

# Arkirutiinit suomalaisnuorten nettirikosuhrikokemusten selittäjänä

*Marko Mikkola*



Sosiaalisen median alustat palveluineen ovat osa nuorten arkea, jossa mainittuja palveluita käytetään rutiininomaisesti päivittäin. Rutiininomaiseen sosiaalisen median käyttöön liittyy kuitenkin lieveilmiöitä, kuten nettirikollisuutta. Tässä tutkimuksessa tarkastelen 15–25-vuotiaiden suomalaisnuorten ( $N = 1200$ ) nettirikosuhrikokemusten taustalla olevia syitä rutiinitoimintojen teorian kahden ydintekijän, rikoksen kohteen näkyvyys motivoituneelle tekijälle ja kohteen soveltuvuus rikoksen uhriksi avulla. Rutiininomaiseen sosiaalisen median käyttöön liittyy kuitenkin myös erilaisia lieveilmiöitä, kuten nettirikollisuutta. Muina nettirikosuhrikokemusta selittävinä tekijöinä tutkimukseen on otettu aiempien kriminologian tutkimusten pohjalta ikä, sukupuoli, impulsiivisuus ja yksinäisyys. Logistisen regressioanalyysin tulosten mukaan nettirikosuhrikokemusta suomalaisnuorten osalta selittää kohteen näkyvyys motivoituneelle tekijälle. Muista tekijöistä impulsiivisuus ja yksinäisyys osoittautuivat uhrikokemusta selittäviksi syiksi. Tutkimustulosten mukaan kohteen näkyvyys motivoituneelle tekijälle näyttää olevan merkitsevämpi asia kuin kohteen soveltuvuus rikoksen uhriksi.

Asiasanat: Internet, sosiaalinen media, nettirikosuhri, rutiinitoimintojen teoria

Internetin ja sosiaalisen median käytön kiihkeä kasvu on mahdollistanut uusia keinoja rikoksenteleeseen (Jämsén 2020).

Internetissä tapahtuvaa tai internetiä hyödyntävää rikollisuutta nimitään vaihtelevasti nettirikollisuudeksi, internetirikollisuudeksi, verkkorikollisuudeksi tai kyberrikollisuudeksi. On jopa sanottu, että perinteinen rikollisuus on siirtymässä nettirikollisuuden mahdollistaville uusille alustoille internetissä. (Kivivuori ym. 2018, 402.) Nettirikollisuuden erikoisuus on, että se ulottuu valtiorajojen yli, koska internetissä ei ole samanlaisia rajoitteita tiedon liikkumiselle kuin mitä perinteiset valtion rajat asettavat fyysiselle liikkumiselle (Jämsén 2020). Nettirikollisuuden kasvussa on kyse erityisesti siitä, että internet ja sen palvelut ovat arkipäiväistyneet (Kivivuori ym. 2018, 402).

Koska nuoret käyttävät erityisen paljon internetiä, on kyberrikoksen uhriksi joutumisen todennäköisyysskin korkeimmillaan nuoruudessa (Näsi & Tanskanen 2016). Internetin käytön kontekstissa erityisesti sosiaalisessa mediassa mukana oleminen on nuorille tärkeää, koska sosiaalisessa mediassa he voivat rakentaa suoria ja epäsuoria ihmiskontakteja erityisesti niiden ihmisten kanssa, jotka jakavat tai tuntuvat jakavan samoja näkemyksiä ja mielipiteitä (Gao & Liu & Li 2017). Sosiaalisen median yhteisöt tarjoavat siten kasvualustan yhteenkuuluvuuden tunteelle, sosiaalisten verkostojen kasvattamiselle sekä henkiselle tuelle ja turvalle. Samanaikaisesti ne linkittyvät myös negatiivisiin lieveilmiöihin, kuten kiusaamiseen, rikollisuuteen, alkoholin tai huumaavien aineiden väärinkäyttöön, syömishäiriöihin tai rahapelaamiseen (Marcum & Higgins & Ricketts 2010; Näsi ym. 2016; Oksanen & Keipi 2013).

Riski joutua nettirikoksen kohteeksi on siten olemassa kaikilla nuorilla, mutta riski ei ole kaikilla samanlainen: vain osa nuorista joutuu rikoksen uhriksi internetissä. (Keipi

ym. 2017; Marcum & Higgins & Ricketts 2010; Näsi 2016; Näsi & Tanskanen 2016, 213; Oksanen & Keipi 2013.) Jotta nettirikosuhrikokemuksia voitaisiin ennaltaehkäistä, on ymmärrettävä millaisissa tilanteissa ja minkä tekijöiden takia netin rikollisten kohteesta voi tulla uhri ja ketkä nuorista erityisesti ovat riskiryhmässä. Rutiinotoimintojen teoria (Cohen & Felson 1979) on yleisesti käytetty teoria kriminologiassa kyberrikollisuuden tutkimuskentällä. Tästä syystä tarkastelen tutkimuksessani rutiinotoimintojen teorian kontekstissa 15–25-vuotiaiden ( $N = 1200$ ) suomalaisnuorten nettirikosuhrikokemuksia vastatessani tutkimuskysymykseeni: millaiset rutiinotoimintojen teorian mukaiset tekijät kasvattavat suomalaisnuorten riskiä joutua nettirikoksen uhriksi?

## Kyberrikollisuus ja kyberrikosuhrikokemus

Kyberrikollisuus ei ole rikosoikeudellinen nimike, vaan termin tarkoituksena on korostaa teknologiaa rikoksen tekovälineenä tai rikoksen tapahtumaympäristönä. (Näsi & Tanskanen 2016, 147; Kivivuori ym. 2018.). Kyberrikollisuuden muodot ovat moninaiset, samoin kuin kyberrikollisten kohteet. Uhriksi tai rikoksen kohteeksi voi joutua tietojärjestelmän lisäksi ihminen, organisaatio tai valtio. Tässä tutkimuksessa kyberrikollisuus tarkoittaa tietokoneavusteista rikollisuutta, jossa rikollisen tai rikollisten kohteena on toinen yksilö (Keipi 2015, 14–15; Kivivuori & Honkatukia 2006; Näsi & Tanskanen 2016, 151–154; Yar 2005, 409–411). Vaikka internetissä tapahtuvaa kiusaamista tai häiriköintiä ei sellaisenaan ole määritelty rikokseksi Suomen rikoslaisissa, on kiusaaminen ja häiriköinti tässä tutkimuksessa huomioitu rikosuhrikokemuksena niissä tapauksissa, joissa tutkimukseen osallistunut henkilö oli

merkinnyt mahdollisen kiusaamiseksi tai häiriköinniksi tulkittavan tilanteen tai tapahtuman rikokseksi. Rajauksessa korostuu siten vastaajan oma kokemus tapahtuneesta. Rajausta perustelee se, että raja kiusaamisen ja häiriköinnin sekä rikoslain määrittelemän rikoksen välillä on häilyvä.

