyberturvallisuuden toimintasuunnitelma vuosille 2019–2022. Siinä on eritelty jokaiseen osa-alueeseen liittyvät toimenpiteet ja vastuut. Niistä erityisesti erilaiset kampanjat näkyvät suoraan kansalaisille. Kyberrikollisuuden ehkäisemiseksi suunnitellaan kampanjoita, joissa hyödynnetään Europolin tarjoamia resursseja ja tehdään yhteistyötä muiden Pohjoismaiden kanssa. Kansallisella ”Tänk säkert” (”Ajattele turvallisesti”) -kampanjalla levitetään kansalaisille ja pienyrityksille tietoa kyberturvallisuusuhkista ja tiedon suojaamisesta. Kampanjoita järjestetään esimerkiksi Euroopan kyberturvallisuuskuukauden (ECSM) aikana.[675]

Ruotsin tavoitteena on olla maailman paras maa digitalisaation tarjoamien mahdollisuuksien hyödyntämisessä. Tätä tavoitetta ohjaa hallituksen digitalisointistrategia, jonka toimeenpanosta vastaa kansallinen digitalisointineuvosto Digitaliseringsrådet. Strategian osa-alueet ovat digitaalinen osaaminen, turvallisuus, innovaatiot, infrastruktuuri ja johtaminen. Digitaalisen turvallisuuden tavoitteena on luoda hyvät edellytykset digitaalisen yhteiskunnan luottamukselle, jotta kaikki voivat tuntea olonsa turvalliseksi. Yksi digitaalisen osaamisen ja turvallisuuden kulmakivistä on, että jokaisella on riittävät digitaalisen osaamisen perustaidot.[676]

3.19.2. Kyberkansalaistaitojen opettamisen nykytila

Ruotsissa on useita julkisen, yksityisen ja kolmannen sektorin toimijoita, jotka tarjoavat kyberkansalaistaitojen koulutusta. Kyberturvallisuudesta vastaavia viranomaisia ovat Ruotsin turvallisuusvirasto (Myndigheten för Samhällsskydd och Beredskap, MSB), puolustusmateriaalihallinto (Försvarets materielverk, FMV),

puolustusradiolaitos (Försvarets radioanstalt, FRA), puolustusvoimat, posti- ja telehallintoviranomainen (Post- och telestyrelsen, PTS), poliisiviranomainen ja turvallisuuspoliisi (Säkerhetspolisen, Säpo). Viranomaiset ovat muodostaneet yhteistyössä Ruotsin kansallisen kyberturvallisuuskeskuksen (National Cyber Security Center for Sweden, NCSC).[677]

Turvallisuusvirasto MSB tarjoaa koulutuksia organisaatioille ja kansalaisille. Sen koulutusvalikoimaan kuuluu useita eri tason kursseja perustason kyberturvallisuudesta omaan MSB Collegeen asti.[678] MSB:n verkkosivuilla on kansalaisille tarkoitettuja kyberturvallisuusohjeita ja viranomaisten yhteistyössä laatimia raportteja, joiden tarkoituksena on lisätä kyberturvallisuustietoa[679]. MSB:n Disa (Digital informationssäkerhetsutbildning för alla, ”digitaalisen turvallisuuden koulutus kaikille”) on erityisesti eri kokoisille organisaatioille suunnattu maksuton ja kaikille avoin kyberturvallisuuden perusteiden verkkokoulutus. Kurssilla käsiteltävät aihepiirit ovat turvallinen käyttäytyminen, salasanat, varmuuskopiointi, pilvipalvelut, sähköposti, sosiaalinen media, lähettäjän tarkistaminen, haittaohjelmat, verkkoturvallisuus työpaikan ulkopuolella ja ongelmatilanteet. Kurssin suorituksesta saa todistuksen.[680]

Ruotsin peruskouluissa opetetaan tietojenkäsittelyä osana muiden aineiden opetusta. Toisella asteella tietojenkäsittelyn voi ottaa valinnaiseksi oppiaineeksi. Turvallisuuteen liittyvää opetusta annetaan peruskoulun kaikilla luokka-asteilla osana tietojenkäsittelyn oppimistavoitteita.[681] ENISAn CyberHEAD-tietokannan mukaan Ruotsin korkeakouluissa on tarjolla kolme kyberturvallisuuden koulutusohjelmaa.[682] Mastersportal-tietokanta luettelee seitsemän kyberturvallisuuden tai informaatioturvallisuuden koulutusohjelmaa, joita tarjoavat University West, KTH Royal Institute of Technology, Stockholm University, Linköping University, University of Skövde, Halmstad University sekä Luleå University of Technology. Edellä mainittujen yliopistoiden verkkosivut vahvistavat, että ohjelmat ovat tällä hetkellä mukana koulutustarjonnassa. [683] Ruotsin Maanpuolustuskorkeakoulu (Försvarshögskolan) tarjoaa koulutuksia sekä turvallisuusviranomaisille että siviileille.[684] Suunnitteilla on lisäksi kyberturvallisuuden tutkimukseen, koulutukseen ja innovointiin erikoistunut Cybercampus Sweden, jonka tavoitteena on vahvistaa Ruotsin kyberturvallisuutta.[685]

Valtion medianeuvosto (Statens medieråd) ja lasten oikeuksia ajava järjestö Bris ylläpitävät Ruotsin Safer Internet Centreä (SIC), joka on osa Euroopan komission tukemia kansainvälisiä Insafe-, INHOPE- ja Better Internet for Kids -verkostoja. SICin tavoitteena on edistää lasten ja nuorten verkkoturvallisuutta. Se toimii ennaltaehkäisevästi tarjoamalla tietoa ja tukea lapsille, nuorille, ammattilaisille ja huoltajille. SIC muun muassa tuottaa raportteja, kehittää opetusvälineitä ja -menetelmiä sekä järjestää tapahtumia ja kampanjoita. Lapset ja nuoret osallistuvat SICin toimintaan eri tavoin, esimerkiksi toimimalla nuorisopaneelissa. Valtion medianeuvosto koordinoi lisäksi kansallisia toimia ruotsalaisten media- ja informaatiolukutaidon vahvistamiseksi.[686] Se on ollut päävastuussa MIK-tietopankin (MIK Sveriges kunskapsbank) kehittämisessä ja vastaa sen toiminnasta. Tietopankissa on eri toimijoiden tietomateriaaleja kaikille, jotka haluavat kehittää media- ja informaatiolukutaitojaan, aina lapsista ikääntyneisiin. Esimerkiksi Utbildningsradionin tuottamissa ohjelmissa käsitellään myös kyberturvallisuusaiheita.[687]

Internetstiftelsen on riippumaton säätiö, joka huolehtii .se- ja .nu-verkkotunnuksista. Sen tavoitteena on rakentaa internetiä, joka vaikuttaa myönteisesti ihmisiin ja yhteiskuntaan. Visiona on, että jokaisen tulisi haluta ja uskaltaa käyttää sekä pystyä käyttämään internetiä. Säätiön Internetkunskap- ja Digitala lektioner -verkkosivuilla on laajasti digitaalisen osaamisen parantamiseen tähtäävää tietoa ja materiaaleja. Yksi osa-alueista on verkkoturvallisuus, josta on tarjolla pikakursseja ja syventäviä artikkeleita, joissa käsitellään muun muassa verkkohuijauksia, salasanoja, kalastelua ja haittaohjelmia. Sivustoilla opastetaan, miten kannattaa toimia, jos on joutunut verkkohuijauksen kohteeksi. Digitala lektioner -sivusto sisältää valmiita oppitunteja peruskoulun eri luokille. Ne täyttävät opetussuunnitelman vaatimukset.[688,689]

Vuonna 2019 käynnistetyn Cybersecurity Academyn tavoitteena on antaa yläkoulu- ja lukioikäisille nuorille tietoa verkkoturvallisuudesta koulutusmateriaalien, luentojen ja työpajojen kautta. Nuorille tarjotaan välineitä, joiden avulla he pystyvät tunnistamaan riskejä ja suojautumaan verkossa. Tarkoituksena on samalla herättää nuorten uteliaisuutta tietotekniikkaan ja teknologiaan. Cybersecurity Academy tarjoaa kouluille ilmaiseksi

erilaisia opetusmateriaaleja, asiantuntijaluentoja ja opettajille täydennyskoulutusta. Yläkoulun ja toisen asteen opettajille on laadittu lisäksi opettamista tukevia oppaita. Tietotekniikasta ja tietoturvasta innostuneiden oppilaiden on mahdollista saada ilmaista opetusta myös kouluajan ulkopuolella. Tähän mennessä hanke on tavoittanut noin 340 000 oppilasta ja noin 4 700 koulua. Nopeasti suosiota kasvattanut Cybersecurity Academy on Unga Forskare -järjestön ja IBM:n yhteishanke, jota MSB tukee ja jolla on useita yhteistyökumppaneita.[690,691]

Ruotsi osallistuu vuosittain ENISAn järjestämään Euroopan kyberturvallisuuskuukauteen. Kyberturvallisuusstrategian toimintasuunnitelmassa mainittua ”Tänk säkert” -kampanjaa on hyödynnetty onnistuneesti jo usean vuoden ajan. Kampanjan tavoitteena on nostaa koko yhteiskunnan kyberturvallisuusosaamista lisäämällä tietoisuutta kyberhygieniasta, kuten hyvistä salasanakäytännöistä, kalastelun tunnistamisesta ja tärkeiden tietojen suojaamisesta. Kampanjan verkkosivuilla on tietoa kyberturvallisuuden eri aiheista. Materiaalit on suunnattu eri kohderyhmille, kuten vanhemmille, opettajille ja yli 65-vuotiaille. Materiaaleja on julkaistu myös eri kielillä. Sivuilla voi tehdä testin, jossa arvioidaan, kuinka suuri turvallisuusriski testaaja itse on. MSB ja poliisi toteuttavat kampanjaa yhteistyössä, ja sen levittämiseen osallistuu lisäksi suuri määrä yhteistyökumppaneita. Vuoden 2021 kyberturvallisuuskuukauden aikana kampanja tavoitti 12,6 miljoonaa kansalaista (1,5 miljoonaa vuonna 2020). Kuukauden aikana järjestettiin yli 60 webinaaria ja luentoa. Kampanjan yhteydessä tehdyn tutkimuksen mukaan väestön kyberturvallisuuskäyttäytyminen muuttuu hitaasti ja siksi kampanjointityön on oltava pitkäjänteistä. Saadut tulokset ovat osoittaneet kampanjan tärkeyden.[692,693,694]

3.19.3. Kansalliset erityispiirteet

Ruotsi on yksi maailman digitalisoituneimpia maita. Se tuo mukanaan monia etuja, mutta myös riskejä – Ruotsi on houkutteleva verkkohyökkäysten kohde ja samalla haavoittuvainen. Ruotsalaisten kyberturvallisuusosaaminen on yleisesti ottaen vielä riittämätöntä, vaikka tilanne on viime vuosina kohentunut. Internetstiftelsen-järjestön mukaan yleistä internetosaamista olisikin parannettava, jotta entistä useammat ymmärtäisivät digitaalisten palveluiden riskit ja osaisivat ehkäistä niitä. On esimerkiksi ehdotettu, että kyberturvallisuutta opetettaisiin erillisenä oppiaineena peruskoulussa.[695,696]

Ruotsalaisten internetin käyttöä tutkivassa raportissa (2022) kerrotaan, että suurin osa kansalaisista rajoittaa internetin käyttöään jollakin tavoin. Yleisimmät syyt tähän ovat oman yksityisyyden suojaaminen ja huoli verkkohuijauksista. Nuoremmat käyttäjät ovat enemmän huolissaan yksityisyydensuojasta. Hakkereiden ja huijareiden pelko on puolestaan suurempaa ikääntyneiden keskuudessa. Puolet ruotsalaisista rajoittaa internetin käyttöään jollakin tavoin turvattomuuden tunteen takia.[697]

3.19.4. Kyberkansalaistaitojen määrittäminen

Digitaliseringsrådetin määritelmän mukaan digitaalinen osaaminen sisältää: 1) taidon etsiä tietoa, viestiä, olla vuorovaikutuksessa ja tuottaa sisältöä digitaalisesti, 2) valmiudet käyttää digitaalisia työvälineitä ja palveluita, 3) ymmärryksen digitalisaation tuomasta muutoksesta yhteiskunnassa mahdollisuuksineen ja riskeineen ja 4) motivaation osallistua kehitykseen. Digitaalinen osaaminen näyttäytyy neljällä elämänalueella: yksityiselämässä, sosiaalisessa elämässä, koulutuksessa ja työelämässä.[698] Kyberkansalaistaitoja on määritelty myös DigComp-viitekehyksen pohjalta. DigComp 2.2 -versio on julkaistu ruotsin kielellä lokakuussa 2022.[699] Tänk säkert -kampanjassa kerrotaan, miten jokainen kansalainen voi omalta osaltaan panostaa Ruotsin kyberturvallisuuteen. Ohjeistuksessa käsitellään hyviä salasanakäytäntöjä, turvallista sähköistä tunnistautumista, varmuuskopiointia sekä haittaohjelmilta, kiristyshaittaohjelmilta ja kalastelulta suojautumista.[700]

Viitteet

[673] Government Offices of Sweden, *Ministry of Justice, A national cyber security strategy, Skr. 2016/17:213* (2017).
[674] Government Offices of Sweden, *Ministry of Justice, A national cyber security strategy, Skr. 2016/17:213* (2017).
[675] Swedish Civil Contingencies Agency (MSB), *Comprehensive Information and Cyber Security Action Plan for the years 2019–2022* (2020).
[676] ”Sveriges digitalisering,” *Digitaliseringsrådet*, luettu 14.12.2022, https://digitaliseringsradet.se/sveriges-digitalisering/.
[677] ”Vårt uppdrag: Att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot,” *Nationellt cybersäkerhetscenter*, luettu 14.12.2022, https://www.ncsc.se/.
[678] “Training and exercises,” *Swedish Civil Contingencies Agency (MSB)*, luettu 13.12.2022, https://www.msb.se/en/training--exercises/.
[679] ”Informationssäkerhet,” *MSB Myndigheten för Samhällsskydd och Beredskap*, luettu 13.12.2022, https://www.msb.se/sv/rad-till-privatpersoner/informationssakerhet/.
[680] ”Digital informationssäkerhetsutbildning för alla (Disa),” *MSB Myndigheten för Samhällsskydd och Beredskap*, luettu 16.12.2022, https://www.msb.se/sv/utbildning--ovning/alla-utbildningar/datorstodd-informationssakerhetsutbildning-for-anvandare-disa/.
[681]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 23-53.
[682] ”CYBERHEAD - Cybersecurity Higher Education Database,” *ENISA*, luettu 13.12.2022, https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/.
[683] ”Studyportals,” luettu 14.12.2022, https://www.mastersportal.com/study-options/268861763/cyber-security-sweden.html.
[684] ”Swedish Defence University,” luettu 13.12.2022, https://www.fhs.se/en/swedish-defence-university.html.
[685] ”Cybercampus Sweden,” luettu 14.12.2022, https://cybercampus.se/.
[686] ”Swedish Safer Internet Centre,” *Better Internet for Kids*, luettu 13.12.2022, https://www.betterinternetforkids.eu/sic/sweden.
[687] ”MIK Sveriges kunskapsbank,” *Statens Medieråd*, luettu 13.12.2022, https://www.statensmedierad.se/mik-sveriges-kunskapsbank.
[688] ”Säkerhet på nätet,” *Internetkunskap, Internetstiftelsen*, luettu 15.12.2022, https://internetkunskap.se/sakerhet-pa-natet/.
[689] ”Fria lektioner i digital kompetens,” *Digitala Lektioner, Internetstiftelsen*, luettu 15.12.2022, https://digitalalektioner.se/.
[690] ”Cybersecurity Academy,” *Unga Forskare*, luettu 16.12.2022, https://ungaforskare.se/cybersecurityacademy/.
[691] ”Stärk ungas kunskaper inom cybersäkerhet,” *Cybersecurity Academy*, luettu 16.12.2022, https://cybersecurityacademy.se/.
[692] ”Informationssäkerhetsmånaden,” *MSB Myndigheten för Samhällsskydd och Beredskap*, luettu 14.12.2022, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/informationssakerhetsmanaden/.
[693] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 139-140.
[694] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022).
[695] Emmy Englund ja Linnéa Tullin, *Cybersäkerhet, En kartläggning av Sveriges nuläge 2020 och framtidsutsikter för branschen* (2020), 20-21.
[696] Digitaliseringsrådet, *En lägesbild av digital trygghet* (2018), 22.
[697] ”Svenskarna och internet 2022,” *Internetstiftelsen*, luettu 15.12.2022, https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2022/.
[698] Digitaliseringskommissionen, *Gör Sverige i framtiden – digital kompetens* (SOU 2015:28), 102-103.
[699] ”Lansering av DigComp 2.2 på svenska,” *Dataföreningen*, luettu 15.12.2022. https://dfs.se/pa_gang/lansering-av-digcomp-2-2-pa-svenska/.
[700] MSB Myndigheten för Samhällsskydd och Beredskap, *Alla kan bidra till Sveriges cybersäkerhet. Du också! Tänk säkert*, https://rib.msb.se/filer/pdf/30140.pdf.

3.20. Saksa

ITU, Global Cybersecurity Index (GCI) 2020	13/182 (Global), 5/46 (Europe)
National Cyber Security Index (NCSI) 2022	6/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	13/27

3.20.1. Strategiset kyberkoulutuslinjaukset

Saksa on hyväksynyt viime vuosien aikana jo useamman kyberturvallisuuteen liittyvän strategian, kuten Kansallisen suunnitelman tietoinfrastruktuurien suojaamiseksi vuonna 2005, ensimmäisen kyberturvallisuusstrategian 2011, toisen kyberturvallisuusstrategian 2016 ja viimeisimmän päivityksen Saksan kyberturvallisuusstrategiasta 2021.[701] Saksassa liittovaltion sisäministeriöllä (Bundesministerium des Inneren, BMI) on tärkeä rooli kansallisiin tieto- ja kyberturvaan liittyvissä asioissa. Sisäministeriö toimii tiiviissä yhteistyössä Saksan tietoturvaviraston, BSI:n (Bundesamt für Sicherheit in der Informationstechnik) kanssa ja pyrkii kehittämään liittovaltion tieto- ja kyberturvallisuutta. Vuonna 2011 liittovaltion sisäministeriö julkaisi Saksan kyberturvallisuusstrategian (Cyber-Sicherheitsstrategie für Deutschland 2011). Strategiassa hallitus nosti esille kyberturvallisuuden tärkeyden osana Saksan muuttunutta turvallisuusympäristöä. Saksan kyberturvallisuusstrategia päivitettiin vuosina 2016 ja 2021. Alusta alkaen Saksan kyberturvallisuus on pyrkinyt noudattamaan teknistä ja ennalta ehkäisevää lähestymistapaa, jonka keskiössä on tietojärjestelmien ja kriittisen infrastruktuurin suojaaminen väestönsuojelun näkökulmasta.[702] 2016 päivitettyä kyberturvallisuusstrategiaa on luonnehdittu ensimmäiseksi strategiaksi, joka keskittyy yhteiskunnallisen näkökulman lisäksi myös yksittäisten käyttäjien erityistarpeisiin.[703] Tämä vuoden 2016 strategiassa esitetty koko yhteiskunnan kattava lähestymistapa käynnisti myös kansallisen kyberturvallisuussopimuksen toimeenpanon. Sopimuksen tavoitteena on vahvistaa kaikkien yhteiskunnan toimijoiden yhteistä vastuuta digitaalisesta turvallisuudesta.[704] 2016 strategian mukaan vastuullinen käyttäytyminen kyberavaruudessa ja internetin käytön tuomat mahdollisuudet sekä siihen liittyvät riskit ovat olennainen osa tämän päivän digitaalisia kansalaistaitoja. Tämän vuoksi digitaalinen koulutus tulee strategian mukaan integroida tiukasti maan koko koulutusjärjestelmään. Liittovaltion tavoitteena on, että nuorien ihmisten valmistuessa opinnoistaan heillä olisi riittävät tiedot ja taidot tieto- ja informaatiotekniikan turvallisuudesta. Strategian mukaan hallituksen tavoitteena on myös tulevaisuudessa pyrkiä lisäämään ja laajentamaan kurssitarjontaa IT-alalla perustamalla lisää opiskelupaikkoja yliopistoihin ja tukemaan johtavia instituutioita, etenkin tietojenkäsittelytieteessä esimerkiksi big data -analyysien, teollisuuden ohjelmistojen ja IT-turvallisuuden osalta.[705]

3.20.2. Kyberkansalaistaitojen opettamisen nykytila

Saksan kyberturvallisuusstrategian mukaisesti kyberturvallisuuteen liittyviä opintoja on pyritty lisäämään kaikille kouluasteille ja useat yliopistot tarjoavatkin kyberturvallisuuteen liittyviä opintokokonaisuuksia sekä maisteriohjelmia. ENISAn (The European Union Agency for Cybersecurity) mukaan Saksassa on vuonna 2022 viisi suoraan kyberturvallisuuteen keskittyvää korkeakouluohjelmaa. [706] Koulutusohjelmien lisäksi lähestulkoon kaikissa Saksan yliopistoissa on nykypäivänä tarjolla tietotekniikan opintoja, joihin sisältyy myös tietoturvallisuuden ja kyberturvallisuuden opetuskokonaisuuksia.

Saksan tietoturvavirasto BSI:llä on tärkeä rooli maan kyberturvallisuuden kehittämisessä ja ylläpitämisessä. BSI tarjoaa kattavasti tietoa tietoturvasta ja kyberturvallisuudesta toimimalla aktiivisessa yhteistyössä eri organisaatioiden ja yksityisen sektorin kanssa. BSI tarjoaa kansalaisille tietoa, kuinka suojautua erilaisilta kyberhyökkäyksiltä ja kuinka toimia jouduttaessa hyökkäyksen uhriksi. Materiaalia on saatavilla myös

opetusvideoina. BSI on toteuttanut myös lukuisia kampanjoita, joilla pyritään parantamaan kansalaisten osaamista kyberturvallisuuden osalta.

Kyberturvallisuuteen liittyvä koulutus ja opetus Saksassa on kattavasti integroitu koulutusjärjestelmään ja näin ollen kuuluu pääosin osaksi oppilaitoksissa opiskelevien opintoja, kuten vuoden 2016 kyberturvallisuusstrategiassa tuodaan esille. Tarve tarjota kansalaisille kyberturvallisuuteen liittyvää peruskoulutusta on tiedostettu Saksassa, mutta koulutus on tällä hetkellä enemmän yhdistysten ja yksityisen sektorin toteuttamaa. Deutschland sicher im Netz e.V. (DsiN) -niminen yhdistys perustettiin vuonna 2006 edellä mainittua tarkoitusta varten ensimmäisessä kansallisessa IT-huippukokouksessa. DsiN on liittovaltion sisäministeriön tukema yhdistys ja sen tarkoituksena on tukea kuluttajia ja pienempiä yrityksiä toimimaan turvallisesti ja luottavaisesti digitaalisessa maailmassa. Se tarjoaa yhdessä jäsentensä ja kumppaneidensa kanssa apua ja oppia turvalliseen internetin käyttöön kaikenikäisille yksityishenkilöille työssä ja arjessa. Tukea on tarjolla muun muassa erilaisten oppimateriaalien ja tarkastuslistojen muodossa. Yksityishenkilöiden lisäksi DsiN tarjoaa tukeaan myös pienille ja keskisuurille yrityksille.[707]

Kansalaisille ja etenkin lapsille suunnatun tieto- ja kyberturvallisuuskoulutuksen osalta tärkeässä roolissa BSI:n ja DsiN:n lisäksi on Saksan Safer Internet Centre. Keskus on ollut toiminnassa jo vuodesta 2008 ja yhdistänyt aiemmin erikseen rahoitetut internetin turvalliseen käyttöön ja neuvontaan keskitetyt palvelut yhdeksi kokonaisuudeksi. Näitä ovat esimerkiksi Klicksafe-palvelu, internettukilinjat internet-beschwerdestelle.de ja jugendschutz.net sekä lapsille, nuorille ja heidän vanhemmilleen suunnattu auttava puhelin Nummer gegen Kummerin. Safer Internet Centre Germany on osa Euroopan komission vuonna 1999 kehittämää strategiaa, jonka avulla pyritään lisäämään kansalaisten tietoisuutta turvallisesta internetin käytöstä. Ohjelma rahoittaa turvalliseen internetin käyttöön erikoistuneita keskuksia (Safer Internet Centre) 27 Euroopan maassa, myös Saksassa. Keskusten päätavoitteena on lisätä lasten, vanhempien, opettajien ja nuorisotyöntekijöiden tietoisuutta internetin käyttöön liittyvistä riskeistä sekä tarjota nuorille neuvoja internetin turvalliseen käyttöön. Toimintaan kuuluu myös auttavia yhteyspisteitä, joihin on mahdollista ilmoittaa internetissä havaitusta laittomasta sisällöstä.[708] Osana Safer Internet DE:tä on perustettu myös niin kutsuttu nuorisopaneeli, joka perustettiin Rheinland-Pfalzin akateemisessa lukiossa vuonna 2009. Se tarjoaa nuorille paikan, jossa on mahdollista ilmaista näkemyksiä ja mielipiteitä sekä vaihtaa tietoa ja kokemuksia erilaisten verkkoteknologioiden käytöstä. Lisäksi Saksan tiedotuskeskus ja vihje- sekä auttava puhelin tekevät jatkuvaa yhteistyötä asiaankuuluvien organisaatioiden kanssa niin kansallisesti kuin Euroopankin tasolla, esimerkiksi osallistumalla erilaisiin tietoisuuden lisäämiseen liittyviin tapahtumiin ja tietoiskuihin, joista esimerkkinä on muun muassa Safer Internet -päivä.[709]

Klicksafe on kahden Saksan liittovaltion mediaviranomaisen yhteinen projekti. Nämä mediaviranomaiset ovat Median ja viestinnän keskusviranomainen Rhineland-Palatinate (LMK), joka toimii toiminnan koordinointivastaavana, ja North Rhine-Westphalian mediaviranomainen (LfM). Mediaviranomaisten lakisääteisiin velvollisuuksiin kuuluvat lisensointi, tuen antaminen, medialukutaidon edistäminen ja telemedian valvonta. Valvontaa hallinnoi alaikäisten turvallisuutta ja suojelemista mediassa käsittelevä komissio (KJM). KJM on LMK:n täysivaltainen jäsen.[710] Klicksafen tarkoituksena on pyrkiä edistämään ihmisten verkko-osaamista. Palvelu on suunnattu ihmisille, jotka tukevat lapsia ja nuoria heidän internettaitojensa kehittämisessä, kuten esimerkiksi opettajille ja vanhemmille, ja se tarjoaa yleiskatsauksen ajankohtaisista verkkoaiheista sekä konkreettisia vinkkejä ja oppeja jokapäiväiseen elämään digitaalisessa ympäristössä. Palvelun tietoportaalista käyttäjät löytävät muun muassa erilaisia ajantasaisia tietoja, käytännön vinkkejä ja hyödyllistä materiaalia digitaalisista palveluista ja niihin liittyvistä aiheista. Toiminta-alueeseen kuuluvat myös erilaisten aiheeseen liittyvien kampanjoiden toteuttaminen. Klicksafe toteuttaa myös erilaisia lapsille, nuorille, vanhemmille, opettajille ja asiantuntijoille suunnattuja kursseja internetin käyttöön ja erilaisista internetiin liittyvistä riskitekijöistä. Klicksafe nostaa myös tavoitteekseen medialukutaidon edistämisen internetissä. Saksassa ja muualla Euroopassa Klicksafe toimii aktiivisesti ja julkaisee erilaisia tietopaketteja ja asiaankuuluvia julkaisuja eri kohderyhmille. Klicksafen internetsivuilta löytyy myös interaktiivisia opetustehtäviä, joissa palvelun käyttäjät voivat harjoitella tietoteknisiä taitoja muun muassa pelinomaisesti.[711]

Yksityisellä sektorilla toimiva IMC on saksalaisen Saarland-yliopiston perustama yritys, joka tarjoaa kokonaisvaltaista tukea julkiselle sektorille, yrityksille ja oppilaitoksille digitaalisten koulutusstrategioiden suunnittelussa ja toteuttamisessa. IMC tarjoaa myös verkko-oppimisympäristöjä ja erilaisia pelejä. Peleistä mainittakoon Cyber crime time -peli, jota yritys tarjoaa ilmaisella lisenssillä yksityisille henkilöille ja maksullisella lisenssillä yrityksille. Pelin ajatus perustuu erilaisiin kyberrikollisuuteen liittyviin aiheisiin ja se valmentaa palvelun käyttäjää tunnistamaan ja ennaltaehkäisemään erilaisia kyberriskejä. Pelissä käsiteltävät aiheet liittyvät esimerkiksi käyttäjän sosiaaliseen manipulointiin, turvallisten salasanojen muodostamiseen, tietojen kalasteluun, etätyöskentelyn aiheuttamiin uhkiin, erilaisiin haitta- ja kiristyshaittaohjelmiin, identiteettivarkauksiin ja yleisten langattomien verkkojen turvallisuusuhkiin.[712]

