Joona Kauranen

Digitaalinen väkivalta ja vaino

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Joona Kauranen

Yhteystiedot: joona.e.kauranen@student.jyu.fi

Ohjaaja: Sanna Juutinen

Työn nimi: Digitaalinen väkivalta ja vaino

Title in English: Digital violence and stalking

Työ: Kandidaatintutkielma

Sivumäärä: 20+0

Tiivistelmä: Tämä kandidaatintutkielma on kirjallisuuskatsaus digitaaliseen väkivaltaan ja vainoon. Erityisesti kartoitetaan vainon välineitä digitalisaation muokkaamassa maailmassa. Katsauksesta voi olla apua ohjelmistojen ja laitteiden kehittäjille, sekä digitaalista väkivaltaa kohtaaville ammattilaisille.

Avainsanat: digitaalinen väkivalta, vaino, kandidaatintutkielmat

Abstract: This bachelor's thesis was conducted as literature review on digital violence and stalking. In particular, the tools of stalking in a world shaped by digitalization are studied. The review can be helpful for software and device developers, as well as for professionals working at digital violence.

Keywords: digital violence, stalking, Bachelor's Theses

Termiluettelo

Jailbreak	Laitteen suojauksien murtaminen niin, että ohjelmistorajoitusten ohittaminen mahdollistuu (NordVPN 2022).

Taulukot

Taulukko 1. By means of what technologies were you stalked? (Kaspersky 2021). 9
Taulukko 2. Evolution of affected users year-on-year (Kaspersky 2023). 9

Sisällys

1 JOHDANTO 1

2 VÄKIVALTA JA VAINO 3
2.1 Lähisuhdeväkivalta 3
2.2 Lähisuhdeväkivalta digitaalisessa ympäristössä 4
2.3 Teknologia ja vaino 4

3 DIGITAALISEN VÄKIVALLAN VÄLINEET 6
3.1 Seurantalaitteet 6
3.2 Vakoiluohjelmat 7
3.3 Sosiaalinen media 7

4 TEKNOLOGISOITUMINEN 9
4.1 Tilastoja 9
4.2 Nykytilanne 10
4.3 Tulevaisuus 10

5 POHDINTA 12

LÄHTEET 13

1 Johdanto

Teknologia ja tietotekniikka muuttaa kiihtyvällä tahdilla asioita maailmassamme. Moni arkinen tai työläs asia helpottuu ja nopeutuu teknologian myötä. Saamme haluamiimme asioihin sekä henkilöihin yhteyden missä vain ja milloin vain. Lisäksi saamme tietoa salamannopeasti mukana kulkevilla älylaitteilla. Suomalaisista lähes jokainen käyttää internetiä päivittäin tai lähes päivittäin (Eurostat 2022). Kehityksestä seuraavilla positiivisilla asioilla kuitenkin voi olla kääntöpuolensa, kuten tässä kandidaatintutkielmassa tullaan saamaan selville. Yksi asia johon teknologia on hiljattain tuonut uusia haasteita, on lähisuhdeväkivalta ja siihen liittyvä vainoaminen.

Tänä päivänä teknologian nopea kehittyminen on tuonut lähisuhdeväkivaltaan uusia ulottuvuuksia, josta seuraavia asioita voidaan kutsua digitaaliseksi väkivallaksi (Rikosuhripäivystys 2023a). Lähisuhdeväkivalta on aihe, mikä saattaa koskettaa monia elämän aikana ja kuka vain lapsesta vanhukseen voi joutua kokemaan sitä. Rikosuhripäivystyksen (2023b) mukaan tekijänä on usein läheinen, rakas tai muuten luotettu ihminen. Suomessa 30 prosenttia naisista on kokenut fyysistä väkivaltaa parisuhteessa (Hakkarainen 2019).

Tämän kandidaatintutkimuksen tarkoituksena on tehdä katsaus digitaaliseen väkivaltaan, sekä tutustua erityisesti digitalisaation myötä helpottuneeseen seurantaan ja vainoamiseen. Kiinnostavaa on erityisesti erilaiset seurantaohjelmistot ja -välineet, jotka on usein kehitetty täysin muuhun tarkoitukseen, kuten esineiden tai omien lasten seuraamiseen.