Viimeisen vuosikymmenen aikana nettirikoksia käsittelevät tieteelliset tutkimukset ovat lisääntyneet paljon. Tutkimuksissa on tarkasteltu niin nettirikosten esiintyvyyttä (Kivivuori & Niemi 2015; Kaakinen & Näsi 2021; Näsi & Kaakinen 2020) kuin niihin johtaneita syitä (Holt ym. 2020; Mikkola ym. 2020; Oksanen & Keipi 2013). Nettirikosten ja uhrikokemusten osalta kuitenkin pitkän aikavälin vertailuluvut ovat ongelmallisia muun muassa rikoslaissa tapahtuvien muutosten takia. Muutokset rikoslaissa johtavat kasvuun ilmoitetuissa ja tilastoiduissa rikoksissa sekä piilorikollisuudessa. Esimerkiksi identiteettivarkaudesta tuli rikos vasta vuonna 2015. Samana vuonna identiteettivarkauksia raportoitiin 518 kappaletta ja vuonna 2018 yli 3800 kappaletta 17–74-vuotiaiden keskuudessa. Vastaavasti myös esimerkiksi tietomurtojen ja törkeiden tietomurtojen osalta kehitys on ollut kasvava vuodesta 2014 asti (Näsi & Kaakinen 2020, 142–143).

Suomessa nuorten tekemiä rikoksia ja uhrikokemuksia tutkitaan muun muassa Nuorisorikollisuuskyselyllä. Vuoden 2020 Nuorisorikollisuuskyselyyn (Kaakinen & Näsi 2021) vastasi 5674 15–16-vuotiaista nuorta 74 koulusta. Tutkimuksen mukaan nettirikosten yleisin muoto oli laitton verkkolataaminen ja koetuista nettirikoksista nettikiusaaminen. Muissa tutkimuksissa nettirikosuhrikokemusten määrä on vaihdellut. Atte Oksasen ja Tero Keipin (2013) tutkimuksen mukaan 15–24-vuotiaista suomalaisnuorista 5,3 % oli joutunut nettirikoksen uhriksi. Näsin ym. (2015) mukaan 15–30-vuotiaista suomalaisista 6,2 % oli joutunut nettirikoksen uhriksi.

Näissä tutkimuksissa raportoidut rikosuhrikokemusten luvut eivät ole suoraan verrannollisia keskenään tutkimusten metodologisista eroista ja laissa tapahtuneista muutoksista johtuen. Kuitenkin aikaisemman tutkimuksen valossa näyttää siltä, että suomalaisnuorten uhrikokemukset netissä olisivat kasvussa.

## Rutiinotoimintojen teoria

Kyberrikollisuutta ja kyberrikosuhrikokemuksia selittäviä teorioita on kriminologiassa useita, joista yleisesti käytetty on rutiinotoimintojen teoria (Cohen & Felson 1979). Teoria pyrkii selittämään rikostapahtumaa huomioimalla säännönmukaisuudet ihmisten laillisessa ja laittomassa toiminnassa. Rutiinotoimintojen teorian mukaan rikollisuus toimii ja kehittyy ihmisten arkisten rutiininomaisen toimintojen rinnalla. (Cohen & Felson 1979.) Ihmisten rutiininomainen toiminta ei ole jotain, mikä on kirjoitettu vain yksilön mieleen, vaan rutiinit ohjaavat meitä yhtä lailla niin yksilönä kuin yhteiskunnan jäsenenä. Rutiinit voidaan siten nähdä sosiaalisesti luotuina ja jaettuina toimintoina. (Reckwitz 2002, 250–260.) Rutiinotoimintojen teorian mukaisesti internetin ja sen palveluiden käytön kasvaessa ja käytön muuttuessa rutiininomaiseksi, kasvaa myös nettirikollisten määrä (Grabosky 2017, 18).

Rutiinotoimintojen teorian ytimessä on kolme osatekijää: motivoitunut rikosentekijä ja potentiaalinen kohde sekä tilanne, josta puuttuu rikoksen ehkäisevä toimija (Cohen & Felson 1979, 588). *Motivoitunut tekijä* voi olla yksilö tai se voi olla ryhmä yksilöitä, joilla on jokin motiivi rikoksen tekemiseen. *Potentiaalinen kohde* voi olla kuka vain, jonka kohtaa rikosentekijä tai -tekijät tilassa, josta puuttuu rikoksen tapahtuman *ehkäisevä toimija* (Cohen & Felson 1979; Felson 2016). Rutiinotoimintojen teorian mukaisesti

tilanteessa, joissa kaikki kolme edellä mainittua ehtoa toteutuvat, rikoksen tapahtumisen todennäköisyys on suuri.

Vaikka rutiinotoimintojen teoria kehitettiin aikana, jolloin internet oli vain harvojen käytettävissä, eikä sosiaalisesta mediasta puhuttu, on teoriaa käytetty hyvin laajasti selittämään kyberrikosuhrikokemuksia (Marcum & Higgins & Ricketts 2010; Näsi ym. 2016; Oksanen & Keipi 2013; Reyns & Henson & Fisher 2011). Fyysisessä maailmassa rutiinotoimintojen teoria lähtee liikkeelle oletuksesta, että motivoitunut tekijä ja potentiaalinen kohde kohtaavat samassa ajassa ja tilassa ja tilanteessa, josta puuttuu ehkäisevä toimija. Internetin kontekstissa tätä tekijän ja kohteen kohtaamista samassa ajassa ja paikassa ei kuitenkaan välttämättä tapahdu. Tästä syystä rutiinotoimintojen teorian käyttöä nettirikosten yhteydessä on myös kritisoitu (Yar 2005). Esitettyyn kritiikkiin on vastattu sillä, että sosiaalisen median alustat toimivat digitaalisessa maailmassa fyysistä maailmaa vastaavina kohtaamispaikkoina tietoverkkojen avulla, vaikka motivoitunut tekijä ja potentiaalinen kohde eivät kohtaa samassa ajassa ja paikassa (Eck & Clarke 2003; Reyns 2011). Nettirikosuhrikokemuksia selitettäessä rutiinotoimintojen teorian avulla teorian ytimiksi ovat muotoutuneet: *rikoksen kohteen näkyvyys motivoituneelle tekijälle, kohteen soveltuvuus rikoksen uhriksi ja ehkäisevän toimijan puuttuminen tilanteesta* (ks. Marcum & Higgins & Ricketts 2010; Reyns, Henson & Fisher 2011; Näsi ym. 2016).