3.20.3. Kansalliset erityispiirteet

Kyberturvallisuus nähdään Saksassa keskeisenä osana sisä- ja ulkopolitiikkaa sekä turvallisuuspolitiikkaa. Vuosien saatossa kyberturvallisuuden ympärille on kehittynyt Saksassa laaja ja tiivis toimijaverkosto, jolla on lukuisia yhteyksiä kansallisella ja kansainvälisellä tasolla. Toimijaverkosto luo edellytykset jäsennellylle ja kestävälle kyberturvallisuuspolitiikalle. Tähän monimutkaiseksikin kutsuttuun ekosysteemiin on mahdollista tutustua asiantuntijaorganisaatio Stiftung Neue Verantwortungin (SNV) kahdesti vuodessa julkaistavassa ”Saksan kyberturvallisuusarkkitehtuurissa” (Deutschlands staatliche Cybersicherheitsarchitektur).[713] Saksassa järjestetään vuosittain erittäin laaja-alainen Wirtschaftsinformatik-konferenssi, jossa käsitellään digitalisaatiota ja kyberturvallisuutta yhteiskunnan eri toimintojen näkökulmasta.[714] Erillinen Dagstuhl Institute järjestää ympäri vuoden lyhyitä vuoropuheluita, keskusteluja ja ideoiden vaihtoja tiedeyhteisön sidosryhmien kanssa muun muassa kyberturvallisuudesta.[715]

Saksan osavaltioilla on laaja itsehallinto, joka näkyy myös kyberturvallisuuteen liittyvissä asioissa. Eräät osavaltiot, kuten esimerkiksi Nordrhein-Westfalenin osavaltio, ovat laatineet myös oman kyberturvallisuusstrategian, joka pohjautuu liittovaltion kyberturvallisuusstrategiassa määritettyihin tavoitteisiin. Strategiassa painotetaan muun muassa yksittäisten henkilöiden tieto- ja kyberturvallisuusosaamisen tärkeyttä kokonaisvaltaisen kyberturvallisuuden kannalta.[716] Liittovaltion tutkimus- ja opetusministeriö koordinoi liittovaltion ja osavaltioiden yhteistyötä sekä kansainvälistä ja EU-yhteistyötä koulutusasioissa, ja koulutuspolitiikka on yleisesti osavaltioiden vastuulla. Näin ollen koulutusjärjestelmän organisointi ja päätöksenteko eivät tapahdu liittovaltion tasolla, vaan ne on jalkautettu kunkin 16 osavaltion opetusministeriöille. Tämän vuoksi kussakin osavaltiossa on erilainen sääntely, joka koskee tutkintojen tarjontaa ja opetussuunnitelmia, mikä heijastuu myös tarjolla olevaan koulutukseen kyberturvallisuuden osalta. Osavaltiokohtaisiin eroihin vaikuttavat myös digitaalisen infrastruktuurin laadun vaihtelu ja tarkka tietosuojapolitiikka, joka saattaa aiheuttaa esimerkiksi rajoitteita etäopiskelulle ja digitaalisten oppimisympäristöjen hyödyntämiselle. Vuonna 2019 tehdyn perustuslakimuutoksen jälkeen liittovaltio on voinut tukea osavaltioita rahallisesti koulutussektorilla ja edistää yhteistyötä osavaltioiden kanssa etenkin digitalisaation kehittymiseen liittyvissä kysymyksissä.[717]

3.20.4. Kyberkansalaistaitojen määrittäminen

Kyberkansalaistaidoiksi katsotaan kybertoimintaympäristössä tarvittavat perustaidot, joita kansalaisilta vaaditaan jokapäiväisessä arjessa, oman ja muiden turvallisuuden parantamiseksi. Liittovaltion sisäministeriön ja Saksan tietoturvaviraston BSI:n yhteistyössä hiljattain kansalaisille toteuttama informaatiokampanja #einfachaBSIchern keskittyy kansalaisten digitaaliseen turvallisuuteen liittyvien tietojen ja taitojen kehittämiseen. Kampanjan tavoitteena on kehittää kansalaisten ”kybertaitoja”, kuten tietoisuutta kybermaailmassa vallitsevista uhkista, ymmärrystä digitaalisen tiedon arvokkuudesta eri osapuolille ja tiedon suojaamiseen liittyvien perustaitojen tärkeyttä.[718]

Viitteet

[701] Martin Schallbruch ja Isabel Skierka, "The Evolution of German Cybersecurity Strategy," *Cybersecurity in Germany* (Springer Cham, 2018), 15, doi: 10.1007/978-3-319-90014-8.
[702] Schallbruch ja Skierka, "The Evolution of German Cybersecurity Strategy," 16.
[703] Schallbruch ja Skierka, "Cybersecurity in Germany," 27.
[704] Bundesministerium des Innern und für Heimat, *Online kompendium Cybersicherheit in Deutschland: National Pakt Cyber Sicherheit* (Bundesministerium des Innern, für Bau und Heimat, 2021), 1.
[705] Federal Ministry of the Interior and Community, *Cyber Security Strategy for Germany*, (Federal Ministry of the Interior, Building and Community, 2016), 10.
[706] "CYBERHEAD - Cybersecurity Higher Education Database", *ENISA*, luettu 30.11.2022, https://www.enisa.europa.eu/topics/education/cyberhead#/.
[707] "DsiN," *Deutschland sicher im Netz*, luettu 25.10.2022, https://www.sicher-im-netz.de/.
[708] LMK, LfM, eco, FSM, jugendschutz.net ja NgK, *Final public report for publishing, SI-2009-SIC-123906, Safer Internet DE SIC* (Safer Internet plus, 2012).
[709] LMK ym., *SI-2009-SIC-123906.*
[710] "Klicksafe, " *Media Authority Rhineland-Palatinate,* luettu 12.9.2022, https://www.klicksafe.de.
[711] "Klicksafe".
[712] "Part of scheer," *imc*, luettu 11.10.2022, https://www.im-c.com.
[713] "Deutschlands staatliche Cybersicherheitsarchitektur," *Stiftung Neue Verantwortung*, luettu 10.11.2022, https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur.
[714]"W23," *Universität Paderborn*, luettu 27.12.2022, https://wi2023.de/en/scientific-tracks/
[715] "Schloss Dagstuhl Where Computer Scientists Meet," *Leibniz-Zentrum für Informatik GmbH*, luettu 27.12.2022, https://www.dagstuhl.de/en/
[716] Hendrik Wüst ja Herbert Reul, *Cybersicherheitsstrategie des Landes Nordrhein-Westfalen* (Die Landesregierung Nordrhein-Westfalen, 2021).
[717] "Saksan koulutusjärjestelmä, koulutusalan toimijat ja suurtapahtumat koulutusviennin näkökulmasta", *Suomen suurlähetystö, Berliini*, luettu 13.11.2022, https://finlandabroad.fi/web/deu/ajankohtaista/-/asset_publisher/TV8iYvdcF3tq/content/saksan-koulutusjarjestelma-koulutusalan-toimijat-ja-suurtapahtumat-koulutusviennin-nakokulmasta/384951.
[718] "#einfachaBSIchern," Bundesamt für Sicherheit in der Informationstechnik, luettu 13.11.2021, https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html.

3.21. Slovakia

ITU, Global Security Index (GCI) 2020	34/182 (Global), 21/46 (Europe)
National Cyber Security Index (NCSI) 2022	17/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	23/27

3.21.1. Strategiset kyberkoulutuslinjaukset

Slovakian tasavallan kansallinen kyberturvallisuusstrategia vuosille 2021–2025 julkaistiin vuonna 2021. Kansallisen kyberturvallisuusstrategian tarkoitus on yksinkertainen: valmistautua ja saattaa Slovakia tasolle, jolla se on aina askeleen edellä mahdollisia kyberuhkia. Kansallisen turvallisuusviranomaisen visio on vahvistaa ja luoda avointa, vapaata ja turvallista kyberavaruutta kaikille. Perusihmisoikeudet ja -vapaudet ovat kyberavaruudessa ensisijaisia. Slovakian tasavalta lupaa kunnioittaa perusihmisoikeuksia ja edistää ihmisoikeuksien asemaa sekä ”offline- että online-tilassa”. Slovakian tasavalta tukee ja valvoo tätä asemaa pitkällä aikavälillä ja sitoutuu muihin valtioihin, joilla on sama arvojärjestelmä. Se myös tukee muiden valtioiden vastuullista käyttäytymistä ja pyrkii yhtenäistämään kansainvälisen oikeuden tulkintaa kyberavaruudesta.[719] Kyberturvallisuusstrategia painottaa jatkuvaa kyberturvallisuuden kapasiteetin kehittämistä. Strategiassa määritellään käsite, jossa yhdistyvät valtion pyrkimykset varmistaa korkea kyberturvallisuus ja yksilöiden vastuu oman turvallisuutensa edistämiseen tähtäävistä toimista. Päätavoitteena on varmistaa, että ammattilaisilla ja kansalaisilla on riittävä kyberturvallisuusosaaminen. Slovakian opetus-, tiede-, tutkimus- ja urheiluministeriö (Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky) vastaa toimintasuunnitelman mukaan innovatiivisesta kyberturvallisuuden koulutusjärjestelmästä perus- ja lukioasteella sekä toisen asteen ja korkeakoulutason erityiskoulutuksesta ja asiantuntijoista. Suunnitteilla on perustaa ammatillinen koulutusjärjestelmä uusien ammattilaisten kouluttamiseksi ja lisätä turvallisuus- ja tilannetietoisuutta uhista, haavoittuvuuksista, vaaratilanteista ja suojausmenettelyistä kyberavaruudessa.[720]

Strategian mukaan koulutus on yksi kyberturvallisuuden pääalueista, joka mahdollistaa kyberturvallisuusvalmiuksien kehittämisen ja parantamisen. Tavallisten käyttäjien turvallisuustietoisuuden parantaminen toimii varotoimena kyberturvallisuushäiriöitä vastaan, koska koulutetut käyttäjät voivat vastata paremmin tietoturvauhkiin. Kyberturvallisuuskasvatus ei ole tällä hetkellä järjestelmällistä, eikä kyberturvallisuudesta ole kuin yksi yliopisto-ohjelma. Tämä liittyy kyberturvallisuusalan opettajien vähäiseen määrään. Saatavilla on useita yksityisiä erikoiskursseja ja koulutuksia, mutta ne eivät voi korvata järjestelmällistä julkista koulutusta. Turvallisuustietoisuuden rakentaminen ja peruskoulusta lukioon asti kestävä perusturvallisuuskoulutus vastuulliseen käyttäytymiseen internetissä puuttuu huolimatta siitä, että huomattava määrä käyttäjiä on jo saavuttamassa tämän tason. Julkishallinnon henkilöstön koulutus ei ole ollut systemaattista. Kyberavaruuden riskeistä ja kyberhyökkäysten estämisestä ei puhuta peruskoulutuksessa, mikä voi johtaa siihen, etteivät ihmiset juurikaan tiedä kyberuhkista. On tärkeää ymmärtää, mitä turvallisuustietoisuuden lisääminen koulutusjärjestelmään merkitsee. Koulutettu henkilö ei pelkästään ymmärrä ongelmaa, vaan kykenee proaktiivisesti myös tunnistamaan sen.[721]

Vuonna 2019 Slovakian tasavallan investointi-, aluekehitys- ja tietoministeriö (Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky) julkaisi Slovakian digitaalisen muutoksen strategian, Stratégia digitálnej transformácie Slovenska 2030.[722, 723] Strategiana on tukea tehokkaammin digitaalisen aikakauden koulutusta. Kursseilla opiskelijat ja opettajat oppivat ymmärtämään oman tietoisen toiminnan merkityksen, henkilöiden ja yritysten turvallisen digitaalisen identiteetin muodostamisen ja ylläpitämisen, analysoinnin ja tiedon luokittelun sekä perustaitoja, joita tarvitaan syvempään ymmärrykseen. Tietotekniikoiden, kuten ohjelmistojen koodauksen opettelu, alkaa varhaisiästä. Aikomuksena on valmistella

koulutusta järjestelmällistä tiedon luokittelua varten ja jatkaa toimenpiteitä aina vuoteen 2030 asti. Tiedon luokittelussa painotetaan digitaalisen aikakauden osaamista ja koulutuksen digitaalista muutosta kouluissa. Tarkoitus on myös tukea digitaalisten taitojen ja osaamisen kehittämistä varhaisesta iästä alkaen, jotta jokaisella olisi tarvittavat taidot digitaalisessa maailmassa. Samalla tuetaan digitaalisten teknologioiden käyttöä, mikä tehostaa koulutuksen onnistumista. Järjestelmät rakennetaan niin, että ne tukevat digitaalisten taitojen elinikäistä oppimista. Suunnitteilla on myös valmistella analyysi digitaalisten taitojen tilasta Slovakiassa ja luoda tehokkaat mekanismit disinformaation torjumiseksi. Tavoitteena on, että Slovakiasta tulee vuoteen 2030 mennessä moderni maa, jossa innovatiivinen ja ekologinen teollisuus hyötyy tietopohjaisesta digitaalisesta datataloudesta. Pyrkimyksenä on luoda tietoyhteiskunta, jossa kansalaiset voivat hyödyntää täysimääräisesti potentiaaliaan ja elää laadukasta ja turvallista digitaalisen aikakauden elämää. Kohteena on tavallinen kansalainen**,** jonka pitää saada elää turvallisempaa, yksinkertaisempaa ja laadukkaampaa arkea työpaikalla ja yksityiselämässä, sekä kansalainen-yrittäjä, jonka hallinnollista taakkaa tulisi mahdollisimman paljon vähentää ja tukea riittävillä kannustimilla.[724]

3.21.2. Kyberkansalaistaitojen opettamisen nykytila

Kansallinen kyberturvallisuuskeskus (Národné centrum kybernetickej bezpečnosti SK-CERT) on osa kansallista turvallisuusviranomaista. Se avustaa kyberturvallisuuden osaamiskeskusten hallintoa, kehittämistä ja hallintaa sekä tukee niitä, mukaan lukien kyberturvallisuuden koulutusta ja tutkimusta.[725] Näitä osaamis-, tutkimus- ja kyberturvallisuuden kehittämiskeskuksia ovat seuraavat: Euroopan unionin kyberturvallisuusvirasto ENISA (European Union Agency for Cybersecurity), Yhdysvaltojen kyberturvallisuuden ja infrastruktuurin turvallisuusvirasto US-CERT (Cyber Security & Infrastructure Security Agency), CERT.org, Yhdysvalloissa sijaitseva Carnegie Mellon yliopisto (Carnegie Mellon University) ja kyberrikollisuuden tutkimusryhmä TURLA (National Cyber Security Center TURLA group).[726,727,728,729]

Ainoa yliopisto, joka järjestää kyberturvallisuuden maisteriopintoja, on Slovak University of Technology in Bratislava, Information Security.[730]

Slovakian Safer Internet Centressä (SK SIC) on kolme osaa: tietoisuuskeskus Zodpovedne.sk, Helpline ja Stopline.[731] SK SICin filosofia heijastuu sen graafisesta viestinnästä. Keskuksen symboli muistuttaa lapsen kättä ja www-lyhennettä ja värit kuvastavat liikennevaloja. Internetin ja modernin teknologian vastuulliselle käytölle annetaan vihreää valoa. Oranssi tarkoittaa auttavaa kättä. Punainen symboloi stop-merkkiä laittomalle sisällölle ja toiminnalle internetissä. Tietoisuuskeskuksen tavoitteena on kertoa lapsille, vanhemmille ja opettajille internetin turvallisemmasta käytöstä ja ottaa käyttöön erityisiä tietoisuuden lisäämisen työkalupakkeja ja palveluita yhteistyössä kolmansien osapuolten (koulujen) kanssa.[732,733,734,735,736]

SK SIC suunnittelee lapsille, vanhemmille, isovanhemmille, opettajille ja sosiaalityöntekijöille suunnattuja tietoisuuskampanjoita ja resursseja. Tavoitteena on antaa lapsille digitaaliset taidot ja työkalut, joita he tarvitsevat liikkuakseen turvallisesti verkossa. Se edistää vanhempien ja lasten tietoisuutta laadukkaasta verkkosisällöstä ja tuo niihin liittyvät resurssit saataville palveluidensa kautta. Se arvioi tietoisuuskampanjoiden vaikutusta kohderyhmiin ja antaa laadullista ja määrällistä palautetta Euroopan tasolla. SK SIC solmii ja ylläpitää kumppanuuksia sekä edistää vuoropuhelua ja tiedonvaihtoa keskeisten toimijoiden (valtion virastot, internetpalveluntarjoajat, käyttäjäjärjestöt, koulutusalan sidosryhmät) kanssa kansallisella tasolla.[737]

SK SIC on toiminut vuodesta 2007 ja toteuttanut jatkuvasti Safer Internet- ja Safer Internet Plus -ohjelman tavoitteita. Viimeisten kahdeksan vuoden aikana SK SIC on vakiinnuttanut asemansa lasten ja nuorten suojelussa internetissä. Se osallistuu parhaiden käytäntöjen kehittämiseen Euroopassa ja maailmanlaajuisesti. SK SIC ylläpitää kahdeksaa verkkosivustoa ja viittä sosiaalisen median kanavaa, joilla on tähän mennessä yhteensä 14,1 miljoonaa katselukertaa ja lähes seitsemän miljoonaa verkkotyökalujen latausta. Mediajulkaisuja on yli 11 000. SK SIC on kouluttanut yli 50 000 aikuista (muun muassa opettajia, vanhempia, sosiaalityöntekijöitä), 123 000 lasta ja nuorta, ja vaikutusten piirissä on laskettu olleen mukana yli miljoona lasta ja nuorta. Hotlinen kautta on

vastaanotettu yli 11 000 ilmoitusta. SK SIC on myös erittäin aktiivinen internetin turvallisuutta koskevissa lainsäädäntöprosesseissa. Se on saanut yli 20 palkintoa, jotka osoittavat toimintojen ja työkalujen erinomaisuuden.[738]

Kyberturvallisuuspeli CyberGame [739] on tarkoitettu opiskelijoille, lahjakkaille pelaajille ja eri tasoisille ammattilaisille. Kyseessä on kaksi kertaa vuodessa järjestettävä turnausmuotoinen tapahtuma. Seuraavat järjestetään vuoden 2023 maalis- ja toukokuussa. Kyberturvallisuuspeli on suunniteltu sisältämään eri vaikeusasteisia tehtäviä, joissa osallistujat voivat saada palkintoja useissa eri kategorioissa. Peli sisältää neljä eri päähaaraa ja niissä jokaisessa erilaisia skenaarioita, joissa on yhteensä 50 eri tehtävää. Niitä ovat esimerkiksi haittaohjelman analyysi, jossa pelaajien on selvitettävä, miten haitallinen koodi toimii, ja skenaariosoveltaminen ja kryptografia, jossa analysoidaan salattujen ja koodattujen tiedostojen toimintatapaa. Yksi osio on oikeustekninen analyysi, jossa pelaajien on etsittävä digitaalisia vihjeitä saastuneilta tietokoneilta kerätyistä tiedoista, ja skenaario, jossa on julkisiin lähteisiin perustuvaa tiedon keruuta eli OSINT-analyysia (Open Source Intelligence)[740], jossa avointen tietolähteiden ja internetin tiedonetsinnällä perehdytään haitalliseen toimintaan tai haittaohjelmaan. Slovakian kansallinen kyberturvallisuuskeskus SK-CERT suosittelee peliä.

Yrityksille tarkoitetussa verkossa järjestettävässä pelimuotoisessa Guardians-kilpailussa yritykset voivat testata omaa osaamistaan muita vastaan. Testattavia taitoja ovat esimerkiksi digitaaliset taidot verkossa, kybertapahtumien tutkinta ja haavoittuvuuksien etsintä. Valtavasti lisääntyvästä kyberhyökkäyksien määrästä huolimatta kyberturvallisuus on edelleen aliarvioitua ja alirahoitettua monissa yrityksissä. Guardians-pelin tehtävänä on lisätä yleistä tietoisuutta tietoverkkorikollisuudesta ja sen kielteisistä vaikutuksista yhteiskunnan kaikkiin osa-alueisiin. Seuraava järjestetään vuonna 2023.[741]

3.21.3. Kansalliset erityispiirteet

Slovakia poikkeaa siinä muista Euroopan maista, että se pitää perusihmisoikeuksia ja -vapauksia yhtenä tärkeimpänä asiana kyberturvallisuusstrategiassaan. [742] Kyberavaruutta on pidettävä fyysistä maailmaa vastaavana tilana. Siihen sovelletaan samalla lailla selkeitä sääntöjä, jotka kunnioittavat perusihmisoikeuksia, ja taataan perustuslaissa määrätyt oikeudet ja vapaudet, mukaan lukien oikeus yksityisyyteen verkossa, jotta se on turvallinen. Myös tiedon ja tietoisuuden on oltava kaikille avointa, ilmaista ja saatavilla kaikkialla. Kyberavaruuden turvallisuuden on oltava yhteydessä sen vapauteen. Perusihmisoikeudet ja -vapaudet digitaalimaailmassa voidaan taata vain, jos digitaalinen suvereniteetti Euroopan unionin valtioissa kokonaisuudessaan säilytetään. Se varmistaa myös itsenäisyyden ja suvereniteetin kyberavaruudessa.[743]

3.21.4. Kyberkansalaistaitojen määrittäminen

Slovakiassa ei ole varsinaisesti määritelty kyberkansalaistaitoja. Digitaaliset taidot ja kyberturvataidot määrittelee Slovakian kyberturvallisuusstrategian kansallinen viitekehys. Luodaan ”turvallinen internet kaikille” -käsite ja lisätään jatkuvasti tietoturvatietoisuutta keskittyen laajaan väestöryhmään ja haavoittuvimpiin ryhmiin, kuten lapsiin ja ikääntyneisiin. Myös digitaalisten taitojen elinikäinen oppiminen on keskiössä kansalaisten tietoisuuden lisäämisessä ja kyberturvauhkiin varautumisessa. Kansalaisten omaa vastuuta painotetaan digitaalisessa maailmassa ja verkossa liikuttaessa. Sillä on vaikutusta kaikkien kyberturvallisuuteen, niin kansallisella tasolla kuin lähipiirissä. [744] Lisäksi voidaan katsoa, että Slovakian digitaalisen muutoksen strategia on omalta osaltaan kyberkansalaistaitojen määrittelyä.[745]

Viitteet

[719] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021-2025* (2021).
[720] "Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky," luettu 28.10.2022. https://www.minedu.sk/.
[721] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021-2025* (2021).
[722] "Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky," luettu 3.12.2022, https://www.mirri.gov.sk/index.html.
[723] "Stratégia digitálnej transformácie Slovenska 2030," luettu 3.12.2022, https://www.mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/strategia-digitalnej-transformacie-slovenska-2030/.
[724] "Stratégia digitálnej transformácie Slovenska 2030," luettu 29.11.2022, https://www.mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/strategia-digitalnej-transformacie-slovenska-2030/index.html.
[725] "Národné centrum kybernetickej bezpečnosti SK-CERT," luettu 26.11.2022, https://www.sk-cert.sk/sk/o-nas/index.html.
[726] "European Union Agency for Cyber Security," luettu 6.12.2022. https://www.enisa.europa.eu/.
[727] "US-Cert, Cyber Security & Infrastructure Security Agency," luettu 6.12.2022. https://www.cisa.gov/uscert/.
[728] "Cert.org, Carnegie Mellon University," luettu 6.12.2022, https://www.cmu.edu/.
[729] "Turla Group Malware," *National Cyber Security Centre*, luettu 6.12.2022. https://www.ncsc.gov.uk/news/turla-group-malware.
[730] "Information Security," *Slovak University of Technology*, luettu 1.12.2022, https://www.fiit.stuba.sk/study-programs.html?page_id=2090.
[731] "Stopline.sk," luettu 24.11.2022, https://stopline.sk/sk/uvod/.
[732] "Stopline.sk," luettu 24.11.2022, https://stopline.sk/sk/uvod/.
[733] "Zodpovedne.sk," luettu 26.11.2022, https://www.zodpovedne.sk/index.php/sk/.
[734] "Pomoc.Sk Helpline," luettu 24.11.2022, https://pomoc.sk/.
[735] "Stopline.sk," luettu 24.11.2022, https://stopline.sk/sk/uvod/.
[736] "Slovak Safer Internet Centre," luettu 22.11.2022, https://www.zodpovedne.sk/index.php/en/.
[737] "Slovak Safer Internet Centre," luettu 22.11.2022, https://www.zodpovedne.sk/index.php/en/.
[738] "Slovak Safer Internet Centre," luettu 22.11.2022, https://www.zodpovedne.sk/index.php/en/.
[739] "Cybergame," luettu 22.11.2022, https://cybergame.sk-cert.sk/.
[740] "OSINT Analytics," luettu 4.12.2022, https://www.osintanalytics.com/.
[741] "Guardians," luettu 26.11.2022. https://www.guardians.sk/.
[742]Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021-2025, luettu 22.11.2022, https://www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf.
[743] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021-2025* (2021).
[744] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021-2025* (2021).
[745] "Stratégia digitálnej transformácie Slovenska 2030," luettu 2.12.2022, https://www.mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/strategia-digitalnej-transformacie-slovenska-2030/.

3.22. Slovenia

ITU, Global Cybersecurity Index (GCI) 2020	67/182 (Global), 34/46 (Europe)
National Cyber Security Index (NCSI) 2022	51/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	11/27

3.22.1. Strategiset kyberkoulutuslinjaukset

Sloveniassa Digital Slovenia 2020 on kattostrategia, johon liittyvä asiakirja kyberturvallisuusstrategia 2016 on. Digitaalisuuden kehittämisen tavoitteet ovat laaja-alaisia, kuten tehdä Sloveniasta osallistava digitaalinen yhteiskunta sekä luoda turvaa ja luottamusta kyberavaruudessa muun muassa lisäämällä slovenialaisten kybertietoisuutta ja digilukutaitoa sekä suojelemalla yksityisyyttä ja kulttuuri-identiteettiä.[746] Digital Slovenia 2030 -strategia on valmisteilla ja uusi kansallinen kyberturvallisuusstrategia on myös työn alla.[747]

Slovenian kyberturvallisuusstrategia 2016 painottaa vahvasti tietoisuuden merkitystä kyberturvallisuuteen. Tietoisuuden lisääminen ja koulutus edesauttavat poistamaan riskejä ja luovat turvallisen teknologian käytön kulttuuria. Sloveniassa rakennetaan tietoisuusohjelmia, joiden menetelmät ja sisältö sovitetaan mahdollisimman hyvin kullekin kohderyhmälle sopivaksi. Lasten ja nuorten osalta kyberturvallisuuteen liittyvät aiheet sisällytetään opetussuunnitelmiin eri koulutusasteilla. Muulle väestölle ja yrityksille kehitetään heille mukautettuja ohjelmia. [748] Sloveniassa akateeminen tutkimusyhteisö osallistuu omalta osaltaan kyberturvallisuuden turvaamiseen lisäämällä tietoisuutta, koulutusta ja tutkimusta koulutusohjelmiensa ja aihetta käsittelevien kurssiensa kautta, kaikilla koulutustasoilla, sekä tutkimusorganisaatioiden tulosten kautta. Slovenian kyberturvallisuusmalli huomioi myös kansalaisyhteiskunnan aloitteet. Erityisesti huomioidaan ammatillisten järjestöjen parannusehdotukset ja apu tietoisuuden lisäämiseen. Tietoisuuden lisääminen nähdään tärkeänä, koska tietoisuuden lisääminen parantaa kyberturvallisuuskulttuuria ja opettaa käyttäjiä huolehtimaan itsenäisesti omasta kyberturvallisuudestaan. Tämän vuoksi nykyisiä tietoisuusohjelmia jatketaan ja lisäksi kehitetään uusia, hankkeisiin osallistumiseen kannustetaan ja kansalaisyhteiskunta otetaan mukaan toimintaan. Tiedotus keskitetään tehokkaasti tiettyihin kohderyhmiin (kuten lapset, eri-ikäiset kansalaiset ja liike-elämän yksiköt). Toimenpiteet kansalaisten kyberturvallisuuden varmistamiseksi ovat tietoisuusohjelmien säännöllinen toteuttaminen ja kyberturvallisuussisältöjen sisällyttäminen koulutusohjelmiin. Kyberturvallisuuteen liittyvät aiheet halutaan sisällyttää koulujen opetussuunnitelmiin kaikilla koulutusjärjestelmän tasoilla. Yliopistoja kannustetaan tarjoamaan itsenäisiä opinto-ohjelmia kyberturvallisuudesta. Lisäksi kyberturvallisuuden keskeisten sidosryhmien kyberturvallisuuden varmistamiseen osallistuvan suorittavan henkilöstön osaaminen varmistetaan jatkuvalla koulutuksella ja sertifioinnein.[749]

3.22.2. Kyberkansalaistaitojen opettamisen nykytila

Sloveniassa on kaksi julkisesti rahoitettua kyberturvallisuustietoisuuden lisäämiseen tähtäävää hanketta: 1) SI-CERT:in ”Safe on the Internet” -koulutusohjelma[750] ja 2) ”Safer Internet Centre Slovenia” -ohjelma (SIC), jonka alla toimii SAFE.SI-tietoisuuskeskus.[751] Ensimmäinen, ”Safe on the Internet” -hanke on suunnattu suurelle yleisölle ja erityissisällön kautta myös pk-yrityksille (pienyritykset, käsityöläiset ja yksityisyrittäjät). Tämä hanke osallistuu myös EU:n kyberturvallisuuskuukauden kampanjoihin. Toinen, Safer Internet Centre -hanke on suunnattu lapsille ja nuorille, ja sitä kautta myös vanhemmille ja muille kasvattajille (kuten opettajat ja nuorisotyöntekijät). Sen on toteuttanut Ljubljanan yliopiston yhteiskuntatieteiden tiedekunnan koordinoima yhteistyökumppanien yhteenliittymä. Valtion tietoturvavirasto URSIV rahoittaa molempia tiedotusohjelmia kokonaan tai osittain.[752,753,754] SI-CERT osallistuu myös SAFE.SI-hankkeeseen.[755]

