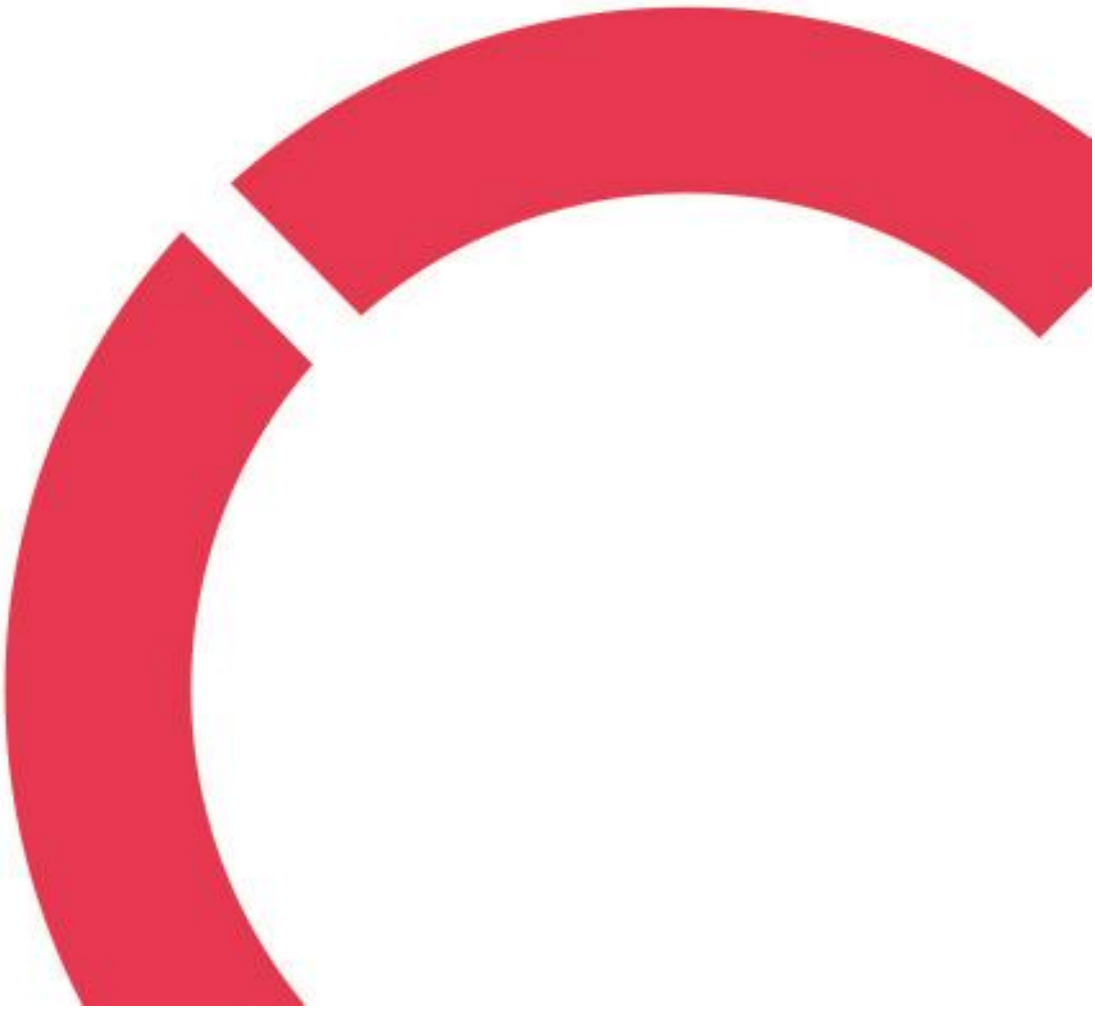
Minna Nyström

YKSILÖ JA KYBERTURVALLISUUS

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Joulukuu 2023



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Joulukuu 2023	**Tekijä/tekijät** Minna Nyström
Koulutus Tieto- ja viestintätekniikan koulutus		☒ AMK ☐ YAMK
Työn nimi YKSILÖ JA KYBERTURVALLISUUS		
Työn ohjaaja Jari Isohanni		**Sivumäärä** 27

Tavoitteena tässä opinnäytetyössä oli tunnistaa ja löytää inhimilliset tekijät, joilla on merkittävin vaikutus kyberturvallisuuteen. Lisäksi tavoitteena oli herätellä lukijaa tunnistamaan omia toimiaan, jotka aiheuttavat riskejä verkossa toimittaessa.

Opinnäytetyössä selvitettiin, mitkä kyberuhat tällä hetkellä uhkaavat käyttäjiä, tietovuotojen merkitystä talouteen, inhimillisten tekijöiden ominaisuuksia ja pohdittiin, mitä ratkaisuja ja uhkia tulevaisuudessa kohtaamme kyberturvallisuuden saralla.

Tutkimuksen perusteella havaittiin, että yksilö on avainasemassa taistelussa kyberuhkia vastaan. Yksilön pyrkiessä huolehtimaan omien tietojensa ja laitteidensa turvallisuudesta, edistää hän samalla myös kansallista turvallisuutta.

Opinnäytetyö voi toimia ohjeena henkilöille, jotka ovat kiinnostuneita minimoimaan riskejä verkossa toimiessaan.

Asiasanat
Internet, internet of things (IoT), kyberturvallisuus, tietoturva, älylaitteet

ABSTRACT

Centria University of Applied Sciences	Date December 2023	Author Minna Nyström
Degree programme Bachelor of Engineering, Information Technology		
Name of thesis INDIVIDUAL AND CYBERSECURITY		
Centria supervisor Jari Isohanni		**Pages** 27

The goal of this thesis was to identify and discover the human factors that have the most significant impact on cybersecurity. In addition, the aim was to awaken the reader to identify their own actions that pose risks when operating online.

The thesis examined which cyber threats currently threaten users, the significance of data leaks in the economy, the characteristics of human factors and considered what solutions and threats we will face in the future in the field of cyber security.

The study found that the individual plays a key role in the fight against cyber threats. As an individual strives to ensure the security of their own data and equipment, they also contribute to national security.

The thesis can serve as a guideline for individuals who are interested in minimizing risk when operating online.

Key words
Cybersecurity, information security, internet, internet of things (IoT), smart devices

TIIVISTELMÄ
ABSTRACT
SISÄLLYS

KUVIOT

1 JOHDANTO

Bittien maailma on kietoutunut fyysiseen maailmaan niin tiiviisti, ettemme voi enää sivuuttaa kyberturvallisuuden merkitystä elämässämme. Olisi suuri virhe ajatella kyberturvallisuuden olevan vain pienen asiantuntijajoukon hallitsema aihealue. Turvallisuus bittien maailmassa koskettaa jokaista internetin käyttäjää ja jokainen käyttäjä on myös vastuussa kyberturvallisuudestaan verkossa. Osa verkon käyttäjistä ei kuitenkaan tiedosta vastuutaan ja käyttäytyy huolimattomasti verkossa. Tämä on huolestuttavaa, koska käyttäjät ovat avainasemassa ja ”eturintamassa” taistelussa kybermaailman uhkia vastaan. Kyberuhkia vastaan on vaikea taistella, jos käyttäjä ei edes ymmärrä, mitä kyberturvallisuus ja tietoturva tarkoittavat.

Verkon käyttäjä kohtaa verkkoa käyttäessään niin paljon erilaisia uhkia, että niitä voidaan pitää jo lähes arkipäiväisenä asiana. Palvelunestohyökkäykset ovat myös yleisiä ja haittaavat usein toimintaamme eri verkkopalveluissa.

Tämän tutkielman tavoitteena on selvittää, kuinka inhimilliset tekijät vaikuttavat tietoturvaan ja kuinka kyberrikollisuudelta voidaan suojautua yksilötasolla. Tutkielma voi toimia myös ohjeena henkilöille, jotka ovat kiinnostuneita minimoimaan inhimillisten tekijöiden avulla kyberturvallisuusriskejä.

2 KYBERTURVALLISUUS JA TIETOTURVA

Tässä tutkielmassa käytetään termejä kyberturvallisuus ja tietoturva. Näitä termejä näkee käytettävän usein toistensa synonyymeina, mutta molemmissa termeissä on kyse tietojärjestelmien toiminnan varmistamisesta ja datan suojaamisesta (Järvinen 2018, 14). Näillä termeillä on kuitenkin joitain eroja ja ne menevät helposti sekaisin, koska ne sisältävät päällekkäisyyksiä.

Tietoturvallisuus tunnetaan lyhemmin tietoturvana. Tietoturvallisuus on laajempaa tiedon turvaamista. Fyysinen tallentaminen ja pääsyn rajoittaminen tietoon digitaalisen ympäristön ulkopuolella kuuluvat myös tietoturvaan. (F-Secure 2023.) Tietoturvallisuus perustuu luottamuksellisuuteen, käytettävyyteen ja eheyteen. Kun järjestelmä on luottamuksellinen, on sen data vain oikeutettujen toimijoiden saatavissa ja muokattavissa. Eheään järjestelmään pystyvät vaikuttamaan vain oikeutetut toimijat säännellyllä tavalla. Eheydellä varmistetaan, että tieto on oikeaa ja ajantasaista. Käytettävyydellä varmistetaan, että oikeutetut toimijat pääsevät käsittelemään tietoa hallitusti ja ennustettavasti tiettyjen etukäteen sovittujen vasteaikojen puitteissa. (Waschke 2017, 188–189.)

Kyberturvallisuus on digitaalisen maailman turvallisuutta, joka käsitteenä tulisi olla selkeä kaikille yhteiskunnan jäsenille. Kyberturvallisuus-käsitteen popularisointi olisi tärkeää, koska jokainen yhteiskunnan jäsen on osa kybertoimintaympäristöä (Limnéll, Majewski & Salminen 2014, 39). Jos halutaan parantaa kyberturvallisuuden tasoa, tulee kyberturvallisuuden ymmärryksen kasvaa väestössä.

2.1 Kybermaailman ominaisuuksia

Koska kybermaailma on kaikkialla läsnä, ei sen merkitystä yhteiskunnassa voi väheksyä. Monet arkiset toimintomme ovat riippuvaisia bittien maailmasta. Bittien maailman tapahtumilla on selkeitä fyysisiä vaikutuksia ja näiden kahden maailman rajat ovat osittain hämärtyneet. Vaikka tietotekniikka on oleellinen osa monen arkea, eivät kaikki osaa suhtautua tietoturvallisuuteen tarvittavalla vakavuudella. Kotoa poistuessamme lukitsemme ovet varmistaaksemme, ettei kotiimme pääse sinne kuulumattomat henkilöt. Osa hankkii kodin valvontajärjestelmiä ja suojaa muutenkin omaisuuttaan parhaansa mukaan ulkopuolisen aiheuttamalta vahingolta. Tietoturvallisuus vaatisi ja ansaitsisi vähintään samanlaisen panostuksen asiaan. Bittien maailma on osittain petollinen. Se mahdollistaa monta positiivista asiaa käyttäjilleen, mutta myös uhat ovat hyvin todellisia ja helpompia toteuttaa verkkorikollisen silmin.