Empiirisesti rutiinotoimintojen teoriaan kyberrikosten uhriksi joutumisen selittämisessä on käyttänyt muun muassa Marcum työryhmineen (2010), joka tutki yhdysvaltalaisen yliopiston ensimmäisen vuoden opiskelijoiden nettirikoskokemuksia ( $N = 744$ ). Tutkimuksen mukaan kohteen näkyvyys rikoksen tekijälle internetissä ja soveltuvuus rikoksen uhriksi iän ja sukupuolen kanssa

kasvattivat nuorten riskiä joutua nettirikoksen uhreiksi. Suomessa Oksanen ja Keipi (2013) ovat tutkineet 15–24-vuotiaiden suomalaisnuorten nettirikosuhrikokemuksia ( $N = 1074$ ) osana laajempaa tutkimusta niin ikään rutiinotoimintojen teorian avulla todeten, että näkyvyys rikoksen tekijälle lisää riskiä uhriksi joutumiselle iän ja sukupuolen lisäksi. Näsi ja kumppanit puolestaan havaitsivat (2016) kansainvälisessä tutkimuksessaan, että 15–30-vuotiaiden suomalaisnuorten ( $N = 555$ ) nettirikosuhrikokemuksia selittivät kohteen näkyvyys rikoksen tekijälle, kohteen soveltuvuus nettirikoksen uhriksi ja sukupuoli.

Tämä tutkimus täydentää tätä kotimaisten tutkimusten kenttää tarkastelemalla laajalla iän, sukupuolen ja asuinalueen mukaan kansallisesti edustavalla aineistolla rutiinotoimintojen teorian elementtien *rikoksen kohteen näkyvyys motivoituneelle tekijälle ja kohteen soveltuvuus rikoksen uhriksi* yhteyttä suomalaisten nuorten kyberrikosuhrikokemuksiin. Koska internetin ja sosiaalisen median käyttötavat muuttuvat ajassa, on tärkeää, että uusien tutkimusten avulla seurataan vastaavasti mahdollista muutosta rikosuhrikokemuksia selittävissä tekijöissä. Tällöin voidaan ylläpitää ja tarvittaessa muuttaa ohjeita ja oppaita, joiden avulla pyritään ennaltaehkäisemään tai vähentämään nuorten nettirikosuhrikokemuksia.

## Tutkimusasetelma

Artikkelin analyysi perustuu YouGamble-aineistoon, joka kerättiin osana Rahapeli-ongelmat ja verkkoyhteisöt -hanketta 16.3–12.4.2017 välisenä aikana. Aineisto kerättiin internetkyselynä, ja sen keräämisestä vastasi Dynata (ent. Survey Sampling International). Aineiston kerääminen toteutettiin LimeSurvey-ohjelmistolla ja strukturoidun verkkolomakkeen avulla. Aineistonkeruussa käytettiin

Taulukko 1. Aineiston kuvailevat tiedot.

Muuttuja	Keskiarvo	Keskihajonta	Vaihteluväli	Cronbach $\alpha$
Ikä	21,29	2,85	15–25	
Näkyvyys sosiaalisessa mediassa	5,30	3,10	0–14	0,764
Yksinäisyys	5,53	1,78	3–9	0,830
Vaaralliset sivustot	0,93	1,37	0–9	0,703
Aggressiivinen viestintä	0,59	1,31	0–7	
Impulsiivisuus	1,96	1,69	0–5	0,745
Kategoriset muuttujat	Arvo	<i>n</i>	%	
Rikosuhri	Kyllä	95	7.9	
	Ei	1105	92.1	
Sukupuoli				
Mies	1	600	50	
Nainen	2	600	50	
Rikosuhri, sukupuolen mukaan	Mies	56	59	
	Nainen	39	41	

kiintiöotantaa. Kyselyn toteutuksessa kyselyyn asetettiin ikäryhmiä, sukupuolta ja asuinalueita koskevat kiintiöt, jotka vastasivat 15–25-vuotiaiden suomalaisten väestöstä vuonna 2016.

Kyselyyn vastasi 1200 vastaajaa. Tutkimuksessa käytettyjen muuttujien tunnusluvut on esitetty Taulukossa 1. Vastaajien joukossa oli suurempi määrä opiskelijoita ja pienempi määrä alle 18-vuotiaita kuin suomalaisten väestössä tilastojen mukaan on. Erot ovat kuitenkin niin pieniä, että aineistoa voidaan pitää luotettavana, ja painotuksia iän tai koulutustaustan suhteen ei tarvitse tehdä. (ks. Oksanen ym. 2018; Sirola & Kaakinen & Oksanen 2018).

## Muuttujat

### Selitettävä muuttuja

Tutkimuksen selitettävä muuttuja perustuu kysymykseen ”Oletko joutunut Internetis-

sä rikoksen kohteeksi viimeisen kuluneen kolmen vuoden aikana?”. Vastaajille tarjottiin vastausvaihtoehtoiksi ”Kyllä” tai ”Ei” ( $0 = ei$ ,  $1 = kyllä$ ). Kaiken kaikkiaan 95 nuorta (naiset  $n = 39$ ) vastasi joutuneensa rikoksen uhriksi. Nämä vastaajat saivat tämän jälkeen valita mielestään parhaiten soveltuvan rikosnimikkeen vastauslomakkeesta valmiiden vaihtoehtojen joukosta tai kirjoittaa itse parhaiten rikosta kuvaavan nimikkeen lomakkeen vapaaseen kenttään. Vastaajista osa käytti molempia vaihtoehtoja vastatessaan kysymykseen. Tämän vuoksi ilmoitettujen rikosnimikkeiden määrä ylittää rikosuhrien kokonaismäärän. Rikosuhrikokemus tutkimuksen aineistossa perustuu vastaajan näkemys siihen, tapahtuiko tilanteessa rikos vai ei. Vastaavaa kysymystä rikoksen kohteeksi joutumisesta on käytetty aiemmissa tutkimuksissa (Kaakinen ym. 2018; Oksanen & Keipi 2013).

## Selittävät muuttajat

Tutkimuksen selittävät muuttajat muodostuvat rutiinitoimintojen teorian (Cohen & Felson 1979) kahden ydintekijän mukaisista kyberrikollisuuden uhrikokemuksia selittävästä muuttujista: rikoksen kohteen näkyvyys motivoituneelle tekijälle ja kohteen soveltuvuus rikoksen uhriksi. Kohteen näkyvyyttä motivoituneelle tekijälle mitataan muuttujilla *Näkyvyys sosiaalisessa mediassa* ja *Vaaralliset sivustot*. Kohteen soveltuvuutta rikoksen uhriksi mittaa muuttuja *Aggressiivinen viestintä*. Lisäksi analyysiin otettiin selittäviksi muuttujiksi *Impulsiivisuus*, *Yksinäisyys*, *Ikä* ja *Sukupuoli*, joiden on aikaisemmassa kotimaisessa tutkimuksessa osoitettu olevan yhteydessä nettirikosuhrikokemuksiin (Mikkola ym. 2020; Näsi ym. 2016; Oksanen & Keipi 2013).