Euroopan Unionin Perusoikeusviraston (2012) teettämän tutkimuksen mukaan vuonna 2012 suomalaisista naisista 8 % oli kokenut digitaalista vainoa elämänsä aikana. Aiheesta ei löydy tuoreempaa dataa Suomessa, mutta esimerkiksi Britanniassa aihe on ajankohtainen (ks. esim. Moore 2022). Digitaalista väkivaltaa on kuvailtu ja tutkittu erilaisissa suomenkielisissä oppaissa (ks. esim. Hakkarainen 2019), mutta erityisesti seurannan välineisiin ei ole Suomessa perehdytty. Ulkomailta löytyy kuitenkin lisääntyvissä määrin uutisia siitä, kuinka esineiden seurantaan tarkoitettuja välineitä käytetään väärin ja haitallisesti (ks. esim. Moore 2022). Erityisesti niiden laaja saatavuus ja halpa hinta edesauttanee tapausten yleistymistä.

On siis tärkeää tuoda ilmi, kuinka väkivallan tekijät voivat väärinkäyttää arkipäiväisiäkin

esineitä. Asian tiedostaminen voi tarpeen tullen olla avuksi suurestikin. Lisäksi tutkimus toivottavasti tuottaa ohjelmistojen sekä laitteiden kehittäjille tietoa, jonka avulla tuotteiden mahdollista väärinkäyttöä voidaan estää.

Seuraavaksi tässä kandidaatintutkielmassa tullaan selittämään muutama avainkäsite, pohjanaan aiheeseen liittyvä tieteellinen lähdeaineisto. Myöhemmin tutustutaan digitaalisen väkivallan välineisiin, ja lopuksi tarkastellaan tilastoja ja niiden perusteella tehtyjä pohdintoja.

2 Väkivalta ja vaino

Digitaalisen maailman asiat heijastuvat oikeaan maailmaan, jossa elämme ja toisinpäin. Ehkei tulisikaan kutsua internetiä miksikään erilliseksi ulottuvuudeksi vaan asiaksi, joka on elämässämme. Asiat, jotka liittyvät oikean maailman asioihin, liittyy ne myös internetiin. Rikokset, jotka tapahtuvat todellisuudessa, voivat tapahtua myös netissä.

Lähisuhdeväkivalta, jota saatetaan väärinajatella pelkästään fyysisenä väkivaltana, on todellisuudessa myös paljon muuta. Lähisuhdeväkivallan ytimessä on toisen ihmisen kontrollointi (Hakkarainen 2019), joten internet tuo valitettavan monia mahdollisuuksia lisää siihen. Seuraavaksi tutustutaan lähisuhdeväkivaltaan yleisellä tasolla, jotta voidaan sen jälkeen tuoda mukaan digitaalinen ulottuvuus asiaan.

2.1 Lähisuhdeväkivalta

Lähisuhdeväkivalta on laaja ja monialainen aihe, joten sen käsittely lyhyesti on vaikeaa. Tiivistettynä lähisuhdeväkivallalla on monia eri muotoja ja tunnetuimmin se voi ilmentyä henkisenä tai fyysisenä väkivaltana. Henkinen väkivalta saattaa olla uhkailua, painostamista ja haukkumista. Fyysinen väkivalta taas voi esimerkiksi olla lyömistä tai hiuksista repimistä. Lähisuhdeväkivallan muita muotoja ovat taloudellinen-, seksuaalinen- tai uskonnollinen väkivalta. Väkivalta pysyy usein kodin seinien sisällä eikä se näy muille ulos päin. Tilanteesta on vaikea lähteä, sillä tekijä on itselle usein läheinen ja luotettu ihminen, kuten oma puoliso tai vanhempi. (Laitinen, Kinnunen ja Hannus 2017). Lähisuhdeväkivalta on sukupuolittunutta, sillä useimmiten tekijänä on mies ja väkivallan kokijana nainen (THL 2023).