2.2 Bittien maailma

Maailma koostuu fyysisen maailman lisäksi bittien maailmasta. Fyysinen eli atomien maailma on konkreettista, havaittavissa olevaa. Tämän maailman rinnalle on ihminen luonut keinotekoisen bittien maailman, johon sisältyvät muun muassa internet ja digitaaliset järjestelmät. (Limnéll ym. 2014, 29.) Nämä kaksi maailmaa ovat tiiviisti toisiinsa sidoksissa. Bittien maailma ei olisi mahdollinen ilman fyysisen maailman konkreettisia asioita, kuten tietokoneita. Koska nämä maailmat ovat vahvasti kytköksissä toisiinsa, on bittien maailman häiriöillä välitön vaikutus fyysiseen maailmaan. Tämän vuoksi on tärkeää varmistaa digitaalisen maailman toimivuus, jotta yhteiskunnan kriittinen infrastruktuuri voi toimia häiriöttä. (Limnéll ym. 2014, 32.)

2.3 ATTAT-Kaava

ATTAT-kaavalla tarkoitetaan kybermaailman lainalaisuuksista tiivistettyä muistisääntöä. Aika, tila, tunnistamattomuus, asymmetrisyys ja tehokkuus, näistä sanoista muodostuu ATTAT-kaava. Sen avulla voidaan toimia turvallisesti ja menestyksekkäästi kybermaailmassa. (Limnéll ym. 2014, 63.) Kybermaailmassa pätevät erilaiset lainalaisuudet kuin fyysisessä maailmassa. Sen vuoksi kybermaailmassa on mietittävä erilaisia turvallisuusnäkökulmia fyysiseen maailmaan verraten.

Aika on kybermaailmassa hyökkääjän puolella. Kyberhyökkäys voi tapahtua välittömästi napin painalluksen jälkeen, kun taas fyysisessä maailmassa esimerkiksi välimatkat aiheuttavat ajallisesti viivettä hyökkäyksen toteutuksessa. Hyökkääjä voi hyödyntää aikaa myös sitä pidentäen, sillä haittaohjelma voi odottaa valmiina toimintakäskyä vuosia. (Limnéll ym. 2014, 63.)

Tila on merkittävä mahdollistaja kybermaailmassa. Hyökkäyksiä ajatellen, tilan merkitys katoaa, sillä kybermaailmassa maantieteellinen etäisyys ei ole oleellista. Aika ja tila kulkevat myös käsi kädessä, koska bittien maailma mahdollistaa kommunikoinnin kenen tai minkä tahansa välillä, milloin ja missä tahansa. (Limnéll ym. 2014, 65.)

Tunnistamattomuus bittien maailmassa lisää houkutusta tehdä pahantahtoisia asioita, sillä kybermaailmassa mahdollistuu tunnistamattomana toimiminen ja eri identiteettien käyttö. Tämä vähentää kiinnijäämisen riskiä. (Limnéll ym. 2014, 67.) Tunnistamattomuus vaikeuttaa vahingonteon tekijän kiinnisaamista, sillä koskaan ei voida varmuudella sanoa, kuka yhteyttä käyttää.

Asymmetrisyys tarkoittaa tilannetta, jossa esimerkiksi toimijoiden strategiat ja suhteellinen voima poikkeavat toisistaan huomattavasti. Kybermaailmassa resursseilla ei niinkään ole merkitystä, sen sijaan osaaminen ja asiantuntijuus muodostavat keskeisen roolin. (Limnéll ym. 2014, 68.) Kynnys osallistumiselle madaltuu, sillä käytössä ei tarvitse olla rajaton määrä resursseja.

Tehokkuus kybermaailmassa viittaa tilanteeseen, jossa hyökkääjällä on mahdollista tehdä useita asioita kerralla ja nopeasti. Hyökkäys voi tapahtua tunkeutumalla suojaamattomiin järjestelmiin, muuttamalla tietoa, häiritsemällä kriittistä infrastruktuuria eli eri ulottuvuuksilla pyritään saamaan mahdollisimman paljon vahinkoa aikaan mahdollisimman pienillä resursseilla. (Limnéll ym. 2014, 70.) Tehokkuutta kybermaailmassa voidaan hyödyntää myös hyviin tarkoituksiin, esimerkiksi tuotanto- ja palveluketjuissa voidaan vähentää välivaiheita ja näin nopeuttaa tuotantoprosessia. Verkkokauppa palvelee asiakkaita vuorokauden ympäri kaikkina päivinä vuodessa ilman jatkuvaa työntekijöiden panosta.

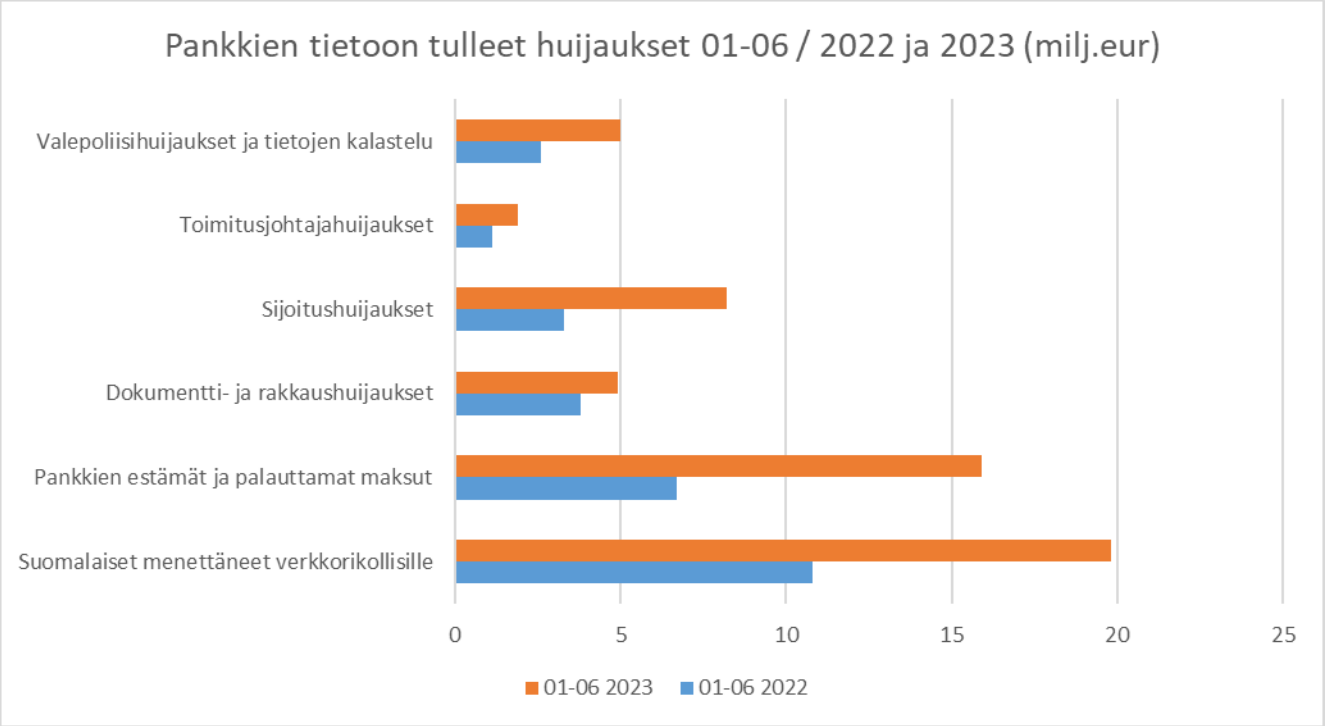
3 KYBERTURVALLISUUS AIKAMME YHTEISKUNNASSA

Kyberuhat ovat merkittävästi yleistyneet globaalilla tasolla viime vuosina. Tietomurrot ovat kaksinkertaistuneet parissa vuodessa Suomessa. Merkittävää kasvua on havaittavissa myös erilaisten kyberhyökkäysten ja verkkohuijausten saralla. Uutena kohteena kyberhyökkäyksille ovat verkkoon kytkettävät laitteet (engl. Internet of Things, IoT): niihin kohdistuvissa kyberuhissa on odotettavissa yli kymmenkertaista kasvua verrattaessa vuoteen 2019. (Ali-Yrkkö, Mattila & Seppälä 2020.) LähiTapiolan teettämästä kyselystä käy ilmi, että vuonna 2023 huijausyrityksiä on kohdannut 47 prosenttia suomalaisista. Suomalaisilta huijauksilla viedyt rahasummat jatkavat tasaisesti kasvuaan. (Palmgren 2023.)

Aikakaudellemme on jo tyypillistä, että käytämme digitaalisia palveluita tai välineitä lähes jokaisella elämämme osa-alueella. Digitalisaation myötä myös kyberrikollisuus on saanut lisää mahdollisuuksia laajentua. Tietoturvayhtiö McAfee ja ajatushautomo CSIS arvioivat vuonna 2018, että kyberrikollisuuden maailmanlaajuiset kustannukset ovat n. 0,8 prosenttia maailman bruttokansantuotteesta eli noin 600 miljardia euroa (Ali-Yrkkö ym. 2020). Lokakuussa 2020 julkisuuteen tullut psykoterapiakeskus Vastaamon tietomurtotapaus on koskettanut jopa 33 000 suomalaista, kun heidän henkilötietonsa ja arkaluontoiset potilaskertomuksensa julkaistiin Tor-verkossa (Hämäläinen 2021).

Vastaamon tapauksessa yksilön, tässä tapauksessa potilaan, toimilla ei ollut merkitystä tietomurron syntymiseen. Yrityksen palvelujen käyttäjä tulisi pystyä luottamaan, että arkaluontoiset ja salassa pidettävät asiakastiedot ovat turvassa. Vastaamon tapauksessa sekä tietomurron tekijä, että tietomurrosta vastuussa ollut yrityksen johto joutuvat rikosoikeudelliseen vastuuseen teoistaan. Tietomurron uhreille on kuitenkin aiheutunut valtavasti kärsimystä, sillä heidän arkaluontoiset potilastietonsa ovat nyt suojaamattomana internetissä, ja riski tietojen joutumiseen vääriin käsiin on suuri (Lapinkangas 2023).

Vastaamon tapaus on saanut runsaasti julkisuutta, koska uhrien määrä on suuri. Yksittäisiä tietomurtojen uhrien tarinoita näkee harvemmin mediassa. Syynä voi olla myös uhrien kokema häpeä tapahtuneesta. Tietoturvayhtiö F-Secure kertoo rikollisten salaisen aseen olevan häpeä: kun uhri ei uskalla puhua tapahtuneesta, saa pahantekijä näin työrauhan (Linnake 2022).