URSIVin rahoittama ”Safe on the Internet” -hanke on tarkoitettu jatkuvaksi pitkäaikaiseksi toiminnaksi. Sen päätavoitteena on auttaa parantamaan tavallisen slovenialaisen internetin käyttäjän tietoturvaa koskevaa lukutaitoa. Hankkeella on myös lyhyen aikavälin tavoitteita. Ohjelman avulla halutaan lisätä tietoisuutta erilaisista verkkouhista, opastaa verkkopankin käytössä, ohjeistaa turvalliseen verkko-ostamiseen ja -myymiseen sekä informoida erityyppisistä verkkopetoksista. Sivustolla käyttäjää informoidaan, opastetaan ja myös annetaan käytännön ratkaisuja itsensä ja identiteetin suojaamiseen sosiaalisissa verkostoissa. Hankkeen kohderyhmänä on suuri yleisö ja painotus on aikuisissa käyttäjissä (noin 24–54-vuotiaat), koska he ovat niitä, jotka tekevät eniten verkko-ostoksia, käyttävät verkkopankkia ja sosiaalista mediaa. Toisena kohderyhmänä ovat pk-yritykset, koska pienyrityksillä on rajalliset budjettiresurssit ammatilliseen IT-tukeen. CI-CERT on tuottanut lukuisia materiaaleja viimeisen kymmenen vuoden aikana. Varninainternetu.si-koulutusportaali on tärkein viestintäkanava. Sivusto sisältää esimerkiksi yli 500 artikkelia, viimeisimmät uutiset ja ilmoitukset tietoturvauhkista. Sosiaalisen median kanavat ovat myös tärkeä osa toimintaa ja tiedottamista (kuten Facebook, Instagram) samoin Safe News -uutiskirje ja erilaiset aineelliset materiaalit, kuten esitteet, julisteet ja opetusvideot (40 kyberturvallisuusaiheista videota). Viime vuoden lopulla lanseerattiin pk-yrityksille suunnattu ”Varni v pisarni” (Turvallisesti toimistossa) -kyberturvallisuuskurssi.[756] Toinen ohjelma, tietoisuuskeskus SAFE.SI, joka toimii ”Safer Internet Centre Slovenia” (SIC) -ohjelman alla, on EU:n käynnistämä ja osarahoittama projekti. Hanketta rahoittavat valtion tietoturvavirasto (URSIV) ja HaDeA (European Health and Digital Executive Agency). Hanke vastaa kohderyhmänsä (lapset ja nuoret sekä vanhemmat ja kasvatusalan ammattilaiset) tietoisuuden lisäämisestä.[757] Kouluväestö (verkkotyöpajat ja työpajat paikan päällä) kuuluu ohjelman piiriin ja ainakin osittain myös päiväkotilapset.[758] SIC on osa EU:n Better Internet for Kids -ohjelmaa. Tietoisuuskeskuksen ja Safe.si-verkkosivuston lisäksi, jossa on omat osiot kullekin kohderyhmälleen, SIC-ohjelman piirissä on myös auttava ”TOM-telefon” nuorille ja heidän vanhemmilleen ongelmatilanteisiin sekä vihjepuhelin ”Spletno oko”.[759,760]

Nuorten mielenkiintoa kyberturvallisuutta kohtaan pyritään aktiivisesti lisäämään. Vuonna 2021 URSIV aloitti Cybertalent-projektin kyberturvallisuuden suosion lisäämiseen. Projektissa järjestetään online-kyberturvallisuustyöpajoja ja rahoitetaan slovenialaisen tiimin koulutusta ja osallistumista jokavuotiseen European Cybersecurity Challenge -tapahtumaan. Tässä yhteydessä URSIV suunnittelee myös yhteistyötä toisen asteen oppilaitosten, tiedekuntien ja yritysten kanssa luodakseen ekosysteemin kyberturvallisuusvalmiuksien kehittämiseksi.[761] IT tai kyberturvallisuus sisältyy useiden korkeakoulujen opintoihin, esimerkiksi Mariborin ja Ljubljanan yliopistojen ja yksityisen GEA Collegen opinto-ohjelmiin.[762] Kyberturvallisuuden ja digitaalisten kansalaistaitojen koulutusta on Sloveniassa saatavilla verkko-ohjelmien kautta peruskouluille ja opettajille. Verkko-ohjelmien kautta voidaan suorittaa myös kandidaatin tutkinto. Yrityksille ja oppilaitoksille on tarjolla myös ammatillista koulutusta ja sertifiointijärjestelmiä.[763] Elinikäiseen oppimiseen panostetaan, esimerkiksi työ-, perhe-, sosiaali- ja tasa-arvoministeriö MoLFSA (Ministrstvu za delo, družino, socialne zadeve in enake možnosti) on Slovenian julkisen stipendi-, kehitys-, vammaisuus- ja ylläpitorahaston (Javni štipendijski, razvojni, invalidski in preživninski sklad Republike Slovenije) kanssa ottanut käyttöön toimenpiteitä työntekijöiden ammattitaidon lisäämisen tukemiseksi yrityksissä, erityisesti aktiivisen ikääntyvän työvoiman osalta. Näissä ohjelmissa kehitetään muun muassa digitaitoja, kuten digitaalisten välineiden ja ohjelmien käyttöä ja digitaalista viestintää. Hallintoakatemia puolestaan järjestää digitaalisten taitojen kursseja virkamiehille.[764]

Slovenian SIC-ohjelmassa julisteiden, lehtisten ja e-kirjojen avulla annetaan neuvoja ja työkaluja internetin turvalliseen käyttöön, kuten vanhemmille suunnattu 44-sivuinen ”Vzgoja za internet” -käsikirja, joka kouluttaa vanhempia lapsien internetin käytön kasvatukseen. Sloveniassa painotetaan vahvasti myös kansalaisten hyvinvointia kyberavaruudessa. Painotus on digitaalisen hyvinvoinnin aiheissa. Sieltä löytyy esimerkiksi ohjeita puhelimen ja tabletin hyvinvointiasetuksiin yli 25-vuotiaille tai esimerkiksi digitaalisen hyvinvoinnin tietovisa 10–12- ja 12–15-vuotiaille nuorille. Moni kampanjoista on Ljubljanan yliopiston yhteiskuntatieteellisen tiedekunnan tuottamia.[765] SIC:llä on myös muutama mobiilisovellus.[766,767] ”Odklikni” (Klikkaus) liittyy verkkoväkivaltaan ja "Reši spletno dilemo!"(Ratkaise online-dilemma) auttaa tekemään päätöksiä verkossa.

URSIV aikoo valmistella ja esitellä perusopetuksen opetussuunnitelmiin kyberturvallisuuden teemoja. Tässä yhteydessä URSIV tekee yhteistyötä hallituksen digitaalisen muutoksen toimiston (Služba vlade za digitalno

preobrazbo), joka suunnittelee pakollisten tieto- ja viestintätekniikkaohjelmien sisällyttämistä koulujen opetussuunnitelmiin, sekä opetus-, tiede- ja urheiluministeriön (Ministrstvo za izobraževanje, znanost in šport) kanssa. Rahoitus tähän on saatu Slovenian palautumis- ja elpymissuunnitelmasta, ja materiaaleja valmistellaan yhdessä joidenkin tiedekuntien kanssa.[768]

Kyberturvallisuuskampanjoissa ja -koulutuksissa kahta kohderyhmää, seniorit ja toimintarajoitteiset kansalaiset, ei ole vielä riittävästi huomioitu. Toimintarajoitteisille ratkaisuna olisi nykyisten materiaalien päivittäminen käyttäjäystävällisiksi. Uusille materiaaleille käyttäjäystävällisyys on vaatimuksena. Senioreille, joilla ei yleensä ole niin kehittyneitä teknisiä taitoja, ohjelmat tullaan todennäköisesti tekemään digitaalisen lukutaidon lisäämiseen tähtäävien ohjelmien yhteydessä. [769] Tulevaisuudessa toiveena on tuottaa enemmän erilaisia ohjelmia erilaisille taidoille ja koulutustasoille sekä tietoisuutta lisääviin ohjelmiin. Uusien maisteri- ja tohtoriohjelmien käyttöönotto on parhaillaan käynnissä.[770] Kansalaisten kyberturvallisuustietoisuuden tasoa ja tietoa mahdollisista kyberuhkista halutaan tulevaisuudessa lisätä sekä lisätä myös tietämystä sellaisten peruskybervaaratilanteiden tunnistamiseen, joita peruskansalainen voi kohdata.[771] Ajantasaisille päivittyville koulutusohjelmille on myös tarve, koska kyberuhat kehittyvät jatkuvasti.[772]

Slovenia voitti vuoden 2022 Euroopan kyberturvallisuuskuukauden paras video -palkinnon videoteoksellaan ”Darko haluaa viedä tyttöystävänsä matkalle”, jonka aiheena ovat nettihuijaukset.[773] Voiton myötä materiaali tekstitetään kaikille virallisille EU-kielille, viitteessä esimerkkinä englanniksi tekstitetty versio.[774]

3.22.3. Kansalliset erityispiirteet

Slovenian kyberturvallisuusstrategia painottaa oikeudenmukaisuutta ja yksilön kyberturvan merkitystä. Jokaisella on oltava mahdollisuus käyttää tieto- ja viestintätekniikkaa mahdollisimman turvallisesti yksityisyyttä ja ihmisoikeuksia kunnioittaen. Kansalaisilla on oltava mahdollisuus tutustua kyberavaruuden riskeihin, keinoihin niiden hallitsemiseksi ja vastuuseen omasta turvallisuudestaan. Käyttäjien tietoisuuden lisääminen on erittäin tärkeää, koska se kehittää kyberturvallisuuskulttuuria, jossa käyttäjät oppivat huolehtimaan itse omasta kyberturvallisuudestaan. Tämän vuoksi on tärkeää jatkaa jo voimassa olevia tietoisuusohjelmia, kehittää uusia ohjelmia ja kannustaa kansalaisia osallistumaan näihin ohjelmiin.[775]

Sloveniassa on 2022 säädetty Digital Inclusion Act -laki. Sen tavoitteena on muun muassa lisätä ymmärrystä digitaalisten teknologioiden vastuullisesta ja turvallisesta käytöstä sekä edistää kansalaisten digitaalisia taitoja. Yksi lain perusteella toteutettavista toimenpiteistä on digitaalinen arvoseteli (150 euroa), jonka siihen oikeutettu kansalainen (myös tietyt opiskelijaryhmät) voi käyttää tietokoneen hankintaan. Yli 55-vuotiaat saavat setelin osallistuttuaan digitaaliset perusosaamiset -kurssille, johon sisältyy myös internetin turvallisuus -osio.[776,777]

3.22.4. Kyberkansalaistaitojen määrittäminen

Slovenian kansallinen koulutusinstituutti ZRSS[778] tukee opettajia oppilaiden digitaalisen osaamisen kehittymisen määrittelyssä päiväkodista lukioon indikaattoreilla, joiden avulla digitaalisen osaamisen kehittämistoimintaa voidaan suunnitella. Jokaista DigComp-mallin 21 digitaalista osaamisaluetta käytetään indikaattoreiden laatimisessa. Opettajatiimi, joka työskentelee samassa luokassa, voi indikaattoreiden avulla koordinoida, kuka kehittää mitäkin DigComp-mallin osaamista ja millä tasolla sekä mitä taitoja tietyllä luokalla pitäisi olla. Lisäksi kukin koulu voi mukauttaa indikaattorit omaan erityistilanteeseensa. [779] Kaikkia viittä osaamisaluetta määriteltyine alaosaamisalueineen hyödynnetään Slovenian kansallisessa opiskelijoiden pätevyyskehyksessä. DigComp po razherid (DigComp luokittain) -taulukosta (sloveniaksi) löytyvät indikaattorit, jotka kuvaavat yksilön digitaalisia taitoja.[780]

Viitteet

[746] The Republic of Slovenia, Digital Slovenia, *Digital Slovenia 2020 – Development Strategy for the Information Society until 2020*, Digitalisation of Slovenia by Intense and Innovative Use of ICT and Internet in all Segments of Society (2016).
[747] Henkilökohtainen tiedonanto tutkijalle, 20.6.2022.
[748] The Republic of Slovenia, Digital Slovenia, *Cyber Security Strategy*, *Establishing a System to Ensure a High Level of Cyber Security* (2016), 10-11.
[749] The Republic of Slovenia, *Cyber Security Strategy*, 9-10, 13.
[750] ”VARNI NA INTERNETU,” luettu 29.11.2022, https://www.varninainternetu.si/.
[751] ”Safe.si,” luettu 29.11.2022, https://safe.si/.
[752] The Republic of Slovenia, *Cyber Security Strategy*, 5.
[753] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[754] Henkilökohtainen tiedonanto tutkijalle, 23.6.2022.
[755] ”About SI-CERT,” luettu 4.11.2022, https://www.cert.si/en/about-si-cert/.
[756] Henkilökohtainen tiedonanto tutkijalle, 23.6.2022.
[757] Henkilökohtainen tiedonanto tutkijalle, 23.6.2022.
[758] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[759] Henkilökohtainen tiedonanto tutkijalle, 23.6.2022.
[760] ”Slovenian Safer Internet Centre,” luettu 10.11.2022, https://www.betterinternetforkids.eu/sic/slovenia.
[761] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[762] The Republic of Slovenia, *Cyber Security Strategy*, 5-6.
[763] Henkilökohtainen tiedonanto tutkijalle, 20.6.2022.
[764] European Commission, *Digital Economy and Society Index (DESI) 2022: Slovenia* (2022), 7, 16.
[765] ”Better Internet for Kids Slovenia,” luettu 8.7.2022, https://www.betterinternetforkids.eu/sic/slovenia.
[766] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[767] ”Safe.si Aplikacije,” luettu 6.9.2022, https://safe.si/orodja/aplikacije.
[768] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[769] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[770] Henkilökohtainen tiedonanto tutkijalle, 20.6.2022.
[771] Henkilökohtainen tiedonanto tutkijalle, 7.7.2022.
[772] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[773] ”The European Cybersecurity Month 2022 Awards,” *ECSM*, luettu 8.11.2022, https://cybersecuritymonth.eu/awards.
[774] ”Slovenia - Darko EN.m4v,” katsottu 29.11.2022, https://cybersecuritymonth.eu/countries/slovenia/slovenia-darko-en.m4v.
[775] The Republic of Slovenia, *Cyber Security Strategy*, 13.
[776] Henkilökohtainen tiedonanto tutkijalle, 7.7.2022.
[777]European Commission, *Digital Economy and Society Index (DESI) 2022: Slovenia* (2022), 6.
[778] ”Zavod Republike Slovenije za šolstvo, About us,” luettu 29.11.2022, https://www.zrss.si/en/.
[779] European Commission, Joint Research Centre, Pujol Priego, L., Cabrera, M., Kluzer, S., et al., *DigComp into action, get inspired make it happen: a user guide to the European Digital Competence framework*, Punie, Y.(editor), Carretero, S.(editor), Vuorikari, R.(editor) (Publications Office, 2018), https://data.europa.eu/doi/10.2760/112945, 138.
[780] ”DigComp po razredih,” luettu 11.7.2022, https://docs.google.com/spreadsheets/d/1I6fOc-D3KK945ZC5nMJDHaBDm2kNhpJ25Ucl1PPM2BE/edit#gid=1097700938.

3.23. Suomi

ITU, Global Cybersecurity Index (GCI) 2020	22/182 (Global), 14/46 (Europe)
National Cyber Security Index (NCSI)	11/160 (24.10.2022)
The Digital Economy and Society Index (DESI)	1/27

3.23.1. Strategiset kyberkoulutuslinjaukset

Suomen kyberturvallisuusstrategiassa 2019 todetaan, että Suomen tavoitteena on olla kyberturvallisuuden kärkiosaajien joukossa kansainvälisellä tasolla; yksi strategisista linjauksista on: ”Kyberturvallisuuden osaamisen kehittäminen – arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina.” Jokainen yksilö nähdään tärkeänä kyberturvallisuustoimijana, ja strategiassa painotetaan sen varmistamista, että jokaisella on riittävät valmiudet toimia turvallisesti digitaalisessa ympäristössä. Tavoitteena on parantaa kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä. Suomen oma kyberturvallisuusstrategia ja EU:n kyberturvallisuusstrategia nähdään toisiaan täydentävinä. Toimenpiteitä kyberturvallisuuden osaamisen edistämiseksi ovat ammatillisen koulutuksen, ammattikorkeakoulujen ja yliopistojen kyber- ja tietoturvallisuuteen, ohjelmisto- ja sovelluskehitykseen sekä tietoverkkoihin ja tietoliikenteeseen liittyvien koulutusohjelmien vahvistaminen sekä valtakunnallisen digiturvallisuuden koulutus- ja harjoitusjärjestelmän vahvistaminen osana julkisen hallinnon digitaalisen turvallisuuden koulutusta. Viimeksi mainitun toimenpiteen tavoitteena on parantaa julkishallinnon, yritysten ja muiden sidosryhmien työntekijöiden sekä kansalaisten osaamista.[781] Kyberturvallisuusstrategian toimeenpano-ohjelmassa otetaan tarkemmin kantaa siihen, millaisilla käytännön toimenpiteillä asetettuihin tavoitteisiin pyritään pääsemään, toimeenpano-ohjelma on tosin tehty ennen viimeisintä strategiaa. Toimenpiteenä kyberosaamisen kehittämiseksi esitetään koulutus- ja harjoitustoiminnan suunnittelua ja toteutusta, jonka yhtenä tavoitteena on kansalaisten tieto- ja kyberturvallisuusosaamisen kehittäminen. Vastuuta koulutustoimenpiteistä annetaan erityisesti kolmannen sektorin toimijoille, kuten Maanpuolustuskoulutusyhdistykselle ja Vanhustyön keskusliitto ry:lle Myös Digi- ja väestötietoviraston (DVV) yhdessä liikenne- ja viestintäministeriön kanssa toteuttama digiturvaviikko ja sen osana järjestettävä kansallinen tietoturvapäivä nähdään kansalaisten tietoa lisäävänä tekijänä. Opetushallituksen vastuulle osoitetaan lisämateriaalin tuottaminen yleissivistävään ja ammatilliseen koulutukseen. [782] Suomen kyberturvallisuuden kehittämisohjelmassa todetaan, että kansalaisten kyberturvataidot tulee saada hyvälle tasolle. Toimenpiteinä esitetään aiemmin mainittujen lisäksi vapaaehtoispohjalta toimivien kyberturvallisuusyhteisöjen tukemista sekä niiden osaamisen hyödyntämistä yleisen kyberosaamisen kehittämisessä. Lisäksi todetaan, että viestintäsuunnitelma kansalaisten kyberturvatietoisuuden kasvattamiseksi tulee luoda.[783] Suomen digitaalinen kompassi julkaistaan pian, ja se on parhaillaan valiokuntien lausuntokierroksella. Kompassi toimii strategisen etenemisen ohjenuorana vuoteen 2030 saakka, ja sen on tarkoitus ohjata Suomen digitaalisen kehitystyön suuntaa. Kompassin osa-alueet ovat osaaminen, yritysten digitaalinen muutos, julkisten palveluiden digitalisointi sekä turvalliset ja kestävät digitaaliset infrastruktuurit. Kompassissa (Valtioneuvoston selonteko -versio) todetaan: ”Medialukutaito ja kyky torjua informaatiovaikuttamista puolestaan ovat luottamukseen perustuvan, avoimen ja demokraattisen yhteiskunnan säilymisen edellytyksiä.” Kompassissa pidetään tärkeänä, että kansalaisten taidoista huolehditaan, mutta nähdään kuitenkin, että Suomen vahvuutena ovat digitalisaatio-osaaminen, koulutus ja digitaidot (joiden osana kyberturvallisuustaidot voidaan nähdä). Suomen osalta mahdollisuutena nähdään profiloituminen kyberturvallisuuden osaamisessa. Tällä hetkellä uhkina Suomessa nähdään erityisesti kyberhyökkäykset, informaatiovaikuttaminen sekä tieto- ja identiteettivarkaudet. Kyberturvallisuuden tulisikin olla mukana

kaikessa toiminnassa digitaalisessa maailmassa ja kompassissa todetaan, että vastuu turvallisuudesta on jokaisella yksilöllä.[784]

3.23.2. Suomen kyberkansalaistaitojen opettamisen nykytila

Suomessa on tarjolla suhteellisen paljon sekä muodollista (osana virallisia opetus- tai koulutusohjelmia) että epämuodollista (muita koulutuksia) kyberturvallisuuden koulutusta. Koulutussisällöt eivät ole yhdenmukaisia muodollisellakaan tasolla ja se, kuinka paljon kyberturvallisuuteen liittyvää koulutusta saa, on paljolti yksilöiden oman aktiivisuuden varassa. Kyberturvallisuuskoulutusmateriaalia ja koulutusta on verkossa kaikkien saatavilla, mutta ongelmana on erityisesti sellaisten kansalaisten saaminen koulutuksen pariin, jotka sitä eniten tarvitsisivat. Koulutuksia on hankala löytää, eivätkä kaikki koulutusta tarvitsevat välttämättä tunnista omia koulutustarpeitaan. Koulutusta erityisesti tarvitsevia ryhmiä ovat muun muassa seniorit, nuoret, lapset ja lasten kanssa työskentelevät (lasten ja nuorten osalta tilanne on sinänsä parempi, sillä he saavat osana muodollista koulutuspolkuaan kyberturvallisuuskoulutusta). Lisäksi myös aikuiset, jotka eivät työpaikkansa kautta kyberturvallisuuskoulutusta saa, jäävät mahdollisesti kokonaan ilman. [785] , [786] Suomessa on kyberturvallisuuskoulutusta kyllä tarjolla, mutta koulutus kohdistuu määrällisesti ja laadullisesti eri ikäryhmille eri tavoin. Suomen digitaalisessa kompassissa esitetään tavoitteena, että kyberturvallisuuden koulutus tai opetus saadaan kiinteäksi osaksi kaikkien koulutusasteiden opetus- tai koulutustarjontaa ja tätä kautta kansalaisten kybertaidot paranevat.[787]

Kyberturvallisuuden kouluttamista ja opettamista on kartoitettu laajasti Jyväskylän yliopiston vuonna 2022 julkaisemassa tutkimuksessa. Kyberturvallisuuden peruskouluopetuksen kehittämiseen liittyviä hankkeita, kuten ”Kyberturvallisuuden kehittämisohjelma” sekä ”Uudet lukutaidot” -kehittämisohjelma, on parhaillaan käynnissä eli opetusta kehitetään aktiivisesti. Tällä hetkellä kyberturvallisuuden opetus kuuluu erityisesti ”Tieto- ja viestintäteknologia” -osaamisalueeseen, mutta myös muussa opetuksessa käsitellään kyberkansalaistaitojen rakentumisen kannalta olennaisia asioita, esimerkiksi laaja-alaiset osaamisalueet ”Itsestä huolehtiminen ja arjen taidot” sekä ”Monilukutaito” ovat kyberturvallisuustaitojen kannalta olennaisia. [788] Myös toisen asteen koulutuksessa käsitellään kyberturvallisuuden teemoja, mutta siinä, miten ja missä laajuudessa, on paljon koulutuksen järjestäjä- ja koulutusohjelmakohtaisia eroja. Vuotuinen ITK-konferenssi on suuri digitaalisen koulutuksen ja oppimisen kehittämisen tapahtuma, joka on suunnattu peruskoulun ja toisen asteen opettajille, konferenssi on tärkeä opettajien kyberturvallisuuden täydennyskoulutuksen näkökulmasta. [789] Suomessa nähdään tärkeäksi kyberosaajien määrän kasvattaminen. [790] Erityisesti kyberturvallisuuteen keskittyviä korkeakoulututkintoja tarjoavat Suomessa sekä ammattikorkeakoulut että yliopistot, koulutusohjelmia on tällä hetkellä 15 (kahdeksan ammattikorkeakoulututkinto-ohjelmaa, neljä ylempää ammattikorkeakoulututkinto-ohjelmaa ja kolme maisteriohjelmaa) ja myös uusia ohjelmia on suunnitteilla. Tulee kuitenkin huomioida, että kyberturvallisuuteen liittyvät teemat ovat osana useaa muutakin korkeakoulututkinto-ohjelmaa.[791,792]

Suomessa kansalaisopistot ja kirjastot kouluttavat eri ikäryhmille kyberturvallisuustaitoja, mutta haasteena on, että tämä on kovasti riippuvaista henkilökunnan omista taidoista ja siitä, että ylipäätään tunnistetaan, mitä kannattaisi kouluttaa. Kaikille avointa koulutusta tarjoaa myös Digi- ja väestötietovirasto yhteistyössä valtionhallinnon sidosryhmäyksikkö HAUS Kehittämiskeskus Oy:n kanssa. Näiden koulutusten pääkohderyhmänä ovat julkisen hallinnon työntekijät, mutta koulutuksia voivat hyödyntää myös yritykset ja kansalaiset. Yksi suurimmista kansalaisten kouluttajista on Maanpuolustuskoulutusyhdistys (MPK), joka järjestää runsaasti eritasoisia kyberturvallisuuskursseja verkossa ja lähiopetuksena ympäri Suomea. Osa näistä kursseista on kaikille avoimia, osa on tarkoitettu reserviläisille. Edellä mainittujen lisäksi kansalaisille kyberturvallisuuskoulutusta tarjoavat muun muassa Naisten valmiusliitto, kansalaisopistot ja kesäyliopistot, kirjastot, Vanhustyön keskusliitto, Teknologiateollisuus, Digi- ja väestötietovirasto (DVV), Liikenne- ja viestintäviraston (Traficom) alainen Kyberturvallisuuskeskus sekä KyberVPK, Rikosuhripäivystys (RIKU) ja muut kyberturvallisuuteen liittyvät järjestöt. [793] Suomen kielellä on saatavilla useita kyberturvallisuuspelejä, kyberturvallisuuskoulutukseen keskittyviä verkkosivustoja ja materiaaleja. Teknologiateollisuuden ”Tämä

toimii!" -teknologiakasvatusprojekti ekaluokkalaisille sisältää kyberturvallisuusmoduulin. Kyseessä on tilattava materiaalipaketti opettajille. [794] MPK on julkaissut yhteistyössä Jyväskylän yliopiston kanssa "Kansalaisen kyberturvallisuus" -kurssin. Kurssi on suunnattu kaikille, eikä sen suorittamiseen vaadita aiempaa osaamista. Kurssi tarjoaa tietoa ja taitoa turvalliseen toimintaan digitaalisessa maailmassa. [795] DVV on tuottanut "Digiturvallinen elämä" -koulutuskokonaisuuden, joka sisältää myös pelin. Koulutuskokonaisuuden tavoitteena on kouluttaa turvallista toimintaa digitaalisessa maailmassa erityisesti erilaisten organisaatioiden henkilöstölle.[796] "Spoofy" on alakoululaisille tarkoitettu mobiilipeli, joka opettaa, kuinka häiriköille vastataan netissä.[797] Yleisradio (YLE) on julkaissut informaatiovaikuttamista havainnollistavan Trollitehdas-pelin. Pelissä pelaaja näkee, kuinka valeuutisia, tunteita herättävää sisältöä ja bottiverkkoja käytetään hyväksi ihmisiin vaikuttamisessa.[798] YLE on luonut myös Trollibunkkeri-pakopelin, jossa pelaaja on toimittaja, joka on joutunut virheellistä tietoa levittävän trollin vangiksi. Pelissä perehdytään erityisesti valeuutisiin.[799]

Euroopan kyberturvallisuuskuukautta on vietetty Suomessa jo usean vuoden ajan lokakuussa, Suomessa erityisesti elinkeinoelämä on ollut aktiivinen kyberturvallisuuskuukauden toimija. Kuukauden aikana sekä julkiset toimijat että monet kyberalan yritykset nostavat kyberteemoja esiin ja järjestävät laajasti erilaisia tapahtumia ja kampanjoita sekä henkilöstölleen että sidosryhmilleen. [800] Laajimmin sisältöä suurelle yleisölle on viime vuosina Suomessa tuottanut Kyberturvallisuuskeskus, joka on järjestänyt tapahtumia ja tuottanut vuosittaisten teemojen mukaista materiaalia kyberturvallisuusasioista kansalaisille. Vuonna 2022 materiaalina oli muun muassa videoita, joissa teemoina olivat kiristyshaittaohjelmat sekä tietojenkalastelu.[801] Myös DVV järjestää vuosittain lokakuussa Digiturvaviikon, joka on suunnattu erityisesti erilaisille organisaatioille.[802]Tämän tutkimuksen haastatteluissa esitettiin toiveita ja odotuksia Cyber Citizen -hankkeeseen liittyen. Toiveena esitettiin suomalaisten kyberkansalaistaitotason parantaminen, mutta myös todettiin, että kyberkansalaistaitojen tasoa ei juurikaan mitata tällä hetkellä, ja pohdittiin, josko Cyber Citizen -hankkeessa tuotettu materiaali ja siihen liittyvät suoritteet voisivat tarjota mahdollisuuksia tähän. Lisäksi toiveina esitettiin jatkuvuutta hankkeen aikana luoduille sisällöille ja verkostolle sekä kyberkansalaistaitojen tuominen osaksi olemassa olevia kokonaisuuksia, eikä niiden esittäminen erillisenä asiana, ja kansalaisten kiinnostuksen herättäminen pelottelun sijasta hyödyillä.[803,804,805]

