



SEINÄJOEN AMMATTIKORKEAKOULU  
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

# Tämä on alkuperäisen artikkelin rinnakkaistallenne (kustantajan versio).

Viite:

Haasio, A. 2020. Verkkorikollisuuden eri muodot. Teoksessa: A. Haasio, S. Joensuu-Salo & S. Saarikoski (toim.) Luovaa liiketoimintaa, kestävää kulttuuria. Seinäjoki: Seinäjoen ammattikorkeakoulu. Seinäjoen ammattikorkeakoulun julkaisusarja B. Raportteja ja selvityksiä 158, 247 - 259. <http://urn.fi/URN:NBN:fi-fe20201209100081>



# VERKKORIKOLLISUUDEN ERI MUODOT

Ari Haasio, FT, yliopettaja  
SeAMK Liiketoiminta ja kulttuuri

## 1 JOHDANTOA

Verkkorikollisuudesta on tullut yhä merkittävämpi uhka yhteiskunnallemme. Perinteisten rikosten rinnalle on tullut uudenlaisia rikollisuuden muotoja. Samalla verkko on mahdollistanut rikollisuuden globalisaation. Hyvä esimerkki tästä on kansainvälinen huumekauppa, joka toimii yli rajojen. Monien rikosten takana ovat järjestäytyneet rikollisliigat, joiden toiminta on maailmanlaajuista. Verkkorikokset voivat kohdistua joko henkilöihin, omaisuuteen ja tiettyä valtiota tai organisaatiota vastaan (Haasio 2013).

Verkkorikollisuudella on useita erilaisia muotoja ja ilmiötä voidaan tarkastella useasta eri näkökulmasta. Ensinnäkin verkkorikokset voidaan jakaa puhtaasti verkossa tapahtuviin rikoksiin, jotka uusi teknologia on mahdollistanut. Tällaisia ovat esimerkiksi palvelunestohyökkäykset. Toisaalta iso osa rikoksista on aivan perinteisiä, mutta niissä hyödynnetään uutta teknologiaa. Esimerkiksi huijauksia on esiintynyt kautta aikain, mutta nyt niitä tehdään myös verkossa. (Haasio 2017.) Voidaan myös puhua tietotekniikkarikoksista, jotka on jaoteltu 1) tietotekniikkaan ja tietoverkkoihin kohdistuviin rikoksiin ja 2) tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtyihin rikoksiin (Poliisi 2020).

Haasio (2013) on jaotellut verkon vaaroja käsittelevässä teoksessaan internetin pimeän puolen mustaan ja harmaaseen vyöhykkeeseen. Ensin mainittuun ryhmään kuuluvat verkkosisällöt ja verkossa tapahtuvat asiat ovat selkeästi laittomia, jälkimmäiseen

kuuluvat taas sellaiset palvelut, joita voimme pitää moraalittomina. Laittomia ne eivät kuitenkaan ole.

Internet mahdollistaa myös rikollisen kommunikaation ja anonyymi Tor-verkko toimiikin rikollisten keskinäisenä kommunikatiovälineenä, jota täydentää anonyymi pikaviestipalvelu Wickr. Se on Messengerin kaltainen puhelimeen asennettava sovellus, mutta toisin kuin muut pikaviestimet, se toimii täysin anonyymisti.

Tässä artikkelissa tarkastellaan verkkorikollisuuden keskeisiä muotoja ja niiden vaikutusta kansalaisten elämään pähkinäkuoressa. Samalla annetaan myös ohjeita siihen, kuinka tulee toimia verkkorikoksen uhriksi jouduttaessa ja kuinka niitä voidaan ennaltaehkäistä. Tavoitteena on antaa yleiskuva siitä, millaisia rikoksia netissä tehdään.

## **2 VERKKORIKOKSET TOR-VERKOSSA JA AVOIMESSA VERKOSSA**

Osa verkkorikoksista tapahtuu avoimessa verkossa (Clear Web), osa taas pimeässä netissä (Dark Web). Ensin mainittu on meidän kaikkien käyttämä internet, jälkimmäinen taas on anonyymi verkko, johon pääsemiseksi tarvitaan erillinen ohjelmisto, kuten Tor-selain (Gehl 2018). Pimeän internetin toiminta perustuu kerrokselliseen salausjärjestelmään, joka mahdollistaa anonymiteetin. Tämän ansiosta verkkosivuja voi käyttää ilman, että kolmas osapuoli voi jäljittää mitä henkilö tekee verkossa. (Haasio & Harviainen 2019.)