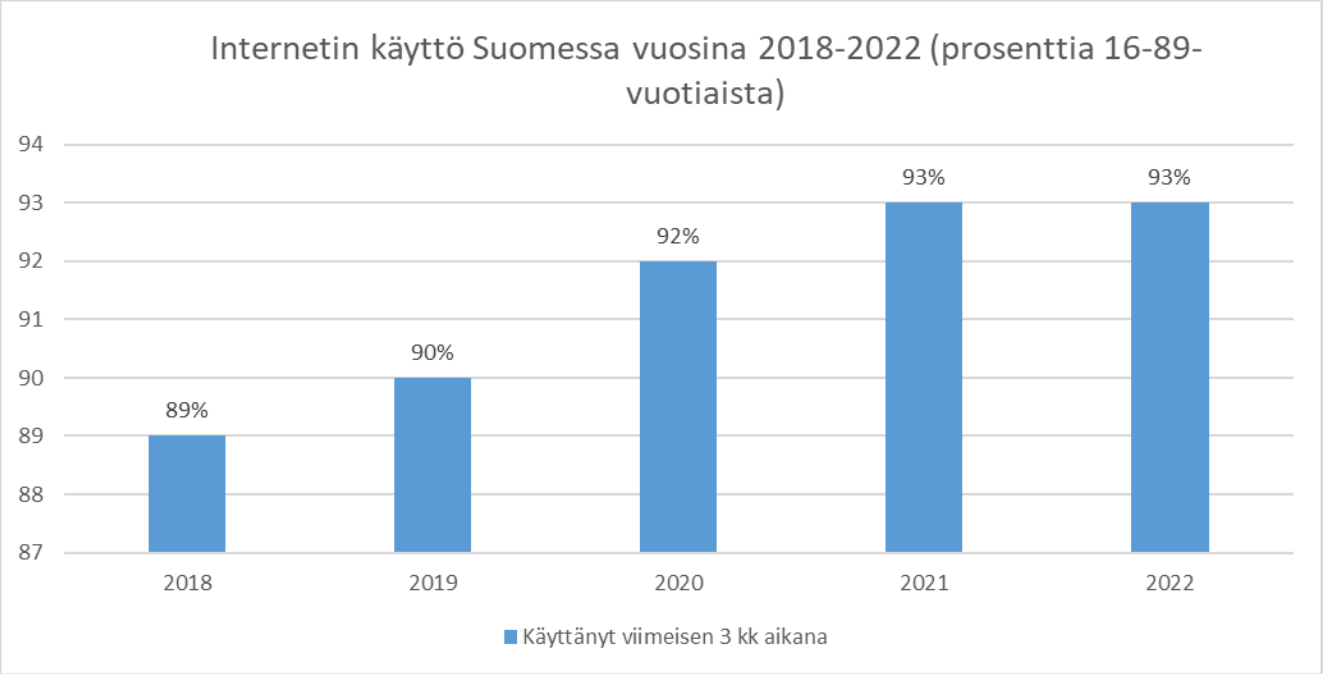


KUVIO 1. Pankkien tietoon tulleet huijaukset 01–06 / 2022 ja 2023 (mukaillen Palmgren 2023)

Finanssiala ry keräsi pankeilta tietoa huijausten ja petosten määristä, joissa pankit ovat niitä onnistuneet estämään. Vuoden 2023 tammi–kesäkuussa olivat pankit estäneet 15,9 miljoonan euron edestä huijauksia. Luvussa on mukana myös petoksella viedyt rahat, jotka pankit olivat saaneet palautettua asiakkaille. Vuoden 2022 lukuihin verrattuna, on tämä määrä yli kaksinkertaistunut. (Palmgren 2023.) Verkkohuijausten voidaan siis olettaa jatkavan kasvuaan tulevaisuudessa.

3.1 Yksilön kyberturvallisuus

Matkapuhelimia käytetään niin runsaasti verkkoselailuun, että haittaohjelmilta ja muilta uhilta on vaikeaa välttyä. Matkapuhelinta käytetään moniin muihin tarkoituksiin varsinaisen kommunikaation lisäksi ja se voi sisältää meistä paljon henkilökohtaista tietoa. (Kyberturvallisuuskeskus 2014.) Verkossa käytettävien laitteiden suojaaminen ja ohjelmistopäivitysten pitäminen ajan tasalla on tärkeää, mutta myös käyttäjän varsinaisiin toimiin kybermaailmassa tulisi suhtautua vakavasti.



KUVIO 2. Internetin käyttö Suomessa vuosina 2018-2022 (mukaillen Tilastokeskus, 2022)

Tilastokeskuksen teettämän Väestön tieto- ja viestintätekniikan käyttö -tutkimuksen mukaan 16–89-vuotiaista suomalaisista vuonna 2022 internetiä oli käyttänyt 93 prosenttia viimeisen kolmen kuukauden aikana (Tilastokeskus 2022). Ajan trendi on, että yhä useammat palvelut siirtyvät verkkoon ja käyttäjät palveluiden mukana myös.

Liian helpot salasanat ja monivaiheisen tunnistautumisen laiminlyönti voivat aiheuttaa suuriakin vahinkoja tietomurron sattuessa. Identiteettivarkauksien määrä on poliisin mukaan kasvanut merkittävästi vuodesta 2021. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus kertoo saavansa viikoittain tietoonsa toista sataa huijausta, tietojenkalastelua tai niiden yritystä. Suurin osa näistä on verkkopankkitunnuksien kalasteluyrityksiä ja myös sosiaalisen median huijauksia tulee Kyberturvallisuuskeskuksen tietoon päivittäin. Sometilin kaappaamisella voi olla yllättäviäkin vaikutuksia. Meri-Lapin eläinsuojeluyhdistyksen Facebook-tili joutui kaappauksen uhriksi. Tämän vuoksi yhdistys joutui luomaan uuden sometilin ja se myös menetti kaappauksen vuoksi tuhansia seuraajia. Facebook-tilin kaappauksen vuoksi myös löytöeläinten adoptioiden määrä väheni, kun yhdistys ei enää pystynyt lisäämään kotia etsiviä eläimiä sivuilleen. Yhdistys havaitsi pian, että seuraajien takaisinsaaminen yhdistyksen Facebook-tilille on haastavaa. (Koskinen 2023.) Sosiaalisessa mediassa työkseen sisällöntuotantoa tekevien määrä kasvaa vauhdilla ja heille tietomurto voi olla kohtalokas, kun kovalla työllä hankitut seuraajat

eivät löydäkään takaisin sisällöntuottajan sivuille. Sisällöntuottajille seuraajien määrä on ratkaisevassa asemassa mm. palkkioiden määrää tarkasteltaessa.

Aiemmin suomenkieliset huijaukset olivat kömpelösti kirjoitettuja ja näin niitä oli helpompi tunnistaa. Verkkorikolliset ovat kuitenkin kehittyneet tällä osa-alueella ja huijausten kieliasu on jo niin hyvää, ettei sen perusteella voi tehdä johtopäätöksiä viestin oikeellisuudesta. Tekstiviestihuijauksissa uhria hämää myös helposti viestin tuleminen samaan viestiketjuun, johon aidot viestit ovat aiemmin tulleet.

3.2 Fyysiset tekijät tietoturvassa

Käyttäjä voi vaikuttaa merkittävästi tietoturvaansa myös fyysisten tekijöiden osalta. Yksi konkreettinen fyysinen tietoturvauhka laitteelle on sen katoaminen. Laitteen katoamisen ja varkauden estämiseksi huolellinen laitteen säilytys on tärkeää. Mikäli laitteen tietojen varmuuskopiointi on laiminlyöty, on todennäköistä, että kaikki laitteen sisältämät tärkeät tiedot menetetään laitteen kadotessa.

Mikäli laite pääsee kuitenkin häviämään, voi pilvipalveluiden avulla käyttää puhelimen etähallintaa ja puhelin voidaan näin paikallistaa. Etähallinnan avulla voidaan myös puhelin lukita, jottei ulkopuolinen henkilö voi sitä käyttää. Puhelimen tyhjentäminen on myös tarvittaessa mahdollista etähallinnan kautta. (Kyberturvallisuuskeskus, 2014.)

Elektroniikalle säilytysolosuhteet ovat myös tärkeitä, ne tulisi säilyttää vain kuivassa ja huoneenlämmössä. Tietokone olisi hyvä säännöllisesti puhdistaa vähintään pintapuolisesti ja varmistaa etteivät tietokoneen tuuletusaukot tukkeudu. Tietokoneisiin kulkeutuu ajan kanssa pölyä mm. tuulettimen ympärille, siksi kone tulisi ajoittain puhdistaa myös sisältä. Mikäli käyttäjällä ei siihen ole osaamista, on tähän erikoistuneiden palveluntarjoajien käyttö suositeltavaa. Mikäli tietokoneen puhdistuksen laiminlyö, voi siitä aiheutua laitteelle vauriota, jolloin tärkeitä tietoja voidaan menettää. Tulipalon tai muun vastaavan katastrofin varalta olisi tärkeää säilyttää varmuuskopiot muualla kuin alkuperäisen tiedoston kanssa samassa sijainnissa tai pilvipalveluissa.

Uuden laitteen hankkimisen myötä jää käyttäjälle yleensä vanha laite turhaksi. Laitetta hävitettäessä on hyvä muistaa tietoturvan osalta, ettei pelkkä laitteen tietojen poistaminen riitä. Myöskään käyttöjärjestelmän poistaminen ei ole riittävä toimenpide, eivätkä edes tehdasasetusten palautus välttämättä poista

kaikkia laitteessa olleita tietoja. (YLE 2018, 08:59.) Toimivan laitteen voi myös myydä, tällöin on tärkeää viedä toimiva laite yritykselle, joka on erikoistunut käytettyjen laitteiden jälleenmyyntiin. Yritys huolehtii laitteen jälleenmyynnin tietoturvallisesti. Tällöin laitteen muistille tehdään tyhjennys ylikirjaamisen avulla, jolloin laitteen tiedot eivät voi joutua vääriin käsiin. Paras vaihtoehto käyttökelvottomalle laitteelle on kierrätys.

Asianmukaisesti tehtynä kierrätys on ympäristöteko. Tietotekniikan keskusliiton FiCom ry:n mukaan matkapuhelimen materiaaleista jopa 99 % on kierrätettäviä. Samalla saadaan arvokkaita metalleja uusiokäyttöön ja kierrätyksen ansiosta ympäristöhaitat, kaivostoiminta ja energiankulutus vähenevät. (Laine 2020.)

Muiden kuin omien USB-laitteiden käytössä piilee riskejä. USB-muistitikku voi sisältää haittaohjelmia ja myös USB-latureihin ja välijohtoihin on mahdollista sisällyttää haittaohjelmia. Tämän vuoksi esimerkiksi ulkomaanmatkoilla tulisi käyttää vain omia USB-laitteita tietoturvasyistä. (Järvinen 2018, 311.)

Webkameran kautta voivat verkkorikolliset saada tietoon henkilökohtaisia tietoja ja arkaluontoista kuvamateriaalia. Lisäksi hyökkääjät voivat käyttää hyvälaatuista kasvokuvaa kirjautumiseen kasvojentunnistuksen avulla. Webkameroiden ja kannettavien tietokoneiden kiinteiden kameroiden osalta olisi järkevää peittää kameran linssi aina kun kameraa ei käytetä. Tämä on ainut tapa varmistua, ettei kameraa käytetä ilman käyttäjän suostumusta. Kameran peittämiseen on saatavissa erillisiä siihen tarkoitettuja sulkijoita. Joissain kannettavissa tietokoneissa on myös sisäänrakennettu kameran sulkija. Jos näitä vaihtoehtoja ei löydy, olisi suositeltavaa käyttää vähintään tarraa tai laastaria kameran peittämiseen.

Huolimaton salasanojen hallinta muodostaa myös riskin. Käyttäjä saattaa säilyttää salasanoja laitteiden läheisyydessä niin, että kuka tahansa laitteen käsiinsä saava voi saada salasanat haltuunsa. Yksi ongelmallinen salasanojen säilytystapa on puhelimen tiedostoissa. Vaikkakin se on käytettävyyden kannalta kätevä paikka säilyttää salasanoja, jotta ne ovat aina helposti saatavilla, muodostuu tässä suuri riski salasanojen joutumiselle vääriin käsiin. Puhelin voidaan varastaa ja näin menettää kirjautumistiedot, mikäli laitteen omistaja on laiminlyönyt vielä puhelimen lukituskoodin asettamisen. Henkilökohtaisten salasanojen luovutus toiselle henkilölle on aina myös riski.