Lähisuhdeväkivalta ei usein lopu suhteen päättymiseen, vaan se voi jatkua mm. vainoamisena. Kuitenkaan sitä ei ole aina tunnistettu yhteiskunnassa, vaan vainoaminen kriminalisoitiin Suomessa vasta vuonna 2014 (Laitinen, Kinnunen ja Hannus 2017). Vainon keskellä saattaa monesti olla lapsia, jotka ovat tilanteessa erityisen haavoittuvaisia. Laitisen, Kinnusen ja Harjuksen (2017) mukaan kohde taas kärsii jatkuvasta varpaillaan olon tunteesta, sillä vainoaminen vaikuttaa henkiseen hyvinvointiin. Vainoaminen voi olla toistuvaa epätoivottua yhteydenottoa, pelottelua, perättömien tietojen levittelyä sekä seuraamista ja tarkkailua.

2.2 Lähisuhdeväkivalta digitaalisessa ympäristössä

Digitaalinen väkivalta on teknologiavälitteistä häirintää tai vainoamista. Sitä ei ole sellaisenaan kirjattu rikoslakiin, mutta tiettyjen kriteerien täyttyessä voidaan puhua vainoamisesta, salakuuntelusta tai identiteettivarkaudesta, joiden voidaan katsoa olevan tuomittavia rikoksia (Rikosuhripäivystys 2023a). Väkivallan välineenä voidaan käyttää sosiaalisen median alustoja, viestipalveluita, seurantalaitteita tai esineiden internet-laitteita. Digitaalinen väkivalta alkaa usein parisuhteen aikana ja jatkuu usein jopa kiihtyen eron jälkeen (Hakkarainen 2019).

Oulun ensi- ja turvakoti ry:n (2020) mukaan digitaalista lähisuhdeväkivaltaa voi olla esimerkiksi digitaalinen seuranta ja vaino, seksuaalisen materiaalin julkaisulla uhkailu ja seksuaalisiin tekoihin painostaminen, sekä taloudellinen väkivalta kuten rakkauspetokset. Kyseiseen väkivaltaan puuttuminen voi olla vaikeaa sillä uhri voi tuntea häpeää, pelkoa tai hän voi kieltää koko tilanteen (Mitchell ja Anglin 2009). Kieltäminen johtunee uhrin ja väkivallan tekijän läheisestä suhteesta, jolloin uhri ei halua tekijälle negatiivista mainetta.

2.3 Teknologia ja vaino

Vainoaminen on lain mukaan toistuvaa uhkaamista, seurantaa, tarkkailua tai yhteyden ottamista. Sillä tarkoitetaan esimerkiksi jatkuvaa tekstiviestillä uhkailua. Vainon tunnistaminen voi olla vaikeaa, sillä se ei jätä samanlaisia jälkiä kuin fyysinen väkivalta. Uhrit ovat kuvailleet vainoamista verkoston tai rihmaston metaforilla (Laitinen, Kinnunen ja Hannus 2017). Tunne voi olla yhtä haitallista, kuin fyysinen väkivalta. Tekijä voi seurata tai tarkkailla uhriaan tavalla, mikä luo uhrille poispääsemättömän tunteen.

Teknologia on luonut vainoamiselle uusia tapoja. Vainoaja voi käyttää teknologiaa hyväkseen, esimerkiksi asentamalla seurantaohjelmia puhelimeen tai käyttämällä erilaisia seurantalaitteita. Digitaalinen vaino tulisi ottaa vakavasti sillä se voi pahimmillaan johtaa murhaan ja lievimmilläänkin se aiheuttaa stressiä ja pelkoa (Laitinen, Kinnunen ja Hannus 2017). Tekijä voi seurata teknologian avulla uhriaan ajasta ja paikasta riippumatta. Tästä seuraa, että vainoaja voi luoda ilmapiirin, jossa hän tietää uhristaan kaiken aina tekemisistä sanomisiin (Fraser ym. 2010).

Teknologiavälitteinen vaino voi esimerkiksi olla jatkuvaa soittelua tai viestittelyä, seurantaa seurantaohjelmien tai seurantalaitteiden avulla, salakuvaamista tai salakuuntelua. Näistä kerrotaan lisää seuraavassa kappaleessa, jossa tutustutaan tarkemmin eri välineisiin ja ohjelmistoihin teknologisesta näkökulmasta.