*Näkyvyys sosiaalisessa mediassa* -muuttuja muodostettiin kysymyksistä ”Kuinka usein jaat sisältöä sosiaalisessa mediassa?” ja ”Kuinka usein lataat kuvia itsestäsi sosiaaliseen mediaan?”. Vastausvaihtoehdot olivat 7-portaisella Likert-asteikolla välillä 0 = *En koskaan* ja 7 = *Päivittäin*. Muuttuja saa arvon välillä 0–14 vastaajan aktiivisuuden perusteella. Aiemmissä tutkimuksissa kohteen näkyvyyttä potentiaaliselle rikolliselle on mitattu sosiaalisen median käytön ja käyttötavan mukaan (Bossler, Holt & May 2012; Mikkola ym. 2020; Näsi ym. 2016).

*Vaaralliset sivustot* -muuttuja (ks. Mikkola ym. 2020) muodostettiin kysymyksen ”Kuinka usein käytät seuraavia sosiaalisen median palveluita?” vastausvaihtoehdoista Anonyymi verkko (esim. Tor, Freenet, I2P), Rahapeliyhdistöiden ja/tai nettikasinoiden sivustot (esim. Veikkaus, NettiCasino tai muut vastaavat) ja Rahapeliaiheiset keskustelufoorumit tai yhteisöt, joissa vastausvaihtoehdot olivat 0 = *En koskaan* ja 3 = *Useita kertoja päivässä* välillä. Lopullinen muuttuja saa arvon 0 ja 9 välillä sivustojen kokonaiskäytön aktiivi-

suuden mukaan. Muuttuja arvioi kohteen soveltuvuutta kyberrikoksen uhriksi rutiinitoimintojen teorian mukaisesti.

*Aggressiivinen viestintä* -muuttuja on muodostettu kysymyksestä ”Kuinka usein lähetät sosiaalisessa mediassa toisia käyttäjiä loukkaavia tai uhkaavia viestejä?”. Vastausvaihtoehdot olivat 7-portaisella Likert-asteikolla välillä 0 = *En koskaan* ja 7 = *Päivittäin*. Ihmiset, jotka tekevät rikoksia tai joiden käyttäytyminen on riskialtista ovat suuremmissa vaarassa joutua rikoksen uhriksi kuin muut (Cohen & Felson 1979; Felson 2016). Voidaan siis ajatella, että ne nuoret, jotka käyttävät aggressiivista viestintää muita kohtaan ovat suuremmissa riskissä joutua itse rikoksen kohteeksi kuin muut (Kulig ym. 2017).

## Impulsiivisuus, yksinäisyys, ikä ja sukupuoli

Impulsiivisella käyttäytymisellä tarkoitetaan tässä sellaista käyttäytymisen muotoa, jossa tavoitellaan välitöntä palkintoa ajattelematta käyttäytymisen seurauksia. (Gottfredson & Hirschi 1990; Reyns ym. 2014; Schreck 1999; Tagney, Boone & Baumeister 2018.) Impulsiivisuuden on aiemmissa tutkimuksissa osoitettu olevan yhteydessä sekä rikoksen tekemiseen että rikoksen uhriksi joutumiselle niin fyysisen kuin digitaalisen maailman kontekstissa (Kivivuori & Honkatukia 2006; Mikkola ym. 2020). Tässä tutkimuksessa *Impulsiivisuus* muuttuja mitattiin käyttämällä Eysenckin impulsiivisuusasteikkoa, Eysenck Impulsiveness Scale (EIS; Eysenck & Eysenck 1978). Asteikko muodostuu viidestä kysymyksestä, joista kysymys ”Harkitsetko usein etukäteen tarkkaan tekemisiäsi?” vastaukset on uudelleen koodattu käänteisiksi. Lopullinen muuttuja saa arvon 0–5. Ikää tutkimuksessa käsiteltiin jatkuvana muuttujana. Tutkimuksen osallistuneiden keski-ikä oli 21,3 vuotta ja iän keskihajonta 2,9 vuotta.

*Yksinäisyyden* on havaittu johtavan negatiivisiin käyttäytymismalleihin kuten pakonomaiseen sosiaalisen median käyttöön ja siten negatiivisiin kokemuksiin internetissä (Griffiths 2000; Kim & Larose & Peng 2009; Yen ym. 2008) ja uusimman kotimaisen tutkimuksen mukaan sen on osoitettu selittävän myös nettirikosuhrikokemuksia (Mikkola ym. 2020). *Yksinäisyys*-muuttujaa mitataan yleensä laajalla R-UCLA (Revised UCLA Loneliness Scale) yksinäisyysasteikolla. R-UCLA-mittarin ongelmana pidetään sen laajuutta, mistä syystä mittarista on luotu lyhyempi kolmen kysymyksen yksinäisyysasteikko. Kyseisen asteikon luotettavuutta on tutkittu kansainvälisissä, monikulttuurisissa tutkimuksissa (De Jong Gierveld & Van Tilburg 2010; Hughes ym. 2004). Yksinäisyyttä tutkittiin kysymällä vastaajilta ”Kuinka usein tunnet itsesi yksinäiseksi?”, ”Kuinka usein tunnet itsesi ulkopuolelle jätetyksi” ja ”Kuinka usein tunnet itsesi eristäytyneeksi muista ihmisistä?”. Vastausvaihtoehdoiksi oli annettu 1 = *En juuri koskaan*, 2 = *Silloin tällöin* ja 3 = *Useasti*. Lopullinen muuttuja *Yksinäisyys* saa arvon 3 ja 9 välillä. Yksinäisyyden on nähty ennustavan yksilön psykologista hyvinvointia (Baumeister & Leary 1995).

## Analyyysi

Analyyysi toteutettiin logistisella regressioanalyysillä (Taulukko 3.). Logistisen regres-

sioanalyysin tulokset raportoidaan riskisuhteina (OR) ja marginaaliefekti-kertoimina (AME). Riskisuhde kertoo, kuinka paljon vertailtavien ryhmien riskit (odds) eroavat toisistaan. Riskisuhteiden vertailua selkeämpää on käyttää marginaaliefektiä, jonka avulla voidaan tulkita, miten selittävä muuttuja vaikuttaa todennäköisyyteen, että tutkimukseen osallistunut kuuluu selitettävään luokkaan, nettirikoksen uhreihin. Marginaaliefektien luvut ovat muutettavissa prosenttiluvuiksi. (Mood 2010).

## Tulokset

Kaikista tutkimukseen osallistuneista ( $N = 1200$ ) 95 henkilöä (8 %) ilmoitti joutuneensa viimeisen kolmen vuoden aikana kyberrikoksen kohteeksi. Tutkimukseen osallistuneista miehistä 56 (9,3 %) ilmoitti joutuneet kyberrikoksen kohteeksi, kun vastaava luku naisilla oli 39 (6,5 %). Yleisimmät raportoidut rikollisuuden muodot tutkimusaineiston valmiiden vaihtoehtojen mukaan olivat petos (33 tapausta) ja kunnianloukkaus (32 tapausta) ja harvinaisin identiteettivarkaus (14 tapausta). Vastaajista ne, jotka olivat valinneet vastausvalikon kohdan ”Muu, mitä?” olivat ilmoittaneet yleisimmäksi rikoksen muodoksi varkauden (4 tapausta).