3.23.3. Suomen kansalliset erityispiirteet

Kyberturvallisuuden koordinaatio Suomessa on tällä hetkellä hajallaan, mutta sitä kehitetään jatkuvasti eteenpäin. [806, 807] Vuonna 2020 julkiseksi tullut Vastaamon tietomurto toi kyberturvallisuusuhkille paljon näkyvyyttä ja kosketti laajasti väestöä, kun yli 30 000 ihmisen arkaluontoiset potilastiedot varastettiin (tämä tapaus tosin oli sellainen, että kansalainen ei olisi voinut tilannetta omalta osaltaan mitenkään estää). Myös Venäjän hyökkäys Ukrainaan sekä Suomen Nato-jäsenyysprosessi ovat osoittaneet digitaalisen turvallisuuden merkityksen valtioiden välisissä haittaamis- ja vahingoittamispyrkimyksissä, lisänneet kyberuhkista uutisointia ja kansalaisten kiinnostusta aiheeseen. Suomalaiset ovat digitaalisessa maailmassa aktiivisia ja yhteiskunnassa vallitsee luottamus erilaisia palveluita ja instituutioita kohtaan. Tämä luottamus on läsnä myös digitaalisessa maailmassa, joten tietoisuutta uhkista tulee lisätä. [808, 809] Kuten aiemmassa kyberturvallisuuskoulutusta käsittelevässä tutkimuksessa[810], myös tämän tutkimuksen aikana on tullut esiin kyberturvallisuuteen liittyvän käsitteistön ja termistön kirjavuus.[811]

3.23.4. Suomen kyberkansalaistaitojen määrittäminen

Vaikkakaan kyberkansalaistaitoja ei tällä termillä ole määritetty, toteaa esimerkiksi yksi suurista kouluttajista, MPK, että "kyberturvallisuuteen liittyvästä osaamisesta on kehittymässä uusi kansalaistaito". [812] Myös tutkimushaastatteluissa todettiin, että kyberturvallisuutta ei voida enää ulkoistaa, vaan jokaisen tulisi hallita perusasiat.[813] Jyväskylän yliopiston tutkimuksessa kyberkansalaistaitoina mainittiin muun muassa tietoisuus uhkista sekä medialukutaito.[814] DVV työstää parhaillaan digiosaamisen ja digitaalisen sivistyksen määritelmiä, joissa huomioidaan myös turvallisuuteen liittyvä osaaminen. Myös Suomen digitaalisessa kompassissa nähdään

tarve digitaitojen (ja myös kyberturvallisuustaitojen) tarkempaan määrittelyyn ja todetaan, että on päästävä teknisten perustaitojen määrittelystä syvempään ja monipuolisempaan ymmärrykseen digitaidoista. Ajankohtaisiksi teemoiksi todetaan ”lähteiden arviointi, erilaisten tarkoitusperien ja mis- ja disinformaation tunnistaminen sekä turvallinen toiminta verkossa”. [815]

Viitteet

[781] Turvallisuuskomitean sihteeristö, ”Suomen kyberturvallisuusstrategia 2019,” *Valtioneuvoston periaatepäätös 3.10.2019,* (Turvallisuuskomitea, 2019).
[782] Turvallisuuskomitea, *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020* (Turvallisuuskomitea, 2017).
[783] Liikenne- ja viestintäministeriö ja Rauli Paananen, ”Kyberturvallisuuden kehittämisohjelma,” *Liikenne- ja viestintäministeriön julkaisuja 2021:7* (Helsinki: Liikenne- ja viestintäministeriö, 2021).
[784] Liikenne- ja viestintäministeriö, ”Valtioneuvoston selonteko – Suomen digitaalinen kompassi,” *VNS 10/2022 vp* (Helsinki: Liikenne- ja viestintäministeriö, 2022).
[785] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* (Jyväskylä: Jyväskylän yliopisto, Informaatioteknologian tiedekunta, 2022), 11-12, 109-110.
[786] Henkilökohtainen tiedonanto tutkijalle, 4.8.2022.
[787] Liikenne- ja viestintäministeriö, ”Valtioneuvoston selonteko – Suomen digitaalinen kompassi”.
[788] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 7, 20-22.
[789] ”ITK2023,” *ITK-konferenssi*, luettu 27.12.2022, https://itk-konferenssi.fi/en/.
[790] Myös Suomen informaatioturvallisuusklusterin (Finnish Information Security Cluster, FISC ry) tuoreessa strategiassa vuosille 2023–2025 yhtenä viidestä pääteemasta on kyberosaamisen lisääminen varmistamalla kotimaisten ja kansainvälisten osaajien saatavuus ja maahantulon sujuvuus. Henkilökohtainen tiedonanto tutkijalle, 12.12.2022.
[791] ”Oulun yliopisto vahvistaa kyberturvallisuuden osaajien koulutusta,” *Oulun yliopisto*, luettu 26.11.2022, https://www.oulu.fi/fi/uutiset/oulun-yliopisto-vahvistaa-kyberturvallisuuden-osaajien-koulutusta.
[792] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 33-53, 88-89.
[793] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 93-94, 97-98.
[794] ”Tämä toimii!,” *Teknologiateollisuus*, luettu 30.7.2022, https://tamatoimii.fi/.
[795] ”Kansalaisen kyberturvallisuus,” *Jyväskylän yliopisto*, luettu 15.6.2022, https://www.avoin.jyu.fi/fi/opintotarjonta/informaatioteknologia/kyberturvallisuus.
[796] ”Digiturvallinen elämä,” *Digi- ja väestötietovirasto*, luettu 3.8.2022, https://dvv.fi/digiturvallinen-elama.
[797] ”Spoofy,” *CGI Inc*, luettu 15.7.2022, https://www.spoofy.fi/.
[798] ”Trollitehdas,” *Yleisradio*, luettu 6.8.2022, https://trollitehdas.yle.fi/.
[799] ”Trollibunkkeri,” *Yleisradio*, luettu 7.8.2022, https://yle.fi/aihe/artikkeli/2020/11/11/trollibunkkeri.
[800] Henkilökohtainen tiedonanto tutkijalle, 19.12.2022.
[801] ”Euroopan kyberturvallisuuskuukausi - European Cyber Security Month,” *Traficom*, luettu 15.11.2022, https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month.
[802] ”Kutsu digiturvaviikolle,” *Digi- ja väestötietovirasto*, luettu 30.10.2022, https://dvv.fi/-/kutsu-digiturvaviikolle-2022.
[803] Henkilökohtainen tiedonanto tutkijalle, 4.8.2022.
[804] Henkilökohtainen tiedonanto tutkijalle, 14.7.2022.
[805] Henkilökohtainen tiedonanto tutkijalle, 19.12.2022.
[806] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti*, 110.
[807] Henkilökohtainen tiedonanto tutkijalle, 4.8.2022.
[808] Henkilökohtainen tiedonanto tutkijalle, 14.7.2022.
[809] Henkilökohtainen tiedonanto tutkijalle, 19.12.2022.
[810] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 6.
[811] Henkilökohtainen tiedonanto tutkijalle, 19.12.2022.
[812] ”Kyber- ja informaatioturvallisuus,” *MPK*, luettu 10.10.2022, https://mpk.fi/koulutukset/kyber-ja-informaatioturvallisuus/
[813] Henkilökohtainen tiedonanto tutkijalle, 14.7.2022.
[814] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 15.
[815] Liikenne- ja viestintäministeriö, ”Valtioneuvoston selonteko – Suomen digitaalinen kompassi”, *VNS 10/2022 vp* (Helsinki: Liikenne- ja viestintäministeriö, 2022).

3.24. Tanska

ITU, Global Cybersecurity Index (GCI) 2020	32/182 (Global), 19/46 (Europe)
National Cyber Security Index (NCSI) 24.10.2022	15/160 (24.10.2022)
The Digital Economy and Society Index (DESI, 2022)	2/26

3.24.1. Strategiset kyberkoulutuslinjaukset

Tanskan kansallisen kyber- ja informaatioturvallisuuden strategian julkaisi Tanskan hallitus vuonna 2021. Strategian toimeenpano on määritelty vuosille 2022–2024. Koulutuksellisten linjausten osalta strategiassa mainitaan digitaalisten taitojen opettamisen tärkeys erityisesti lapsille ja nuorille, jotta heidän olisi mahdollista välttää joutumasta kyberrikosten ja -petosten uhreiksi. Strategiassa mainitaan yhdeksi keskeiseksi tavoitteeksi lasten, nuorten ja aikuisten kansalaisten digitaalisen lukutaidon lisääminen toteuttamalla laaja-alaisesti opetusohjelmia eri koulutuksien yhteydessä. Tilannetta voidaan parantaa myös lisäämällä tietoisuutta kaikilla koulutustasoilla kiinnostavien oppimateriaalien ja tapahtumien avulla. Kansalaisten mahdollisuuksia kyber- ja tietoturvaosaamiseen vahvistetaan lukion jälkeisellä aikuiskoulutuksella sekä jatkokoulutuksella. [816]

Kyberturvallisuuden kansalaispolitiikka ja -opastus nojaa vahvasti kahteen strategiaan; jo aiemmin mainittuun kansalliseen kyberturvallisuusstrategiaan, mutta myös yhteiseen julkiseen digitaalistrategiaan, joka on valtion, kuntien ja alueiden yhteinen strategia. [817]

3.24.2. Kyberkansalaistaitojen opettamisen nykytila

Kyber- ja informaatioturvallisuuden strategian sekä digitalisointistrategian ohjaamana on perustettu kansallinen sikkerdigital.dk-tietoportaali. Portaalin tarkoituksena on varmistaa kansalaisten, viranomaisten ja yritysten korkea tietämys ja osaaminen. Portaali tarjoaa tietovisoja, neuvoja, erilaisia kyberturvallisuutta käsitteleviä oppaita sekä kampanjamateriaalia. Portaali ei pedagogisesta näkökulmasta ole koulutussivusto, vaan sitä voidaan luonnehtia paremminkin tiedotussivustoksi. Tanskassa on yleisesti ottaen useita julkisia ja yksityisiä organisaatioita, jotka työskentelevät kyberturvallisuuden kansalaistaitojen parissa. Keskeisiä toimijoita ovat kirjastot, Cybernauterne, Ældresagen, Digitaalisen koulutuksen keskus (Center for Digital Dannelse) sekä Turvallisempi Internet -keskus Tanska (Safer Internet Center Denmark). Eri toimijoiden keskeisenä ongelmana ovat olleet erilaiset tavoitteet kyberturvallisuuden tietoisuuden lisäämisen osalta, mikä on johtanut siihen, että työtä tehdään ilman yhteistä koordinoitua verkostoa.[818]

Tietotekniikan ja mediataitojen tarve on tunnistettu jo esikoulusta lähtien. Esikoulun opetussuunnitelmassa osaksi opetusta on määritelty ”IT ja digitaalinen media”, jossa lapsille opetetaan kokemuksellisen harjoitteluun perustuvien pelien ja digitaalisten medioiden kautta tietoisuuden lisäämistä. Esikoulussa IT- ja mediataidot jaetaan neljään oppimisnäkökulmaan, jotka ovat kriittinen tutkija, analysoiva vastaanottaja, määrätietoinen ja luova tuottaja sekä vastuullinen osallistuja.[819]

Kansallisessa opetussuunnitelmassa ei ole erikseen määritelty tietoturvallisuutta tai kyberturvallisuutta. Näistä käytetään yleisesti nimitystä digitaaliset taidot. Opetussuunnitelmassa ei ole pakollisia digitaalisiin taitoihin liittyviä oppiaineita. Sen sijaan nämä tulisi integroida kaikkiin oppiaineisiin. Valtakunnalliset kokeet ja arvioinnit opiskelijoiden oppimistuloksissa arvioivat vain välillisesti opiskelijoiden ICT-kompetenssia. Tanskan opetusministeriö aloitti 2018 kokeilun ”Teknologinen lukutaito” sekä oppiaineena että materiaalina integroituna oppiaineisiin. Tanskan peruskouluissa digitaalinen osaaminen sisältyy kansalliseen opetusohjelmaan poikkiopetusaiheena (IT ja media), joka tulisi sisällyttää kaikkiin oppiaineisiin kaikilla tasoilla sekä joidenkin

oppiaineiden yhteisiin tavoitteisiin. Nimensä mukaisesti se keskittyy teknologiaan ja viestintään. Opintojaksojen teemat keskittyvät siihen, että oppilaat osaavat hallita erilaisia kokonaisuuksia. Kokonaisuudet liittyvät eri medioiden kriittiseen etsintään ja tulkintaan, näiden sisällön kriittiseen analysointiin ja arviointiin sekä siihen, miten erilaisia työvälineitä voi hyödyntää eettisesti ja itsetietoisesti.[820]

Lasten ja nuorten verkko-osaamisen vahvistamiseksi tehtiin kansallinen aloite ja sen seurauksena Tanskan hallitus solmi joulukuussa 2021 useiden poliittisten puolueiden kanssa sopimuksen, jonka tavoitteena on vahvistaa lasten ja nuorten kykyä navigoida digitaalisessa maailmassa. Sopimuksen tavoitteena on perustaa yksiköitä, jotka voivat tukea digitaalisen yhteiskunnan ”digitaalisten liikennesääntöjen” tuntemista. Nämä ovat sääntöjä, jotka kaikkien on tiedettävä – pienestä pitäen. Aloitteet kattavat perus-, lukio- ja ammatillisen koulutuksen. Tärkeimmät aloitteet ovat: ”Digitaalinen liikenneklubi”, joka keskittyy siihen, miten lapsille ja nuorille saadaan tietoa ja pätevyyttä siitä, miten heistä tulee kriittisiä digitaalitekniikan käyttäjiä, sekä ”Digitaalisen turvallisuuden koulupartiot”, joiden pitäisi tukea tervettä digitaalista kulttuuria kouluissa ja lukioissa.[821]

Tanskalaisia lukioita koskevassa laissa kuvataan, että oppilaitosten tulee tarjota mahdollisuudet ja koulutussisällöt opiskelijoiden digitaalisten taitojen kehittämiseen. Tämä sisältää myös kybertaidot. Opetusaine kulkee lukioissa nimellä informatiikka. Opiskelijan tulee osata suojata oma digitaalinen identiteettinsä ja datansa verkossa sekä osata selittää IT-turvallisuuden teknisiä ja inhimillisiä puolia. Koska Tanskassa on sekä tavallisia lukioita, teknisiä lukioita että kaupallisia lukioita, voi informatiikan opetus olla joko pakollista tai vapaaehtoista. Ainoastaan teknisessä lukiossa aine on vapaaehtoinen.[822]

Digitaalisia taitoja käsitellään kaikissa aikuiskoulutuksen ja yleisen aikuiskoulutuksen opetussuunnitelmissa. Ohjelmat koostuvat laajasta aihevalikoimasta. Digitaaliset taidot sisältyvät kaikkiin opetusohjelmiin. Tavoitteena on vahvistaa yksilön digitaalista osaamista sekä valmentaa oppijoita työ- ja sosiaaliseen elämään, jossa nopea teknologinen kehitys lisää digiosaamisen kysyntää. Vuodesta 2017 lähtien työllisillä on ollut mahdollisuus suorittaa työtehtäviensä kannalta tärkeitä digitaalisia kursseja, joiden sisältöä voidaan priorisoida tarpeen mukaisesti. [823]

Tanskassa useat yliopistot ja korkeakoulut tarjoavat kyberturvallisuuden opetusta. Yleiskatsaus tarjontaan osoittaa, että suurin osa koulutusohjelmista painottaa opetuksen kyberturvallisuuden teknistä näkökulmaa, mutta esimerkiksi Kööpenhaminan kauppakorkeakoulussa on tarjolla kaupalliseen kyberturvallisuuteen suuntautunut kurssi. Kaikkiaan yliopistoissa on tarjolla ainoastaan neljä varsinaista kyberturvallisuuden koulutusohjelmaa, joista kaksi on ylempää maisteritasoa ja kaksi alempaa kandidaattitasoa.[824]

Tanskassa kansalaisille suunnattuja kyberaiheisia taitoja ja tietoja lisääviä sivustoja on useita. Tällaisia ovat muun muassa emu.dk-sivusto (Denmark’s learning portal), joka tarjoaa koulutuskursseja tukemaan keskittymistä kyberturvallisuuteen ja digitaaliseen harkintaan monissa aiheissa ja monilla tasoilla[825], sekä Cyber hub -sivusto, joka tarjoaa ilmaisia kursseja kyberturvallisuudesta kiinnostuneille, harrastajille ja ammattilaisille. Tämän sivuston sisällöt painottuvat tekniseen osaamiseen. [826] Sikker:Cyber-sivusto tarjoaa eri kyberturvallisuuden aiheita käsitteleviä moduulimuotoisia kursseja vasta-alkajista osaavampiin käyttäjiin. Sivuston on kehittänyt IT University Copenhagen.[827] The Cyber Mission -sivusto on toteutettu yhteistyössä Tanskan IT- ja opetusviraston kanssa. Alusta tarjoaa kokonaisuutena ammatillisen kurssin kyberturvallisuudesta. [828] Safer Internet Center Denmark -keskuksen tavoitteena vahvistaa lasten ja nuorten digitaalisen ja sosiaalisen median käyttöä sekä torjua lapsia ja nuoria koskevaa laitonta ja ei-toivottua sisältöä.[829] The Media Council for Children and Young People ylläpitää erityisesti lapsille ja nuorille suunnattua sivustoa, joka opastaa ja jakaa tietoa digitaalisen median käytöstä.[830] ”My digital self Defence” on sovellus, jonka tarjoaa Tanskan kuluttajaneuvosto kansalaisille välittääkseen ajantasaista tietoa kybermaailmassa tapahtuvista uhista. Sovellus tarjoaa myös neuvoja, miten toimitaan, jos vahinko sattuu ja tiedot varastetaan. Sovellus on ladattavissa sekä Androidille että Applelle.[831] Digitaalisen koulutuksen keskus (Center for Digital Dannelse) tarjoaa maksullista materiaalia digitaalisen maailman ilmiöiden opetukseen ja opiskeluun lähinnä ala- ja yläkouluikäisille. Sivustolta löytyy myös paljon lasten vanhemmille suunnattuja ohjeita asioiden opettamiseen.[832] Digitaalisen pedagogiikan keskus (Center for

Digital Pædagogik) on Tanskan johtava lasten ja nuorten digitaalisen neuvonnan järjestö. Järjestö järjestää käytännön tietoon perustuvia työpajoja ja luentoja digitaalisesta hyvinvoinnista ja pedagogiikasta.[833] Cyber Hub -sivusto keskittyy auttamaan nuoria digitaalisessa toimintaympäristössä. Sivustolla voi valita, mistä haluaa kysyä, ja vastauksena sivusto tuottaa valmiita vastauksia eri tilanteisiin. Kysymyksiä voi esittää myös sähköpostilla, tekstiviestillä tai nuori voi kysyä toiselta nuorelta.[834] Coding Pirates -järjestö on voittoa tavoittelematon organisaatio, jonka tarkoituksena on kehittää lasten teknologista rohkeutta kekseliäisyyden ja luovan voiman avulla. Järjestö toteuttaa projekteja, joista yksi on kyberturvallisuuden opetteluun suunnattu peli.[835]

Tanskassa kyberturvallisuustietoa on pääsääntöisesti jaettu julkisesti rahoitettujen internetsivustojen sekä tiedotuskampanjoiden kautta. Tanskassa on kansalaisille suunnattu sivusto Sikkerdigital.dk, joka toimii keskeisenä foorumina, kun puhutaan kyberturvallisuuden tietoisuuden lisäämisestä. Portaali järjestää vuosittain kyberturvallisuuteen suuntautuvia yleisötilaisuuksia.[836] Tanskassa on myös vuodesta 2013 lähtien DKCERT tehnyt raportteja kansalaisten tietoturvasta. Aiheina ovat kokemukset, tietämys sekä käyttäytyminen.[837]

3.24.3. Kansalliset erityispiirteet

Tanskassa on vahva kansallinen ennakoivan kyberosaamisen koulutusjärjestelmä, jonka juuret juontavat 1990-luvun lopun päätöksiin luoda kaksi koulutusrakennetta, IT-yliopisto itä ja länsi. IT yliopisto länsi syntyi osaksi Aarhusin yliopiston teknillistä tiedekuntaa ja itä täysin uutena IT Yliopisto Kööpenhaminana.[838]

Tekoälyn mahdollisuuksia kartoittava SIRI-komissio suositteli vuonna 2019 julkaistussa raportissaan, että ”koko väestölle, ei ainoastaan lapsille ja nuorille, tulisi laatia digitaalinen koulutusohjelma, joka perustuu oppimiseen, luovuuteen ja interaktiivisuuteen ja joka aktivoi kaikki toimijat kirjastoista kansanopistoihin, siviiliyhteiskuntaan, medioihin ja muihin sidosryhmiin.”[839]

Tutkimuksen aikana eri alan asiantuntijoiden kanssa käytyjen keskustelujen pohjalta tulevaisuudessa tulisi Tanskassa panostaa eri toimijoiden välisen yhteistyön kehittämiseen. Keskiössä näyttäisivät olevan sellaiset toimijat, jotka ovat avainasemassa, kun puhutaan erilaisten kyberturvallisuuteen kohdistuvien kampanjoiden ja sivustojen tuottamisesta kansalaisten tarpeisiin. Kansalaisille suunnattua Sikkerdigital.dk-sivuston kehittämistä tulisi jatkaa, jotta mahdollisimman moni kansalainen löytäisi sen ja saisi sitä kautta tietoa ja välineitä digitaalisessa maailmassa toimimiseen turvallisesti. Tarvetta olisi myös enemmän huomioida ikäihmisiä digitaalisen maailman uhkien havaitsemisessa. Vastauksista saadut tiedot viittaavat myös siihen, että koulutusta tulisi uudistaa. Havainnot ovat osoittaneet, että suurelta osin tekniikan opetukseen painottuva opetus ei riitä täyttämään osaajapulaa vaan osaajia tarvitaan myös ymmärtämään liiketoimintaa digitaalisessa maailmassa.[840]

3.24.4. Kyberkansalaistaitojen määrittäminen

Tutkittujen materiaalien ja saatujen vastausten perusteella Tanskassa ei ole olemassa määrittelyä sille, mitä kyberturvallisuustaidot kansalaisilla tarkoittavat. Tästä huolimatta yleisesti on nähtävillä, että kansalaisten taitojen osaamista tulisi vahvistaa. Kansalaisten tulisi kyetä toimimaan turvallisesti internetissä sekä pystyä suojaamaan omat tietonsa. Yleisesti on myös havaittavissa, että kansalaisten osaamiseen pyritään vaikuttamaan ennen kaikkea lisäämällä tietoa kybermaailman uhista, eikä niinkään opettamaan, miten erilaisissa tilanteissa tulisi menetellä. Eri julkaisuissa puhutaan tietojen ja taitojen lisäämisestä kansalaisten keskuudessa, mutta kantaa ei oteta siihen, mitä nämä taidot ovat.

Viitteet

[816] The Danish Government, *The Danish National Strategy for Cyber and Information Security 2022-2024* (2021), 23-25.
[817] The Danish Government, *The Danish National Strategy,* 23-25; Henkilökohtainen tiedonanto tutkijalle, 30.6.2022*;* ”Sikkerdigital.dk,” luettu 30.6.2022, https://sikkerdigital.dk/.
[818] Henkilökohtainen tiedonanto tutkijalle, 30.6.2022; ”Sikkerdigital.dk,” luettu 30.6.2022, https://sikkerdigital.dk/.
[819] Børne- og Undervisningsministeriet, *Børnehaveklassen. Faghæfte 2019* (København K: Emu.dk, 2009), 75.
[820] Henkilökohtainen tiedonanto tutkijalle, 12.6.2022; *It og Medier – Vejledning*, luettu 24.10.2022, https://emu.dk/sites/default/files/2020-04/It%20og%20Medier%20-%20vejledning.pdf.
[821] Henkilökohtainen tiedonanto tutkijalle, 10.8.2022 ja 22.8.2022.
[822] Henkilökohtainen tiedonanto tutkijalle, 5.7.2022.
[823] Henkilökohtainen tiedonanto tutkijalle, 2.9.2022.
[824] ”Study in Denmark, Find your Study Programme,” *Danish Agency for Higher Education and Science*, luettu 12.7.2022, https://studyindenmark.dk/portal.
[825] ”EMU, Denmark’s learning portal,” luettu 14.7.2022, https://emu.dk/.
[826] ”Industriens Fond. Cyber Hub,” luettu 12.8.2022, https://cyberhub.dk/.
[827] ”Sikker: Cyber,” luettu 22.7.2022, https://sikkercyber.dk/.
[828] “Cybermissionen,” *Ministry of Education, Agency for IT and Learning; Cyber Skills*, luettu 10.8.2022, https://cybermissionen.cyberskills.dk/.
[829] “Safer Internet Centre Denmark,” *Sikkert Internet*, luettu 30.6.022, https://sikkertinternet.dk/english.
[830] “Om Medierådet for Børn og Unge,” luettu 14.5.2022, https://www.medieraadet.dk/.
[831] “Forbrugerrådet Tænk,” luettu 23.8.2022, https://taenk.dk/om-os/vores-apps.
[832] ”Center for Digital Dannelse,” luettu 10.7.2022, https://digitaldannelse.org/.
[833] ”Center For Digital Pædagogik,” luettu 29.6.2022, https://cfdp.dk/.
[834] “CyberHus,” luettu 23.7.2022, https://cyberhus.dk/.
[835] ”Coding Pirates,” luettu 22.9.2022, https://codingpirates.dk/.
[836] Henkilökohtainen tiedonanto tutkijalle, 2.7.2022 ja 22.8.2022.
[837] DKCERT, *Danskernes informationssikkerhed* (The Danish Agency for Digitalisation, 2020).
[838] ”Center for Information Security and Trust,” *ITU CISAT*, luettu 27.12.2022 https://cist.dk/.
[839] Henkilökohtainen tiedonanto tutkijalle, 26.9.2022.
[840] Henkilökohtainen tiedonanto tutkijalle, 24.5.2022, 6.6.2022 ja 17.6.2022.