3 Digitaalisen väkivallan välineet

Digitaalista väkivaltaa ja vainoamista voi tapahtua eri alustoilla. Vainoaminen saattaa olla puhelimeen ladattu ohjelma tai autoon kiinnitetty seurantalaite. Digitaalista väkivaltaa on myös netissä tapahtuva häirintä ja vainoaminen, joka johtaa poispääsemättömään turvattomuuden tunteeseen. Väkivallan tekijä yrittää erilaisin keinoin saada uhrin taipumaan tahtoonsa kontrolloimalla, uhkailemalla tai painostamalla toista osapuolta (Hakkarainen 2019). Teot voivat olla jatkuvaa seurantaa ja toiminnan rajoittamista eri välinein, joista seuraavaksi on lueteltu yleisimpiä tapoja.

3.1 Seurantalaitteet

Erilaisia GPS-laitteita on ollut pitkään tarjolla. Ne tarjoavat reaaliaikaista seurantamahdollisuutta omaisuudelle tai vaikka lapsille. Niitäkin on käytetty pitkään väärin. Esimerkiksi jo vuodelta 2004 löytyy esimerkki missä tekijä on ostanut halvan kännykän, laittanut siitä GPS:n päälle ja piilottanut sen uhrin autoon (Fraser ym. 2010).

Apple julkaisi vuonna 2021 pienen seurantalaitteen esineille, mutta lähes heti sitä ryhdyttiin käyttämään väärin (Moore 2022). Siinä on pitkään kestävä akku, joten sen voi huoletta pudottaa uhrin taskuun ja seurata sijaintia pitkään. Tavallisia GPS-laitteita joutuu ostamaan netistä tai erikoisliikkeistä, mutta AirTageja löytyy normaaleista elektroniikkaliikkeistä ja isommista ruokakaupoista suhteellisen halpaan hintaan.

Toinen vastaavanlainen laite on elektroniikkayhtiö Tilen valmistama seurantalaite. AirTagin toiminta perustuu *Ultra Wideband* -radioteknologiaan, kun taas Tile käyttää *Bluetooth Low Energy*ä. Tiivistettynä molemmat käyttävät vähän energiaa, joten laitteita ei tarvitse ladata useasti. Tile julkaisi oman sovelluksen väärinkäyttöjen estämiseksi (Tile 2023), mutta sekin vaatii taas yhden erillisen sovelluksen, jotta käyttäjä voisi tietää mahdollisesta seurannastaan. Tavalliselle ihmiselle tuskin tulee mieleen ladata montaa erillistä sovellusta, joista hän ei ole kuullutkaan.

3.2 Vakoiluohjelmat

Vakoiluohjelmia (engl. *spyware*) käytetään perinteisesti tietojenkalasteluun ja ne voivat tarttua koneeseen verkkosivuilta tai ilmaisohjelmista. Vakoiluohjelmien juuret ulottuvat 90-luvulle asti ja ne ovat vuosien varrella kehittyneet eri tarkoituksiin. Yleisimmin halutaan kalastella luottokorttitietoja ja salasanoja mahdollisimman monelta uhrilta.

Vakoiluohjelmien rinnalle on tullut kyttäysohjelmat (engl. *stalkerware*), joiden käyttötarkoitus on seurata omia lapsia tai työntekijöitä. Jos kyttäyssovelluksia käytetään alkuperäiseen käyttötarkoitukseen, niin niistä tavallisesti käytetään termiä seurantaohjelmistot tai termiä vanhempia varten kehitetty valvontaohjelma (engl. *parental control*). Ne ovat alun perin luotu ”viattomaan” seurantaan. Niillä voidaan saada halutessa tietoa oikeastaan laitteen kaikesta toiminnasta, kuten sijainnista, selaushistoriasta, viesteistä. Kyttäyssovellukset on kielletty yleisimmistä sovelluskaupoista, mutta jailbreakkaamalla voidaan sovelluksia asentaa. (Chatterjee ym. 2018).