Taulukko 2. Ilmoitetut rikosmuodot ja jakaumat sukupuolittain

Rikosmuoto	Sukupuoli				Yht.
	Mies	%-osuus	Nainen	%-osuus	
Kunnianloukkaus	19	59,4	13	40,6	32
Laiton uhkaus	15	60,0	10	40,0	25
Identiteettivarkaus	11	78,6	3	21,4	14
Petos	19	57,6	14	42,4	33
Seksuaalinen ahdistelu	7	35,0	13	65,0	20
Muu	6	58,9	7	41,1	13

Taulukko 3. Logistisen regressioanalyysi, vastemuuttujana kyberrikosuhrikokemus ( $N = 1200$ ).

Selittävä muuttuja	OR	P	AME
Ikä	0,967	0,393	-0,002
Sukupuoli	0,771	0,300	-0,018
Näkyvyys sosiaalisessa mediassa	1,006	0,870	0,000
Impulsiivisuus	1,350	0,000	0,021***
Yksinäisyys	1,174	0,012	0,011*
Vaaralliset sivustot	1,174	0,021	0,011*
Aggressiivinen viestintä	1,114	0,141	0,007
$N$	1200		
Log-likelihood	-307,485		
LR $\chi^2$	49,18***		
Cragg & Uhler's $R^2$	0,094		

\* $p < 0,05$ . \*\* $p < 0,01$ . \*\*\* $p < 0,001$ .

Sukupuoli 1 = mies, 2 = nainen

Muu kyberrikosmuodot, kuten kuvien luvaton levittäminen ja pornomainonnan näyttö alaikäiselle saivat vain yksittäisiä mainintoja. Rikosmuodot ja jakaumat ovat sukupuolittain Taulukossa 2. Tutkimuksen nettirikosuhrien kokemukset vastaavat suhteellisesti poliisin tilastoimia lukuja (Jämsén 2020).

Logistisen regressioanalyysin mukaan rutiinitoimintojen teorian ydintekijöistä ainoastaan *Vaaralliset sivustot* (OR = 1,174,  $p = 0,021$ , AME = 0,011) olivat tilastollisesti merkitsevässä yhteydessä nettirikosuhrikokemuksiin, kun muut mallissa mukana olleet tekijät huomioitiin. Muista analyysissä mukana olleista selittäjistä *Impulsiivisuus* (OR = 1,350,  $p < 0,000$ , AME = 0,021) ja *Yksinäisyys* (OR = 1,174,  $p = 0,012$ , AME = 0,011) selittivät nettirikosuhrikokemuksia. (Taulukko 3.).

## Pohdinta

Tässä tutkimuksessa tarkasteltiin, miten rutiinitoimintojen teorian mukaiset muuttujat

selittävät suomalaisnuorten nettirikosuhrikokemuksia. Nettirikosuhrikokemuksilla tarkoitettiin vastaajien omaa kokemusta teon kohteeksi joutumisesta, jolloin nettirikokset voivat tässä yhteydessä sisältää muitakin tekoja kuin rikoslaisa rikokseksi määriteltyjä tekoja. Rikollisuuden syiden ymmärtäminen on ehdoton edellytys sille, että rikollisuutta voidaan ennaltaehkäistä (Kivivuori ym. 2018, 144–245). Ennaltaehkäisy tarkoittaa puuttumista rikollisen toimintaan, mutta myös pohdintaa siitä, miten yhteiskunta ja yksilöt omilla toimillaan voisivat pienentää rikoksen tapahtumisen todennäköisyyttä. Koska internet tarjoaa alati muuttuvan ympäristön rikostentekijöille, on syytä nettirikollisuuden taustalla vastaavasti tarkasteltava säännöllisesti.

Nettirikosuhrikokemukset ovat tämän tutkimuksen mukaan varsin yleisiä (8 % vastaajista) ja miehet joutuvat useammin nettirikoksen uhriksi kuin naiset. Naisten kohdalla yleisin rikosmuoto on tämän tutkimuksen mukaan petos. Aikaisemman tutkimuksen



mukaan juuri petosten määrissä on havaittu eniten kasvua Suomessa (Jämsén 2020). Samoin aiemmissa tutkimuksissa seksuaalinen häirintä on ollut yleisin naisten kohtaama rikosmuoto (Duggan 2014; Näsi ym. 2016). Tässä tutkimuksessa seksuaalinen ahdistelu on toiseksi yleisin naisten raportoima nettirikosuhrikokemuksen laji, jota raportoi-tiin yhtä usein kuin kunnianloukkauksia. Miesten kohdalla yleisimpiä rikosmuotoja olivat petos ja kunnianloukkaus. Aiemmissa tutkimuksissa yleisimpiä miesten kokemia rikosmuotoja olivat kunnialoukkaus ja väkivallalla uhkaaminen (Näsi ym. 2015). Erot tuloksissa aiempiin tutkimustuloksiin nähden voivat selittyä muutoksilla laissa, mutta myös sillä, kuinka aktiivisesti nuoret ilmoittavat kokemuksistaan (Kivivuori & Niemi 2015).

Tutkimuksessa rutiinotoimintojen teorian ydintekijöistä, rikoksen kohteen näkyvyys motivoituneelle tekijälle ja kohteen soveltuvuus rikoksen uhriksi, ainoastaan vaarallisten sivujen käyttö rikoksen kohteen näkyvyyttä kuvaavana tekijänä selitti nettirikosuhrikokemuksia. Huomioiden sen, että suomalaisnuorista noin 92 % käyttää sosiaalisen median palveluita (SVT 2020) on mahdollista, että pelkkä sosiaalisen median käyttö omien tietojen ja kuvien jakamiseen ei ole yleisyytensä takia enää merkittävä nettirikosuhrikokemusta kasvattava riski. Kohteen soveltuvuutta rikoksen uhriksi tutkimuksessa indikoi aggressiivinen viestintä internetissä, joka ei tässä tutkimuksessa muodostunut merkitseväksi selittäjäksi. Löydös on mielenkiintoinen, sillä rutiinotoimintojen teorian mukaisesti aggressiivinen viestintä kiinnittää muiden huomion ja lisää kohteen soveltuvuutta rikoksen uhriksi. Tulos voi johtua siitä, että aggressiivista viestintää on sosiaalisessa mediassa siinä määrin, että erottuakseen muista vastaavista viesteistä, viestin sisällössä pitäisi olla jotain varsin poikkeavaa. Tällöin voidaan pohtia, indikoisiko kohteen soveltuvuutta

joku muu tekijä herkemmin. Toisaalta rutiinotoimintojen teorian näkökulmasta on myös mielenkiintoista pohtia, onko nettirikoksissa kohteen näkyvyys soveltuvalle tekijälle kuitenkin merkitsevämpi asia kuin kohteen soveltuvuus. Samoin tulosta voi selittää myös se, että aggressiivisen viestinnän arviointi perustuu vastaajan omaan arvioon, jolloin vastaaja itse voi arvioida viestintänsä aggressiiviseksi mutta vastaanottajat eivät.