Pimeän verkon, eli Tor-verkon, rikollisuuteen tavallinen netin käyttäjä ei törmää, ellei hän erikseen hakeudu sinne. Suomessa keskeisin pimeässä verkossa tapahtuva rikollisuuden muoto on huumekauppa, joka on nykyisin siirtynyt yhä enenevässä määrin

verkkoon (Haasio & Harviainen 2019). On kuitenkin syytä huomata, että vaikka rikolliset hyödyntävät runsaasti Tor-verkkoa, kyse ei ole puhtaasti rikolliseen toimintaan tarkoitettusta palvelusta. Tor-verkossa on paljon täysin laillista toimintaa ja esimerkiksi Electronic Frontier of Finland (EFFI) perusteleekin Tor-verkon hyödyllisyyttä ennen muuta sanavapauden turvaajana, verkko-vakoilun estäjänä ja sensuurin kiertäjänä (Electronic Frontier of Finland, [viitattu 21.8.2020]).

Keskeisimmät Tor-verkossa tapahtuvat rikokset liittyvät huume-kauppaan sekä pedofiliaan. Myös erilaiset äärioliikkeet hyödyntävät pimeää verkkoa ja Wickr-pikaviestintä toiminnassaan. Tämä mahdollistaa esimerkiksi erilaisten iskujen suunnittelun ilman, että viranomaiset voisivat jäljittää keskusteluja.

Avoimen verkon rikoksiin taas voi kuka tahansa verkon käyttäjä törmätä ja joutua niiden uhriksi. Siksi eri tyyppisten verkkorikosten tuntemus on osa digitaitoja, koska se mahdollistaa ennakkoinnin ja eri tyyppisten rikosten tunnistamisen. Näin voidaan uhriksi joutuminen välttää useissa tapauksissa. Mediakasvatuksessa tulisikin huomioida paitsi esimerkiksi lähteistön luotettavuuteen liittyvät kysymykset, myös verkon vaaroihin erityisesti verkkorikosten näkökulmasta liittyvä osaaminen. Näin voidaan parhaiten ennakoida ja välttää vaaratilanteita.

### **3 KESKEISIMMÄT VERKKORIKOSTEN TYYPIT**

Haasion (2013; 2017) mukaan tyypillisimpiä verkkorikoksia avoimessa verkossa ovat esimerkiksi:

- huijaukset
- varastetun tavaran myynti

- identiteettivarkaudet
- kunnianloukkaukset
- seksuaalirikokset
- tietomurrot
- palvelunestohyökkäykset
- rasiset rikokset
- verkkoväkivalta.

Verkkorikollisuuden aiheuttamat taloudelliset vahingot ovat mittavat. FBI:n mukaan kyberrikolliset aiheuttivat toiminnallaan yli 3,2 miljardin euron edestä vahinkoa vuonna 2019 (Korhonen 2020). Verkkorikosten määrä on kasvanut Suomessa joka vuosi. Esimerkiksi vuonna 2018 poliisille tehtiin yhteensä reilut 12 000 ilmoitusta nettipetoksista (Tietoverkkorikollisuus poliisin silmin 2019). Tämä osoittaa hyvin sen, että verkkorikollisuudessa on kyse mittavasta ja koko yhteiskuntaa koskevasta ilmiöstä.

### 3.1 Huijaukset ja varastetun tavaran myynti

Poliisin (2020) mukaan monissa kyberrikoksissa hyödynnetään haittaohjelmia, joista yleisimpiä ovat viime aikoina olleet erilaiset kiristysohjelmat. Myös tietojen kalastelu eli phishing on yleistä. Rikolliset pyrkivät saamaan haltuunsa tietoja, joita voidaan hyödyntää rikosten tekemisessä. Esimerkiksi sosiaaliturvatunnusten, pankkitietojen ym. hankkiminen epärehellisiä tarkoituksia varten sosiaalisen median tai sähköpostin avustuksella on malliesimerkki tämän tyyppisestä toiminnasta. Samalla tavalla pyritään myös hankkimaan esimerkiksi salasanoja eri palveluihin. Hakkerit voivat myydä näitä tietoja eteenpäin muille verkkorikollisille ja kaapata esimerkiksi käyttäjätilejä, ostaa tuotteita verkkokaupoista sekä käyttää tietoja kiristykseen ja yrityksiin kohdistuviin hyökkäyksiin (Miksi hakkerit haluavat 2020).