Sovelluskauppojen sallittujakin seurantaohjelmistoja voidaan väärinkäyttää epähaluttuun seurantaan. Seurannan ja vainoamisen kohteena voi olla oma puoliso, joka ei välttämättä tiedä seurannasta. Harkinin, Molnarin ja Volwesin (2020) mukaan sovelluksen tarjoajat ehdottavat seurannan kohteeksi omia lapsia, työntekijöitä ja läheisiä. Seuraaja saa tietoja laitteen toiminnasta sijainnista viestihistoriaan. Esimerkkinä vanhempia varten kehitetty valvontaohjelma mSpy mainostaa kuinka sitä voidaan käyttää kaikkeen seurantaan ilman jailbreakkaamista (Chatterjee ym. 2018). Kyseisen sovelluksen avulla saadaan tietoa seurattavan laitteen viesteistä, puheluhistoriasta, sijainnista ja selaushistoriasta. Tietoturvayhtiö Kasperskyn (2021) mukaan kyttäysohjelmien käyttö kasvoi koko maailmassa puolella vuodesta 2018 vuoteen 2019.

3.3 Sosiaalinen media

Sosiaalinen media (*Facebook, Instagram, TikTok, Twitter*) on luonut digitaaliselle väkivallalle ja vainolle uusia välineitä. Väkivaltaa ja vainoa voi tapahtua sekä suhteen aikana, että suhteen päättymisen jälkeen. Monelle sosiaalinen media on arkipäivää ja jos sitä rajoitetaan tai sen kautta kontrolloidaan, niin seuraukset voivat olla vakavat väkivallan kokijalle. Tämä

voi aiheuttaa poispääsemätöntä turvattomuuden tunnetta, sillä sosiaalinen media seuraa laitteissa kaikkialle (Hakkarainen 2019). Voidaan myös todeta, että monelle sosiaalinen media on normaalia ihmissuhteiden ylläpitoa ja sosiaalista toimintaa, joten ratkaisuna ei ole sieltä poistuminen.

Sosiaalisessa mediassa voidaan luoda kontrolloinnin ja pelon tunnetta seuraamalla toisen tykkäyksiä, paikallaoloa ja kommentteja. Moni sosiaalisen median alusta näyttää oletuksena käyttäjän paikallaolon. Osassa alustoista on kaikkien nähtävillä käyttäjän tykkäykset. Tekijä voi painostaa näiden tietojen avulla toista (Hakkarainen 2019). Yhdysvaltalaistutkimuksen mukaan häiritsevään käytökseen netissä ja sosiaalisessa mediassa syyllistyy suurimmaksi osaksi tuntemattomat henkilöt, mutta myös nykyiset tai entiset kumppanit (Lenhart ym. 2016).

Sosiaalisessa mediassa tapahtuva vainoaminen voi olla myös luvaton kirjautuminen tai hakkerointi toisen henkilön tunnuksille. Väkivallan kokijat ovat kertoneet, kuinka tekijä on kirjautunut heidän tunnuksilleen ja seurannut heidän elämäänsä (Messing ym. 2020). Sosiaalisen median tileiltä voi saada paljonkin tietoa henkilöiden läheisistä ja tekemisistä. Läheisten käyttäjätietojen kautta tekijä voi saada myös tietoja, jos läheinen jakaa paljon vainottavan henkilön asioita sosiaalisen median kanavissa. Facebook ja Twitter ovat kuitenkin tehneet työtä parantaakseen naisten turvallisuutta ja yksityisyyden ylläpitämistä palveluissaan (Dragiewicz ym. 2018).

4 Teknologisoituminen

Tässä kappaleessa tutustutaan digitaalisen väkivallan tilastoihin. Selvitetään millä alustoilla digitaalista väkivaltaa ja vainoa tapahtuu, sekä kuinka yleistä se voi olla. Niiden pohjalta pohditaan digitaalisen väkivallan nykyhetkeä ja tulevaisuutta.

4.1 Tilastoja

Taulukko 1. By means of what technologies were you stalked? (Kaspersky 2021).

technology	share %
phone app	50
tracking devices	29
laptop app	27
access to webcam	22
through (smart) home devices	18
health monitoring devices	14
other	7

Taulukko 2. Evolution of affected users year-on-year (Kaspersky 2023).

year	unique users
2018	40 173
2019	66 927
2020	53 870
2021	32 694
2022	29 312

Taulukosta 1 nähdään millä eri teknologian tavoin on vainottu henkilöitä ketkä ovat joutuneet vainon kohteiksi. Tulokset ovat tietoturvayhtiö Kasperskyn tutkimuksesta vuodelta 2021 (Kaspersky 2021). Taulukosta 2 nähdään kyttäysohjelmien, joita voivat olla erilaiset puhelin-

ja tietokonesovellukset, yleisyys koko maailmassa vuosilta 2018-2022. Tutkimuksen on suorittanut tietoturvayhtiö Kaspersky (Kaspersky 2023).