3.3 Älylaitteet

Tässä tutkimuksessa älylaitteella viitataan elektroniikkaan, joka on mahdollista yhdistää internetiin. Myös Bluetooth-laitteet kuuluvat tähän kategoriaan, koska Bluetoothin avulla laitteet voivat muodostaa yhteyden eri laitteiden välillä. Bluetooth voi tiedonsiirtotekniikkana aiheuttaa tietoturvariskin, jos käytettävä laite on vanha ja päivittämätön (Kyberturvallisuuskeskus 2020). Laitetta ei tulisi liittää tuntemattomaan Bluetooth-laitteeseen. Jos käyttäjä yhdistää vihamieliseen laitteeseen omansa Bluetoothin avulla, pääsee verkkorikollinen käyttäjän laitteeseen käsiksi, vaikka laitteen tietoturvapäivitykset olisivatkin kunnossa (Kyberturvallisuuskeskus 2020). Kalifornian yliopiston tutkimuksessa todetaan, että Bluetooth-laitteiden signaalien avulla voidaan laitteita yksilöidä ja seurata. Tutkijat olivat onnistuneet kehittämään algoritmin, jonka avulla pystyttiin määrittämään Bluetooth-signaaleille yksiköllinen ”sormenjälki”. Sen avulla laitetta pystyttiin seuraamaan. Signaalin yksilöiminen ei ole helppo toteuttaa, lisäksi asiaan vaikuttaa ympäristön olosuhteet, esimerkiksi lämpötilan vaihtelut. Myös Bluetooth-signaalien voimakkuus vaihtelee laitteitten takia, näin ollen signaalin seuraamiseen mahdollistava välimatka vaihtelee. Tutkijat havaitsivat myös, että osa laitteista lähettää Bluetooth-signaalia, vaikka Bluetooth olisi laitteessa kytkettynä pois päältä. Tällöin ainoa tapa lopettaa Bluetooth-signaalien lähetys laitteessa, on koko laitteen sammuttaminen. (Kailio 2022.)

IoT- laitteet tarjoavat käyttäjille arjen mukavuutta ja helpotusta moneen arkiseen ongelmaan. Ne kasvattavat jatkuvasti suosiotaan ja uusien käyttökohteiden määrä vain jatkaa kasvuaan. Mikä tahansa fyysinen laite on muunneltavissa IoT-laitteeksi, jolloin se voidaan yhdistää internetiin. (Empirica Finland Oy.) IoT-laitteita kutsutaan myös älylaitteiksi. Älylaitteet ovat helpottaneet elämäämme merkittävästi, kun laitteita on mahdollista hallita etänä. Näin voi esimerkiksi kesämökin lämmitysjärjestelmän kytkeä päälle etänä tarvittaessa. Tai robotti-imurin voi työpaikalta käsin ohjata aloittamaan imurointi, jotta koti on imuroitu kotiin tultaessa. Myös talotekniikkaa on saatavilla ns. älykkäänä mallina, jolloin voidaan älytekniikan avulla säästää asumiskustannuksissa ja parantaa asumismukavuutta (Järvinen 2018, 350).

Älylaitteilla on kuitenkin haavoittuvuutensa, sillä mikä tahansa verkkoon liitetty laite on potentiaalinen kohde hakkeroinnille. Käyttäjän yksityisyydensuoja on suuressa vaarassa, jos kodin kameravalvontajärjestelmä joutuu hyökkääjän käsiin. Hakkereita kiinnostavat muut kodin älylaitteet mm. siksi, että ne voidaan valjastaa osaksi palvelunestohyökkäystä (Yle 2018, 00:38). Näin älyjääkaappi tai robotti-imuri

voivat olla valjastettuna hyökkääjän omiin käyttötarkoituksiin. Palvelunestohyökkäyksille on olennaista niiden onnistumisen kannalta, että kaapattuja laitteita on määrällisesti paljon mukana hyökkäyksessä.

Puettavat älylaitteet toimivat älypuhelimien jatkeena. Ne kulkevat mukanamme kaikkialle samalla keräten meistä valtavan määrän dataa: terveystietoja, sijaintitietoja ja jopa taloudellisia tietojamme, jos laitteella on mahdollista suorittaa maksuja. Niillä saa pääsyn tarvittaessa sähköpostiin ja tekstiviesteihin sekä moniin muihin puhelimen sovelluksiin. Näistä henkilökohtaisista tiedoista voidaan väärissä käsissä muodostaa yksityiskohtaista tietoa esim. päivärutiineista. Näin hyökkääjä voisi uhrin älykellon tiedoista päätellä hyvinkin tarkasti, milloin tämä käy pyörälenkeillä, missä liikkuu ja milloin yleensä kotiutuu.

3.4 Avoimet langattomat verkot

Avoimet langattomat verkot eli Wi-Fi-verkot avaavat uusia mahdollisuuksia kyberhyökkäyksille. Avoimia langattomia verkkoja on käytettävissä yleensä julkisissa tiloissa, kuten kirjastoissa, kahviloissa, lentokentillä ja ostoskeskuksissa. Ne tarjoavat ilmaisen pääsyn verkkoon ja ovat helposti käytettävissä. Ongelmana avoimissa verkoissa on, että kenellä tahansa verkkoon liittyneellä on pääsy kaikkeen verkossa liikkuvaan dataan. (Waschke 2017, 9.) Salasanalla suojattuun Wi-Fi-verkkoon ei myöskään ole luottaminen, koska yleensä Wi-Fi-verkkojen salasana on kaikkien sitä pyytävien saatavilla.

Heikoilla salasanoilla tai muuten heikosti suojatut kodin langattomat verkot ovat myös alttiita hyökkäyksille. Verkkorikollinen voi liikkua naapurustossa kannettava tietokone mukanaan ja näin havaita avoimia suojaamattomia kodin verkkoja. Sopivan verkon löydettyään, hakkeri voi seurata Wi-Fi-verkon liikennettä tai käyttää kyseistä verkkoa hyökkäysalustana verkkohyökkäyksissä. (Waschke 2017, 9.)

Vaikka käyttäjä tunnistaisi Wi-Fi-verkkojen uhat, voi käyttäjän laite muodostaa tietoturvauhan. Useat älypuhelimet on asetettu oletuksena hakemaan Wi-Fi-verkkoja ja myös liittymään niihin. Laitteen käyttäjä voi huomaamattaan olla yhdistyneenä Wi-Fi-verkkoon ja näin luulla käyttävänsä turvallisesti verkkoa laitteellaan. Käyttäjän laite voi olla yhdistyneenä verkkorikollisen saastuttamaan avoimeen

langattomaan verkkoon ja näin ollen verkkorikollinen pääsee käsiksi käyttäjän verkossa liikuttamaan dataan.

Ratkaisuna Wi-Fi-verkon turvattomuuteen on käyttää VPN-palvelua. VPN tulee sanoista Virtual Private Network eli virtuaalinen erillisverkko. VPN:n avulla tiedonsiirto on turvallista, koska siinä tieto kulkee ikään kuin salattua putkea pitkin. Käyttäjän data kulkee tässä putkessa suojatulle palvelimelle ja tämän jälkeen sivustolle jonne käyttäjä oli menossa. VPN-palvelu piilottaa käyttäjän IP-osoitteen ja sen avulla voidaan valita käyttäjälle virtuaalisijainti ympäri maailmaa. VPN-palvelu estää siis käyttäjän seurannan ja mahdollistaa Wi-FI-verkon turvallisen käytön, koska dataliikenne ei näy verkkorikollisille. (Kaspersky 2023.)

Kodin langattoman verkon suojaaminen on myös tärkeää. Huomioitavia asioita ovat kodin verkon oletusnimi ja salasana. Ne suositellaan vaihdettavaksi sellaisiksi, jotka vain käyttäjä tietää. Verkon nimessä eli SSID:ssä ei kannata käyttää mitään sanoja, joilla ulkopuolinen voisi arvata, kenen verkko on kyseessä tai missä se sijaitsee. Langattoman verkon salaustekniikka on yleensä verkkolaitteissa valmiiksi asetettuna parhaaksi mahdolliseksi. Se on kuitenkin hyvä varmistaa itse, suositeltava vaihtoehto on WPA2 tai sitä uudemmat tekniikat. Vanhojen verkkolaitteiden käyttöä tulee välttää ja vaihtaa laite säännöllisesti uuteen. Kotiverkon reitittimen tai modeemin hankinnassa on hyvä muistaa, ettei halvin ole välttämättä paras tai turvallisin. On järkevää hankkia laite tunnetulta valmistajalta, jotta päivityksiä ja tukea on saatavilla pidempään. (Laaksonen 2018.)

Kodin verkko olisi järkevää jakaa erillisiin osioihin. Yksi osio verkosta olisi tietokoneille, toinen kodin muille älylaitteille ja kolmannen voisi osoittaa vierasverkoksi (Laaksonen 2018). Tietoturvan kannalta verkkojen eristäminen toisistaan on tärkeää, jotta mahdollinen verkon tunkeilija ei pääse kaikkiin verkon laitteisiin käsiksi. Tällainen ratkaisu olisi järkevää toteuttaa, mutta monella kotiverkon käyttäjällä tietotaito ei välttämättä riitä erillisten verkkojen toteutukseen. Apuna voi käyttää verkosta löytyviä oppaita, tai tietoverkkoyhteyksien ammattilaisia, jotka voi tilata kotiin tekemään asennuksen oikein.

3.5 Sääntely ja lait verkonkäyttäjän turvana

Huijauspuhelut alkoivat lisääntyä Suomessa 2020-luvulla. Nämä puhelut ovat petoksia, joiden avulla rikolliset yrittävät päästä käsiksi uhrien pankki- ja henkilötietoihin, salasanoihin, käyttäjätunnuksiin ja muihin luottamuksellisiin tietoihin. Kyberturvallisuuskeskukseen raportoitiin lyhyessä ajassa useista

Microsoftin teknisen tuen nimissä tehdyistä huijauspuheluista 2020-luvun alussa. Näiden puheluiden motiivina oli päästä uhrin käyttämään tietokoneeseen kiinni etäyhteyden avulla. (F-Secure.) Huijarit ovat voineet esiintyä myös viranomaisina, sijoittajina, pankkivirkailijoina tai muina tahoina. Lisäksi rikollisilla on monia muita puhelimitse tapahtuvia hyökkäystekniikoita käytössään. Yksi tapa saada suomalainen uhri vastaamaan huijauspuheluun, on suomalaisen puhelinnumeron kaappaus ulkomailta. Näin uhri uskaltaa helpommin vastata puheluun, joka näyttää tulevan suomalaisesta numerosta.

Teleoperaattori Elisan mukaan vuonna 2021 sen verkossa jopa 80 prosenttia ulkomailta tulleista puheluista suomalaisiin puhelinliittymiin oli huijauspuheluita. Elisa aloitti omista puhelinnumeroistaan tulevien huijaussoittojen suodattamisen elokuussa 2021. Operaattori tunnisti ulkomailta tulevan soiton olevan väärennetty ja korvasi soittajan numeron tuntematon soittaja- tiedolla. Tällä toimenpiteellä oli tarkoitus saada puhelun vastaanottaja varovaiseksi. Elisa ei kuitenkaan voinut vaikuttaa muiden operaattoreiden numeroista tulleisiin puheluihin. Lokakuussa 2023 Suomen teleoperaattorit ottivat käyttöön tekniikan, jolla pyritään estämään ulkomailta tulevia huijaussoittoja. Nopeasti tämän tekniikan käyttöönoton jälkeen oli havaittavissa, että tekniikka tehosi huijaussoittoihin. Ne vähenivät merkittävästi, sillä rikolliset havaitsivat nopeasti, ettei huijauspuheluita saatu enää läpi Suomen verkkoon. (Kärkkäinen & Linnake 2023.) Uuden huijauspuheluiden estävän teknologian ansiosta rikollisten saama taloudellinen hyöty väheni merkittävästi. Vuosina 2020 ja 2021 verkkorikolliset saivat näiden huijauspuheluiden avulla taloudellista hyötyä suomalaisilta 7,1 miljoonalla eurolla. Ulkomailta tulevien huijaussoittojen estävän tekniikan ansiosta rikollisten saama taloudellinen hyöty putosi alle 3 000 euron. (Stubin 2023.)