Tutkimuksen tulokset rutiinotoimintojen teorian mukaisten muuttujien osalta ovat siten saman suuntaiset kuin Oksasen ja Keipin (2013) sekä Näsin ym. (2016) tutkimustulokset, joiden mukaan rikoksen kohteen näkyvyys lisää nettirikosuhrikokemuksen riskiä. Sen sijaan kohteen soveltuvuus ei tässä tutkimuksessa selittänyt nettirikosuhrikokemusta, toisin kuin Näsin ja hänen tutkimusryhmänsä (2016) tutkimuksessa. Erot tuloksissa voivat selittyä eroilla tutkimusten metodologiassa tai sillä, että eri tutkimuksissa on keskitytty erilaisiin rikosnimikkeisiin. Toisaalta erot tutkimusten välillä voi selittyä myös sillä, että rutiinotoimintojen teoria kykenee selittämään joitain nettirikoksen muotoja paremmin kuin toisia.

Tässä tutkimuksessa vastaajan sukupuoli ja ikä eivät olleet yhteydessä nettirikosuhrikokemuksiin. Tulos eroaa aikaisemmista kotimaisista ja kansainvälisistä tutkimuksista, joiden mukaan sekä sukupuoli että ikä olivat yhteydessä uhrikokemukseen (Marcum ym. 2010; Oksanen & Keipi 2013; Näsi ym. 2016.). Syy tulokselle voi selittyä sillä, että tässä tutkimuksessa oli mukana useampia erilaisia rikosmuotoja, mistä syystä ikä tai sukupuoli erot eivät korostu tuloksissa. Sen sijaan, kuten aikaisemmissakin nettirikollisuutta käsittelevissä kotimaisissa ja kansainvälisissä tutkimuksissa (Kivivuori & Honkatukia 2006; Mikkola ym. 2020; Reyns ym. 2014; Tagney ym. 2018), yksinäisyys ja impulsiivisuus lisäsivät riskiä nettirikosuhrikokemuk-

sille myös tässä tutkimuksessa. Tulos antaa viitteitä siitä, että nettirikosuhrikokemuksia pystytään selittämään parhaiten yhdistämällä eri teorioista nousevia selittäjiä sen sijaan, että pitäydytään yksinomaan rutiinitoimintojen teoriassa. Rutiinitoimintojen teoria on integroitu muihin kriminologian teorioihin myös aikaisemmissa tutkimuksissa pyrkimyksenä selittää nettirikosuhrikokemuksia mahdollisimman kokonaisvaltaisesti (ks. Holt & van Wilsem, van de Weijer & Leukfeldt 2020; Ngo & Paternoster 2011, Reisig & Golladay, 2019; Turanovic & Pratt, 2014).

Aikaisempien tutkimusten mukaan syyt nettirikoksen uhriksi joutumiselle voivat olla moninaiset ja seuraukset negatiivisen vaikutuksensa takia kauaskantoiset sekä yksilöllä että yhteiskunnalle (Kivivuori ym. 2018, 118–126). Rikoksen uhriksi joutuminen yleisesti, riippumatta siitä tapahtuiko rikos fyysisessä vai virtuaalisessa maailmassa, voi johtaa moninaisiin sosiaalisiin ja mielenterveydellisiin ongelmiin (Kivivuori ym. 2018; Oksanen & Keipi 2013, 2; Saari 2009). Onkin erittäin tärkeää ymmärtää, mitkä tekijät kasvattavat nuorten riskiä joutua nettirikoksen uhriksi, jotta yhteiskunnan eri osa-alueilla kyetään suunnittelemaan ja toteuttamaan oikeanlaiset rikosuhrikokemusten ennaltaehkäisyyn tähtäävät toimet. Myös YK:n lapsen oikeuksien komitean 25. yleiskommentti lapsen oikeuksista digitaalisissa ympäristöissä velvoittaa jäsenmaita lasten suojelemiselle digitaalisen maailman haittavaikutuksilta (Lapsiasiavaltuutettu 2018).

Tämä tutkimus perustui laajaan ja kansallisesti edustavaan otokseen 15–25-vuotiaista suomalaisnuorista, mikä vahvistaa saatujen tulosten merkitystä. Nettirikosuhrikokemuksen määrittelyssä huomioitiin laajasti vastaajien erilaiset uhrikokemukset. Analyysissä huomioitiin kaksi rutiinitoimintojen teorian ydintekijöistä eli rikoksen kohteen näkyvyys motivoituneelle tekijälle ja koh-

teen soveltuvuus rikoksen uhriksi. Aineisto ei tarjonnut mahdollisuutta huomioida teorian kolmannen tekijän merkitystä, eli ehkäisevän toimijan puuttumista. Tätä voidaan pitää analyysin rajoituksena. Tulevissa tutkimuksissa myös tämä tekijä olisi hyvä huomioida. Kohteen soveltuvuutta rikoksen uhriksi mitattiin aggressiivisella viestinnällä, joka ei analyysissä osoittautunut merkitseväksi selittäjäksi. Jatkossa olisi hyvä tarkastella kohteen soveltuvuuden merkitystä myös muunlaisella muuttujalla.

Näistä rajoituksista huolimatta tämä tutkimus osoittaa vaarallisten sivustojen, kuten anonyymien verkon ja rahapelisivustojen tai -foorumien käytön lisäävän nettirikosuhrikokemusten riskiä yksilön itsekontrollin ja yksinäisyyden rinnalla. Mikäli näillä sivustoilla vierailu on osa nuoren arkipäivää, on kasvanut riski uhrikokemuksille tärkeä tunnistaa. Kyberrikosuhrikokemuksen yhteydessä merkityksellistä on myös avun saanti mahdollisen uhrikokemuksen jälkeen. Tämä vaade tuli selkeästi esille esimerkiksi Vastaamo-tietomurron yhteydessä (Valtioneuvosto 2020). Tätä silmällä pitäen on olennaisen tärkeää, että nuorten vanhemmat kykenevät tunnistamaan nuorten nettikäyttäytymisen lisäksi nettirikoksen ja ymmärtävät kuinka toimia tilanteessa, jossa tapahtuma on ilmoitettava poliisille ja nuori on tarvittaessa saatava ammattiavun piiriin.

## Lähteet

- Baumeister, Roy & Leary, Mark Richard (1995) The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin* 117 (3), 497–529. (Viitattu 24.4.2021.)
- Bossler, Adam & Holt, Thomas & May, David (2012) Predicting online harassment victimization among a juvenile population. *Youth and Society* 44 (4), 500–523. <https://doi.org/10.1177/0044118X11407525> (Viitattu 17.2.2021.)