Verkkohuijaukset ovat arkipäivää internetissä. Ne perustuvat ihmisten hyväuskoisuuteen. Tyypillisiä ovat esimerkiksi seuraavat huijaustyytit (Haasio 2013; 2017):

- nigerialaiskirja
- vastanigerialainen
- tyttöystävähuijaus
- lottovoitto
- verkkokauppahuijaukset
- henkilö pulassa.

Sähköpostitse lähetetyt nigerialaiskirjeet, vastanigerialaiset, ilmoitukset lottovoitosta tai sosiaalisen median kautta lähetetyt avunpyynnöt ovat tyypillisiä huijauksia. Uhria saatetaan lähestyä esimerkiksi ystävän kaapatun tai hänen nimiinsä tekaistun Facebook-profiilin kautta ja pyytää rahaa hätätilanteessa. Myös tyttöystävähuijaukset, joissa kaunis nainen lupaa tulla uhrin luo, mutta tarvitsee rahaa matkalippuihin yms., ovat tavallisia. Ne kohdistuvat myös yhtä lailla naisiin. (Haasio 2017.)

Jatkuvasti kasvanut huijaustyyppi, joka kohdistuu tavallisiin kansalaisiin, on verkkokauppahuijaus. Siinä myydään verkon osto- ja myyntipalstoilla olematonta tavaraa. Monissa tapauksissa vaarana on myös se, että verkosta ostettu tavara on varastettua. Esimerkiksi elektroniikkaa ja polkupyöriä myydään runsaasti netin markkinapaikoilla ja sieltä ostoksia tehdessä on hyvä olla tarkkaavainen. Myös Tor-verkon sivustoilla liikkuu aivan avoimesti varastettuja tavaroita. Myytävänä on myös pankkikortteja, sosiaaliturvatunnuksia ja muita henkilöllisyystodistuksia (Haasio, Harviainen & Savolainen 2020).

### 3.2 Seksuaalisuuteen kohdistuvat rikokset

Internetistä on tullut merkittävä seksuaalirikollisten toimintapaikka. Rikoslaisissa (L 19.12.1889/39) seksuaalirikoksiksi määritellään raiskaukset, lapsiin kohdistuvat seksuaalisen hyväksikäytöt ja seksikauppaan liittyvät rikokset, sukupuolisiveellisyyteen liittyvät rikkomukset, kuten lapsipornon levittäminen ja hallusapito sekä seksuaalinen ahdistelu. Uudessa lainsäädännössä on myös huomioitu verkossa toimivat pedofiilit, minkä vuoksi lapsiin

kohdistuva seksuaalinen puhe, kuvien ja videoiden jakaminen yms. on lain mukaan tuomittava teko.

Kenties näkyvin seksuaalirikollisuuden muoto verkossa on lapsiin ja nuoriin kohdistunut seksuaalinen väkivalta, joka on viime vuosina ollut kasvussa (Ellonen, Fagerlund & Haapakangas 2019). Kansainvälisissä tutkimuksissa on arvioitu, että noin viidennes (18 %) tytöistä ja kahdeksan prosenttia pojista on kokenut seksuaalista väkivaltaa (Karhu 2020).