Verkkopalvelut kasvavat niin vauhdilla, että lainsäädännön on haastavaa seurata ajantasaisilla lakipykälillä perässä. Uusia keinoja internetjättien rajoittamiseen on kuitenkin jo kehitetty. Euroopan unioni on ryhtynyt toimiin verkon käyttäjien suojelemiseksi verkon uhilta. Sen kehittämä uusi laki digitaalisista palveluista tuo palveluille merkittävää luotettavuutta ja läpinäkyvyyttä. Se lisäksi antaa valtaa kuluttajille, lisää verkossa alaikäisten yksityisyydensuojaa, ja pakottaa mm. sosiaalisen median palveluita moderoimaan paremmin sisältöään. Lisäksi uusi laki velvoittaa, ettei mainoksia voida enää kohdentaa arkaluontoisen datan, kuten poliittisen mielipiteen tai seksuaalisen suuntautumisen perusteella. Laki myös määrittää mainonnan osalta, ettei lapsille saa enää kohdentaa mainontaa. (Ahosola 2023.)

Ison tietoturvariskin aiheuttavat verkkolaitteiden puute uusista ohjelmistopäivityksistä, sillä tuotteisiin ei aina sisälly päivitysmekanismia. On myös yleistä, että päivitykset päättyvät ennen kuin laitteen käyttöikä tulee täyteen. Ongelmaan on tulossa muutos vuonna 2024, kun EU ottaa käyttöön tietoturva-

vaatimukset älylaitteille sääntelyllä. Sen ansiosta voidaan poistaa myynnistä tietoturvavaatimusten vastaiset laitteet. Jatkossa eri toimijoiden tulee ottaa tietoturvavaatimukset vakavasti. Valmistaja vastaa, että tuote täyttää tietoturvan osalta sitä koskevat vaatimukset. Maahantuojat ja myyjät puolestaan vastaavat, että myynnissä olevat tuotteet ovat vaatimustenmukaisia. (Kyberturvallisuuskeskus 2023.)

4 LAAJEMPIA TIETOTURVAUHKIA

Kyberturvallisuutta tutkittaessa, on tärkeää tarkastella yksilön toimien vaikutuksia laajempaa turvallisuustilannetta ajatellen. Verkkorikollisia kiinnostavat verkon käyttäjien henkilötietojen lisäksi verkon laitteet, joita rikolliset käyttävät hyväksi palvelunestohyökkäyksissä. Näin käyttäjän kotiverkko ja sen laitteet voivat olla osana verkkohyökkäystä. (Järvinen 2018, 351.) Verkkoon kytketty suojaamaton laite voi mahdollistaa myös ulkomaisen vakoilun (Joukanen 2023). Näin ollen, ei yksilön osuutta kansallisessa turvallisuudessa tule väheksyä.

4.1 Kybermaailma sodankäynnin osana

Kybermaailmassa sodan käsite ei ole yksiselitteinen. On mahdollista, että valtiot tekevät kyberhyökkäyksiä ja saavuttavat näin poliittisia tavoitteitaan ilman, että varsinaiseen fyysiseen sodankäyntiin on tarvetta. Kyberhyökkäys ainoana hyökkäyksenä ei vielä välttämättä aloita varsinaista sotaa, mutta toimet bittien maailmassa voivat johtaa fyysiseen konfliktiin, jossa käytetään hyväksi fyysisen voimankäytön lisäksi kybermaailman vaikutuskeinoja. Koska tänä päivänä maailma on tiiviisti verkottunut internetin ansiosta, voi suurilla kyberhyökkäyksillä olla vaarallisia sivu- ja seurannaisvaikutuksia myös hyökkääjämaalle itselleen. Tämä hillitsee kyberkykyjen käyttämistä. Psykologinen sodankäynti on tärkeä osa sodankäyntiä, sillä sen avulla voidaan vaikuttaa päättäjiin ja kansalaisiin pitemmällä aikavälillä. (Limnéll ym. 2014, 147–148.)

Kybermaailma mahdollistaa psykologisen ulottuvuuden hyödyntämisen tehokkaasti. Informaatiovaikuttamisella pyritään vaikuttamaan ihmisten mielikuviin ja mielipiteisiin. (Tuhkanen 2022.) Informaatiovaikuttaminen ei ole uusi ilmiö: vieraan valtion kansalaisiin on pyritty vaikuttamaan niillä keinoilla, jotka ovat olleet kullekin aikakaudelle tyypillisiä (Järvinen 2018, 179). Digitalisaation myötä arkeemme on muodostunut paljon erilaisia kanavia, joiden avulla ihmisiä on helpompi lähestyä erilaisilla sanomilla.

On tärkeää, ettei kansalainen jaa väärää tietoa. Väärän tiedon jakaminen tukee informaatiovaikuttamista, jolla vihollinen yrittää vaikuttaa kohteeseensa. Lähdekritiikki onkin tärkeä osa päivittäistä elämäämme. Sosiaalisessa mediassa on vielä helpompi jakaa haluamaansa sanomaa isoille massoille. Pelkkä sosiaalisen median julkaisusta tykkääminen lisää julkaisun näkyvyyttä ja julkaisun jakaminen

tai kommentointi ovat nekin tehokkaita keinoja lisätä näkyvyyttä. Kansalainen voi tietämättään olla mukana informaatiovaikuttamisessa jakamalla julkaisua eteenpäin. Informaatiosodassa ei pyritä pelkästään levittämään tekstiä ja puheita, vaan yhtä lailla tarkoituksena on levittää kuvia ja videoita. (Tuhkanen 2022.)

Yksi informaatiovaikuttamisen metodi on tehdä uskottavia valeuutisia, joissa usein sekoittuvat fakta ja fiktio. Deepfake-tekniikassa pyritään saamaan aikaan tekoälyn ja kuvien avulla mahdollisimman aidolta vaikuttava video, jonka avulla pyritään vaikuttamaan videon yleisöön. (Järvinen 2018, 371–374.) Deepfake-tekniikalla toteutetut videot ovat jo niin taitavasti toteutettuja, että on välillä vaikeaa erottaa keinotekoisesti tuotettuja videoita oikeista. Tätä teknologiaa olisi mahdollista käyttää myös moneen yleishyödylliseen tarkoitukseen, mutta se on saanut negatiivista huomiota varsinkin valeuutisten levityksessä. (YLE 2023.) Deepfake-teknologia kehittyy jatkuvasti ja sen osalta uusia uhkia tullaan näkemään tulevaisuudessa. Joidenkin arvioiden mukaan kohta emme voi enää varmuudella tietää, edes videopuhelun aikana, onko puhelun vastapuoli todellinen henkilö. (Kullas 2022.) On siis ilmeistä, ettei voida loputtomiin olettaa, että yksilö pysyy kehityksen mukana ja tunnistaa huijaukset parhaansa mukaan. Huijausten torjuntakeinojen on pakko kehittyä myös.

4.2 Yksilön osuus kansallisessa turvallisuudessa

Suojelupoliisi kertoo havainneensa autoritaaristen valtioiden käyttävän suomalaisten verkkolaitteita ja palvelimia kybervakoiluoperaatioissaan. Kybervakoilu on tehokas keino saada luottamuksellista tietoa kybervakoilun kohdemaasta. Esimerkiksi kotireitittimen haltija voi mahdollistaa ulkomaisen vakoilun omalla huolimattomuudellaan: laiminlyömällä laitteen suojauksen ja ohjelmistopäivitykset. Suojelupoliisin mukaan erityisesti kotireitittimet muodostavat tällä hetkellä suuren riskin kansallista turvallisuutta ajatellen. (Suojelupoliisi.) Käytännössä verkkorikolliset käyttävät kansalaisen verkkolaitetta tunkeutuakseen Suomen tietojärjestelmiin (Joukanen 2023). Natoon liittymisen jälkeen Suomeen on kohdistunut nelinkertainen määrä kiristyshaittaohjelmaiskuja, kertoo ylijohtaja Sauli Pahlman Traficomin Kyberturvallisuuskeskuksesta (Heleskoski 2023). Kiristyneen ulkopoliittisen tilanteen vuoksi on suomalaisten syytä suhtautua tietoturvaan entistä suuremmalla vakavuudella.

5 IHMINEN – HEIKOIN LENKKI VAI VOIMAVARA?

Jokaisen tietomurron -tai vuodon taustalla on aina tekninen tai inhimillinen virhe. Tyypillinen tekninen virhe on ohjelmointivirhe verkkopalvelussa, josta aiheutuu haavoittuvuus. Vaikkakin haavoittuvuudet ovatkin kalliita ja hitaita korjata, ovat ne kuitenkin korjattavissa etsimällä virhe, korjaamalla se ja etsimällä kaikki haavoittuvat järjestelmät sekä päivittämällä ne. Inhimillisten virheiden korjaaminen aiheuttaa enemmän haasteita. Käyttäjät mm. sortuvat käyttämään samoja salasanoja eri palveluissa, availevat sähköpostitse tulleita liitetiedostoja huolettomasti, avaavat verkosta peräisin olevia Office-dokumentteja ja klikkaavat dokumentin kohdasta ”Ota sisältö käyttöön”, sillä dokumentti itsessään näin neuvoo tekemään. Koska ihmisaivoihin ei ole olemassa päivityspakettia, on koulutus ainoa tapa päivittää ihmisten osaamista. (Hyppönen 2021, 102.)

Tietoturvayhtiö F-Secure teki kenttäkokeen, jossa pystytettiin Wi-Fi Hotspot -palvelu Lontoon keskustaan. Se oli Wi-Fi-verkko, johon sai liittyä kuka tahansa ilmaiseksi, jos hyväksyi verkon käyttöehdot. Käyttäjät liittyivät verkkoon ja saivat ennen liittymistä käyttöehdot luettavaksi. Ne oli kirjoitettu tiheän lakitekstin tavoin, kuten käyttöehdot yleensä kirjoitetaan. Näiden käyttöehtojen loppupuolella oli kuitenkin poikkeuksellinen teksti: (Hyppönen 2021, 137.)

> SAADAKSESI KÄYTTÖOIKEUDEN TÄHÄN LANGATTOMAAN VERKKOON SINUN PITÄÄ LUOVUTTAA VANHIN LAPSESI F-SECURE OYJ:LLE. TÄMÄ PITÄÄ TEHDÄ HETI, KUN YRITYS PYYTÄÄ SITÄ. JOS SINULLA EI OLE LAPSIA, OTAMME RAKKAIMMAN LEMMIKKIELÄIMESI LAPSEN SIJAAN. TÄMÄ EHTO ON VOIMASSA MAAILMANLOPPUUN ASTI. (Hyppönen 2021, 137.)