- Cohen, Lawrence & Felson, Marcus (1979) Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44, 588–608. [https://www.researchgate.net/publication/238322365\\_Social\\_Change\\_and\\_Crime\\_Rate\\_Trends\\_A\\_Routine\\_Activity\\_Approach](https://www.researchgate.net/publication/238322365_Social_Change_and_Crime_Rate_Trends_A_Routine_Activity_Approach). (Viitattu 26.1.2021.)
- Duggan, Maeve (2014) *Online harassment*. [www.pewinternet.org/2014/10/22/online-harassment](http://www.pewinternet.org/2014/10/22/online-harassment). (Viitattu 24.4.2021.)
- Eck, John & Clarke, Ronald (2003) *Classifying common police problems: A routine activity approach*. *Crime Prevention Studies*. Monsey, NY: Criminal Justice Press.
- Felson, Marcus (2016) Routine Activity Approach. Teoksessa Richard Wortley & Michael Townsley (toim.) *Environmental Criminology and Crime Analysis*, 87–97. New York: Routledge.
- Gao, Wei & Liu, Shaopeng & Li, Jingyuan (2017) How does social presence influence SNS addiction? A belongingness theory perspective. *Computers in Human Behavior* 77, 347–355. <https://doi.org/10.1016/j.chb.2017.09.002> (Viitattu 4.2.2021.)
- Gottfredson, Michael & Hirschi, Travis (1990) *A general theory of crime*. Stanford University Press.
- Grabosky, Peter (2017) The Evolution of Cybercrime, 2006–2016. Teoksessa Thomas Holt (toim.) *Cybercrime Through an Interdisciplinary Lens*. New York: Routledge, 15–36.
- Griffiths, Mark (2000) Excessive Internet Use: Implications for Sexual Behavior. *CyberPsychology & Behavior* 3 (4). <https://doi.org/10.1089/109493100420151> (Viitattu 24.4.2021.)
- Holt, Thomas & van Wilsem, Johan & van de Weijer, Steve & Leukfeldt, Rutger (2020) Testing an Integrated Self Control and Routine Activities Framework to Examine Malware Infection Victimization. *Social Science Computer Review* 38, 187–206. <https://doi.org/10.1177/0894439318805067> (Viitattu 7.2.2021.)
- Kivivuori, Janne & Honkatukia, Päivi (2006) Nuorten rikollisuuden ja sen kontrollin kehityssuuntia. Teoksessa Päivi Honkatukia & Janne Kivivuori (toim.) *Nuorisoriikollisuus määrä, syyt ja kontrolli*, 341–361. Helsinki: Oikeuspoliittinen tutkimuslaitos. [https://helda.helsinki.fi/bitstream/handle/10138/152459/221\\_Honkatukia\\_Kivivuori\\_2006.pdf?sequence=1](https://helda.helsinki.fi/bitstream/handle/10138/152459/221_Honkatukia_Kivivuori_2006.pdf?sequence=1) (Viitattu 13.2.2021.)
- Hughes, Mary Elizabeth & Waite, Lind & Hawkey, Louise & Cacioppo, John (2004) A short scale for measuring loneliness in large surveys: Results from two population-based studies. *Research on Aging*, 26 (6), 655–672. <https://doi.org/10.1177/0164027504268574> (Viitattu 13.2.2021.)
- Jämsén, Christian (2020) *Tietoverkkorikollisuus poliisin silmin 2019–2020*. Keskusrikospoliisi. Poliisin kyberrikostorjuntakeskus. <https://poliisi.fi/blogi/-/blogs/tietoverkkorikollisuus-poliisin-silmin-2019-2020>. (Viitattu 25.1.2021.)
- Kaakinen, Markus & Keipi, Teo & Räsänen, Pekka & Oksanen, Atte (2018) Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking* 21 (2), 129–137. <https://doi.org/10.1089/cyber.2016.0728> (Viitattu 1.3.2021.)
- Kaakinen, Markus & Näsi, Matti (2021) *Nuorten rikoskäyttäytyminen ja uhrikokemukset 2020*. Katsauksia 47/2021. Helsinki: Kriminologian ja oikeuspolitiikan instituutti. <http://hdl.handle.net/10138/326622> (Viitattu 7.3.2021.)
- Keipi, Teo & Näsi, Matti & Oksanen, Atte & Räsänen, Pekka (2017) *Online Hate and Harmful Content. Cross-national perspectives*. London: Taylor & Francis.
- Kim, Junghyun, Larose, Robert & Peng, Wei (2009) Loneliness as the cause and the effect of problematic internet use: The relationship between internet use and psychological well-being. *Cyberpsychology & Behavior* 12 (4), 451–455. <https://doi.org/10.1089/cpb.2008.0327> (Viitattu 24.4.2021.)
- Kivivuori, Janne & Aaltonen, Mikko & Näsi, Matti & Suonpää, Karoliina & Danielsson, Petri (2018) *Kriminologia. Rikollisuus ja kontrolli muuttuvassa yhteiskunnassa*. Helsinki: Gaudeamus.
- Kivivuori, Janne & Niemi, Hannu (2015) *Rikollisuutta kuvaavan tiedon lähteet. Rikollisuustilanne 2015: Rikollisuuskehitys tilastojen ja tutkimusten valossa*. Katsauksia 14, 2016. Kriminologian ja oikeuspolitiikan instituutti, 147–158. [https://helda.helsinki.fi/bitstream/handle/10138/164434/Katsauksia\\_14\\_Rikollisuustilanne\\_2015\\_2016.pdf?sequence=1](https://helda.helsinki.fi/bitstream/handle/10138/164434/Katsauksia_14_Rikollisuustilanne_2015_2016.pdf?sequence=1) (Viitattu 34.4.2021.)
- Kulig, Teresa & Pratt, Travis & Cullen, Francis & Chouhy, Cecilia & Unnever, James (2017) Explaining bullying victimization: Assessing the generality of the low self-control/risky lifestyle model. *Victims & Offenders* 12 (6), 891–912. <https://doi.org/10.1080/15564886.2017.1307297> (Viitattu 24.4.2021.)
- Lapsiasiavaltuutettu (2018) *YK:n lapsen oikeuksien komitean yleiskommentit*. Lapsiasiavaltuutetun toimisto. <https://lapsiasia.fi/yleiskommentit> (Viitattu 20.4.2021.)