Pedofiilien toiminta voidaan jakaa yhtäältä lapsiin kohdistuvan seksuaalista väkivaltaa sisältävän materiaalin, kuten kuvien ja videoiden keskinäiseen jakamiseen ja toisaalta pyrkimykseen päästä henkilökohtaiseen kontaktiin lapsen kanssa. Ensin mainittu tapahtuu yhä useammin salatussa Tor-verkossa, mikä vaikeuttaa rikollisten kiinnisaamista. Jälkimmäinen toiminta eli lapsen houkuttelu seksuaalisiin tarkoituksiin, taas tapahtuu avoimessa netissä niillä foorumeilla missä lapset ja nuoret liikkuvat. Lasten seksuaalinen houkuttelu eli grooming tapahtuu esimerkiksi sosiaalisessa mediassa, chateissa ja keskustelupalstoilla. Monet lasten ja nuorten suosimat verkkopalvelut, kuten lyhytvideosovellus TikTok, Instagram ja Snapchat ovat myös pedofiilien metsästysmaita (vrt. Pelastakaa lapset 2018).

Grooming perustuu verkossa tapahtuvaan kanssakäymiseen, joka alkaa viattomalla verkkojuttelulla lapsen kanssa. Näin tekijä pyrkii voittamaan uhrin luottamuksen. Pikkuhiljaa lapselle ryhdytään puhumaan seksuaalisväritteisistä sisällöistä, ehdotellaan nettikameran avaamista ja kuvien lähettämistä tekijälle. Harmittomalta tuntuva juttelu saattaa johtaa esimerkiksi alastonkuvien kiristämiseen ja fyysiseen kontaktiin. (Haasio 2017.) Suurin syy siihen, että lapsiin kohdistuva seksuaalinen häirintä ja väkivalta jää ilmoittamatta, eikä tule edes vanhempien tietoon, on lasten oma häveliäisyys (Pelastakaa Lapset 2018). Asiasta ei uskalleta kertoa häpeän ja rangaistusten takia vanhemmille.

Valtaosa verkon seksuaalirikoksista kohdistuu nimenomaan lapsiin ja nuoriin. Prostituutio on siirtynyt pitkälti verkkoon, mutta itsensä myyminen tai seksin ostaminen ei ole rikos, ellei kyse ole parituksesta. Käytännössä verkkoprostituutioon liittyvissä tapauksissa parituksen toteennäyttö on hyvin vaikeaa.

### 3.3 Identiteettivarkaudet, vihapuhe ja kunnianloukkaukset

Identiteettivarkaudella tarkoitetaan toisen henkilön tietojen, kuten nimen tai sosiaaliturvatunnuksen laiton käyttöä. Identiteettivarkauden turvin voidaan tavoitella esimerkiksi taloudellista hyötyä, mutta sitä on käytetty myös henkilön mustamaalaamiseen ja kiusaamiseen. Esiintymällä toisen henkilön identiteettiä käyttäen voidaan esimerkiksi tilata tavaroita tai esiintyä sosiaalisessa mediassa ja levittää perättömiä väitteitä ym.

Kunnianloukkaukset ovat yleisiä rikoksia etenkin sosiaalisessa mediassa. Monissa tapauksissa ne liittyvät vihapuheeseen, joka kohdistuu vähemmistöihin. Vihapuhe voidaan määritellä esimerkiksi seuraavasti (Mattila & Haasio 2019):

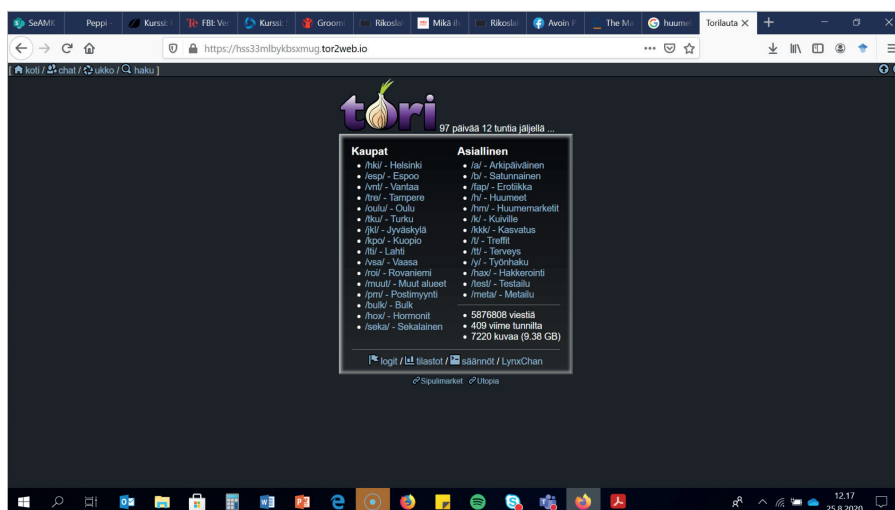
1. Suomen lainsäädännön lähtökohdista vähemmistöryhmiä leimaavaa ja halventavaa puhetta, joka saattaa yllyttää väkivaltaan näitä ryhmiä kohtaan.
2. Yksityisiin henkilöihin kohdistuvaa leimaavaa tai halventavaa puhetta, joka johtuu yksityisen henkilön todella ilmenneestä tai oletetusta myönteisestä tai neutraalista asenteesta tai toiminnasta jotain vähemmistöryhmää kohtaan tai sen hyväksi.