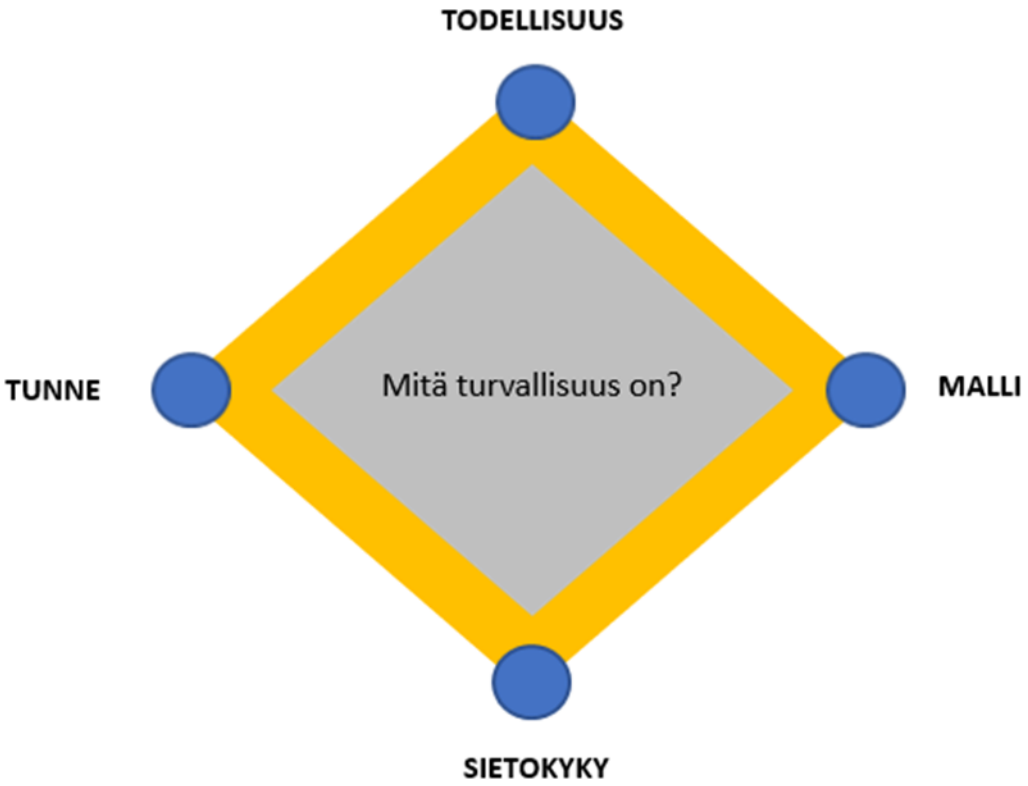
Verkkoon liittyi satoja käyttäjiä erikoisista käyttöehdoista huolimatta (Hyppönen 2021, 137). On siis selvää, etteivät käyttäjät lue käyttöehtoja. Mikäli haluamme palvelun käyttöömme, emme enää sen käyttöönottovaiheessa juurikaan mieti seuraamuksia. Kun asiasta tulee arkipäiväinen, uskallamme helpommin toimia huolettomasti.

Jos koulutus olisi ratkaisu kaikkien inhimillisten virheiden poistamiseen, olisi meillä täysin erilaiset turvallisuusnäkymät ihmisten käyttäytymisen osalta. Käyttäjät jatkavat esimerkiksi sähköpostiliitteiden availua riippumatta koulutuksen määrästä. Koulutusta on myös vaikeaa järjestää niin, että kaikilla kansalaisilla olisi tasapuoliset mahdollisuudet siihen osallistua. Voidaanko olettaa, että käyttäjillä tulisi olla loputon vastuu verkossa toimimisesta? Ratkaisuna voisi olla siirtää vastuuta tietoturvasta eri osapuolille:

käyttöjärjestelmien tekijöille, ohjelmistoyrityksille, tietoturvayrityksille ja operaattoreille. (Hyppönen 2021, 103.)

5.1 Turvallisuus on tunne

Kyber- ja tietoturvallisuudessa on pohjimmiltaan kyse turvallisuudesta. Turvallisuus on subjektiivinen kokemus, ei ole olemassa yksiselitteistä kuvausta turvallisuudelle. Jokainen myös kokee turvallisuuden omalla tavallaan: sama turvallisuusuhka voi toisessa yksilössä aiheuttaa paljon vahvemman turvattomuuden tunteen kuin toisessa. Turvallisuus koostuu useasta tekijästä: tunteesta, opituista malleista, todellisuudesta sekä kyvystämme sietää häiriö- ja kriisitilanteita. Turvallisuus on tunnetila, joka vaihtelee yksilön kokeman tilanteen mukaan. Todellisuus on merkittävä tekijä turvallisuudessa, se kertoo, miten asiat ovat ympärillämme ”kylminä faktoina”. Oppimamme arvot ja mallit ohjaavat meitä, kun arvioimme turvallisuutta ja annamme sille painoarvoa. Häiriö- ja kriisitilanteiden sietokyky eli resilienssi määrittää sen, kuinka reagoimme häiriötilanteisiin. Hyvän sietokyvyn avulla häiriöistä selvitään ilman paniikkiin menemistä. (Limnéll ym. 2014, 34–35.)



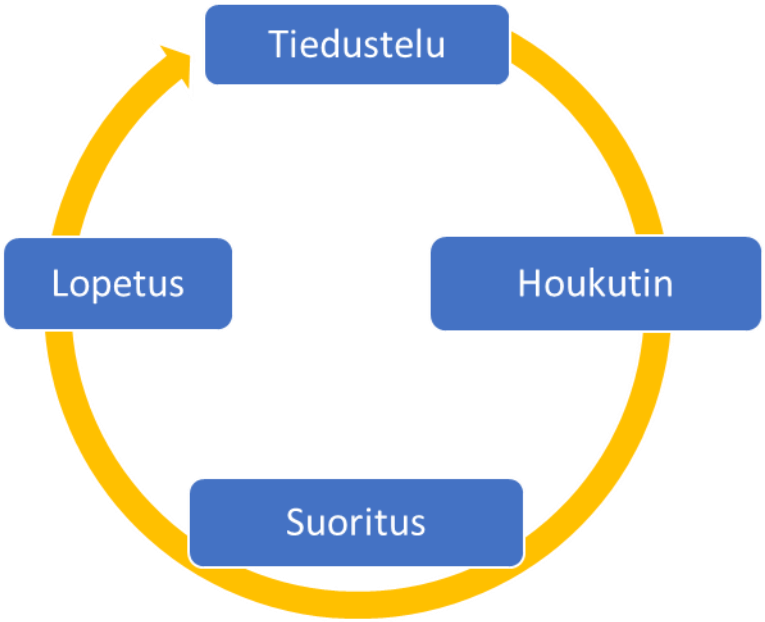
KUVIO 3. Mitä turvallisuus on? (mukaillen Limnéll ym. 2014, 36)

Nykyhetkeä tarkasteltaessa, varsinkin sietokyvyn voidaan todeta heikentyneen. Riippuvuutemme tämän päivän mukavuuksista ja bittien maailmasta on saanut aikaan sen, että jo lyhyt sähkökatko voi saada aikaan suurtakin vaikutusta arkiseen toimintaamme. Pahimmillaan yhteiskunnan toiminnot voivat pysähtyä kokonaan sähkökatkon seurauksena. Sata vuotta takaperin, sen ajan yhteiskunta tuskin olisi lamaantunut sähkökatkon vuoksi, vaan olisi jatkanut toimiaan ilman suurempaa vaikutusta.

Todellisuus muuttuu jatkuvasti alati muuttuvan kybermaailman ohella. Todellisuuden ymmärtäminen on ensiarvoisen tärkeää, jotta turvallisuuden tunteemme ei ole vääriin oletuksiin perustuva. Vain oikealla todellisuuden ymmärryksellä voidaan vahvistaa sietokykyä ja luoda turvallisuutta kehittäviä malleja. (Limnéll ym. 2014, 36.) Tunteisiimme vedotaan jatkuvasti mediassa, tunteita synnyttämällä ihmiseen voidaan hyvin vaikuttaa. Ei ole väliä, perustuuko käsityksemme ja pelkomme kuviteltuihin vai todellisiin uhkiin, joka tapauksessa käsitykset ja pelot ohjaavat käyttäytymistämme ja vaikuttavat suuresti hyvinvointiimme. Jos turvallisuutta halutaan kasvattaa, tulee kaikissa neljässä turvallisuuden osa-alueessa tapahtua kehitystä (Limnéll ym. 2014, 36).

5.2 Social engineering

Vahvan salasanan murtaminen on haastavaa. Hyökkääjä pyrkii siis saamaan sen suoraan käyttäjältä. (Waschke 2017, 12.) Hyökkääjä voi esimerkiksi luoda valesivuston, jonka tarkoituksena on saada uhri luovuttamaan kirjautumistietonsa. Käyttäjän manipuloinnin tarkoituksena on saada uhrin luottamus. Kun luottamus on saatu, saadaan uhri tekemään jotain sellaista, mitä tämä ei normaalisti tekisi, kuten avaamaan verkkorikollisten lähettämä linkki tai liitetiedosto. Tätä menetelmää käytetään tietoturvahyökkäyksissä. Sen avulla käyttäjiä huijataan tekemään virheitä tietoturvassa ja antamaan hyökkääjille arkaluontoisia tietoja. Social engineering hyödyntää ihmisten käyttäytymistä ja luonnollisia taipumuksia. Hyökkäykset etenevät yleensä yhdessä tai useammassa vaiheessa. (Cisco 2023.) Yleisin manipuloinnin tapa on tietojenkalasteluhyökkäys (Lehto & Limnéll 2017).



KUVIO 4. Hyökkäyksen elinkaari käyttäjän manipuloinnissa (mukaillen Imperva 2023)

Kuviossa 4 on kuvattuna tietoturvahyökkäyksen elinkaari käyttäjän manipulointia hyväksi käyttäen. Tiedusteluosuudessa hyökkääjä tunnistaa uhrit ja kerää taustatietoa. Siinä myös valitaan hyökkäystavat. Seuraavaksi uhria houkutellaan ja johdetaan harhaan. Uhria yritetään sitouttaa mahdollisimman paljon ja hyökkääjä pyrkii saamaan yliotteen vuorovaikutuksesta. Suoritusosuudessa varsinainen hyök-

käys suoritetaan ja haluttua informaatiota kerätään uhrilta. Lisäksi siinä pyritään saamaan lisää jalansijaa uhrin vaikuttamisessa. Tarvittaessa uhrin dataa jo ohjaillaan hyökkääjän toimesta. Lopuksi, kun uhrilta on saatu haltuun tarvittavat tiedot, vuorovaikutus pyritään lopettamaan epäilyksiä herättämättä. Vuorovaikutus päätetään mahdollisimman luonnollisella tavalla ymmärrettäviin syihin vedoten. Samalla hyökkäyksen jäljet peitellään ja jäljet haittaohjelmista poistetaan. (Imperva 2023.)

Vaikka ihminen on taitava havaitsemaan huijauksia ja epäilyttäviä seikkoja, joita tekoäly ei onnistu havaitsemaan, tekevät inhimilliset piirteemme meistä myös haavoittuvaisia. Jokainen on joskus väsynyt, tai arviointikykymme voi madaltua esimerkiksi meitä kohdanneen tragedian vuoksi. Tietoturva-ammattilainen Sami Laiho kertoi tapauksesta, jossa hän oli joutua itse verkkohuijarin uhriksi. Hän oli hoitanut isänsä kuolinpesää ja samoihin aikoihin oli hänen sähköpostiinsa saapunut viesti, joka oli otsikoitu liittyen isän omaisuuteen. Koska huijausviestin otsikko sattui liittymään syvästi häneen vaikuttaneeseen asiaan, oli Laiho lähellä astua verkkorikollisen ansaan. (Linnake 2023.) Tapaus muistuttaa, etteivät verkkohuijausten uhreiksi joudu pelkästään ikääntyneet tai heikot it-taidot omaavat henkilöt, kuka tahansa on potentiaalinen uhri. Verkkorikoksia tapahtuu kaikille yhteiskuntaluokasta riippumatta.