4.2 Nykytilanne

Taulukosta 2 voidaan huomata, että stalkkausohjelmien yleisyys on laskenut vuodesta 2019 vuoteen 2022. Laskevuuteen on voinut vaikuttaa tietoturvallisuuden parantuminen laitteissa. Myös mobiililaitteiden yleistyminen vaikuttanee asiaan, sillä niihin haittaohjelmien asentaminen on vaikeampaa mobiililaitteiden käyttäessä useimmiten suljettuja ympäristöjä. Tosin taulukosta 2 voidaan huomata, että vainoamista tapahtuu enemmän puhelimessa olevilla haittaohjelmilla kuin tietokonehaittaohjelmilla. Siihen voi vaikuttaa puhelimesta saatava suurempi päivittäisen tiedon määrä. Väliin jää seurantavälineet, joiden uhriksi 29 prosenttia vainon kohteista on joutunut. Kasperskyn (2023) tutkimuksesta selviää myös, että eniten stalkkausohjelmatartuntoja löytyy Venäjältä, Brasiliasta ja Intiasta.

Vuonna 2020 Google ilmoitti poistavansa loppuvuodesta alkaen Google Play sovelluskaupastaan kyttäyssovellukset, jotka keräävät laitteista dataa piilotetusti ilman käyttäjän tietämystä (Google 2020). Se on saattanut osaltaan vaikuttaa vuoden 2020 ja 2021 laskusuunnassa oleviin kyttäysohjelmatartuntoihin.

4.3 Tulevaisuus

Taulukosta 2 voidaan huomata, että kyttäysohjelmien yleisyys on laskenut muutaman viimeisen vuoden aikana. Lisääntynyt ymmärrys tietoturvan tärkeydestä on saattanut edesauttaa tätä. Vahvan tunnistautumisen yleistyminen on voinut myös vaikuttaa tähän, sillä se estää pääsyn, jos tekijä tietää tunnuksen ja salasanan (Nyman ja Kankaala 2020). Tämän perusteella on jatkossakin suositeltavaa lisätä ymmärrystä oman tietoturvan tärkeydestä.

On tärkeää huolehtia omasta tietoturvasta, jotta haittaohjelmat eivät pääse asentumaan. Tulisikin pitää omat henkilökohtaiset älylaitteet salasanojen takana, jotta mahdollisesti väkivaltainen läheinen ei pääse luvatta niihin käsiksi. Eikä näitä salasanoja tule jakaa muille. Jos huomaa laitteessaan haittaohjelman tulee ottaa yhteyttä viranomaisiin. Omin päin haittaoh-

jelman poistaminen saattaa ilmoittaa asiasta vainoajalle.

Apple ja Google on omista sovelluskaupoistaan kieltänyt stalkkaussovellukset, mutta kolmannen osapuolen sovelluskaupat avaavat laajemmat sovellusvalikoimat. Android-laitteisiin voidaan ladata kolmannen osapuolen sovelluskaupoista sovelluksia, mutta Applen iOS-laitteisiin ei voi. Apple on kuitenkin huhujen mukaan mahdollistamassa kolmannen osapuolen sovelluskaupat tulevaisuudessa, sillä EU pakottaa heidät toimimaan niin (Gurman 2022). Tämä saattaisi mahdollistaa kyttäysohjelmien lataamisen myös Applen laitteille, jos Applella ei ole valtaa muiden sovelluskauppojen valikoimiin.

5 Pohdinta

Tässä tutkimuksessa on huomattu, että digitalisaation vaikutus maailmaamme on vaikuttanut myös lähisuhdeväkivaltaan. Kehityksen myötä on tullut uusia tapoja vainota toista ihmistä, joiden kehityksen perässä voi olla vaikea pysyä. Uusi kehittyvä teknologia lisää haitallisen seurannan mahdollisuuksia. Tutkimuksen tietojen pohjalta voidaan lähteä syventämään ymmärrystä teknologiseen puoleen, joita voidaan käyttää hyväksi väkivallan kokijoiden auttamisessa.