3.25. Tšekki

ITU, Global Cybersecurity Index (GCI) 2020	68/182 (Global), 35/46 (Europe)
National Cyber Security Index (NCSI) 24.10.2022	5/160 (24.10.2022)
The Digital Economy and Society Index (DESI, 2022)	19/26

3.25.1. Strategiset kyberkoulutuslinjaukset

Tšekin hallitus julkaisi kansallisen kyber- ja informaatioturvallisuuden strategian vuonna 2020. Strategia on vuosille 2021–2025. Strategiassa otetaan vahvasti kantaa kyberturvallisuuden sisällyttämiseen osaksi kaikkea koulutusta ja läpi kaikkien alojen. Koulutus nähdään tärkeänä aloittaa jo varhaisessa vaiheessa esikoulusta alkaen. Strategia nostaa esille erityisesti opetushenkilöstön kouluttamisen oppilaiden ja opiskelijoiden ohessa tärkeäksi osaksi tietolukutaidon kehittämisen kannalta. Poikkeuksellista on, että strategia huomioi myös vanhemmat ihmiset. Vanhemmat ihmiset ovat monesti yksi haavoittuvimmista ryhmistä, joihin kohdistuvat modernin digitalisaation negatiiviset puolet. Tätä ryhmää tulee kouluttaa tunnistamaan disinformaatio sekä käyttämään turvallisesti digitaalista teknologiaa. Muun kyberturvallisuuteen tähtäävän koulutustoiminnan osalta tietoisuuden lisäämistä tullaan jatkamaan laajasti tai kohdennetusti hyödyntämällä erilaisia kampanjoita, joita järjestävät vastuulliset toimijat, kuten valtio, yksityiset yritykset, akateemiset sekä voittoa tavoittelemattomat järjestöt.[841]

Kyberturvallisuusstrategian ohelle on laadittu erillinen strategian toimeenpano-ohjelma. Ohjelmassa tavoitteiden saavuttamisen osalta tuodaan esille muun muassa se, että kansallinen kyberturvallisuuden koulutussuunnitelma laaditaan, modernisoidaan perusopetuksen ja lukio-opetuksen opetussuunnitelmat kyberturvallisuuden osaamisen edistämiseksi sekä kehitetään ja ylläpidetään koulutuksellista e-oppimisalustaa.[842] Tšekin tasavallan hallituksen politiikkalausunnossa mainitaan kyberturvallisuuden osalta tuki kansalaisille digitaalisten taitojen koulutus- ja koulutusohjelmien osalta. Tämän mainitaan koskevan kaikkia sukupolvia.[843]

Kyberturvallisuus sisältyy yleisesti Tšekin tasavallan koulutuspolitiikan strategiaan, jossa se on määritelty osaksi perusopetuksen digitaalista osaamista. NCISA vastaa kyberturvallisuuskoulutuksen kehityksestä strategisella tasolla. NCISA tekee yhteistyötä opetus-, nuoriso- ja urheiluministeriön kanssa perusopetuksen puiteohjelman muutoksissa, jotka sisältävät strategian koulutusvaatimukset. NCISA ei kuitenkaan ole vastuussa opetuksen sisällöstä, vaan koulut ovat vastuussa koulutusohjelmien kehittämisestä, ja ne on laadittava puiteohjelman periaatteiden mukaisesti. Opetus-, nuoriso- ja urheiluministeriö käsittelee kyberturvallisuutta kahdesta näkökulmasta: turvallisuuden sekä ennaltaehkäisyn. Turvallisuuteen kuuluu koulujen yhteinen turvattu tietokoneverkko ja ennaltaehkäisy tähtää erityisesti erilaisten konferenssien, webinaarien ja kurssien järjestämiseen. Opetus-, nuoriso- ja urheiluministeriö vetoaa yhteistyössä NÚKIB:n kanssa digitaalisten taitojen ja osaamisen turvaamiseen paitsi tiedon jakamisessa ja arvioinnissa, myös itsenäisessä verkko-opetuksessa, oppilaiden kirjautumistietojen hallinnassa, viestintäalustojen turvaamisessa ja yhdistämisessä.[844]

3.25.2. Kyberkansalaistaitojen opettamisen nykytila

Kyberturvallisuuden opetussisältöjä ei ole erikseen sisällytetty esiopetuksen puiteohjelmaan, jossa määritellään esikouluikäisten lasten laitoskasvatuksen tärkeimmät vaatimukset, ehdot ja säännöt. Kuitenkin Tšekin tasavallassa on jo ollut tarjolla erilaisia aktiviteetteja ja kursseja esikouluikäisille. Kyber- ja tietoturvaviraston koulutusyksikkö on julkaissut vuodesta 2022 lähtien soveltuvia koulutustoimintoja, jotka kaikki käsittelevät internetin turvallista käyttöä.[845]

Kansallisen peruskoulun opetusohjelma (Basic Education Program) sisältää kohdan ”Tieto- ja viestintäteknologiat”, joka sisältää opetusta kansalaisen kyberturvallisuustaidoissa, kuten laitteen perushallinnassa, tiedon etsimisessä sekä tiedon luotettavuuden ja keskinäisten yhteyksien tunnistamisessa. Puiteohjelman asiakirjaa muokattiin 2021 vastaamaan valtakunnallista tarvetta kouluttaa lapsia paremmin tietotekniikassa, ja tuolloin mukaan otettiin uutena digitaidot. Opetus-, nuoriso- ja urheiluministeriön esityksestä kyberturvallisuuden osalta kyberuhkien ehkäisy ja turvallinen käyttäytyminen internetissä sisällytettiin koulutusohjelmiin. Tiettyjen alueiden tekijät ja riskit tulisi ottaa koulutuksessa huomioon. Tällaisia ovat muun muassa internetin maailma ja sen erityispiirteet, riskikäyttäytyminen kyberavaruudessa, tekijänoikeuslaki, kyberpiratismi, digitaalinen identiteetti, kyberhäirintä ja verkkokiusaaminen.[846]

Vuonna 2016 opetus-, nuoriso- ja urheiluministeriö perusti yhteistyössä pedagogisen instituutin kanssa alustan nimeltä DigiKoalice. Alusta yhdistää koulut ja ICT-maailman digitaalisessa koulutuksessa ja keskittyy lasten ja aikuisten digitaalisten taitojen kehittämiseen; kyberturvallisuus on yksi aiheista. Parhaillaan valmistellaan perus- ja toisen asteen koulutuksen laajaa uudistamista, jonka taustalla on koulutuspolitiikan strategia 2030+. Uudistamisessa pääpainona on työskentely turvallisesti digitaalisten teknologioiden kanssa.[847]

Vanhemmat ihmiset on lähtökohtaisesti otettu huomioon kansallista kyberturvallisuusstrategiaa laadittaessa, mutta käytännön tasolle päästiin vasta 1.10.2022, jolloin Kyber- ja tietoturvaviraston koulutusyksikkö julkaisi kehittämänsä verkkokurssin. Julkaisun yhteydessä toteutettiin myös laaja mediakampanja. Työkalu on nimeltään SENIOR. Sen tavoitteena on parantaa ikääntyvien aikuisten henkilökohtaista turvallisuutta internetiä käytettäessä, ja se nähdään erityisen hyödyllisenä haitallisen sähköisen viestinnän havaitsemisessa. Työkalun suunnitteluun ovat osallistuneet vanhemmat aikuiset, mikä näkyy julkaistun työkalun käsikirjamaisuutena.[848]

Kyberturvallisuutta voi opiskella Masarykin yliopistossa kandidaattitasolla, Ambis College -korkeakoulussa on meneillään kolmevuotinen hanke, jossa kehitetään innovatiivista opetusohjelmaa kyberturvallisuudesta. Prahan turvallisuustutkimusinstituutti (Prague Security Studies Institute) tarjoaa myös Security Scholars Program -ohjelmaa, joka sisältää kyberturvallisuutta ja digitaalista turvallisuutta sisältäviä opintoja. Tarjolla on myös yksityisiä tahoja, jotka järjestävät maksullisia kursseja kyberturvallisuudesta. Tällaisia ovat muun muassa Prahan koodauskoulu (Praha Coding School), NH Prahan tietokeskus (NH Prague Knowledge Center) sekä SANS DFIR Europe Prague.[849,850]

Tšekissä kansalaisille suunnattuja kyberaiheisia taitoja ja tietoja lisääviä sivustoja on useita. Kansallinen kyber- ja tietoturvavirasto (NCISA) järjestää oman koulutusosastonsa kautta niin kursseja, luentoja kuin konferenssejakin eri kohderyhmille. Esimerkkinä on vuosittain järjestettävä Festival of Secure Internet sekä lapsille suunnatut erilaiset pelit ja aktiviteetit, kuten Vanda & Eda ja Digital footprint.[851] Cybercon BRNO -konferenssin keskeisenä tarkoituksena on yhdistää kyberturvallisuuden eri alojen asiantuntijoita jakamaan tietoa ja kokemuksia keskenään (viimeksi järjestetty syyskuussa 2021).[852] IS2 Information Security Summit (8. ja 9. kesäkuuta 2022) jakaa myös vuosittain ”The Hall of Fame Cybersecurity” -palkintoa ihmisille, jotka ovat vaikuttaneet positiivisesti Tšekin kyberturvallisuuteen.[853] Qubit cyber security conference in Prague on kansainvälinen konferenssi, joka järjestettiin yhdeksännen kerran vuonna 2022 ja joka kokoaa kasaan kyberturvallisuudesta ja -harjoittelusta kiinnostuneita ympäri maailman.[854]

Future of Cyber Conference -tapahtumassa käsitellään pääasiassa kybertietoisuutta, kyberkasvatusta ja kyberalan tiedon ja tietämyksen vaihtoa eri toimijoiden kesken. Pääjärjestäjänä toimii kansallinen kyber- ja tietoturvavirasto yhteistyössä CzechCyber Centerin, sisäministeriön sekä muiden kumppaneiden kanssa, kuten korkeakoulujen.[855] Czech Cyberton tarjoaa kyberharjoituksia teini-ikäisille[856] ja Internet Highway on verkkopeli[857]. Interland on peli, joka esittelee verkkoturvallisuuden tärkeimpiä näkökohtia. Suorittamisesta saa erillisen diplomin.[858] NÚKIBilla on koulutusportaali, josta löytyy erilaisia kyberturvallisuuteen liittyviä kursseja. Kursseja on tarjolla kansalaisille eri ikäryhmille, kouluille sekä myös terveydenhuollon henkilöstölle. Erityisesti kyberturvallisuuden perusteet -kurssi on suunnattu kansalaisille.[859] Cz.niz Academie -sivustolta löytyy itsenäisesti suoritettavia kursseja, jotka koskevat enimmäkseen teknisiä perusasioita.[860]

3.25.3. Kansalliset erityispiirteet

Haastatteluiden ja aineiston perusteella Tšekissä kyberturvallisuustaidot nähdään kansalaisten näkökulmasta tärkeänä. Merkityksellistä on huomata, että etenkin vanhemmat aikuiset huomioidaan jo strategian tasolla. On mielenkiintoista havaita, että kansalaisten kybertaitojen kouluttamisesta on Tšekin valtio ottanut vastuuta. Tämä onkin johtanut eri kohderyhmille suunnattujen opetusalustojen, pelien, kirjojen ja kampanjoiden syntymiseen. Opetus-, nuoriso- ja urheiluministeriö on ottanut vahvan roolin digitaalisten taitojen ja osaamisen vahvistamisessa. Kansallinen kyber- ja tietoturvaviranomainen on kehittämässä myös erityistä koulutuksellista oppimisalustaa, joka keskittyy laajasti eri kohderyhmille suunnattujen koulutusmateriaalien tuottamiseen. Arviota tämän valmistumisesta ei kuitenkaan ollut saatavilla. Tšekissä toimii erityinen CZ.NIC-yhdistys, joka vastaa kansallisella tasolla koordinoinnista, jolla pyritään parantamaan erityisesti lasten verkkoturvallisuutta. Tšekissä on määritelty oma kyberturvallisuuslaki (Cyber Security Act), joka antaa laissa valtuutetuille instituutioille ja toimielimille keskeisen roolin vaikuttaa tasavallan kyberturvallisuuteen ja koko järjestelmän tehokkuuteen. Saumaton yhteistyö näiden toimijoiden ja yksityisen sektorin toimijoiden välillä ovat keskeistä koko järjestelmän toiminnan kannalta.[861]

Tšekin tasavallan toisen asteen kouluissa on käytössä erityinen Haxagon-kyberturvallisuuden harjoitusalusta, jonka tarkoituksena on tukea yleistä IT-koulutusta. Alustan luomisessa on käytetty pelillistämistä, kuten erilaisia tasoja, merkkejä, saavutuksia sekä tulostaulukoita. Alustaa voi käyttää itsenäisesti paikasta tai laitteesta riippumatta. [862] Saatujen tietojen perusteella Kansallisen kyber- ja tietoturvaviranomaisen tavoitteena on tulevaisuudessa jatkaa kyberturvallisuuden laajempaa sisällyttämistä yhteiskunnan koulutukseen kahdella pääalueella. Ne ovat kybertietoisuuden lisääminen yhteisen tietostandardin rakentamiseksi (koulutus kaikille) ja kyberturvallisuusasiantuntijoiden koulutus työmarkkinoiden kysyntää ajatellen.[863]

3.25.4. Kyberkansalaistaitojen määrittäminen

Keskusteluissa saatujen vastausten perusteella Tšekissä kyberturvallisuuden kansalaistaitoina nähdään muun muassa oikeanlaiset salasana-asetukset, sosiaalinen suunnittelu, turvallinen nettiyhteys sekä digitaalisten laitteiden suojaus. Ennaltaehkäisyä pidetään tärkeänä osana kyberturvallisuutta eli sitä, millaisia ennakoivia toimia tulisi ottaa huomioon, jotta voidaan saavuttaa turvallinen verkkokäyttäytyminen. Tulisi myös sisältöjä määriteltäessä ottaa huomioon, millaisesta näkökulmasta sitä katsotaan. Onko kyse esimerkiksi lainsäädännön näkökulmasta, akateemisten ympäristöjen näkökulmasta vai loppukäyttäjän näkökulmasta.[864]

Viitteet

[841] National Cyber and Information Security Agency, *National Cyber Security Strategy of the Czech Republic for the Period from 2021 to 2025* (2021), 18-19.
[842] National Cyber and Information Security Agency, *Action Plan for National Cyber Security Strategy for the Years 2021 to 2025* (2021), 16-18.
[843] Government of the Czech Republic, *Policy Statement of the Government of the Check Republic* (2022).
[844] Henkilökohtainen tiedonanto tutkijalle, 28.8.2022 ja 9.9.2022; Ministry of Education, Youth and Sport, *Strategy for the Education Policy of the Chech Republic up to 2030+* (2020).
[845] Henkilökohtainen tiedonanto tutkijalle, 26.8.2022; ”Nukib,” luettu 27.8.2022, https://osveta.nukib.cz/course/view.php?id=105.
[846] Henkilökohtainen tiedonanto tutkijalle, 26.8.2022; ”Nukib,” luettu 27.8.2022, https://osveta.nukib.cz/course/view.php?id=105.
[847] Henkilökohtainen tiedonanto tutkijalle, 11.8.2022; Ministry of Education, Youth and Sport, *Basic Education*, 34–35.
[848] Henkilökohtainen tiedonanto tutkijalle, 2.10.2022; ”SENIOR proti internetovým padouchům?,” *Nukib*, luettu 3.10.2022, https://osveta.nukib.cz/course/view.php?id=140#section-0.
[849] “Cybersecurity,” *Masaryk University*, luettu 13.9.2022, https://www.muni.cz/en/bachelors-and-masters-study-programmes/26540-cybersecurity; “Cybersecurity fundamentals,” *Ambis College*, luettu 14.10.2022, https://www.ambis.cz/cybersecurity-fundamentals; “Cyber security Academy,” *Prague Security Studies Institute*, luettu 20.10.2022, https://www.pssi.cz/projects/16-cyber-security-academy.
[850] “Brno University of Technology,” luettu 4.1.2023, https://www.vut.cz/en/.
[851] "Education," *National Cyber and Information Security Agency*, luettu 23.8.2022, https://nukib.cz/en/cyber-security/education/.
[852] ”Cybercon Brno,” luettu 6.8.2022, https://www.cybercon.cz/eng/.
[853] ”Is2,” luettu 17.9.2022, https://is2.cz/en/.
[854] “Qubit Conference,” luettu 24.10.2022, https://prague.qubitconference.com.
[855] “Future of Cyber Konference,” luettu 22.7.2022, http://future-forces-forum.org/events/default/74_future-of-cyber-fcd?lang=cs.
[856] ”Czech Cybertron,” *Network security monitoring cluster*, luettu 4.1.2023, https://www.czechcybertron.cz.
[857] ”Pedagogicka faculta, Univerzita Palackého v Olomouci,” luettu 22.10.2022, https://www.pdf.upol.cz/nc/pl/zprava/clanek/nova-online-hra-vznika-na-pdf-up-a-zaky-zakladnich-skol-uci-jak-se-bezpecne-chovat-na-internetu/.
[858]“Interland. Be internet awesome,” luettu 15.6.2022, https://beinternetawesome.withgoogle.com/cs_cz/interland.
[859] “NÚKIB,” luettu 17.5.2022, https://osveta.nukib.cz/local/dashboard/.
[860] ”CZ.NIC Moodle,” *Cz.nic Akademie*, luettu 20.12.2022, https://moodle.nic.cz/.
[861] National Cyber and Information Security Agency, *National Cyber Security Strategy of the Czech Republic* (2020) 8, 18-19; “CZ.NIC,”luettu 18.9.2022, https://www.nic.cz/; National Cyber and Information Security Agency, *Legislation* (2022), luettu 10.9.2022, https://nukib.cz/en/cyber-security/regulation-and-audit/legislation/; Henkilökohtainen tiedonanto tutkijalle, 14.9.2022.
[862] Henkilökohtainen tiedonanto tutkijalle, 19.9.2022 ja 26.8.2022.
[863] Henkilökohtainen tiedonanto tutkijalle, 9.9.2022.
[864] Henkilökohtainen tiedonanto tutkijalle, 25.8.2022 ja 26.8.2022.

3.26. Unkari

ITU, Global Cybersecurity Index (GCI) 2020	35/182 (Global), 22/46 (Europe)
National Cyber Security Index (NCSI) 2022	35/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	22/27

3.26.1. Strategiset kyberkoulutuslinjaukset

Unkari painottaa vuoden 2013 kyberturvallisuusstrategiassa kansallista kyberturvallisuutta edistävinä keinoina tietoisuuden lisäämistä ja siinä keskitytään erityisesti yksittäisiin käyttäjiin sekä pk-yrityksiin. Myös eri koulutusasteiden koulutuksen kehittämiseen kiinnitetään huomiota, kuin myös valtion virkamiesten koulutukseen ja ammatillisen kehittämisen kursseihin. Kyberturvallisuus tulisi koulutuksessa integroida osaksi tietotekniikan koulutusta. Lapset ovat erityisasemassa. Heille halutaan turvaa tietoisuuden ja muiden toimien kautta. Strategista yhteistyötä tehdään kyberturvallisuuden tutkimukseen ja kehittämiseen osallistuvien yliopistojen ja tutkimuslaitosten kanssa.[865] Vuoden 2018 kyberturvallisuusstrategian päivityksessä (Verkko- ja tietojärjestelmien turvallisuutta koskeva strategia) tavoitteena on edistää koulutus- ja tutkimus- ja kehitysohjelmia sekä lisätä turvallisuustietoisuutta. Kansallisen julkisen palvelun yliopiston kyberturvallisuusakatemia osallistuu kyberturvallisuuteen liittyvän koulutuksen ja täydennyskoulutuksen järjestämiseen sekä kyberavaruuden turvallisuuteen liittyvän koulutus- ja tutkimustoiminnan ja niihin liittyvien resurssien koordinointiin. Unkari järjestää aktiivisesti kotimaisia ja osallistuu aktiivisesti kansainvälisiin kyberturvallisuustietoisuusfoorumeihin ja -kampanjoihin (kuten ECSM, Euroopan kyberturvallisuuskuukausi). Unkarin tavoitteena on, että kyberturvallisuuden koulutus- ja tutkimus- ja kehittämismahdollisuudet auttavat luomaan kilpailukykyisen kotimaisen tietopohjan, joka vastaa sekä kansainvälisiä käytäntöjä että kotimaisten työmarkkinoiden tarpeita. Unkarin digitaalisessa koulutusstrategiassa asetetaan tavoitteet ja toimenpiteet tietoturvaa edistävän digitaalisen osaamisen ja tietoisuuden sekä koulutuksen ja ammatillisen koulutuksen alojen kehittämiseksi.[866] Kyberturvallisuusstrategian seuraava päivitys on näillä näkymin tulossa vuoden 2023 alkupuolella.[867] Unkarin digitaalinen ohjelma (DJP, Digitális Jólét Program 2030) on laaja-alainen ja pitkäaikainen hanke, jonka avulla Unkari valmistautuu digitalisaation mukanaan tuomiin muutoksiin niin jokapäiväisessä elämässä ja yritystoiminnassa kuin taloudessa ja yhteiskunnallisella tasolla. Sen keskiössä ovat ihmiset itse, ja siksi Unkarin hallitus valmistaa kansalaisia ja yrityksiä DJP-ohjelman avulla digitalisaatioon. DJP2030 muodostaa digitaalipolitiikan strategisen toimintakehyksen vuosille 2021–2030. Se on kattostrategia, jonka alle kuuluvat muun muassa lastensuojelustrategia (DCP, Digital Child Protection Strategy of Hungary) ja koulutusstrategia (DES, Digital Education Strategy of Hungary), joka rakentuu DESI:ssä mitatun EU:n Digital Decade -kompassin neljän pääpilarin ympärille, joista yksi on digitaaliset taidot. [868,869]

3.26.2. Kyberkansalaistaitojen opettamisen nykytila

Koululaisille kyberturvallisuuskoulutus on osana peruskoulutuksen opetussisältöjä. Aihealuetta ei kuitenkaan ole liiemmälti korostettu. Perusopetuksessa suoritetaan digitaalinen ajokortti (ICDL International Computer Driving Licence, entinen ECDL[870]) ja siihen kuuluvat kyberturvallisuuteen liittyvät perusteet. Kymmenet tuhannet lapset käyttävät vuosittain myös Googlen opetusmateriaalia. Unkarissa Safer Internet -hanketta, joka on EU-rahoituksella toteutettu, hallinnoi alan kansalaisjärjestö. Yliopistoissa opiskelijat saavat kyberturvallisuuden perustiedot osana IT-opetusta ja alan erityiskursseilta. Suurelle yleisölle on kampanjoita sekä sosiaalisessa mediassa että internetissä. Kansallinen kyberturvallisuuskeskus (NCSC, Nemzeti Kibervédelmi Intézet) toteuttaa suurelle yleisölle suunnatut tiedotushankkeet. Kyberturvallisuuteen liittyviä opetussisältöjä, jotka olisi suunnattu erityisryhmille, ei ole, eikä senioreille suunnattu projekti toteutunut. [871] ENISAn CyberHEAD-

tietokannan mukaan Unkarissa kyberturvallisuutta opetetaan National University of Public Service -yliopistossa.[872] ELTEssä (Eötvös Lórand University) tietotekniikan maisteritutkinnossa voi myös erikoistua kyberturvallisuuteen.[873,874]

Unkarin uudessa opetussuunnitelmassa (2020/2021) tietojenkäsittely-niminen (Informatika, vuoden 2012 opetussuunnitelma) oppiaine muutetaan vaiheittain digitaaliseksi kulttuuriksi (Digitális Kultúra) ja se on pakollinen oppiaine luokille 3–11 (8–17-vuotiaat). Muutoksen myötä sisältöä nykyaikaistetaan kattamaan uudenlaisia sisältöjä. Digitaalinen kulttuuri opettaa tietoyhteiskunnassa tarvittavia jokapäiväisiä taitoja, kuten digitaalisia perustaitoja, ongelmanratkaisutaitoja, digilukutaitoa, digitaalisten laitteiden luovaa ja turvallista käyttöä sekä tietoista käyttäjäasennetta yksilön, yhteisön ja yhteiskunnan kannalta. Digitaalisen kulttuurin oppiminen alkaa opetussuunnitelmassa kolmannella luokalla, mutta sillä on tärkeä rooli oppimisprosessin kehityksessä jo aiemmilla luokilla yksi ja kaksi (kuten digitaalisten oppimateriaalien käyttö ja digilukutaito luokassa).[875,876]

Unkarin Safer Internet Center (SIC), joka on osa EU:n Better Internet for Kids -ohjelmaa (BIK), edistää lasten ja nuorten (ja sitä kautta myös aikuisten) internetin ja mobiiliteknologioiden turvallisempaa käyttöä, muun muassa tietoisuutta lisäämällä. Nuoret osallistuvat tapahtumiin (Safer Internet Day (SID), Lastenpäivä) ja auttavat levittämään internetin turvallisempaan käyttöön liittyvää verkkomateriaalia, kuuntelevat kursseja ja auttavat koulutusmateriaalien kehittämisessä. Nuoret myös keskustelevat todellisista ongelmista verkkoelämässään ja jakavat ideoita kokouksissa. Surf Safely -oppitunneilla, joita pidetään muun muassa kouluissa ja kirjastoissa, käsitellään tärkeitä arkielämään liittyviä aiheita, kuten henkilötietojen suojaamista, verkkokiusaamista, netikettiä, salasanoja ja digitaalisia jalanjälkiä. Vuorovaikutteiset tunnit sisältävät lyhyitä videoita ja helppoja harjoituksia, kun taas vanhemmille ja opettajille aiheita käsitellään kriittisemmin. Kouluttajat, joista monet ovat vapaaehtoisia, ovat alan asiantuntijoita, kuten IT-yritysten työntekijöitä.[877,878] Sivustolta löytyvät myös Googlen opetusmateriaalit, kuten Interland-peli, joka opettaa digitaalisen turvallisuuden periaatteita[879], sekä muuta opetusmateriaalia lapsille ja nuorille, kuten kirja internetin ja sosiaalisen verkostoitumisen sivustojen vaaroista, sekä materiaalia vanhemmille, kuten videoita ja Mongu-mobiilisovellus lapsen älypuhelimen hallinnointiin.

Euroopan kyberturvallisuuskuukauteen osallistuu vuosittain yhä enemmän organisaatioita, mutta pandemiatilanne on aiheuttanut siihen haasteensa ja siksi NCSC (kansallinen ECSM-koordinaattori) painotti vuonna 2021 sellaisten tapahtumien järjestämistä, jotka ovat toimineet hyvin jo vuosia. NCSC järjesti myös tapahtumia, joissa keskityttiin nuorempaan yleisöön, koska sitä kautta tavoitettaisiin laajempi kohderyhmä (kuten vanhemmat, ystävät ja opettajat).[880] Myös Unkarin vuoden 2022 kampanjoista moni oli suunnattu nuorille (koululaiset ja opiskelijat) tai ammattilaisille. Yritysten järjestämistä kampanjoista mainittakoon Unkarin BOSCHin IT-osaston henkilökunnalleen järjestämät tapahtumat. Kaikille unkarilaisille suunnattu kampanja on Kibertámadás!-podcast.[881] Lastensuojeluohjelmaan kuuluvan tietoisempi internetin käyttö Tudatosabb internethasználat -kampanjan osana on nuorille suunnattuja teemavideoita verkkoympäristön kiistanalaisista ja riskialttiista ilmiöistä. Aiheet käsittelevät riippuvuutta, verkkokiusaamista, disinformaatiota ja valeuutisia sekä kehokuvahäiriöiden ongelmia.[882] Vanhemmille suunnatussa Gyerekkel a digitális világban digitaalisen lastensuojelun ja -kasvatuksen perusteissa on viisi lyhyttä moduulia. Aiheina on muun muassa lasten yksityisyys ja henkilötiedot verkossa sekä tietoinen ”mediaruokavalio”; ruutuaika ja riippuvuus.[883] Lastensuojeluohjelman alta löytyy myös nettimentori-ohjelma ikätovereille ja 5–9-vuotiaille Sango-kuvakirja, jonka avulla käydään läpi riskialttiita asioita yhdessä vanhempien kanssa. Kansallinen media- ja viestintäviranomainen (NMHH) on perustanut Magic Valley -mediataitolukukeskuksia (Bűvösvölgy médiaértés-oktató központokat), joissa 9–16-vuotiaat voivat oppia käytännön medialukutaitoa. Internet-työpajoissa käsitellään muun muussa yksityisyyttä, seksiviestittelyä ja kiusaamista sekä opitaan tunnistamaan hyödylliset verkkosivustot ja sovellukset.[884] Gyerek a neten -ohjelma (Nuori internetissä) ja Internet hotline ovat myös osa NMHH-kampanjoita. Samoin on NETRE FEL -ohjelma, jossa sparrataan senioreiden digitaalista oppimista lähipiirin kautta. Ikäihmiset saavat eniten tukea (lapsen)lapsiltaan ja lähipiiriltä. Läheisten neuvoja myös kuunnellaan, siksi näiden auttajien apu ja esimerkki koetaan hyödylliseksi, koska on tärkeää auttaa senioreita oppimaan turvallista digitaalisten laitteiden käyttöä.[885]

Kyberturvallisuusasioiden keskitetylle nettisivustolle on Unkarissa olemassa tarve. Esimerkiksi mikään ministeriö ei tällä hetkellä ole vastuussa yleisestä tietoisuuden lisäämisestä. Kampanjoita ja opetussisältöjä voitaisiin luoda erityisesti EU-rahoituksen turvin. Kyberturvallisuusteemaa tulisi tehdä näkyvämmäksi median kautta, jolloin suuri yleisökin kiinnostuu aiheesta. Kohteina tulisi erityisesti olla ikäihmiset, koska he ovat riskiryhmässä; erityisesti disinformaation ja verkkopetoksien osalta. Hybridiuhkien torjunnan osaamiskeskuksen työ on hyvää, mutta ainakaan vielä ei sen tuloksia ole havaittavissa Unkarissa. Kyberturvallisuusalan lainsäädäntöä tehdään parhaillaan EU:ssa ja lainsäädännön tarpeellisuutta tulisi avata myös suurelle yleisölle. ENISA esimerkiksi voisi ottaa tässä roolin. Ainakin Unkarissa Euroopan kyberturvallisuuskuukausi on tunnettu, mutta pitäisi tuoda enemmän näkyväksi sitä, että se on nimenomaan EU-projekti.[886]

3.26.3. Kansalliset erityispiirteet

Tärkeä osa kansallista kyberturvallisuuskulttuurin vaalimista Unkarissa ovat lapset ja heidän suojelemisensa vaaroilta, siksi Unkarissa on myös oma strategiansa lapsille: Digital Child Protection Strategy of Hungary vuodelta 2016. Unkarissa halutaan ylläpitää ja kehittää lapsiystävällistä kyberturvallisuusympäristöä. Tätä tuetaan myös eurooppalaisen lapsiystävällinen internet -strategian (BIK) tavoittein. Sen mukaisesti lapsille ja nuorille luodaan laadukasta verkkosisältöä ja tuetaan tietoisuuden lisäämistä. Tässä työssä avainasemassa ovat unkarilaiset kansalaisjärjestöt, joilla on osaamista lastensuojelusta verkossa.[887]

Lastensuojeluohjelman älykäs päiväkoti Okosóvoda -ohjelma alkoi vuonna 2018, ja sen jälkeen joka vuosi sata päiväkotia on ollut oikeutettu ilmaisiin verkkosivupalveluihin kolmen vuoden ajan. Ohjelman ”DigiMini” tutkimusosan tavoitteena on ymmärtää muun muassa esikoululaisten älylaitteiden käyttötottumuksia, asenteita ja mediankäytön sääntöjä kotona ja päiväkodissa sekä arvioida esikoulunopettajien käytäntöjä ja asenteita. Tutkimustuloksien mukaan 80–90 prosenttia päiväkotilapsista käyttää älylaitteita päivittäin. Puolet esikoululaisista tietää internetin hyödyt ja sen mahdolliset vaarat. Vanhemmat ja lastentarhanopettajat eivät ole valmistautuneet digitaaliseen vanhemmuuteen tai koulutukseen. Puolet lastentarhanopettajista vastustaa digitaalisten laitteiden käyttöä. Esiopetuksen opettajien mukaan vanhempien vastuulla on opettaa lapsille älylaitteiden käyttöä. Tutkimuksen perusteella kehitetään Älykäs lastentarha 2.0 -ohjelma, johon sisältyy erityisesti esikoulunopettajien koulutus ja voimaannuttaminen.[888]