5.3 Kyberturvallisuus kansalaistaitona

Koska kyberturvallisuus koskettaa meistä jokaista, tulisi se tehdä helposti lähestyttäväksi aiheeksi ilman pelottelua ja epävarmuuden lietsontaa. Liian monimutkaiseksi kokemamme asiat siirrämme helposti sivuun ja ajattelemme, että parempi jättää asia teknologia-asiantuntijoiden hoitoon. Koska kansalaiset ovat eturintamassa kyberuhkien osalta, voisi olla järkevää tuoda kyberuhkatietoisuutta tutuksi jo peruskoulusta alkaen.

Tällä hetkellä perusopetuksen opetussuunnitelma pitää sisällään laaja-alaisen osaamisen osa-alueena tieto- ja viestintäteknologisen osaamisen. Se tarkoittaa käytännössä, että oppilaille opetetaan erilaisten sovellusten käyttöä ja havaitsemaan niiden merkitystä arjessa. Lisäksi opetuksessa pohditaan, miksi tieto- ja viestintäteknologia on tärkeä osa opiskelua, työtä ja yhteiskuntaa. Opetuksessa käydään myös läpi, miten kestävä kehitys ja vastuullinen kuluttaminen liittyvät asiaan. (Opetushallitus 2023.) Digilaitteita käytetään osana opetusta, joten sitä kautta laitteiden käyttö tulee oppilaille viimeistään koulussa tutuksi. Tämän päivän lapset ja nuoret elävät tiiviisti osana digitaalisia palveluita. Käytännössä heidän toimintaansa verkossa valvovat ja opastavat vain huoltajat. Näppärästi mobiililaitteita käyttävät

lapset kuitenkin saavat aikaan harhakuvan suuresta osaamistaidosta tietotekniikkataidoissa. Älypuhelimet ovat helpottaneet palveluita ja tehneet tekstinkäsittelyohjelmat turhaksi. Sähköpostia eivät nuoret tarvitse lukemattomien sosiaalisen median viestipalveluiden lisäksi.

Ohjelmoinnin opetus on ollut Suomessa osana perusopetusta vuodesta 2016 lähtien. On selvää, ettei kaikista peruskoululaisista tule ohjelmoijia, mutta yleissivistyksen kannalta ohjelmoinnin ymmärtäminen on tärkeää. Samalla tavalla kyberturvallisuuden ymmärtäminen on digitaitojen ja yleissivistyksen kannalta tärkeässä asemassa. Kyberturvallisuuden huomioiminen opetussuunnitelmassa olisi järkevää alati digitalisoituvassa yhteiskunnassamme.

Yksi haastava kansalaisryhmä digitaitojen osalta ovat ikääntyneet. Puutteet tietoteknisissä taidoissa altistavat digihuijauksille ja tämän vuoksi ikäihmiset ovat kyberrikollisille otollinen kohderyhmä. Vallin ikäteknologiakeskuksen teettämässä raportissa tutkittiin 75-vuotta täyttäneiden digiosallisuutta heidän kokemuksiinsa, motivaatioonsa ja tarpeisiinsa liittyen. Raportissa kävi ilmi neljä erilaista digitalisaatioon suhtautunutta ryhmää. Digilaitteita jo tottuneesti käyttävät eturintaman aktiivit, joilla oli jo työelämästä hankittuna hyvät tietotekniikan käyttötaidot, heillä oli myös hyvin saatavilla apua tarvittaessa digilaitteiden käyttöön läheisiltä. Mukaan vedetyiksi kutsuttiin ryhmää, jotka olivat joutuneet digilaitteiden käyttäjiksi osin vasten tahtoaan ja tarvitsivat paljon tukea niiden käyttämisessä. Mukaan vedetyistä 96 % saa apua digilaitteiden käyttöön, mutta kolmasosalla heistä on vaikeuksia avun pyytämisessä tai saannissa. Kolmas ryhmä on huolettomasti hämmentyneet, tästä ryhmästä lähes 60 %:lla läheiset huolehtivat digiasioista heidän puolestaan. Tämä ryhmä haluaisi asioida ennemmin kasvokkain kuin sähköisesti esimerkiksi pankkiasioissa. Niinpä he tukeutuvat ennemmin läheisten apuun digiasioinnissa. Neljäs ryhmä raportissa oli turvattomat, heidän digitaitonsa olivat riittämättömät ja heillä ei juuri ollut tietämystä tai motivaatiota digiasioihin liittyen. Tällä ryhmällä 80 %:lla läheiset hoitavat suurimman osan tai jopa kaiken digiasioinnista. Turvattomista joka kolmannella oli ongelmia avun pyytämisessä tai saamisessa. Kaikista vastanneista 79 % sai apua digiasioissa läheisiltään. 37 % sai apua joltain muulta taholta ja 16 % vastanneista kertoi, ettei saa apua digiasioihin mistään. (Ikäteknologiakeskus 2019, 6–8.)

Avun saamisen vaikeuteen tulisi tehdä aktiivisesti toimia tilanteen parantamiseksi. Monet yhdistykset tarjoavat digiapua jopa kotiin saakka. Tällaiselle toiminnalle tulee olemaan tulevaisuudessa varmasti enemmän kysyntää väestön ikääntyessä. Myös muita palveluntarjoajia löytyy, esimerkiksi teleoperaattori Elisa tarjoaa Omaguru-palvelua, jossa digiammattilainen voi auttaa asiakasta niin etänä ottamalla laitteeseen etäyhteyden kuin tulemalla asiakkaan kotiin (Elisa 2023). Ikäteknologiakeskuksen raportin

mukaan yli 75-vuotiaat haluaisivat saada digiopastusta mieluiten heidän vertaisiltaan, jotta mm. käytetty kieli olisi soveltuvaa ja selittäisi asiat yksinkertaisesti (Ikäteknologiakeskus 2019, 9). Nuorempia sukupolvia ikäihmiset pitävät asiantuntevina, mutta heidän käyttämä kieli ja opetustyyli koetaan usein liian nopeatempoisena ja epäselvänä.

Rikolliset kohdentavat huijauksiaan myös muille väestöryhmille, kuten nuorille aikuisille. Nopeita voittoja hakevat nuoret aikuiset ovat sijoitushuijauksien ja petoksien kohderyhmää (Palmgren 2023). Vuonna 2021 n. 40 prosenttia sijoitushuijauksien uhreista oli 30–50-vuotiaita. Sijoitushuijauksia oli vuoden 2023 tammi-kesäkuussa tapahtunut 8,2 miljoonan euron edestä. (Palmgren 2023.) Sijoitushuijauksissa liikkuvat isot rahamäärät ja sijoitusalalle on riskinotto muutenkin tyypillistä. Tämän vuoksi nuoret aikuiset, jotka hakevat nopeita voittoja sijoituksilla, ovat houkuttelevia uhreja verkkorikollisille. Huijausten kohderyhmää ovat myös ulkomaantaustaiset henkilöt. Huonosti suomen kieltä ja käytäntöjä tuntevaa uhria on helppo huijata esimerkiksi tekeytymällä pankin edustajaksi. Pankkitunnusten luovuttamisesta varoitellaan jatkuvasti ikäihmisiä, mutta kielivähemmistöjä nämä varoitukset eivät välttämättä tavoita (Finanssiala ry 2023).

5.4 Kybermaailman mahdollisuudet

Vaikka kybermaailma on pullollaan haittaohjelmia, kiristysohjelmia ja tietojenkalastelua, ei tulevaisuus näytä aivan toivottomalta. Tekoälyn käytön yleistyessä, vaikuttaa se yhä laajemmin ihmisten arkeen. Tekoälyllä on monia hyötyjä, sen avulla kansalaiset voivat hyötyä kehittyneemmästä terveydenhuollosta ja turvallisesta liikenteestä. Tekoälyn avulla voidaan suorittaa ihmiselle vaarallisia työtehtäviä turvallisesti ja vähentää inhimillisen virheen määrää. Tätä voitaisiin hyödyntää missä tahansa ympäristöstä riippumatta, kuten avaruudessa tai valtamerien syvimpien alueiden tutkimisessa.
Tekoälyn haittapuolia ovat työpaikkojen syrjäyttäminen, huoli eettisyydestä ja ihmismäisen luovuuden sekä empatian puutteesta. Mielikuvat tekoälystä ovat myös haasteellisia, monelle mielikuvat tekoälystä ovat syntyneet scifi-tarinoiden perusteella. Niissä on luotu negatiivisia mielikuvia älykkäistä roboteista, jotka tuhoavat ihmiskunnan.

Tekoälyllä on kuitenkin valtavasti potentiaalia tulevaisuudessa kyberturvallisuuden saralla. Sen avulla voidaan automatisoida ja tehostaa tietoturvaprosesseja. Tekoälyalgoritmit pystyvät analysoimaan valtavia tietomääriä ja havaitsemaan lähestyviä tietoturvauhkia. Näin voidaan vähentää viivettä kyberhyökkäyksien havaitsemisessa. (Neenan 2023.)

6 POHDINTA

Kyberturvallisuuteen voitaisiin ottaa oppia liikenneturvallisuudesta, jonka parantaminen on pitkäjänteisen työn ja asenteiden muutoksen ansiota. Vielä 60-luvulla rattijuoppoutta ei pidetty yhtä suurena rikkeenä kuin tänä päivänä. Laki ei tuntenut promille- eikä nopeusrajoituksia. Nopeusrajoituksiin suhtauduttiin yksilönvapautta loukkaavana asiana. Sittemmin asenteiden muututtua ja uusien lakien myötä alkoivat liikennekuolemat vähentyä. Myös teknisten ominaisuuksien kehittyminen autoissa johti kohti parempaa ja turvallisempaa autoilun aikakautta. Liikennemäärien kasvusta huolimatta turvallisuus on jatkuvasti parantunut. Tämä antaa toivoa myös kyberturvallisuuden kehitykselle. Vaikka laitteiden keskihinta laskee ja niiden valmistus siirtyy Kiinaan, ei se estä tietoturvan parantamista, kunhan vain halua asennemuutoksiin löytyy. (Järvinen 2018, 297–298.)

Tieliikennelaki velvoittaa moottoriajoneuvon omistajan tai haltijan hankkimaan liikennevakuutuksen, miksei verkon käyttäjiäkin velvoitettaisi ”vakuuttamaan” toimintansa verkossa esimerkiksi tietoturvaohjelmistoilla? Sekään ei ole ongelmaton ratkaisu, sillä tietoturvaohjelmisto ei estä kaikkia käyttäjän tekemiä virheitä verkossa.