Tutkimusta olisi tärkeää jatkaa, etenkin suomalaisesta näkökulmasta. Erityisesti kuinka erilaisia seurantaohjelmistoja ja -laitteita mahdollisesti käytetään Suomessa väärin olisi kiinnostava jatkotutkimuksen aihe. Aiheesta ei tunnu vielä tänä päivänä olevan paljoakaan tilastoja maastamme.

Tosin onko kuitenkaan tärkeää miettiä yksittäisten laitteiden ja ohjelmistojen vaikutusta kokonaiskuvassa, vai tulisiko asiaa tarkastella yleisemmällä tasolla. Tuottaako tämä tutkimus enemmän haittaa, kuin hyötyä esimerkiksi listaamalla väkivallan tekijöille mahdollisia hyödynnettäviä tapoja. Tutkimuksen tieto on kuitenkin aiemmin ollut hajallaan löydettävissä, joten helpommin asioilta suojautuu, jos niistä on tietoinen.

Ohjelmistojen ja laitteiden kehittäjien tulisi jatkossa miettiä, että voidaanko laitteita käyttää helposti väärin. Laitteiden tulisi alusta alkaen olla testattuja erilaisten väärinkäyttömahdollisuuksien estämiseksi. Toisaalta haittaohjelmia on ollut aina ja niitä vastaan on taisteltu pitkään. Hyvällä tiedottamisella ja kouluttamisella voidaan myös lisätä ihmisten tietoturvallista toimintaa laitteiden kanssa. Tutkimuksen tilastoista huomattiinkin, että haittaohjelmien yleisyys on hieman laskenut. Sen on voinut mahdollistaa suojauksien kehittyminen ja ihmisten kehittyvä ymmärrys ja kouluttuneisuus tietotekniikasta.

Olisi myös tärkeää, että viranomaiset ymmärtäisivät paremmin digitaalisessa ympäristössä tapahtuvan vainoamisen tekniikat. Jos heillä on laajempaa tietoa aiheesta, voivat he auttaa väkivallan kokijoita paremmin ja ottaa heidän kokemuksensa digitaalisesta maailmasta todesta. Digitaalisen väkivallan uhreille tarjoavat apua muun muassa Naisten Linja ja Tukikeskus Varjo. Avun puoleen kannattaa ehdottomasti kääntyä, jos kokee digitaalista väkivaltaa.

Lähteet

Chatterjee, Rahul, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy ja Thomas Ristenpart. 2018. “The Spyware Used in Intimate Partner Violence”. Teoksessa *2018 IEEE Symposium on Security and Privacy (SP),* 441–458. https://doi.org/10.1109/SP.2018.00061.

Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P Suzor, Delanie Woodlock ja Bridget Harris. 2018. “Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms”. *Feminist Media Studies* 18 (4): 609–625. https://doi.org/10.1080/14680777.2018.1447341.

Eurostat. 2022. “Individuals frequently using the internet”. Viitattu 28. maaliskuuta 2023. https://ec.europa.eu/eurostat/web/products-datasets/-/tin00092.

Fraser, Cynthia, Erica Olsen, Kaofeng Lee, Cindy Southworth ja Sarah Tucker. 2010. “The new age of stalking: Technological implications for stalking”. *Juvenile and family court journal* 61 (4): 39–55. https://doi.org/10.1111/j.1755-6988.2010.01051.x.

Fundamental Rights, European Union Agency for. 2012. “Survey on violence against women in EU”. Viitattu 28. maaliskuuta 2023. https://fra.europa.eu/en/publications-and-resources/data-and-maps/survey-data-explorer-violence-against-women-survey.

Google. 2020. “Developer Program Policy: September 16, 2020 announcement”. Viitattu 8. huhtikuuta 2023. https://support.google.com/googleplay/android-developer/answer/10065487.

Gurman, Mark. 2022. “Apple to Allow Outside App Stores in Overhaul Spurred by EU Laws”. *Bloomberg* (13. joulukuuta 2022). Viitattu 8. huhtikuuta 2023. https://www.bloomberg.com/news/articles/2022-12-13/will-apple-allow-users-to-install-third-party-app-stores-sideload-in-europe.