- Marcum, Catherine, Higgins, George & Ricketts, Melissa (2010) Potential factors of online victimization of youth: an examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior* 31, 381–410. <https://doi.org/10.1080/01639620903004903>. (Viitattu 4.2.2021.)
- Mikkola, Marko & Oksanen, Atte & Kaakinen, Markus & Miller, Bryan & Savolainen, Iina & Sirola, Anu & Zych, Izabela & Paek, Hye-Jin (2020) Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. *International Journal of Offender Therapy and Comparative Criminology*. <https://doi.org/10.1177/0306624X20981041> (Viitattu 17.2.2021.)
- Mood, Carina (2010) Logistic regression: Why we cannot do about it we think we can do, and what we can do about it. *European Sociological Review* 26 (1), 67–82. <https://doi.org/10.1093/esr/jcp006>.
- Ngo, Fawn & Paternoster, Raymond (2011) Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology* 5 (1), 773–793. <https://www.cybercrimejournal.com/ngo2011ijcc.pdf> (Viitattu 7.2.2021.)
- Näsi, Matti (2016) *Nuorten rikoskäyttäytyminen ja uhririkokemukset 2016*. Katsauksia 18/2016. Kriminologian ja oikeuspolitiikan instituutti. [https://helda.helsinki.fi/bitstream/handle/10138/169509/Katsauksia\\_18\\_N%C3%A4si\\_2016.pdf?sequence=1](https://helda.helsinki.fi/bitstream/handle/10138/169509/Katsauksia_18_N%C3%A4si_2016.pdf?sequence=1) (Viitattu 4.2.201.)
- Näsi, Matti & Kaakinen, Markus (2019) Kyberrikollisuus. Teoksessa Petri Danielsson (toim.) *Rikollisuustilanne 2018 rikollisuuskehitys tilastojen ja tutkimusten valossa*. Helsinki: Kriminologian ja oikeustieteen instituutti. Katsauksia 36/2019, 137–148. (Viitattu 1.3.2021.)
- Näsi, Matti, Oksanen, Atte, Keipi, Teo & Räsänen, Pekka (2015) Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 16 (2), 203–210. <https://doi.org/10.1080/14043858.2015.1046640>. (Viitattu 6.2.2021.)
- Näsi, Matti, Räsänen, Pekka, Kaakinen, Markus & Keipi, Teo (2016) Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice* 1–15. <https://doi.org/10.1177/1748895816679866>.
- Näsi, Matti & Tanskanen, Maiju (2016) *Kyberrikollisuus. Rikollisuustilanne 2015: Rikollisuuskehitys tilastojen ja tutkimusten valossa*. Katsauksia 14/2016. Kriminologian ja oikeuspolitiikan instituutti, 147–158. [https://helda.helsinki.fi/bitstream/handle/10138/164434/Katsauksia\\_14\\_Rikollisuustilanne\\_2015\\_2016.pdf?sequence=1&isAllowed=y](https://helda.helsinki.fi/bitstream/handle/10138/164434/Katsauksia_14_Rikollisuustilanne_2015_2016.pdf?sequence=1&isAllowed=y) (Viitattu 7.3.2021.)
- Oksanen, Atte & Keipi, Teo (2013) Young People as Victims of Crime on the Internet: A Population-based Study in Finland. *Vulnerable Children & Youth Studies* 8 (4), 298–309. <https://doi.org/10.1080/17450128.2012.752119>. (Viitattu 26.1.2021.)
- Oksanen, Atte, Savolainen, Iina, Sirola, Anu & Kaakinen, Markus (2018) Problem gambling and Psychological Distress: a cross-national perspective on the mediating effect of consumer debt and debt problems among emerging adults. *Harm Reduction Journal* 15 (45) <https://doi.org/10.1186/s12954-018-0251-9>. (Viitattu 4.2.2021.)
- Reckwitz, Andreas (2002) Toward a theory of social practices: a development in culturalist theorizing. *European journal of social theory* 5 (2), 243–265. <https://doi.org/10.1177/1368431022225432>. (Viitattu 2.2.2021.)
- Reisig, Michael & Golladay, Katelyn (2019) Violent victimization and low self-control: The mediating effect of risky lifestyles. *Violence and Victims*, 34 (1), 157–174. <https://doi.org/10.1891/0886-6708.34.1.157> (Viitattu 6.3.2021.)
- Reyns, Bradford, Henson, Billy & Fisher, Bonnie (2011) Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior* 38 (1149), 1148–1169. <https://doi.org/10.1177/0093854811421448>. (Viitattu 26.1.2021.)
- Reyns, Bradford, Henson, Billy & Fisher, Bonnie (2014) Digital deviance: Low self-control and opportunity as explanations of sexting among college students. *Sociological Spectrum* 34 (3), 273–292. <https://doi.org/10.1080/02732173.2014.895642> (Viitattu 24.4.2021.)
- Rikosuhripäivystys (2021) *Vahingonkorvausten hakeminen Vastaamon konkurssipesältä*. <https://www.riku.fi/vahingonkorvausten-hakeminen-vastaamon-konkurssipesalta/>. (Viitattu 18.4.2021.)
- Saari, Salla (2009) *Hädän hetkellä: Psykkisen ensiavun opas*. 1.–3. painos. Helsinki: Duodecim ja Suomen Punainen Risti.
- Schreck, Christopher (1999) Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly* 16, 633–654. <https://doi.org/10.1080/07418829900094291> (Viitattu 17.2.2021.)
- Sirola, Anu & Kaakinen, Markus & Oksanen, Atte (2018) Excessive Gambling and Online Gam-

- bling Communities. *Journal of Gambling Studies*. <https://doi.org/10.1007/s10899-018-9772-0> (Viitattu 2.2.2021.)
- Suomen virallinen tilasto (SVT). (2020) *Väestön tieto- ja viestintätekniikan käyttö*. Helsinki: Tilastokeskus [http://www.stat.fi/til/sutivi/2020/sutivi\\_2020\\_2020-11-10\\_tie\\_001\\_fi.html](http://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tie_001_fi.html) (Viitattu 24.4.2021.)
- Tangney, June, Baumeister, Roy & Boone, Angie (2018) High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. Teoksessa Roy Baumeister (toim.) *Self-regulation and self-control. Selected works of Roy F. Baumeister*, 173–212. Routledge.
- Turanovic, Jillian & Pratt, Travis (2014) “Can’t stop, won’t stop”: Self-control, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology* 30 (1), 29–56. <https://doi.org/10.1007/s10940-012-9188-4> (Viitattu 24.4.2021.)
- Valtioneuvosto (2020) Mistä apua Vastaamo-tietomurron uhreille – lista tärkeimmistä avuntarjoajista. Sosiaali- ja terveysministeriö. <https://valtioneuvosto.fi/-/1271139/mista-apua-vastaamo-tietomurron-uhreille-lista-tarkeimmista-avuntarjoajista> (Viitattu 7.2.2021.)
- Yar, Majid (2005) The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory. *European Journal of Criminology* 2 (4), 407–427. <http://euc.sagepub.com/cgi/content/abstract/2/4/407> (Viitattu 1.2.2021.)
- Yen, Ju-Yu, Ko, Chih-Hung, Yen, Cheng-Fang, Chen, Sue-Huei, Chung, Wei-Lun & Chen, Cheng-Chung (2008) Psychiatric symptoms in adolescents with internet addiction: Comparison with substance use. *Psychiatry and Clinical Neurosciences* 62, 9–16. <https://doi.org/10.1111/j.1440-1819.2007.01770>. (Viitattu 24.4.2021.)