On hyvä huomioida, että media vääristää käsitystämme yhteiskunnasta välillä klikkiotsikoiden toivossa. Medialla on tapana uutisoida pieniä uutisia niitä suurentelemalla ja korostamalla tunteita herättäviä asioita kuten uhkia turvallisuuttamme kohtaan. Voitaneen kuitenkin todeta, että viime aikoina on median uutisoinnissa tapahtunut kehitystä vastuullisuuden osalta. Yhä useampi uutisointi on kirjoitettu kansantajuisesti ja uutisoinnista on aidosti hyötyä käyttäjien tietoturvan ymmärrykselle. Mikään määrä koulutusta tuskin auttaa, jos kansalaisia ei saada kiinnostumaan kyberturvallisuudesta aidosti. Tässä on nähtävissä jo median osalta kehitystä, uutisointi tietoturva-asioista on selvästi lisääntynyt ja uutisointi aiheesta on usein ns. kansantajuista.

Sähköverkon alkuvuosina oli sen toiminnassa omat haasteensa. Sen toimivuuteen kuitenkin panostettiin niin päättäväisellä otteella, että sähköä saadaan tänä päivänä pistorasiasta varsin luotettavasti ja huolettomasti. (Järvinen 2022, 278.) Tietotekniikasta on mahdollista samanlaisella päättäväisyydellä saada luotettava kumppani tulevaisuudessa. Emme voi antaa yhden ihmiskunnan hienoimman keksinnön ottaa meistä yliotetta.

LÄHTEET

Ahosola, J. 2023. *EU rajoittaa internetjättejä: Kohteina Facebook, Instagram, Google, Twitter, Tiktok...* Iltalehti 1.5.2023. Saatavissa: https://www.iltalehti.fi/digiuutiset/a/7c1fd22f-01ef-4977-bf38-daa218e7253a. Viitattu 20.5.2023.

Ali-Yrkkö, J., Mattila. J & Seppälä, T. 2020. *”Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät?”*. ETLA Muistio No 93. Saatavissa: https://pub.etla.fi/ETLA-Muistio-Brief-93.pdf. Viitattu 23.5.2023.

Cisco. 2023. *What Is Social Engineering?* Saatavissa: https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html. Viitattu 9.11.2023.

Elisa. 2023. *Uuden ajan neuvontapalvelu - Kodin tietotekniikan asiantuntija palveluksessasi.* Saatavissa: https://elisa.fi/omaguru/tietoaomagurusta/ Viitattu 10.10.2023.

Empirica Finland Oy. *Mikä on IoT? Esineiden internet yksinkertaisesti selitettynä*. Saatavissa: https://www.empirica.fi/iot.html. Viitattu 25.5.2023.

F-Secure. 2023. *Mitä on kyberturvallisuus?* Saatavissa: https://www.f-secure.com/fi/articles/what-is-cyber-security. Viitattu 7.11.2023

F-Secure. *Mitä ovat huijauspuhelut?* Saatavissa: https://www.f-secure.com/fi/articles/what-is-vishing. Viitattu 5.11.2023.

Heleskoski, J. 2023. *Näin paljon kyberiskujen määrä Suomessa on lisääntynyt Natoon liittymisen jälkeen.* Tivi 4.8.2023. Saatavissa: https://www-tivi-fi.ezproxy.centria.fi/uutiset/nain-paljon-kyberiskujen-maara-suomessa-on-lisaantynyt-natoon-liittymisen-jalkeen/45f6923e-c18d-4d61-b9ab-83f789401e8d. Viitattu 7.11.2023.

Hyppönen, M. 2021. *Internet*. Helsinki: WSOY.

Hämäläinen, V-P. 2021. *Ehkä jopa 32 000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: "Emme tiedä, monenko käsissä tietokanta on"* https://yle.fi/uutiset/3-11757676. Viitattu 23.11.2021

Ikäteknologiakeskus 2019. *Yli 75-vuotiaiden digiosallisuus – kokemukset, tarpeet ja motivaatio.* Saatavissa: https://www.valli.fi/wp-content/uploads/2020/01/yli75_digiosallisuus_raportti.pdf. Viitattu 23.5.2023.

Imperva 2023. Social Engineering. Saatavissa: https://www.imperva.com/learn/application-security/social-engineering-attack/. Viitattu 22.11.2023.

Joukanen, T. 2023. *Supo varoitti reitittimien tietoturvauhasta – tarkista kotona ainakin nämä kuusi asiaa kuntoon.* YLE. Saatavissa: https://yle.fi/a/74-20054897. Viitattu 31.10.2023

Järvinen, P. 2018. *Kyberuhkia ja somesotaa*. Jyväskylä: Docendo.

Järvinen, P. 2022. *Yrityksen tietoturvaopas*. Helsinki: Kauppakamari.

Kailio, A. 2022. *Bluetooth on myös tietoturvariski – vain laitteen sammuttaminen ehkäisee sen tunnistamisen.* Kauppalehti 11.6.2022. Saatavissa: https://www-kauppalehti-fi.ezproxy.centria.fi/uutiset/bluetooth-on-myos-tietoturvariski-vain-laitteen-sammuttaminen-ehkaisee-sen-tunnistamisen/5f151789-77ac-4269-8a53-6e9711c7fc67. Viitattu 7.11.2023.

Kaspersky. 2023. *What is VPN? How It Works, Types of VPN.* Saatavissa: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn. Viitattu 2.12.2023.

Koskinen, R. 2023. *Löytöeläimet jäivät yhtäkkiä ilman uusia koteja, kun yhdistyksen sometili kaapattiin.* YLE. Saatavissa: https://yle.fi/a/74-20018551 . Viitattu 23.3.2023.

Kullas, J. 2022. *Microsoft-pomolta kylmäävä näkemys deepfake-videoista: maailma on matkalla vaaralliseen suuntaan.* Mikrobitti 30.9.2022. Saatavissa: https://www-mikrobitti-fi.ezproxy.centria.fi/uutiset/microsoft-pomolta-kylmaava-nakemys-deepfake-videoista-maailma-on-matkalla-vaaralliseen-suuntaan/b9e43d4f-f7f1-4a32-aed8-dc22763fa940. Viitattu 2.12.2023.

Kyberturvallisuuskeskus. 2014. *Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön*. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvavinkkeja_matkapuhelimen_turvalliseen_kayttoon.pdf. Viitattu 2.5.2023

Kyberturvallisuuskeskus. 2020. *Bluetoothin turvallinen käyttö älylaitteissa*. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/bluetoothin-turvallinen-kaytto-alylaitteissa. Viitattu 7.11.2023.

Kyberturvallisuuskeskus. 2023. *Älylaitteiden heikko tietoturva sääntelyllä kuriin*. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/alylaitteiden-heikko-tietoturva-saantelylla-kuriin. Viitattu 26.5.2023.

Kärkkäinen, H. & Linnake, T. 2023. *Yksi kuva kertoo: Näin huijaus-puheluille kävi*. Iltasanomat 15.10.2023. Saatavissa: https://www.is.fi/digitoday/tietoturva/art-2000009897593.html Viitattu 4.11.2023.

Laaksonen, K. 2018. *10 käskyä kodin tietoturvasta - huolehdi näistä ennen kuin lisäät laitteita kodin verkkoon.* Mikrobitti 2.11.2018. Saatavissa: https://www-mikrobitti-fi.ezproxy.centria.fi/neuvot/10-kaskya-kodin-tietoturvasta-huolehdi-naista-ennen-kuin-lisaat-laitteita-kodin-verkkoon/67defd10-256c-41d7-84ab-e3b09bf90697 . Viitattu 2.11.2023.

Laine, K. 2020. *Puhelimen palauttaminen kierrätykseen on ekoteko*. Saatavissa: https://ficom.fi/ajankohtaista/uutiset/puhelimen-palauttaminen-kierratykseen-on-ekoteko/. Viitattu 9.11.2023.

Lapinkangas, J. 2023. *Näkökulma: Suomea odottaa kaikkien aikojen oikeuskatastrofi*. Iltalehti 27.4.2023. Saatavissa: https://www.iltalehti.fi/kotimaa/a/3ad018f2-fb08-4685-b373-4e9195df77a8. Viitattu 25.11.2023

Lehto, M. & Limnéll, J. 2017. *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Saatavissa: http://urn.fi/URN:ISBN:978-952-287-368-2. Viitattu 8.11.2023.

Limnéll, J., Majewski, K. & Salminen, M. 2014. *Kyberturvallisuus*. Jyväskylä: Docendo.

Linnake, T. 2022. *Nettihuijauksen uhri tekee usein yhden virheen: ”Rikollisten salainen ase”*. Iltasanomat 12.10.2023. Saatavissa: https://www.is.fi/digitoday/tietoturva/art-2000009127197.html. Viitattu 1.11.2023.

Linnake, T. 2023. *Ammattilainen paljastaa: Näin hän oli astua huijarin ansaan*. Iltasanomat 21.5.2023. Saatavissa: https://www.is.fi/digitoday/tietoturva/art-2000009596059.html. Viitattu 29.5.2023

Neenan, J. 2023. *The Role of AI in Cybersecurity: Opportunities and Challenges*. AI & Machine Learning 18.5.2023. Saatavissa: https://www.cyberneticsearch.com/blog/the-role-of-ai-in-cybersecurity--opportunities-and-challenges/. Viitattu 7.11.2023.

Opetushallitus. 2023. *Perusopetuksen opetussuunnitelman ydinasiat*. Saatavissa: https://www.oph.fi/fi/koulutus-ja-tutkinnot/perusopetuksen-opetussuunnitelman-ydinasiat. Viitattu 23.5.2023.

Palmgren, J. 2023. *Kalastelut ja muut huijaukset kasvoivat räjähdysmäisesti alkuvuonna – pankit saivat estettyä huijauksia lähes 16 miljoonan euron edestä.* Finanssiala. Saatavissa: https://www.finanssiala.fi/uutiset/kalastelut-ja-muut-huijaukset-kasvoivat-rajahdysmaisesti-alkuvuonna-pankit-saivat-estettya-huijauksia-lahes-16-miljoonan-euron-edesta/. Viitattu 4.11.2023.

Stubin, T. 2023. *Elisa kehitti ratkaisun, joka pani huijauspuhelut kuriin – ”Paine median ja asiakkaiden suunnalta oli kova”*. Tivi 8.9.2023. Saatavissa: https://www-tivi-fi.ezproxy.centria.fi/uutiset/elisa-kehitti-ratkaisun-joka-pani-huijauspuhelut-kuriin-paine-median-ja-asiakkaiden-suunnalta-oli-kova/1b2bf9ec-1ef5-4cd8-9c5d-4e758b3c64d3. Viitattu 1.12.2023.

Suojelupoliisi. *Suojelupoliisi torjuu vakoilua myös verkossa*. Saatavissa: https://supo.fi/kybervakoilu. Viitattu 9.11.2023.

Tilastokeskus. 2022. *Väestön tieto- ja viestintätekniikan käyttö sukupuolen ja pääasiallisen toiminnan mukaan, 2013–2022*. Saatavissa: https://pxdata.stat.fi/PxWeb/pxweb/fi/StatFin/StatFin__sutivi/statfin_sutivi_pxt_13ts.px/table/tableViewLayout1/. Viitattu 6.11.2023.

Waschke, M. 2017. *Personal cybersecurity: How to avoid and recover from cybercrime.* Bellingham: Apress.

YLE, 2018. *Hyväksyn käyttöehdot - tietosuojan historiaa.* Podcast-tallenne. Julkaistu 9.1.2018. Saatavissa: https://areena.yle.fi/podcastit/1-4315102. Viitattu 2.5.2023.

YLE, 2023. *Deepfakes – hot eller möjlighet?* Ajankohtaisohjelma. Julkaistu 6.3.2023. Saatavissa: https://areena.yle.fi/1-65242550. Viitattu 2.12.2023.