3.26.4. Kyberkansalaistaitojen määrittäminen

Unkarissa kehitetään parhaillaan eurooppalaiseen digitaalisen osaamisen DigComp-malliin (DigComp 2.1, joka on tarkoitus päivittää 2.2-versioon) pohjautuvaa Unkarin DigKomp for Citizens -järjestelmää, joka kuuluu Unkarin DJP-ohjelmaan. Malli on dynaaminen eli sitä päivitetään jatkuvasti. Järjestelmämalli luodaan työkaluksi kansalaisten digitaitojen kehittämistä ja arvioimista varten. Järjestelmään kuuluu DigComp-toimisto, ilmainen ja kaikille avoin DigComp-oppimisalusta (joka sisältää aihe/materiaali- ja opetuspankin), digitaalinen koulutusrekisteri ja DigComp-sertifikaattikeskukset. Alustan oppimisympäristön kohderyhmä ulottuu kouluikäisistä työnväestöön ja eläkeikäisiin. Tiedot, taidot ja asenteet asetetaan taitotasojen, tehtävätyyppien ja mallien mukaisesti. Mallin viisi osa-aluetta ovat DigComp-mallin mukaiset. Unkarissa Viestintä ja yhteistyö -osa-alueen alle kuuluu esimerkiksi verkko-ostaminen ja digipalveluiden käyttö (kommunikointia) ja myös digitaalinen identiteetti -osaaminen (esimerkiksi Netflixiä käytettäessä syntyy kansalaisen digitaalinen jalanjälki). Arjessa menestymiseen tarvittavaa digiosaamisen tasoa kutsutaan nimellä Citizen Basics ja työelämässä ja korkeakoulutuksessa tarvittavaa tasoa nimellä Citizen Plus. Kun ajatellaan peruskansalaistaitoja, informaatio- ja datalukutaito ovat tärkeitä taitoja samoin kuin turvallisuusosaaminen, toisin kuin esimerkiksi digitaalisen sisällön luominen, joka ei ole niin tärkeää arjessa. Tähän tasoon pyritään, kun ajatellaan iäkkäitä (ja kaikkia) kansalaisia. Plus-tasolla työelämässä korostuvat viestintä- ja yhteistyö- sekä turvallisuusosaaminen.[889,890,891]

Viitteet

[865] Viktor Orbán, Prime Minister, MAGYAR KÖZLÖNY, *Magyarország Nemzeti Kiberbiztonsági Stratégiájá* (6338-6341) Unkarin virallinen lehti nro 47 (maaliskuu 2013), 6341.
[866] ”A hálózati és információs rendszerek biztonságára vonatkozó Stratégia,” luettu 24.10.2022, https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf.
[867] Henkilökohtainen tiedonanto tutkijalle, 13.6.2022.
[868] ”About Digital Success Program,” luettu 27.10.2022, https://digitalisjoletprogram.hu/en/about.
[869] European Comission, *Digital Economy and Society Index (DESI) 2022: Hungary* (2022).
[870] ”Digitális érettségi a társadalomnak: új feladatokat kapott az ECDL/ICDL,” luettu 29.11.2022, https://njszt.hu/hu/news/2022-06-28/digitalis-erettsegi-tarsadalomnak-uj-feladatokat-kapott-az-ecdlicdl.
[871] Henkilökohtainen tiedonanto tutkijalle, 13.6.2022.
[872] ”CYBERHEAD – Cybersecurity Higher Education Database,” *ENISA*, luettu 27.11.2022, https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=hun.
[873] ”ELTE Eötvös Lórand University,” luettu 27.11.2022, https://www.elte.hu/en/computer-science-msc.
[874] ”CYBERWISER.eu, Hungary (HU),” luettu 27.11.2022, https://www.cyberwiser.eu/hungary-hu.
[875] MAGYAR KÖZLÖNY, *MAGYARORSZÁG H I VATALOS LAPJA, H I VATALOS*, nro 17, (31. tammikuuta 2020), 427-428.
[876] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 37, 100.
[877] ”Hungarian Safer Internet Centre,” luettu 28.11.2022, https://www.betterinternetforkids.eu/sic/hungary.
[878] ”A biztonságos internetezés kulcsa,” *Saferinternet*, luettu 28.11.2022, https://saferinternet.hu/.
[879] ”Legyél az Internet Ásza!,” *Saferinternet*, https://saferinternet.hu/legyel-az-internet-asza.
[880] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 109.
[881] ”Cybersecurity Activities, Hungary,” *ECSM 2022*, luettu 7.10.2022, https://cybersecuritymonth.eu/activities?containsDate=&country[]=HU&endDate=&perPage=10&reqPage=2&searchText=&sortOrder=ascending&startDate=October%204%2C%202022.
[882] ”Tudatosabb internethasználat,” *DGYS - Magyarország Digitális Gyermekvédelmi Stratégiája*, luettu 28.11.2022, https://digitalisjoletprogram.hu/hu/tartalom/tudatosabb-internethasznalat.
[883] ”Gyerekkel a digitális világban,” luettu 28.11.2022, https://digitalisgyermekvedelem.hu/gyerekkelonline.
[884] ”Hands-on workshops to promote the conscious use of media, Magic Valley Media Literacy Education Centre,” luettu 28.11.2022, https://magicvalley.eu/.
[885] ”Szupersegítő leszek!,” *NETRE FEL, NMHH-program*, luettu 28.11.2022, https://netrefel.hu/segitoknek.
[886] Henkilökohtainen tiedonanto tutkijalle, 13.6.2022.
[887] Orbán, *Kiberbiztonsági Stratégiájá*, 6341.
[888] ”Smart Kindergarten Program, Okosóvoda,” (EN), luettu 28.11.2022, https://digitalisgyermekvedelem.hu/okos-ovoda.
[889] ”30.03 The development of the Hungarian DigKomp System to assess and improve the digital competence of citizens,” luettu 25.11.2022, https://all-digital.org/events/the-development-of-the-hungarian-digkomp-system-to-assess-and-improve-the-digital-competence-of-citizens/.
[890] ”The development of the Hungarian DigKomp System to assess and improve the digital competence of the citizens,” luettu 25.11.2022, https://telecentreeuropeaisbl.sharepoint.com/sites/AllDIGITAL-PublicforExternalSharing/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FAllDIGITAL%2DPublicforExternalSharing%2FShared%20Documents%2FWEBSITE%2FAD%20WEEKS%202022%20PRESENTATIONS%2F30%2E03%20Hungarian%20DigiKomp%2FDigKomp%5FWebinar%5Ffinal%2Epdf&parent=%2Fsites%2FAllDIGITAL%2DPublicforExternalSharing%2FShared%20Documents%2FWEBSITE%2FAD%20WEEKS%202022%20PRESENTATIONS%2F30%2E03%20Hungarian%20DigiKomp&p=true&ga=1.
[891] ”30.03 The development of the Hungarian DigKomp System,” katsottu 26.10.2022, https://www.youtube.com/watch?v=tgP9BC_ahRQ.

3.27. Viro

ITU, Global Cybersecurity Index (GCI) 2020	3/182 (Global), 2/46 (Europe)
National Cyber Security Index (NCSI) 2022	4/160 (24.10.2022)
The Digital Economy and Society Index (DESI) 2022	9/27

3.27.1. Strategiset kyberkoulutuslinjaukset

Viron kyberturvallisuusstrategia on laadittu vuonna 2018. Siinä mainitaan tavoitteeksi kyberlukutaitoisen yhteiskunnan edistäminen, ja sen saavuttamiseksi tulee muun muassa lisätä kansalaisten, valtion ja yksityisen sektorin tietoisuutta kyberturvallisuudesta. Kyberturvallisuustaitojen kehittäminen on kaikkien kyberavaruudessa toimivien kansalaisten vastuulla. Koulutusjärjestelmässä kyberturvallisuutta käsitellään kaikilla koulutustasoilla osana digitaalisen osaamisen kehittämistä. On tärkeää pitää oppilaat ja opettajat ajan tasalla digitaalisten osaamismallien kyberturvallisuuden osataidoista ja huomioida myös osaamisen mittaaminen. Kyberturvastrategia korostaa ennalta ehkäisevien toimien merkitystä. On tarpeen puhua vallitsevista riskeistä suurelle yleisölle ja tarjota neuvoja riskien lieventämiseksi. Eri virastojen tulee tehdä yhteistyötä suuren yleisön tietoisuuden lisäämiseksi internetin uhista ja toimista, joihin on ryhdyttävä mahdollisen hyökkäyksen jälkeen.[892]

3.27.2. Kyberkansalaistaitojen opettamisen nykytila

Digitaalisen osaamisen kehittämistä hallinnoi Virossa Koulutus- ja nuorisolautakunta (Haridus- ja Noorteamet, HARNO), joka toimii opetus- ja tutkimusministeriön (Ministry of Education and Research) alaisuudessa.[893] Kyberturvallisuuden opetuksen kehyksen on vuodesta 2020 määritellyt DigComp[894], jota on sovellettava jokaisessa Viron koulussa.[895] DigCompin Safety-osa-alueen arviointikriteerit on kuvattu yleisesti ja myös täsmennetty yleissivistävän koulutuksen kaikilla tasoilla aina päiväkodista lähtien.[896] Tietotekniikan opetusta annetaan kouluissa resurssien mukaan ja valinnaisilla kursseilla. Pakollisia tietotekniikan tunteja ei ole. Kyberturvallisuutta opetetaan tietotekniikan tuntien yhteydessä alakoulusta lukiotasolle saakka.[897]

Kyberturvallisuuden opetukseen on 1.–6. luokille ja 10.–12. luokille saatavilla opetussuunnitelmat ja opetusmateriaalit. 7.–9.-luokkalaisille on saatavilla vain opetussuunnitelma. Valinnaiseen ”Informatics”-oppiaineeseen on olemassa kouluille alustavat, hieman vielä keskeneräisessä vaiheessa oleva sisältökuvaukset kyberturvallisuuden opetusta varten.[898] Esimerkiksi luokille 1–3 opetetaan salasanojen turvallista käyttöä ja epäilyttävien linkkien havaitsemista. Luokien 4–6 aiheita ovat digitaalisen viestinnän turvallisuus ja digitaalisen identiteetin hallinta, verkkokiusaamiseen puuttuminen sekä tietokonelaitteiden suojaaminen. 7.–9.-luokkalaiset opettelevat yleisimpien uhkien tunnistamista ja niihin reagoimista, kyberturvallisuuteen liittyviä lakeja ja asetuksia, digitaalisen identiteetin suojaamista, sähköistä asiointia ja verkkokeskustelujen turvallisuutta ja eettisyyttä.[899] E-kurssi ”Küberkaitse” (”Cyber defence”)[900] täyttää opetussuunnitelman toisen asteen arviointikriteerit (luokat 9/12) ja sisältää jo hieman monimutkaisempia asioita.[901] Sähköinen asiointi ja lainsäädäntö painottuvat sisällöissä enemmän kuin nuorempien oppilaiden kohdalla. Lisäksi opetellaan tunnistamaan erityyppisiä verkkopetoksia ja suojaamaan tietokonelaitteita.[902]

Koulujärjestelmässä annettavalla kyberturvaopetuksella on oma motivaatiomalli. Koulut voivat arvioida itse menestyksensä tai pyytää paikalle ulkoista arvioijaa. Motivaatiomallin avulla opiskelijat voivat arvioida myös omaa osaamistaan digitaalisessa turvallisuudessa.[903] Korkea-asteella kyberturvallisuuden opiskelu on mahdollista kahdessa eri maisteriohjelmassa. Tallinnan teknillinen yliopisto (Tallinna Tehnikaülikool, TalTech) toteuttaa yhteistyössä Tarton yliopiston (Tartu Ülikool) kanssa maisteriohjelmia ”Cybersecurity”.[904]

Kansainvälistä maisteriohjelmaa Cyberus Erasmus Mundus Master in Cybersecurity hallinnoi Etelä-Bretagnen yliopisto (Université Bretagne Sud). TalTechin vastuulla on osa tämän ohjelman koulutuksesta.[905]

TalTech ja Viron koulut tekevät yhteistyötä oppilaiden kyberturvatietoisuuden lisäämiseksi. Taltechin kyberturvallisuusalan tohtorikoulutettavat vierailevat kouluissa kertomassa internetin turvallisuuteen liittyvistä asioista.[906] Kouluopetusta täydentää myös koulun ulkopuolinen ohjelma Smartly on the web (Safer Internet center in Estonia) ja siihen liittyvät hankkeet.[907] Valtion tietojärjestelmäviranomainen (Riigi Infosüsteemi Amet, RIA) toimii Viron kyberturvaturvatietoisuuden lisäämisen koordinaattorina. Se kerää tietoja kansalaisten kyberturvatietoisuuden tasosta ja järjestää toimintaa niiden perusteella.[908] RIA ylläpitää portaalia ”Ole IT-vaatlik”[909], jonka tavoitteena on opettaa käyttämään internetiä ja älylaitteita turvallisemmin. Portaalissa on oma osionsa työkäyttäjälle, tavalliselle käyttäjälle ja vanhemmille sekä mahdollisuus testata, onko oma toiminta kybermaailmassa turvallista. RIA toteuttaa säännöllisesti valistuskampanjoita Viron kyberturvallisuuden tason parantamiseksi.[910] Suuri osa kansalaisten koulutuksesta liittyy digitaaliseen henkilökorttiin. (Virossa jokaiselta kansalaiselta vaaditaan digitaalinen henkilökortti, jota käytetään esimerkiksi pankkiasioinnissa ja äänestämisessä.)[911] Esimerkiksi vuoden 2021 vaalien yhteydessä RIA järjesti kampanjan verkossa äänestämisen turvallisuudesta ja jakoi Facebookissa ja Twitterissä aiheesta videoita ja infograafeja.[912] Vuoden 2019 kampanja kohdistui yli 55-vuotiaisiin sekä heidän lähipiiriinsä. Kampanjassa korostettiin kyberhygienian merkitystä.[913] RIAn alaisuudessa toimii CERT-EE, jonka tavoitteena on ehkäistä kyberturvallisuuteen liittyviä vaaratilanteita ja vähentää turvallisuusriskejä. CERT järjestää säännöllisesti erilaisia tapahtumia ja tiedotuskampanjoita ja antaa myös varoituksia ja ilmoituksia käyttäjille tietoturva-aukoista, joita on havaittu Viron järjestelmissä ja sovelluksissa.[914]

Erilaiset koulutuskeskukset, kansanopistot ja kulttuurikeskukset tarjoavat epävirallisia, maksullisia koulutuskursseja, joihin sisältyy myös aiheita kyberturvallisuudesta.[915] Kansalaiset voivat kursseilla perehtyä esimerkiksi internetin ja sen palveluiden turvalliseen käyttöön, salasanahallintaan ja autentikointiin.[916] Maksutonta työvoimakoulutusta työttömille tarjoaa Viron työttömyyskassa (Eesti Töötukassa). Koulutustarjonnassa on mukana myös IT-kursseja ja kyberturvallisuuteen liittyviä toteutuksia.[917]

Viron poliisilla on verkkoympäristössä niin sanottuja Web-konstaapeleita eli poliiseja, jotka vastaavat kansalaisten internetin välityksellä lähettämiin kyberturva-aiheisiin kysymyksiin. Myös kolmannen sektorin kansalaisjärjestöt, kuten esimerkiksi Viron lastensuojeluliitto (Eesti Lastekaitse Liit), osallistuvat jossain määrin kouluttamiseen.[918] Lisäksi Virossa on aktiivisia vapaaehtoisia, jotka opettavat vanhuksille, kuinka esimerkiksi digitaalista henkilökorttia, Facebookia ja sähköpostia käytetään.[919]

Mahdollisuuksia osallistua itseopiskelukursseille on useita. Esimerkiksi Naton Cyber Defence Awareness e-Learning -kurssin tarkoitus on lisätä käyttäjän tietoisuutta kyberturvallisuusriskeistä ja toimenpiteistä näiden riskien lieventämiseksi.[920] Cybexer technologies -yritys on suunnitellut itseopiskelumateriaalin ”My Cyber Hygiene”, joka on käännetty 12 eri kielelle.[921] Edellä mainittujen lisäksi Tarton yliopisto tarjoaa kaikille avoimia itseopiskelukursseja myös kyberturva-aiheista. On huomattava, että kyberturvallisuus sisältyy usein digitaitojen opetukseen. Esimerkiksi kirjastojen digikursseilla on annettu neuvoja myös esimerkiksi salasanahallintaan.[922]

Viestintäyhtiöt koordinoivat jossain määrin kyberturvallisuuteen liittyviä kampanjoita. Esimerkiksi Telia on toteuttanut lapsille kampanjan nettikiusaamisen ehkäisemiseksi.[923] Vuosittain toteutuvia kampanjoinnin muotoja ovat EU:n Safer Internet Day ja ECSM (European Cybersecurity Month). Safer Internet Dayn ohjelmaan on kuulunut muun muassa webinaareja kasvatusalan ammattilaisille ja opetusmateriaalin kokoamista lastentarhanopettajille.[924]

Itseopiskelumateriaaleja, kilpailuja ja kyselyitä eri kohderyhmille (lapset ja nuoret, vanhemmat ja opettajat) on saatavilla Safer Internet Centerin portaalissa.[925] Lapsille on esimerkiksi videoita ja vinkkejä internetin käyttöön ja Spoofy-peli. Nuorille on tietoa älylaitteiden ja sosiaalisen median turvallisuudesta sekä nettikiusaamisesta. Opettajat voivat työssään hyödyntää portaalin opetusmateriaaleja ja tuntisuunnitelmia. Nuorisolle suunnatussa

interaktiivisessa ”Nastix ja turvalline Internet” -pelissä [926] on tehtäviä, jotka liittyvät esimerkiksi yksityisyydensuojaan, virusten tunnistamiseen ja mobiililaitteiden turvallisuuteen. Portaaliin on koottu myös haastavampia, esimerkiksi salaukseen ja loogiseen päättelyyn liittyviä tehtäviä edistyneemmille käyttäjille.[927,928]

3.27.3. Kansalliset erityispiirteet

Kyberturvallisuuden toimintakulttuuria Virossa kuvaa sana avoimuus. Ihmiset ovat esimerkiksi omaksuneet melko nopeasti digitaaliseen henkilökorttiin liittyvän Smart-ID-teknologian. He myös luottavat hallitukseen, joka hallitsee tätä tekniikkaa. [929] Kansalaisten kyberhygienian tason mittaamiseksi Viron Tilastokeskus (Eesti statistika) toteuttaa vuosittain kyselyn ”Information technology in the household” vakituisesti Virossa asuville 16–74-vuotiaillle asukkaille ja heidän kotitaloutensa jäsenille. Viime vuosina väestön kyberhygienian taso on parantunut, mutta parantamisen varaa on kuitenkin vielä. Ihmisiä esimerkiksi joutuu tietojenkalastelun uhreiksi tai he menettävät digitaalisten palveluidensa hallinnan klikkaamalla vääriä linkkejä [930] . Ikäihmisten kyberhygienian taso on selvästi alhaisempi kuin nuoremmilla. [931] Toisaalta taas nuorisolle tehdyssä tutkimuksessa havaittiin, että toimiminen haastavimmissa kyberturvaan liittyvissä asioissa tuottaa heillekin ongelmia. Myös asenteessa turvallisuusasioita kohtaan on nuorilla parantamisen varaa. [932] Haasteeksi kouluopetuksessa on muodostunut pula motivoituneista ja pätevistä opettajista, jotka pystyvät integroimaan kyberturvallisuusasioita opetussuunnitelman eri aiheisiin.[933] Puutteeksi koetaan myös se, että kyberturvallisuus ei ole opetussuunnitelmassa pakollisena opiskeltavana asiana ja että kouluissa kyberturvallisuus on usein vain yhden henkilön vastuulla.[934]

Kyberturvallisuuden alkeiden opetuksessa ollaan Virossa siirtymässä yhä nuorempiin ikäluokkiin, ja opetuksen aloittamista suositellaan jo lastentarhassa. [935 , 936] Nuoria pyritään innostamaan kyberturva-alalle erilaisten kilpailujen avulla (esimerkiksi CyberPin, CyberDrill, CyberCracker ja CyberSpike). Kansainvälisestikin suosittuja Cyber security battle -tapahtumia koordinoi CTF Tech -yritys. Tämä kyberturvallisuuden koulutus- ja kilpailutapahtuma on kohdennettu nuorille, mutta yrityksellä on myös verkkokoulutusalusta, joka on avoin ja ilmainen kaikille kiinnostuneille. Opettajat voivat käyttää verkkomateriaalia ja pelejä kouluopetuksessa. [937] Tutkimus kyberturvallisuuskoulutuksen ympärillä on Virossa aktiivista. Vahvoja toimijoita ovat esimerkiksi Tarton yliopisto ja Taltech, jossa on käynnissä mielenkiintoinen pelillistämishanke ”Cyber security awareness and prevention game for schools”.[938,939]

3.27.4. Kyberkansalaistaitojen määrittäminen

DigCompin Digital Competence Model on viitekehys, joka Virossa määrittelee kansalaisten kyberturvallisuustaitoja ja jota on sovellettava kaikkien koulujen opetuksessa. [940] Tämän tutkimuksen haastatteluissa tuli esille, että kohdennettaessa opetusta tavallisiin kansalaisiin on tärkeää opettaa ymmärtämään salasanojen hallintaan ja yksityisyydensuojaan liittyviä asioita. Myös autentikointi on tärkeää, samoin kuin harkinnan käyttö, mitä linkkejä kannattaa klikata. [941] Kansalaisille on tärkeää korostaa, että kyberturvallisuus ei itsessään ole tavoite, vaan mahdollistaja. Eli kun haluaa tehdä jotain, turvallisesti toimiminen mahdollistaa tämän. Myös varovaisuuden korostaminen henkilötietojen luovuttamisessa koetaan tärkeäksi.[942]

Viitteet

[892] Republic of Estonia, *Cybersecurity strategy 2019-2022* (Ministry of Economic Affairs and Communications, 2019), 15, 64, 66-67.
[893] ”The Education and Youth Board Harno,” *European Union digital skills & Jobs Platform*, luettu 3.11.2022, https://digital-skills-jobs.europa.eu/en/organisations/education-and-youth-board-estonia-harno.
[894] Henkilökohtainen tiedonanto tutkijalle 25.6.2022.
[895] Henkilökohtainen tiedonanto tutkijalle 5.12.2022.
[896] Henkilökohtainen tiedonanto tutkijalle 25.6.2022.
[897] Henkilökohtainen tiedonanto tutkijalle 20.6.2022.
[898] Henkilökohtainen tiedonanto tutkijalle 8.6.2022.
[899] Haridus- ja noorteamet, *Lisa 10: Valikõppeaine Informaatika, Tööversioon 19.05.2022* (2022), 3-4, 6-7, 9-10, https://oppekava.ee/wp-content/uploads/2022/06/Lisa-13-PROK-Lisa-10-Valikoppeaine-Informaatika.pdf
[900] ”Küberkaitse,” *Ministry of education and research of Estonia*, luettu 3.11.2022, https://web.htk.tlu.ee/digitaru/kyberkaitse/front-matter/introduction/.
[901] Henkilökohtainen tiedonanto tutkijalle 20.6.2022.
[902] Haridus- ja noorteamet, *Lisa 9: Valikõppeaine Informaatika, Tööversioon 19.05.2022* (2022), 7, https://oppekava.ee/wp-content/uploads/2022/05/Lisa-26-GROK-Lisa-9-Valikoppeaine-Informaatika.pdf.
[903] Lorenz Birgy, “Cybersecurity education and competitions in Estonia,” *Tallinn University of Technology,* luettu 3.11.2022, https://docs.google.com/presentation/d/15d-OGUUNe5IbuBkT_agiVBkT0fHI-F4wa-LE_xAWLeU/present#slide=id.p1.
[904] ”MSc in cybersecurity,” *Tallinn University of technology*, luettu 4.1.2023, https://taltech.ee/en/cyber-msc.
[905] ”Cyberus Erasmus Mundus Master in Cybersecurity,” *ENISA*, luettu 4.1.2023, https://www.enisa.europa.eu/topics/education/cyberhead/#/programme/858795598eed4fe5981803cbfae817bf?programme=Cyberus%20Erasmus%20Mundus%20Master%20in%20Cybersecurity.
[906] ENISA, *Raising Awareness of Cybersecurity A Key Element of National Cybersecurity Strategies* (ENISA, 2021), 14.
[907] Henkilökohtainen tiedonanto tutkijalle 8.6.2022.
[908] ENISA, *Raising Awareness of Cybersecurity,* 14-15.
[909] ”Ole IT-vaatlik,” *Riigi Infosüsteemi Amet,* luettu 3.11.2022*,* https://www.itvaatlik.ee/.
[910] Republic of Estonia Information system authority, *Cyber security in Estonia 2021* (Tallinn: Information system Authority, 2022), 5.
[911] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.
[912] ENISA, *European Cybersecurity Month (ECSM) – Deployment report 2021* (ENISA, 2022), 103.
[913] Republic of Estonia, *Cyber security in Estonia 2021*, 32-33.
[914] ”CERT-EE,*” Information system Authority*, luettu 3.11.2022, https://www.ria.ee/en/cyber-security/cert-ee.html.
[915] ”Koolitused,” *IT Koolitus*, luettu 4.11.2022, https://koolitus.ee/koolitused.
[916] ”Infoturve,” *IT Koolitus*, luettu 4.11.2022, https://koolitus.ee/teemad/infoturve.
[917] ”Training search,” *Eesti töötukassa*, luettu 3.11.2022, https://www.tootukassa.ee/et/koolitused?keyword=cyber&pageSize=20.
[918] ENISA, *Raising Awareness of Cybersecurity*, 14.
[919] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.
[920] ”Cyber defence awareness,” *The NATO Cooperative Cyber Defence Centre of Excellence*, luettu 5.10.2022, https://ccdcoe.org/training/cyber-defence-awareness-e-course/.
[921] ”Estonian Cyber Security Company Provides Free Cyber Hygiene e-Learning in 12 Languages,” *CYBEXER TECHNOLOGIES*, luettu 4.11.2022, https://cybexer.com/news/estonian-cyber-security-company-provides-free-cyber-hygiene-e-learning-in-12-languages/.
[922] Henkilökohtainen tiedonanto tutkijalle 20.6.2022.
[923] ENISA, *Raising Awareness of Cybersecurity*, 41.
[924] ”Estonian Safer Internet Centre - Smartly on the Web,” *European schoolnet*, luettu 4.11.2022, https://www.saferinternetday.org/in-your-country/estonia.
[925] ”Tärgalt Internetis,” *Estonian Union for Child Welfare*, luettu 3.11.2022, https://www.targaltinternetis.ee/en/.
[926] ”Nastix ja turvalline Internet,” *The Tiger Leap Foundation*, luettu 3.11.2022, https://www.targaltinternetis.ee/nastix/.
[927] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.
[928] ”Küberturbe Ülesanded,” *Estonian Union for Child Welfare,* luettu 3.11.2022*,* https://ylesanded.targaltinternetis.ee/index.html.
[929] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.
[930] Henkilökohtainen tiedonanto tutkijalle 20.6.2022.
[931] Republic of Estonia Information system authority, *Cyber security in Estonia 2022* (Tallinn: Information system Authority, 2022), 42.
[932] Lorenz Birgy, Kaido Kikkas ja Kairi Osula, “Development of children’s cyber security competencies in Estonia”, *International Conference on Learning and Collaboration Technologies* (Springer: Cham, 2018), 7-8.
[933] Republic of Estonia, *Cybersecurity strategy 2019-2022, 68.*
[934] Birgy Lorenz, Kaido Kikkas and Kairi Osula. *Development of children’s cyber security competencies in Estonia.* International Conference on Learning and Collaboration Technologies. Springer, Cham, 2018, 2, 8.
[935] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.
[936] ”Cyber security education in Estonia: from kindergarten to NATO Cyber Defence Centre,” *Republic of Estonia Ministry of education and research*, luettu 4.11.2022, https://e-estonia.com/cybersecurity-education-in-estonia-from-kindergarten-to-nato-cyber-defence-centre/ .
[937] ”Cyber battle of Estonia,” *CTF Tech*, luettu 4.11.2022, https://www.ctftech.com/events/cyber-battle-of-estonia-2022/.
[938] Henkilökohtainen tiedonanto tutkijalle 20.6.2022.
[939] Henkilökohtainen tiedonanto tutkijalle 10.6.2022.
[940] Henkilökohtainen tiedonanto tutkijalle 5.12.2202.
[941] Henkilökohtainen tiedonanto tutkijalle 20.6.2022.
[942] Henkilökohtainen tiedonanto tutkijalle 21.6.2022.

4. Kyberturvallisuuden kansalaistaitojen opettaminen Euroopan unionin alueella pelillistämisen avulla

4.1. Johdanto tutkimukseen ja aiheeseen

Euroopan unionin alueella on tuotettu useita eri tapoja kansalaisten kyberosaamisen kehittämiseksi. Kyberkansalaistaitojen opettaminen on keskeisessä osassa nyky-yhteiskunnassa, ja useat EU-maat ovat pyrkineet tuomaan vastaavia tuotteita ja palveluita kansalaistensa käyttöön. Tiedonsiirron ja opetuksen onnistumista kyberosaamisen kansallisen tason parantamisessa on kuitenkin suhteellisen vaikea arvioida tarkasti.

Raportin tässä osassa tarkastellaan kyberturvallisuuden kansalaistaitoja opettavia oppimispelejä. Tarkastelussa keskitytään erityisesti kyseisten oppimispelien opetukselliseen puoleen, pelillisyyteen, sekä nimenomaan kyberturvallisuuden käsittelyyn opetuksessa. Tutkimuksessa on käsitelty ainoastaan yksittäisten ja kansainvälisesti tunnettujen toimijoiden tuottamia pelejä sekä oppimisympäristöjä. Raportissa on kuitenkin huomioitu pienempienkin toimijoiden tuotteita osana kokonaisuutta. Kuitenkin pääpaino on keskitetty kymmeneen laajimman ja kokonaisvaltaisimman oppimispelin pohjalta saatuun dataan.