Etenkin sosiaalinen media toimii kasvualustana vihapuheelle. Paitsi ääri liikkeit, myös monet aivan tavalliset kansalaiset saattavat sortua vihapuheeseen tai kunnianloukkauksiin kommentoidessaan eri asioita.

### 3.4 Huumekauppa verkossa

Verkon huumekauppa on keskittynyt lähes kokonaan Tor-verkoon. Kotimaisen verkossa tapahtuvan huumekaupan laajuutta kuvaa hyvin se, että marraskuun alussa 2017 toimintansa aloittanut Sipulitori, joka on Suomen suurin huumeiden myyntiin erikoistunut sivusto, on elokuun loppuun mennessä 2020 kerännyt yli 5 800 000 palveluun lähetettyä viestiä. Sivustolla myydään huumeiden lisäksi myös varastettua tavaraa, seksipalveluita, henkilöllisyystodistuksia ym. Siellä toimii myös rikollisten ”työvoimatoimisto”; Sipulikanavalla on oma osastonsa laittomia työtehtäviä etsiville ja niitä tarjoaville henkilölle. Tarjolla on esimerkiksi velanperintää, petosten tekoa, huumeiden katukauppaa ja muita laittomuuksia. (Harviainen, Haasio & Hämäläinen 2020.)

Verkossa tarjolla olevien huumeiden kirjo on laaja. Eniten markkinoilla liikkuu kuitenkin kannabinoideja, amfetamiinia ja opioidipohjaisia reseptilääkkeitä sekä Subutexia. Ostaminen on helppoa ja tavara toimitetaan postitse, henkilökohtaisesti ostajalle tai maastokätköön piilotettuna. Kuva 1 esittää Tor-verkon Sipulitori-palvelua.



Kuva 1. Kotimainen huumekauppa on keskittynyt Tor-verkon Sipulitori-palveluun.

Kaupankäynnissä käytetään usein Bitcoin-verkkorahaa, jonka jäljittäminen on vaikeaa. Silloin kun huumeiden toimitus tapahtuu postitse tai maastokätkön avulla, Bitcoinin käyttö on normaali toimenpide. Jos huumeet toimitetaan henkilökohtaisesti kädestä käteen, maksu tapahtuu käteisellä. Huumekauppa alkoi Tor-verkon kauppapaikoilla vuonna 2010. Tänä päivänä laittomien päihteiden hankkiminen on esimerkiksi alaikäisille erittäin helppoa juuri siksi, että huumeet voi ostaa verkon kautta.

### 3.5 Tietomurrot ja virukset

Moderni tekniikka mahdollistaa modernit rikokset. Palvelunestohyökkäykset ja muut tietomurrot sekä virukset ovat tyypillisiä virtuaalirikoksia. Tietomurrolla tarkoitetaan ”tietojärjestelmään, palveluun tai laitteeseen tunkeutumista tai sovelluksen, kuten esimerkiksi sähköpostitilin luvaton käyttöä haltuun saatujen tunnusten avulla” (Näin suojaudut tietomurroilta 2020).

Palvelunestohyökkäyksissä pyritään estämään jonkin tietyn verkkopalvelun tai palvelimen toiminta. Hyökkäys voidaan toteuttaa siten, että hakkeri ylikuormittaa hyökkäyksen kohteen lisäämällä siihen kohdistuvaa tietoliikennettä niin että järjestelmä kaatuu (Haasio 2013). Näin on haavoitettu esimerkiksi isojen yritysten verkkopalveluita ja eri viranomaisten sivustoja.