Hakkarainen, Louna. 2019. *Digitaalinen väkivalta parisuhteessa ja sen jälkeen : Opas väkivallan kokijalle, ammattilaiselle ja läheiselle.* Naisten Linja Suomessa ry.

Harkin, Diarmaid, Adam Molnar ja Erica Vowles. 2020. “The commodification of mobile phone surveillance: An analysis of the consumer spyware industry”. *Crime, media, culture* 16 (1): 33–60. https://doi.org/10.1177/1741659018820562.

Kaspersky. 2021. “Digital Stalking in Relationships”. Viitattu 8. maaliskuuta 2023. https://media.kasperskydaily.com/wp-content/uploads/sites/86/2021/11/17164103/Kaspersky_Digital-stalking-in-relationships_Report_FINAL.pdf.

———. 2023. “The state of stalkerware in 2022”. Viitattu 8. maaliskuuta 2023. https://securelist.com/the-state-of-stalkerware-in-2022/108985/.

Laitinen, Merja, Jaana Kinnunen ja Riitta Hannus. 2017. *Varjosta valoon : eron jälkeisen vainon tunnistaminen, katkaisu ja uhrien selviytymisen tukeminen.* Ensi- ja turvakotien liitto.

Lenhart, Amanda, Michele Ybarra, Kathryn Zickuhr ja Myeshia Price-Feeney. 2016. *Online harassment, digital abuse, and cyberstalking in America.* Data / Society Research Institute.

Messing, Jill, Meredith Bagwell-Gray, Megan Lindsay Brown, Andrea Kappas ja Alesha Durfee. 2020. “Intersections of stalking and technology-based abuse: Emerging definitions, conceptualization, and measurement”. *Journal of family violence* 35 (7): 693–704. https://doi.org/10.1007/s10896-019-00114-7.

Mitchell, Connie, ja Deirdre Anglin. 2009. *Intimate partner violence: A health-based perspective.* OUP USA.

Moore, Anna. 2022. “‘I didn’t want it anywhere near me’: how the Apple AirTag became a gift to stalkers”. *The Guardian* (5. syyskuuta 2022). Viitattu 30. tammikuuta 2023. https://www.theguardian.com/technology/2022/sep/05/i-didnt-want-it-anywhere-near-me-how-the-apple-airtag-became-a-gift-to-stalkers.

NordVPN. 2022. “Mitä jailbreak tarkoittaa ja onko se turvallista?” Viitattu 10. huhtikuuta 2023. https://nordvpn.com/fi/blog/mika-on-jailbreak/.

Nyman, Linus, ja Laura Kankaala. 2020. “Mitä tehdä, jos ex-kumppanisi vainoaa sinua teknologian avulla”. *Disobey Outreach,* viitattu 8. huhtikuuta 2023. https://varjosta.fi/wp-content/uploads/2020/05/Mit%5C%C3%5C%A4_tehd%5C%C3%5C%A4_jos_ex-kumppanisi_vainoaa_sinua_teknologian_avulla.pdf.

Rikosuhripäivystys. 2023a. “Digitaalinen väkivalta ja vaino”. Viitattu 31. tammikuuta 2023. https://www.riku.fi/erilaisia-rikoksia/digitaalinen-vakivalta-ja-vaino/.

———. 2023b. “Lähisuhdeväkivalta voi koskettaa jokaista”. Viitattu 13. maaliskuuta 2023. https://www.riku.fi/erilaisia-rikoksia/lahisuhdevakivalta/.

ry, Oulun ensi- ja turvakoti. 2020. “Digitaalinen väkivalta”. Viitattu 10. huhtikuuta 2023. https://ensijaturvakotienliitto.fi/oulunensijaturvakoti/blogi/digitaalinen-vakivalta/.

THL. 2023. “Sukupuolistuneen väkivallan yleisyys”. Viitattu 10. huhtikuuta 2023. https://thl.fi/fi/web/sukupuolten-tasa-arvo/tasa-arvon-tila/vakivalta-ja-hairinta/sukupuolistuneen-vakivallan-yleisyys#lahisuhdevakivalta.

Tile. 2023. “Tile - How to Handle Unwanted Tracking”. Viitattu 1. maaliskuuta 2023. https://tileteam.zendesk.com/hc/en-150/articles/10532072435223-Tile-How-to-Handle-Unwanted-Tracking.