Tutkimuksessa keskityttiin ainoastaan EU-maihin kohdennettuihin oppimispeleihin. Pelien joukon supistamiseksi kontekstiin soveltuvaksi tutkimuksessa rajattiin pois oppimispelejä, jotka eivät täyttäneet seuraavia kriteereitä. Tutkimuksessa tarkasteltujen oppimispelien täytyy olla jonkin EU-maahan kuuluvan tunnustetun toimijan tuottama. Myös itse pelin tulee olla jonkin EU-alueelle kuuluvan tahon tunnustama. Oppimispeli tulee myös kokea ajankohtaiseksi, eli sen käsittelemä sisältö tulee olla yhä relevanttia kyseisessä kontekstissa. Pelien, joita tutkimuksessa tarkasteltiin, tulee olla tulkittavia nimenomaan oppimispeleiksi. Tämä tarkoittaa selkeää opetuksellista päämäärää sekä sopivaa sisältöä tämän saavuttamiseksi. Raportissa tarkasteltujen oppimispelien tulee myös olla suunniteltuja laajamittaisesti EU-maiden kansalaisille soveltuviksi. Oppimispelien asiasisällön tulee olla neutraalia ilman esimerkiksi poliittista agendaa.

4.2. Kriteereitä tutkimusaineiston vertailuun

Tutkimuksessa keskitytään tarkastelemaan ja vertailemaan oppimispelejä pääasiassa kolmella osa-alueella. Näiden lisäksi on myös huomioitu pelien soveltuminen kohderyhmä huomioiden, joko kansallisella tai kansainvälisellä tasolla. Jokaiseen tarkasteltavaan osa-alueeseen ja niiden mahdollistamaan pelien analysointiin tarvitaan tarkat ja selkeät parametrit, joiden avulla vertailua ja tutkimusta voidaan tehdä. Oppimispelien tarkastelussa käytetyt kriteerit on valittu aiempien tutkimusten pohjalta, joissa on keskitytty nimenomaan tutkimuspelien arviointiin ja analysointiin. [LIITE 1] Vaikka tässä tutkimuksessa oppimispelejä vertailtavat kolme osa-aluetta on mainittu erillään, niillä on kuitenkin pelien toteutuksen ja sen onnistumisen kannalta selkeä korrelaatio.[943,944,945]

Taulukko 3: Lista oppimispeleistä, joita tutkimuksessa keskityttiin tarkastelemaan.

Pelin nimi	Kehittäjä	Kehittäjä (valtio)	Kohderyhmä
Cyber Chronix	EU:n komissio	EU	Lapset
Cyber Crime Time	IMC	Saksa	Nuoret, aikuiset
CyberKid	CANDI	Kreikka	Lapset, nuoret
Digiturvallinen elämä	DVV	Suomi	Aikuiset (/työntekijät)
eFollowMe	Cyprus Pedagogical Institute of Ministry of Educational, Culture, Sports and Youth	Kypros	Nuoret
EveryDay	Göteborg Sivukonttori, Ikämiessuojeluskunnan Säätiö	Suomi	Nuoret, aikuiset
Hackend	INCIBE	Espanja	Yritykset(/työntekijät)
Hackers vs. Cybercrook	INCIBE	Espanja	Lapset, nuoret
Happy Onlife	Euroopan komission tutkimuskeskus, JRC	EU	Lapset
Juego Cyberscouts	INCIBE	Espanja	Lapset, aikuiset
Kyberturvallisuus-pakopeli	Helsingin yliopisto, Teknologiateollisuus ry	Suomi	Nuoret
Nastix	Url OÜ, BadBlock	Viro	Lapset
SecNum Académie	ANSSI	Ranska	Nuoret, aikuiset
Spoofy: Kyberpeli	IT-palveluyhtiö CGI yhteistyössä Liikenne- ja viestintävirasto Traficomin sekä Valtion kehitysyhtiö Vaken kanssa	Suomi	Lapset
Tacos	CASES.LU	Luxemburg	Nuoret, aikuiset

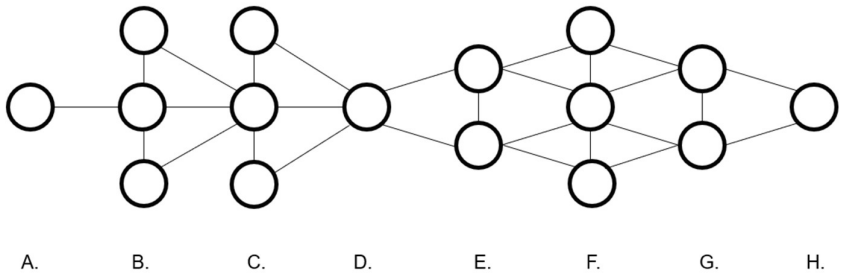
4.2.1. Pelillisyys

Pelillisyydessä keskityttiin erityisesti oppimispelin kehittämisessä tehtyihin ratkaisuihin, jotka valittiin yleisesti pelinkehityksessä tunnettujen parametrien pohjalta. Näitä ovat muun muassa pelattavuus, tarinallisuus, käyttäjäkokemukset ja -tarinat, pelin kehityskulku ja haastavuus sekä sen muotoilu. Pelillisyyteen kuuluu myös vahvasti pelin ulkoasu eli kaikki, mikä on käyttäjälle näkyvää aina pelin muotoilusta käytettävyyteen. Oppimispelin erityispiirteinä ovat erityisesti tarinallisuus, pelin kulku ja rakenne sekä pelin haastavuus ja kehitys.

Pelien varsinaisiin back-end-ratkaisuihin ja valintoihin ei tässä tutkimuksessa keskitytä, sillä niiden suora vaikutus kyseisessä kontekstissa on vähäinen. Kaikki pelit toimivat joko selainpohjaisesti tai olivat saatavilla sovelluksina älypuhelimille. Pelin alustalla ei ollut vaikutusta tutkimukseen.[946,947,948]

4.2.2. Pelilogiikka

Opetuspelien logiikka-analyyseissä pelit edustivat etupäässä yhden polun ja vaihtoehtoisten ratkaisujen logiikkaa. Pelien toteutuksissa oli jonkin verran variaatiota eri valinnoissa, mutta pelit kyettiin tyypillisesti pelaamaan läpi rutiininomaisesti eri vaikeus- ja variaatiotasojen puitteissa.



Kuva 3: Tyypillinen oppimispelin etenemislogiikka.

4.2.3. Opetuksellisuus

Oppimispelejä arvioitaessa itse opetuksellisuus ja pelin pedagoginen puoli korostuvat. Opetuksellisuuden analysoinnissa käytetyt parametrit on valittu muista oppimispeleistä tuotetuista tutkimuksista. Parametrit perustuvat yleisesti tunnettuihin pedagogisiin tuloksiin. Oppimispelien onnistumiseen vaikuttavia tekijöitä on lukuisia, mutta tässä tutkimuksessa on huomioitu ainoastaan kontekstissa oleellisimmiksi koetut parametrit. Tutkimuksen toteutuksen kannalta keskeisiä parametreja oppimispelin onnistumista mitattaessa on käyttäjän motivaatio, emootiot, tavoitteet, interaktiivisuus, menetelmät sekä palaute. Pelin rakenne, kehityskulku ja sen mukautuminen käyttäjän valintojen sekä oppimisen pohjalta ovat myös suuressa roolissa oppimisen tehostamisen kannalta.[949,950,951,952]

4.2.4. Kyberturvallisuus ja sen käsittely opetuksessa

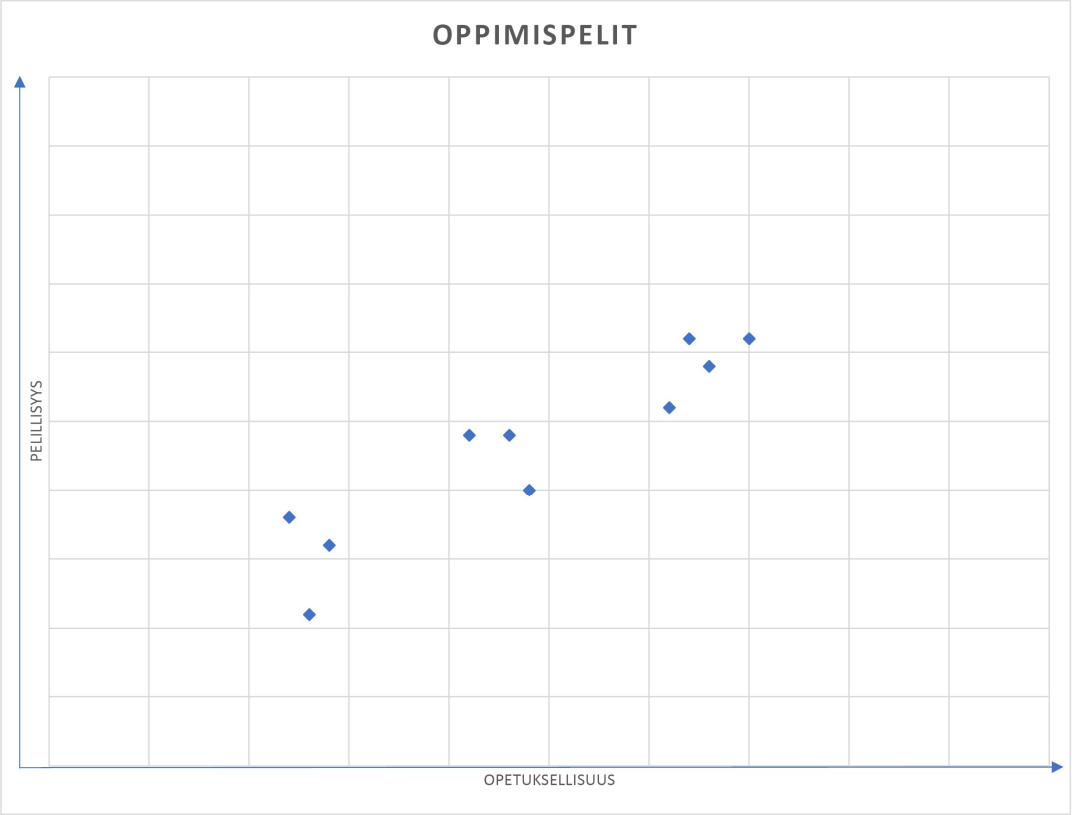
Kansallisen tai kansainvälisen kyberturvallisuutta opettavan pelin aihealueen laajuus, tarkkuus sekä kohderyhmä ovat tärkeitä tekijöitä hyvän ja toimivan oppimispelin tuottamiseksi. Pelissä on tärkeää, että yleinen käsitys kyberturvallisuudesta ja siihen vaikuttavista tekijöistä tulee käyttäjän lähtötasosta huolimatta selväksi. Monipuolisesti tulisi käsitellä myös turvallista verkossa toimimista, sähköpostin ja kalastelun uhkia sekä haittaohjelmia. Salasanojen ja niiden turvallisuuden tulisi myös sisältyä turvalliseen digiympäristössä toimimiseen. Disinformaatio ja informaatiovaikuttaminen on myös tärkeä osa kyberturvallisuuden ymmärtämistä.[953]

4.2.5. Pelit EU-kontekstissa

EU-kansalaisille kohdennettujen oppimispelien yksi tärkeä kriteeri on myös pelin sopivuus kohderyhmälle. Laajan kohderyhmän opettaminen tehokkaasti ja onnistuneesti on vaikeaa, sillä esimerkiksi lähtötaso tai käyttäjän tausta saattaa vaihdella suuresti. Oppimispelin tulee siis olla haluttuun kontekstiin suhteutettu.

4.3. Tutkimustulokset

Oppimispelien laadullisuus on tärkeää, jotta käyttäjä kykenee sisäistämään opetettavan asian vähintään yhtä hyvin kuin perinteisemmillä opetusmetodeilla. Tutkimuksessa tarkoituksena oli tutustua ja tarkastella EU-alueella tuotettuja ja alueen kansalaisille kohdennettuja kyberturvallisuutta opettavia oppimispelejä. Tutkimuksessa keskityttiin tutkimaan ainoastaan tunnustettujen toimijoiden tuottamia oppimispelejä, joista painopiste valittiin kattavimpiin ja kokonaisvaltaisimpiin tuotteisiin. Vertailukohtien pohjalta pelejä tutkittiin aiempien aiheen tutkimuksien tuloksissa hyväksi todettuja kriteereitä käyttäen. Lähtökohtaisesti oppimispelien laadulliset erot näkyvät tutkimustuloksissa, mikä vaikeuttaa yksittäisten tekijöiden vaikutusten erottelua.



Kuva 4: Kaavio kuvaa tarkastelujoukon oppimispelien pelillisyyden korrelaatiota opetuksellisen sisällön laajuuteen. Tarkempi pisteytys löytyy liitteestä 2. Kaikkia pelejä ei voitu pisteyttää, koska pelaaminen ei onnistunut maantieteellisten (pelin lataus ei onnistunut Suomesta käsin) tai kielellisten rajoitusten vuoksi (pelejä pystyttiin pelaamaan suomeksi, englanniksi ja ranskaksi).

Tutkimustuloksissa huomattiin suurta jakaumaa oppimispelien pelillisessä laadussa. Tasoltaan laadukkaimmissa tuotoksissa oli tavallisessa peliteollisuudessakin tunnettuja elementtejä, joihin oli integroitu opetettavat asiat mukaan. Tämä tuli usein parhaiten ilmi muun muassa tarinankerronnassa ja käyttäjäpolkuja tarkasteltaessa. Yksi hyvä nosto onnistuneesta ja käyttäjälle mielekkäästä oppimispelistä on IMC:n tuottama Cyber Crime Time. Peli sopii visuaalisesti sekä tarinallisesti hyvin kohderyhmälleen ja tuo selkeästi esiin opetettavan aiheen perusasiat.

Kuitenkin osassa pelejä itse oppiminen jäi kokonaan taka-alalle pelillisten ratkaisuiden takia. Pelin tuottajan kannalta sopivaa tasapainoa pelillisyyden ja opetuksellisen laadun välillä on tutkimustulosten pohjalta vaikea löytää. Suurimmassa osassa tarkastelujoukon peleistä voidaan todeta kehitysprosessissa selvää painotusta joko opetuksellisuuteen tai pelillisyyteen, mutta harvoin onnistuneesti molempiin.

Pedagogisesti tarkastelujoukon peleissä on myös suurta vaihtelua. Osassa voidaan heti alusta asti huomata käyttäjätarinoiden sekä -polkujen muotoutumisen kautta, kuinka pelin tarinallisuus kulkee nimenomaan opetuksellisuuden ehdoilla. Pelillisyyttä huomioimatta hyvä nosto on Ranskan kansallisen kyberturvallisuuskeskuksen, ANSSIn tuottama SecNum Académie, joka on MOOC-pohjainen oppimisalusta. Oppiminen on alustalla tehokasta ja materiaalit ovat helposti käyttäjän saatavilla, mutta pelillistä puolta oppimisalustasta ei tarkoituksellisestikaan löydy.

Kuitenkin huomattavan monissa niistä peleistä, joissa on panostettu pelilliseen puoleen, itse opetuksellisuus on huomattavasti pelillistä tasoa heikompaa. Pelien laadulliset tasoerot jakautuvat keskenään omiin pienempiin osajoukkoihin, joiden sisällä tämä ilmiö on selkeämmin huomattavissa. Kokonaisvaltaisesti voidaan todeta tarkastelujoukossa pelillisyyden sekä opetuksellisuuden korreloivan positiivisesti keskenään. Tämän voi selittää pelien yleisillä laadullisilla eroilla, huonoilla peleillä on huono opettaa ja päinvastoin.

Suurimmassa osassa oppimispelejä käydään kyberturvallisuus aihealueena kattavasti ja monipuolisesti läpi. Aihealue tulee tutuksi lähtötasosta huolimatta, mutta tiettyä pistettä pidemmälle ei mennä edes aikuisille tai organisaatioille suunnatuissa oppimispeleissä. Toisin sanoen laajamittainen, mutta matalan alkutason osaaminen tulee tarkastelujoukon peleissä suurimmaksi osaksi täytettyä. Kuitenkaan perustasoa korkeamman osaamisen oppimispelejä ei tarkastelujoukossa ollut lainkaan.

Oppimispelien kohderyhmä on myös tärkeä kriteeri oppimispelin onnistumista ja laatua arvioitaessa. Tarkasteltujen pelien pohjalta voidaan todeta, että todella suurelle kohdeyleisölle tarkoitetut pelit ovat harvemmin onnistuneita kuin tarkasti rajatulle kohderyhmälle kohdennetut. Hyvä esimerkki onnistuneesta kohderyhmälle tuotetusta oppimispelistä on CGI:n tuottama Spoofy. Pelin kehitysvaiheessa on alusta asti otettu huomioon nimenomaan kohderyhmänsä (alakouluikäiset lapset) kiinnostuksen kohteet visuaalisella sekä käyttäjätarinoiden puolella. Yksittäisille kohderyhmille, kuten lapsille, nuorille tai organisaatioiden työntekijöille, on helpompi kohdistaa onnistuneesti kohderyhmälle sopivan tasoista opetusta.

4.4. Pohdinta

Kyberturvallisuuden ajankohtaisuuden takia olisi erittäin kriittistä, että kansallisen tason osaaminen olisi vaaditulla tasolla. Tähän kouluttaminen ja opettaminen tulisi aloittaa lapsista ja nuorista alkaen. Kouluttamista tulisi jatkaa ja osaamista ylläpitää jatkuvasti, sillä kyberturvallisuus on keskeisessä osassa organisaatioidenkin uhkakuvia. Suurimmassa osassa tässä tutkimusraportissa analysoiduista oppimispeleistä on vielä paljon puutteita. Kuitenkin on positiivista huomata EU-alueen tahtotila panostaa digitaalisten oppimismetodien kehittämiseen kansallisesti sekä kansainvälisesti. Tällä hetkellä oppimispelien kyberturvallisuustaitojen opettamiseen kansallisella tasolla on kuitenkin panostettu harmillisen vähän. Nyky-yhteiskunnassa luulisi olevan jo näinkin kriittisen taidon oppimiselle valmis oppimisalusta, joka esimerkiksi tarkkailisi kansallista kehitystä ja osaamista kehittäjilleen. Opetusmetodiksi pandemiankin aikana vakiintuneen online-työskentelyn luulisi nopeuttavan kehitystä muillekin virtuaalisille oppimisalustoille, kuten oppimispeleille. Kyberturvallisuuden kansalaistaitojen kehittäminen ja opettaminen tulisi olla huomattavasti nykytasoa suuremmassa roolissa Euroopan unionin alueella.

Viitteet

[943] Esther Oprins, Gillian van de Boer-Visschedijk, Maartje Roozeboom, Mary Dankbaar, Wim Trooster ja Stephanie Schuit, "The game-based learning evaluation model (GEM): Measuring the effectiveness of serious games using a standardised method," *International Journal of Technology Enhanced Learning* 7 (2015), doi: 10.1504/IJTEL.2015.074189
[944] Marcelo Barbosa, Andreza Rêgo ja Igor De Medeiros, "HEEG: Heuristic Evaluation for Educational Games," *Proceedings of SBGames 2015* (Federal Institute of Education, Science and Technology of Rio Grande do Norte, Brazil, 2015).
[945] Segomotso Mosiane ja Irwin Brown "Factors Influencing Online Game-Based Learning Effectiveness," *The Electronic Journal of Information Systems Evaluation* Volume 23 Issue 1 (2020).
[946] Katharina Emmerich ja Mareike Bockholt, "Serious Games Evaluation: Processes, Models, and Concepts," *Entertainment Computing and Serious Games* (2015).
[947] Alejandro Calderón ja Mercedes Ruiz, "A systematic literature review on serious games evaluation: An application to software project management," *Computers & Education*, Volume 87 (2015).
[948] Narda Alvarado ja Konstantin Mitgutsch, "Purposeful by Design? A Serious Game Design Assessment Framework," *Foundations of Digital Games 2012, FDG 2012 - Conference Program* (2012).
[949] Hanif al Fatta, Zulisman Maksom ja Mohd Zakaria, "Systematic literature review on usability evaluation model of educational games : playability, pedagogy, and mobility aspects," *Journal of Theoretical and Applied Information Technology*, 96 (2018): 4677-4689.
[950] Alice Mitchell ja Carol Savill-Smith, *The use of computer and video games for learning* (Lontoo: LSDA, 2004).
[951] Patricia Armstrong, *Bloom's Taxonomy* (Nashville: Vanderbildt University Center for Teaching, 2010).
[952] Akseli Huhtanen, *Verkko-oppimisen Muotoilukirja Käytännön työkaluja laadukkaan verkko-oppimisen muotoiluun* (Aalto-yliopisto, 2019).
[953] Reneé Röpke ja Ulrik Schroeder, *The Problem with Teaching Defence against the Dark Arts: A Review of Game- based Learning Applications and Serious Games for Cyber Security Education* (2019).

Liitteet

Liite 1: Kriteerilista.

Julkaisun nimi	Julkaisijat	Julkaisuvuosi	Lähteestä valitut parametrit
Factors Influencing Online Game-Based Learning Effectiveness	**Segomotso Mosiane, Irwin Brown**	2020	Oppimispelien tehokkuus, palaute, keskittyminen/immersio, flow
The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education	**René Röpke, Ulrik Schroeder**	2019	Kyberturvallisuuden opettaminen, pelien pohjalta oppiminen, riskitietoisuus
A systematic literature review on serious games evaluation: An application to software project management	**Alejandro Calderon, Mercedes Ruiz**	2015	Oppimispelien arviointi, ohjelmistokehityksen arviointi
The game-based learning evaluation model (GEM): Measuring the effectiveness of serious games using a standardised method	**Oprins, E., Visschedijk, G., Roozeboom, M.B., Dankbaar, M., Trooster, W., Schuit, S.C.E**	2015	GEM, evaluaatioparametrit
The use of computer and video games for learning	**Alice Mitchell, Carol Savill-Smith**	2004	Tavoitteet, interaktiot, palaute, adaptoituvuus, tarinankerronta, käyttäjäkokemus, sosiaalinen oppiminen

A Motivational Model of Video Game Engagement	**Andrew K. Przybylski, C. Scott Rigby, Richard M. Ryan**	2010	
Assessing the Core Elements of the Gaming Experience	**Eduardo H. Calvillo-Gámez, Paul Cairns, and Anna L. Cox**	2010	
Serious Games Evaluation: Processes, Models, and Concepts	**Katharina Emmerich, Mareike Bockholt**	2016	Oppimispelien vaikutuksellisuus ja sopivuus, oppiminen, käyttäytyminen, oppimistulokset
Validation of a mobile game-based assessment of cognitive control among children and adolescents	**Hyunjoo Songl, Do-Joon Yi, Hae-Jeong Park**	2020	
Systematic literature review on usability evaluation model of educational games : playability, pedagogy, and mobility aspects	**Hanif Al Fatta, Zulisman Maksom, Mohd Hafiz Zakaria**	2005	Käytettävyys, Arvostelu/palaute, pelattavuus, M-GBL, pelin pedagogiikka, heuristinen arviointi
A systematic literature review of empirical evidence on computer games and serious games	**Thomas M. Connolly Elizabeth A. Boyle, Ewan MacArthur, Thomas Hainey, James M. Boyle**	2012	
Verkko-oppimisen Muotoilukirja Käytännön työkaluja laadukkaan verkko-oppimisen muotoiluun	**Akseli Huhtanen**	2019	Muisti, motivaatio, tarkkaavaisuus, emootiot, muotoiluprosessi, ydinainesanalyysi
Bloom's Taxonomy (Vanderbilt University Center for Teaching)	**Armstrong, P.**	2010	Bloomin taksonomia
Introducing the game design matrix: a step-by-step process for creating serious games	**Aaron J. Pendleton**	2020	MDA, DDE, LM-GM
Using User Created Game Reviews for Sentiment Analysis: A Method for Researching User Attitudes	**Björn Strååt, Harko Verhagen**	2017	
State of the art in Game Based Learning: Dimensions for Evaluating Educational Games	**Rabail Tahir, Alf Inge Wang**	2017	

HEEG: Heuristic Evaluation for Educational Games	**Marcelo B., Barbosa Andreza B., Rêgo Igor de Medeiros**	2015	Heuristinen tutkimusmalli oppimispeleihin
Purposeful by Design? A Serious Game Design Assessment Framework	**Narda Alvarado, Konstantin Mitgutsch**	2012	Game design assessment-framework

Liite 2: Pelien pistelista.

OPETUKSELLISUUS		ASTEIKKO 1-5									
Pelin nimi	**Pelit**	**Muisti**	**Motivaatio**	**Tarkkaavaisuus**	**Emootiot**	**Palaute**	**Tavoitteet**	**Menetelmät**	**Interaktiot**	**Opetusaineisto ja sen käyttö**	**SUMMA:**
Happy Onlife	Peli 1	3	2	2	2	3	3	3	2	3	23
Hackend	Peli 2										
Hackers vs. Cybercrook	Peli 3										
Juego cyberscouts	Peli 4										
CyberKid	Peli 5										
eFollowMe	Peli 6										
Tacos	Peli 7	3	2	2	2	2	3	4	2	4	24
SecNum Académie	Peli 8	4	3	2	2	5	4	4	2	5	31
Cyber Crime Time	Peli 9	3	4	4	3	5	4	4	3	5	35
Digiturvallinen elämä	Peli 10	3	3	3	4	5	4	4	3	4	33
Kyberturvallisuus-pakopeli	Peli 11	2	1	1	1	2	1	1	2	1	12
EveryDay	Peli 12	2	2	3	2	3	3	2	2	2	21
Spoofy: Kyberpeli lapsille	Peli 13	3	4	3	4	4	3	4	3	4	32
Nastix	Peli 14	2	1	1	1	2	2	1	2	1	13
Cyber Chronix	Peli 15	1	2	2	1	2	2	2	1	1	14

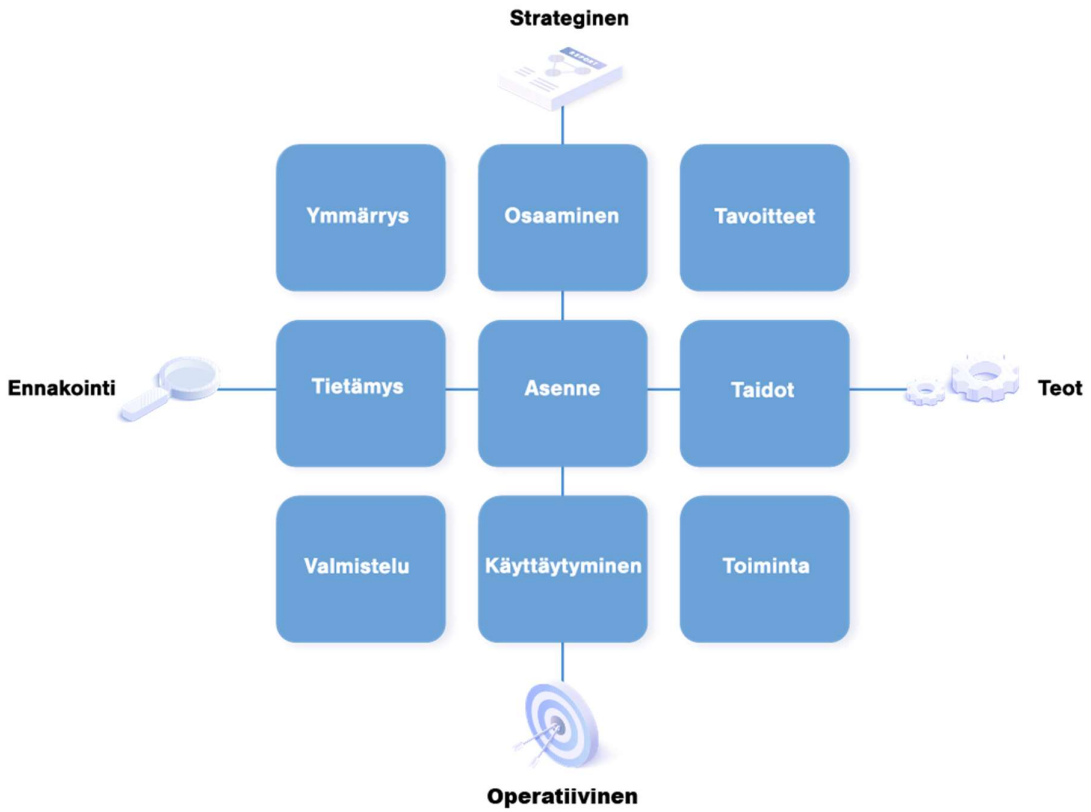
PELILLISYYS		ASTEIKKO 1-5									
Pelin nimi	**Pelit**	**Pelattavuus**	**Tarinallisuus**	**Käyttäjäkokemus**	**Adaptoituvuus**	**Rakenne**	**Muotoilu**	**Kohderyhmälle sopivuus**	**Flow**	**Immersio**	**SUMMA:**
Happy Onlife	Peli 1	3	2	3	2	3	2	3	3	3	24
Hackend	Peli 2										
Hackers vs. Cybercrook	Peli 3										
Juego cyberscouts	Peli 4										
CyberKid	Peli 5										
eFollowMe	Peli 6										
Tacos	Peli 7	2	1	2	2	3	3	3	2	2	20
SecNum Académie	Peli 8	2	2	3	2	4	3	4	3	3	26
Cyber Crime Time	Peli 9	4	5	4	2	3	3	4	3	3	31
Digiturvallinen elämä	Peli 10	4	4	4	2	3	4	3	2	3	29
Kyberturvallisuus-pakopeli	Peli 11	2	2	2	2	2	2	2	2	2	18
EveryDay	Peli 12	3	3	2	2	3	2	3	3	3	24
Spoofy: Kyberpeli lapsille	Peli 13	4	3	4	2	3	4	5	3	3	31
Nastix	Peli 14	2	1	2	1	1	1	1	1	1	11
Cyber Chronix	Peli 15	3	2	2	1	2	1	2	1	2	16

5. Kyberkansalaistaitojen sisällöllinen määrittely

Euroopan unionin talouden rakenteet, kybertoimintaympäristö ja moninaistuva uhkakuvasto muodostavat tarpeen kyberkansalaistaitojen määrittämiselle ja näiden jatkuvaluontoiselle kehittämiselle. Kyberkansalaistaitojen parantaminen vaikuttaa suoraan koko Euroopan unionin kriittisen infrastruktuurin turvallisuuteen ja digitaaliseen talouteen. Hyvät kyberkansalaistaidot kasvattavat yksilöllistä ja yhteiskunnallista turvallisuutta sekä resilienssiä.

Euroopan komission pyynnöstä tässä hankkeessa tunnistettiin konkreettisia kyberkansalaistaitoja, jotka edesauttavat DigComp-viitekehyksen omaksumista jäsenvaltiossa. Pelillistäminen ja digitaalinen oppimisportaali on valittu tunnistettavien tietotaitojen kehittämisen keinoiksi. Kyberkansalaistaitojen kehittämisellä on laaja-alaisia, turvallisuutta parantavia vaikutuksia myös kriittisen infrastruktuurin eri ulottuvuuksissa, joita ovat poliittinen, taloudellinen ja tekninen (Critical Infrastructure Protection -malli, CIP).[954]

Kyberturvallisuudella pyritään sähköisen, tietoteknisen, tiedollisen ja verkotetun toimintaympäristön turvaamiseen useiden eri ulottuvuuksien kautta. Turvallisuutta rakennetaan ennakoimalla, kouluttautumalla, tunnistamalla, ehkäisemällä ja varautumalla eri ulottuvuuksien häiriöiden vaikutuksiin toimintoympäristön kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyvät ennakoiva näkökulma, osaamisen kehittäminen, asenteet, tietoturvallisuus, jatkuvuuden hallinta ja koko toimintaympäristön varautumisen näkökulmat.[955]



Kuva 5: Kyberkansalaistaitojen luokitteluviitekehys. Kyberkansalaistaitojen keskiössä on asenne.[956]

Kyberturvallisuuden oppimisessa tietojen ja taitojen rinnalla tulee tarkastella motivaatioon vaikuttavaa asennenäkökulmaa – kansalaisten asenteet ovatkin kyberturvallisuuden kannalta keskeisiä vaikutuskohteita. Kansalaisten asenteet muodostuvat omien ja yleisten mielikuvien, etujen (ympäristöllinen, sosiaalinen ja taloudellinen kestävyys), vaikuttamismahdollisuuksien ja kyberturvallisuusroolien kautta. Yhteiskunnalla on keskeinen rooli siinä, millaiseksi yleinen asenneilmapiiri ja kyvykkyys kehittyvät tulevaisuudessa.

5.1. Kyberkansalaistaidot

Tutkimusryhmän määritelmän mukaisesti kyberkansalaiseksi katsotaan henkilö, joka vakituisesti tai tilapäisesti asuu tai oleskelee EU-jäsenvaltion alueella ja käyttää digitaalisia palveluita tai hyötyy näiden palveluiden tuottamisesta suoraan tai välillisesti. Kybertoimintaympäristössä tarvittavien tietojen, taitojen ja kykyjen yhdistelmää kutsutaan kyberkansalaistaidoiksi.

Kyberkansalaistaidot muodostuvat sellaisista osatekijöistä, jotka edesauttavat yksilöitä kehittämään ja ylläpitämään tietojaan ja taitojaan siten, että heillä on tarvittava kyky ja motivaatio toimia harkitusti elämän eri tilanteissa. Kyberkansalaistaidot ovat henkilökohtaisen ja sosiaalisen vastuun kantamista sekä tämän vastuun merkityksen ymmärtämistä kybertoimintaympäristössä.

1) Kyberkansalainen ymmärtää normien ja sääntöjen merkityksen sekä omat oikeutensa ja vastuunsa.
2) Kyberkansalainen ajattelee ja suhtautuu kriittisesti tapahtumiin ja tarjolla olevaan tietoon.
3) Kyberkansalaisella on tietotaitoja, jotka auttavat tunnistamaan, mikä on arvokasta eri osapuolille missäkin tilanteessa.
4) Kyberkansalainen tunnistaa ajattelunsa ja tunteidensa vaikutuksen eri tilanteissa.
5) Kyberkansalainen ymmärtää käyttämiensä teknologioiden pääperiaatteet ja osaa käyttää niitä vastuullisesti.

Kuva 6: Ihminen kohtaa ensimmäiseksi internetin ja siirtyy portaittain kohti systeemisen kokonaisuuden ymmärtämistä.

5.2. Kyberkansalaistaitojen kehittäminen DigComp-viitekehyksen tukena

Digital Competence Framework for Citizen (DigComp 2.2) -viitekehys sisältää yli 250 esimerkkiä tiedoista, taidoista ja asenteista, jotka edesauttavat EU-kansalaisia käyttämään digitaalisia teknologioita itsevarmasti, kriittisesti ja turvallisesti. Viitekehys ohjaa Euroopan unionin digitalisaatioon liittyvien taitojen määrittämistä ja kehittämistä. Käynnissä on lukuisia kansallisia ohjelmia, joilla viitekehys jalkautetaan eri jäsenvaltioiden sisäiseen ohjaukseen ja hallintaan.[957]

5.2.1. Kyberkansalaisen taitotavoitteet

Kyberkansalaisen tulee hallita erilaisia tietoja ja taitoja, joita tarvitaan turvalliseen toimintaan elämän eri tilanteissa. DigComp-viitekehys ohjaa EU:n laajuisesti jäsenvaltioiden digitalisaatioon liittyvien ymmärryksen, osaamisen ja kyvykkyyksien kehittämistä. Tulevaisuuden kybertoimintaympäristössä tarvittavia taitotavoitteita tulisi tarkastella DigCompia laajemmassa viitekehyksessä ja arvioida yksilön ja yhteiskunnan resilienssin, suvereniteetin ja hyvinvoinnin kannalta. Seuraavassa määritellään kyberkansalaisen taitotavoitteet, jotka on muodostettu hyödyntäen uuden tiedon kartoittamismenetelmiä, kuten suunnittelumenetelmää ja kartoittavaa kirjallisuuskatsausta. Tavoitteet sisältävät tietoja ja taitoja, joita voidaan kehittää pelillistämisen ja digitaalisen oppimisportaalin avulla.

5.2.1.1. Informaatio- ja datalukutaito

Osaa arvioida tiedon tai tietolähteen luotettavuutta

Tietolähteen arviointiin vaikuttavat lukuisat tekijät aina kansallisesta kulttuurista henkilökohtaiseen sosiaaliseen ympäristöön ja identiteettiin. Luotettavuuden arvioinnissa tilannetietoisuustaidot ja yleinen ymmärrys toimintaympäristöstä vaikuttavat merkittävästi päätöksentekoon ja toimintaan.

Osaa analysoida, vertailla ja käsitellä tietoa

Tiedon analysointiin tarvittavat tietotaidot ovat yksilöllisiä ja tilanneriippuvaisia. Eri lähteistä saatava tieto voi olla ristiriitaista ja laadittu eri tarkoitusperiä varten. Kyberkansalaisen tulee pystyä kriittisesti arvioimaan, kuinka tieto rakentuu, mistä tieto on peräisin, millä foorumilla ja milloin se esitetään, mitkä ovat taustavaikuttimet tiedon tuottamiselle, kuka on tuottanut tiedon ja mihin tarkoitukseen sekä mitä sillä tavoitellaan. Tietoa käsiteltäessä vallitsevaa ja valittua teknologiaa hyödynnetään siten, että tiedon käsittely ja hallinta on järjestelmällistä ja tarkoituksenmukaista.

Ymmärtää toimintaympäristönsä

Toimintaympäristö muodostuu käyttökokemuksesta ja piilossa olevasta järjestelmien laajemmasta yhteiskunnallisesta ulottuvuudesta. Kybertoimintaympäristössä vain harva palvelu tai sovellus on todella maksuton. Verkkoselaimet jo itsessään keräävät tietoja käyttäjistään markkinoinnin ja tuotekehityksen tarpeisiin. Palveluiden ja sovellusten liiketoimintalogiikan pääpiirteiden ymmärtäminen ja tietoisuus siitä, että hakutuloksiin ja sosiaalisen median sisältösuosituksiin vaikuttavat monet tekijät, on kyberkansalaiselle tärkeää.

Kehittää ennakointitaitoja

Ymmärtää kyberturvallisuuteen vaikuttavien, ennakointikykyä parantavien tietojen ja taitojen kehittämisen polut. Osaa valita ennakointikykyä kehittäviä opetus- ja koulutusohjelmia. Ymmärtää laajasti ennalta ehkäisevien toimenpiteiden merkityksen kyberturvallisuuden ja systeemitason turvallisuuden näkökulmista.

5.2.1.2. Viestintä- ja yhteistyötaidot

Ymmärtää säännöt ja niiden vaikutuksen henkilökohtaisella ja yhteisöllisellä tasolla

Kybertoimintaympäristössä vallitsee lukuisia ohjaavia sääntöjä, käyttöehtoja ja pakottavaa lainsäädäntöä niin Euroopan unionin kuin jäsenvaltioiden tasolla. Nämä ohjaavat normit vaikuttavat sekä henkilökohtaisella että yhteisöllisellä tasolla. Lisäämällä ymmärrystä vallitsevasta sääntelystä parannetaan kansalaisten mahdollisuuksia ja kykyä toimia yhteisten sääntöjen mukaisesti.

Ymmärtää oman toimintansa vaikutuksen yleiseen turvallisuuteen

Ymmärtää, miten ja millä tavoin palvelua tai teknologiaa käyttäessään tai tietoa käsitellessään voi vaikuttaa kokonaisturvallisuutta parantavasti tai heikentävästi. Ymmärtää vastuunsa ja osaa toimia oikein häiriö- tai ongelmatilanteissa.

Hallitsee digijalanjälkensä

Ymmärtää pääperiaatteet verkkosivustojen, evästeiden ja järjestelmien systeemisestä toiminnasta. Osaa käyttää valitsemiaan palveluita tai laitteitaan siten, että näiden käytöstä muodostuu mahdollisimman vähän haitallista näkyvyyttä ja altistumista.

Tunnistaa eri vuorovaikutuskanavien merkityksen viestinnässä

Osaa valita viestintäkanavansa tarpeiden ja viestin sisällön perusteella. Ymmärtää, että sosiaalisen median alustat ja keskustelufoorumit voivat olla sisällöltään, kieliasultaan, kulttuuriltaan ja teknisiltä ratkaisuiltaan hyvin erilaisia.

5.2.1.3. Digitaalisen sisällön tuottaminen

Ymmärtää tekijänoikeuksien periaatteet

Ymmärtää, miten immateriaalioikeudet vaikuttavat siihen, mitä ja miten verkosta löytyvää sisältöä voi käyttää, lainata, muokata ja levittää. Osaa tarkistaa ja valita sisällöntuottamiseen sellaisia elementtejä ja tietoja, jotka eivät loukkaa muiden oikeuksia. Osaa suojella myös omia tekijänoikeuksiaan. Ymmärtää kysyä apua tilanteissa, joissa epäilee olevan tietoturvaan tai tietosuojaan liittyviä ongelmia tai riskejä.

Osaa käyttää vallitsevia teknologioita ja palveluita

Ymmärtää pääperiaatteet käytettävistä palveluista ja valituista teknologioista siten, ettei omalla toiminnallaan vaaranna jo olemassa olevaa sisältöä tai tietoturvallisuutta tahallisesti tai tahattomasti.

5.2.1.4. Turvallisuusosaaminen

Osaa käyttää vallitsevaa teknologiaa vastuullisesti

Ymmärtää pääperiaatteet käyttämistään ja valitsemistaan teknologioista ja osaa muuttaa niiden asetuksia tarveperusteisesti sekä jäsentää niiden sisältöä ja tietoa. Osaa käyttää valitsemiaan valmisohjelmistoja vastuullisesti. Ymmärtää pääpiirteissään, mitkä tekijät vaikuttavat merkittävimmin käytettyjen teknologioiden tai sovellusten turvallisuuteen. Osaa varmistaa, että laitteiden viimeisimmät viralliset päivitykset ovat asennettuina ja käyttöjärjestelmäversio on valmistajan tuen piirissä. Kansalainen osaa valita ja uskaltaa vaatia nykyistä turvallisempia digitaalisia tuotteita. Tätä ohjataan myös EU-tasoisella sääntelyllä; esimerkiksi EU:n Cyber Resilience Actissa asetetaan tavoitteeksi luoda olosuhteet, joissa käyttäjän on mahdollista huomioida kyberturvallisuus digitaalisia tuotteita valitessaan ja käyttäessään.

Osaa suojata käyttämänsä tiedon ja pitää huolen digitaalisesta identiteetistään

Osaa suojata käyttämänsä tiedon sen arkaluontoisuuden mukaisesti. Hallitsee digitaalisen identiteetin suojaamisen perusteet, tunnistaa ajankohtaisilta uhkilta suojautumisen merkityksen ja tuntee myös keinoja

tähän (kuten ylimääräiset varmenteet pääsynhallinnassa). Ymmärtää identiteettiin liittyvän digitaalisen jalanjäljen muodostumisen sekä haitallisen altistumisen ja näkyvyyden pääperiaatteet.

Osaa ylläpitää omaa ja muiden turvallisuudentunnetta ja tietoisuutta

Tunnistaa haitalliset käyttäytymismallit ja niiden vaikutukset kybertoimintaympäristössä. Tunnistaa digitaalisen väkivallan tunnuspiirteet, väkivaltaiset teot (kuten yksilöön kohdistuvat kyberrikokset ja kiusaamisen) ja rakenteellisen väkivallan (kuten eriarvoisuuden ja eskalaation mahdollisuudet digitaalisessa ympäristössä) ja osaa toimia tilanteissa oikein. Osaa suojella itseään ja muita digitaalisen ympäristön uhkilta ja vaaroilta (esimerkiksi varoittaa muita havaitsemistaan huijausyrityksistä). Hankkii aktiivisesti kyberturvallisuustietoa ja jakaa sitä myös muille.

5.2.1.5. Ongelmanratkaisutaidot

Osaa ratkaista palveluiden ja laitteiden käyttöön liittyviä ongelmia ja viestiä ongelmatilanteista ymmärrettävästi

Ymmärtää pääperiaatteet käyttämistään teknologioista ja osaa ratkaista niiden käyttöön liittyviä yleisimpiä ongelmia. Osaa hakea apua haastavissa tilanteissa varsinkin, jos epäilee tietoturvaan tai tietosuojaan liittyviä ongelmia.

Ymmärtää oman osaamisensa ja kehittää sitä aktiivisesti

Tiedostaa omat osaamispuutteensa tai epävarmuutensa teknologioiden ja palveluiden käytössä. Haluaa määrätietoisesti kehittää itseään ja ymmärtää omien ajatusvinoumiensa, omintakeisten tosi uskomustensa ja tunnereaktioidensa vaikutuksen käyttäytymiseen ongelmatilanteissa.

Osaa toimia joutuessaan tietoturvarikkeen tai -rikoksen kohteeksi

Osaa toimia tietoturvarikkeen ja -rikoksen tai näiden epäilyn kohdalla siten, että se edistää niin henkilökohtaista kuin yhteisöllistäkin turvallisuutta. Ymmärtää oman toimintansa vaikutuksen häiriönhallintaan aina havainnoinnista alkaen. Kykenee säilyttämään positiivisen asenteen erilaisia ongelmia kohdatessaan ja niistä viestiessä.

Viitteet

[954] David Mussington, *Concepts for enhancing critical infrastructure protection : relating Y2K to CIP research and development* (Santa Monica: RAND Corporation, 2002), 30.
[955] Turvallisuuskomitea, ”Yhteiskunnan turvallisuus: Yhteiskunnan turvallisuusstrategia”, *Valtioneuvoston periaatepäätös 2.11.2017* (Helsinki: Turvallisuuskomitean sihteeristö, 2017).
[956] Mika Helenius, "Human Cyber Security Dimensions - Cognitive Matrix," 21.12.2022, verkkoesitys Aalto yliopiston työpajassa.
[957] Riina Vuorikari, Stefano Kluzer ja Yves Punie, *DigComp 2.2: The Digital Competence Framework for Citizens*, EUR 31006 EN (Luxemburg: Publications Office of the European Union, 2022).

6. Johtopäätöksiä

I. Tässä tutkimuksessa Euroopan unionin jäsenmaista tehdyistä maaraporteista on havaittavissa, että EU-maiden strategiset kyberturvallisuuteen liittyvät koulutuslinjaukset ovat melko tuoreita. EU-maissa ollaan vasta luomassa kyberturvallisuuskulttuuria, ja itsessään digitaalisen maailman kehittyminen on varsin nuori ilmiö verrattaessa esimerkiksi liikenneturvallisuuskulttuurin muodostumiseen. Kulttuurin luominen ja vahvistaminen vie aikaa, minkä vuoksi määrätietoinen työ on tärkeää. Siksi tämän Cyber Citizen -hankkeen kaltaisia toimia tarvitaan juuri nyt. Yhteinen ymmärrys ja laaja-alainen osaaminen muuttuvat ajan saatossa sivistykseksi ja kulttuuriksi, joilla on suuri merkitys koko yhteiskunnan turvallisuudelle sekä kansalaisten omalle arjen turvallisuudelle. Meidän on rakennettava vastaavaa sivistystä ja kansalaiskulttuuria turvallisuutemme eteen, tällä kertaa digitaalisessa toimintaympäristössä, minkä merkitys kasvaa digitalisoinnin ja teknologian kehityksen myötä.

II. EU-maissa ollaan siirtymässä kyberturvallisuuden eriyttämisestä ammattilaisten vastuulta ja hallinnasta (tekniset keinot) siihen, että kyberturvallisuus integroituu kaikkeen muuhun yhteiskunnalliseen toimintaan ja on kiinteä osa digitaalista maailmaa. Käytännössä tämä tarkoittaa sitä, että digitaalisuus ja sen turvallisuus integroituvat lähes kaikkeen ihmisten, organisaatioiden ja yhteiskuntien toimintaan ilman, että se olisi erillinen asia. Tämäkin osaltaan korostaa kyberkansalaistaitojen merkitystä sekä niiden asemaa Euroopan unionin toimivuuden ja itsenäisyyden yhtenä perustekijänä.

III. Kybertoimintaympäristön uhkakuvat ovat monipuolistuneet ja moninaistuneet – ja moninaistuvat entisestään yhä kiihtyvällä vauhdilla. Toimintaympäristön nopea muuttuminen mahdollisuuksineen ja uhkineen on yksi EU-maiden kyberturvallisuusymmärrystä yhdistävä piirre. Euroopan unionissa ja EU-jäsenvaltioissa ymmärretään yhä paremmin kybermaailman kompleksisuus. Tämä korostaa vahvasti kyberkansalaistaitojen jatkuvan oppimisen tärkeyttä sekä tietotaitojen kehittämisen laaja-alaisuutta. Kyberkansalaistaidot on ymmärrettävä taidoiksi, jotka muuttuvat toimintaympäristön muutoksen mukana ja jatkuvan oppimisasenteen merkitys korostuu valppauden ohella.

IV. Euroopan unionin jäsenmaissa on eroja siinä, mitkä tiedot ja taidot ymmärretään kyberkansalaistaidoiksi. Osassa maita ei selkeitä määrittelyjä löydy siitä, mitä kyberkansalaistaidoilla tämän päivän yhteiskunnassa tarkoitetaan ja mitä tietoja ja taitoja siihen yhdistetään kuuluvaksi. Lisäksi on oleellista huomioida, että ne maat, joissa niin sanottuja virallisia määrittelyjä on olemassa, nämä määrittelyt ovat kovinkin erilaisia eri maissa. Suurin ero liittyy siihen, missä määrin teknisenä ja/tai informatiivisena toimintaympäristönä kybertoimintaympäristö lähtökohtaisesti ymmärretään. Määrittelyissä voi myös havaita, että usein tarkoitetaan samaa asiaa, mutta kansallisten ja kulttuuristen erojen johdosta ilmaisutavat saattavat olla varsin erilaisia.

V. Kyberturvallisuuden perusosaaminen vaihtelee Euroopan unionin jäsenmaissa paljon, ja sama koskee kyberturvallisuuden yleistä tasoa. Tämä ilmenee myös varsin suuresta hajonnasta kyberturvallisuuden tasoa mittaavissa eri indekseissä maiden välillä. Niin ikään maissa on erilaisia näkemyksiä siitä, miten kyberturvallisuusosaamista ja kulttuuria tulisi kehittää. Kaikissa maissa on viimeisen kymmenen vuoden aikana luotu kyberturvallisuusstrategia. Näissä strategioissa kuitenkin katsotaan kyberturvallisuutta lähinnä kansallisista näkökulmista, ei EU-näkökulmasta. EU:n yhteiselle kyberturvallisuuskulttuurin kehittämiselle on selkeä tarve ja kyberkansalaistaitojen yhtenäistäminen voisi olla tässä kehittämisessä erinomainen ja mittava askel eteenpäin, etenkin EU:n kyberturvallisen arjen vahvistamisessa.

VI. Euroopan unionin jäsenvaltioista on tehty vähän kyberkansalaistaitoihin liittyvää tutkimusta. Lisäksi olemassa oleva tutkimus keskittyy yksilöiden digi- ja kyberturvallisuustietoisuuteen ja käyttäytymiseen. Sen sijaan aiemmissa tutkimuksissa kuvataan hyvin vähän sitä, mitä kyberkansalaistaitoja opitaan ja opetetaan, sekä miten kyberkansalaistaitoja tulisi opettaa. Kyberkansalaistaitojen tutkimus on

ylipäänsä varsin viimeaikaista ja lisääntynyt viimeisten muutaman vuoden aikana. Kansalaisten tai heiltä odotetun digi- ja kyberturvallisuusosaamisen määrittely on moninaista, vasta muokkautumassa ja tällä hetkellä siinä painottuu digitaalisen kansalaisuuden ajatus. Esimerkiksi vuosikymmen sitten painotus oli asukas- ja käyttäjäkeskeinen.

VII. Kyberkansalaistaitoja ei koeta pelkästään arkipäivän taitoina ja uhkiin varautumisena, vaan mahdollistajana alati digitalisoituvassa maailmassa (arjen taidot ja erikoisosaaminen). Kyberkansalaistaitoja opetettaessa on korostettava voimakkaan uhkapuheen sijasta mahdollistavaa näkökulmaa eli sitä, miten kyberkansalaistaitojen oppiminen on ennen kaikkea mahdollistava asia niin yksilöille, organisaatioille kuin yhteiskunnillekin. Kyberkansalaistaidot on nähtävä myös Euroopan unionille kilpailuvaatimuksena globaalissa teknologiakamppailussa, eli kyberosaamisen kehittäminen on kriittistä.

VIII. Euroopan unionin jäsenmaiden välillä on suuriakin eroja siinä, kuinka vastuuta kyberkansalaistaitojen kouluttamisesta ja opettamisesta jaetaan ja osoitetaan. Tällä on suora vaikutus siihen, miten kyberturvallisuuskoulutusmateriaalia on saatavilla ja kuinka helposti kansalaiset saadaan sen piiriin. Osassa maita on selkeästi määritelty tahot, jotka kyberkoulutusmateriaalia tuottavat ja miten sitä jaetaan mahdollisimman laajalti. Osassa maita kyberkansalaistaitojen opettamista ei tapahdu koordinoidusti, vaan sitä hoitavat yksittäiset tahot ja organisaatiot, jolloin myös vaikuttavuus jää pienemmäksi kuin laajempi taitojen opettamisen koordinointi.

IX. Koska kyberkansalaistaidot koskevat kaikkia, nousee keskeiseksi kysymykseksi eri ikäryhmien sekä ihmisten psyykkisten ja motoristen eroavaisuuksien huomioiminen. Tämä huomioiminen koskee sekä tietoja ja taitoja että niiden opettamisen tapoja, joissa on eroja eri ryhmien välillä. Eri ryhmien kyberturvallisuustaitojen huomioimisessa on varsin paljon vaihteluita eri EU-maiden välillä. Lisäksi eroja löytyy teknisten laitteiden saatavuudessa, kieliasioihin liittyvissä painotuksissa sekä maahanmuuttajien huomioimisessa. Opettamisen tavoitettavuus on olennainen asia huomioitavaksi, kun luodaan koko Euroopan unionin alueelle yhtenäistä kyberturvallisuuskulttuuria osaamisen kautta.

X. Euroopan unionin alueella kyberkansalaistaitoihin liittyvä koulutusmateriaalin tarjonta on hyvin moninaista ja hajanaista. Tämä koskee sekä materiaalin laatua että sisältöjä. Eroja on myös siinä, missä määrin eri maissa kyberturvallisuuden taidot ovat osana opetussuunnitelmaa. Tämä kertoo kaikkinensa siitä, että Euroopan unionissa on tarvetta yhtenäiselle kyberkansalaistaitojen määrittelylle, opetukselle ja opetuksen koordinoinnille. Kun perusta on yhteinen, on myös maiden ja kansalaisten välillä Euroopan unionissa helpompi yhtenäisemmin toimia.

XI. Tutkimuksessa ilmeni selkeästi, että kaikkialla Euroopan unionissa tarvitaan lisää kyberkansalaistaitojen kouluttajia sekä heitä, jotka pystyvät tarjoamaan täydennyskoulutusta esimerkiksi peruskoulun ja toisen asteen opettajille. Tekniikan käytännön osaaminen saa EU-tason valmistelussa ja EU-jäsenvaltioissa liian vähän painoarvoa, eikä strateginen kyberturvallisuuden ennakoiva ja monialainen insinööriosaaminen saa sille tarvittavaa huomiota tiede-, tutkimus- ja koulutuspolitiikassa. Opettajien ammattitaidon puute kyberturvallisuuteen liittyvissä asioissa on selkeä pullonkaula kyberturvallisuustaitojen opettamisessa, sekä yleisten taitojen että erikoisosaamisen kannalta. Opettajien osaamisen kehittämisessä on myös huomioitava näiden taitojen jatkuva kehittäminen kybertoimintaympäristön muuttumisen takia.

XII. Kyberkansalaistaitojen osaamiseen nykytilanteesta johdettu osaamisen kehittämisen malli olisi selkeä ja tärkeä kehitysaskel. Tähän tarvitaan Euroopan unionin tason linjaus, johon jäsenmaat sitoutuvat. Yhtenäinen osaamisen kehittämisen malli edistäisi digitaalisen suvereniteetin ja turvallisuusvalmiuden systemaattista kehittymistä kaikissa EU-maissa.

XIII. Sääntely on yksi tavoista ohjata yhteiskunnan toimintaa ja kehitystä talous- ja informaatio-ohjauksen lisäksi. Hankkeesta syntyvää ymmärrystä ja mallia tulisi hyödyntää Euroopan unionin tasolla

kilpailukyky- ja informaatio-ohjauksessa ja sääntelykysymyksissä niiltä osin, kuin opetussuunnitelmien sisältöjä ohjataan kansallisesti. Tutkimus tekee näkyväksi sen, että kyberkansalaistaidot liittyvät olennaisesti yhteiskunnan jäsenten perusoikeuksien turvaan, mutta samalla myös sen, että ilman kansalaisten itsensä osallistumista ja osaamista tavoitetasoa on vaikea, ellei mahdotonta saavuttaa.

XIV. Pelit ovat vakiinnuttaneet asemansa sosiaalisen käyttäytymisen muotona ja ovat yhä keskeisempi oppimisen väline. Kyberturvallisuuspelien sisällöt painottuvat turvallisuuden perustaitoihin, kriittiseen ajatteluun ja uhkatilanteiden havainnollistamiseen digitaalisessa toimintaympäristössä. Tässä tutkimuksessa käsitellyt pelit ovat melko yksinkertaisia ja lineaarisia. Peleissä olisi tärkeää tunnistaa osaamisen tasot niin, että peli muokkautuisi käyttäjälle sopivaksi. Näin voidaan tarjota tarkempaa ymmärrystä pelaajalle hänen omasta digiosaamisestaan ja kehittää tuota osaamista taitotasosta riippumatta, yksilökohtaisen tarpeeseen perustuen.

XV. Tutkimuksen aikana saadun palautteen perusteella kyberkansalaistaitoja on tarpeellista kehittää ja olisi hyvä, jos taitojen mittaamiseen olisi yhteiset, eurooppalaiset mittarit. Valtaosa nykyisistä kyberkansalaistaitoja käsittelevistä mittareista on pääosin digitalisaation tasosta kertovia. Mittareista puuttuu kyberturvallisuuden kansalaistaitoja tarkastelevat, tarkemmat osiot. Mittarit eivät mittaa esimerkiksi ennakoivia kansalaisten kyberturvallisuuden taitoja, kuten ohjelmointiosaamista. Mittareissa ei myöskään tarkastella Euroopan talousalueen jatkuvuuden ja kestävyyden näkökulmasta strategista suvereniteettia.

XVI. Tämä tutkimus on herättänyt laajaa kiinnostusta Euroopan unionin jäsenmaissa, ja tutkimukselle on todettu olevan selkeä tarve. EU-maista saadun palautteen perusteella on vahvaa yhteistä maaperää ja kiinnostusta luoda yhteisiä kyberturvallisuuden kansalaistaitoja Eurooppaan. Oppimateriaaliin on myös tutkimuksen tekijöille tullut EU-maista paljon ohjeita ja hyviä suosituksia. Tärkeänä pidetään yleisen asennekasvatuksen merkitystä, helppokäyttöisyyttä (käyttäjäystävällisyyttä) oppimateriaaleissa sekä taitojen opettamisen sisältöjen jatkuvaa kehittämistä. Yhteenvetona voi todeta, että EU-maissa suhtaudutaan myönteisesti yhteisten kyberkansalaistaitojen kehittämiseen.