Tietoverkkojen välityksellä jaetaan runsaasti eri tyyppisiä haittaohjelmia. Osa niistä on tietojenkalastelua varten tehty, osa kiristystarkoituksissa ja osa puhtaasti kiusaamismielessä. Virukset voivat tuottaa monenlaista harmia aina koko koneen tuhoutumisesta tietojen urkkimiseen. (Haasio 2017.)

## 4 VARAUTUMINEN VERKKORIKOKSIIN

Verkkorikollisuus on tullut yhteiskuntaa jäädäkseen ja viranomaiset tekevät jatkuvasti töitä sen ehkäisemiseksi. Siitä on kuitenkin

tullut pysyvä ilmiö, johon kansalaisten on osattava varautua toimiessaan verkossa. Varovaisuus ja vaarojen tunnistaminen ovat keskeinen osa medialukutaitoa.

Mitä tämä tarkoittaa käytännössä? Miten minun tulee toimia ja mitä minun tulee kansalaisena tehdä ehkäistäkseni vaaroja?

Aivan ensimmäiseksi on hyvä muistaa eräitä perusasioita. Eri palveluissa tulee käyttää eri salasanoja, jotka ovat hankalammin murrettavissa. Käytännössä tämä tarkoittaa isojen ja pienten kirjainten, numeroiden ja erikoismerkkien (jos palvelu sallii sen) yhdistelyä salasanassa. Myös sellaiset salasanat, jotka perustuvat liian helposti arvattaviin asioihin, kuten lemmikin nimeen, tulee jättää käyttämättä. Toinen keskeinen asia on virusturvan ajantasaisuus. Huolehdi siitä, että tietokoneessasi on ajantasainen viruksentoruntaohjelma sekä palomuuuri. On myös hyvä muistaa, että kännykkä ja tabletti ovat yhtä lailla tietokoneita. Myös niiden virusturvan tulee olla kunnossa.

Useat haittaohjelmat leviävät sähköpostin liitetiedostojen kautta. Siksi epäilyttäviä liitetiedostoja, jotka tulevat tuntemattomalta lähettäjältä, ei koskaan tule avata. Myös ystävän nimissä saatetaan lähettää esimerkiksi Messenger-viestejä, joissa on linkki videoon, kuvaan tai muuhun vastaavaan. Varmistu ensin, että viesti on todellisuudessa ystäväsi lähettämä ennen kuin avaat sen!

Mieti myös mitä kerrot itsestäsi verkossa ja mitä kuvia jaat esimerkiksi sosiaalisessa mediassa. Usein kannattaa myös jakaa asiat esimerkiksi Facebookissa vain ystäville ja tarkistaa, että sosiaalisen median eri tilien yksityisyysasetukset ovat kunnossa. Maalaisjärki on usein hyvä väline verkkorikollisuuden välttämässä.

Jos törmäät esimerkiksi pedofiliaan, vihapuheeseen tai muihin verkkorikoksiin sosiaalisessa mediassa tai muissa verkon palveluissa, asiasta pitää ilmoittaa. Poliisin nettivinkkiin (<https://>

[www.poliisi.fi/nettivinkki](http://www.poliisi.fi/nettivinkki)) voi lähettää ilmoitukset mistä tahansa laittomasta toiminnasta. Lapsiin kohdistuvasta seksuaalisesta väkivallasta verkossa voi ilmoittaa myös Pelastakaa Lapset ry:n Nettivihjeellä, joka löytyy osoitteesta <https://www.pelastakaa-lapset.fi/tyomme-kotimaassa/lasten-suojelu-ja-nettivihje/nettivihje/ilmoita/>.

## 5 LOPUKSI

Verkkorikosten määrän kasvu on selkeä seuraus siitä, että internetistä on tullut iso osa elämäämme. Rikolliset saalistavat siellä, missä me olemme. Verkkorikollisuudesta on tullut pysyvä ilmiö. Sitä ei voi poistaa, mutta siihen voi varautua ja pyrkiä näin ennaltaehkäisemään mahdolliset vahingot.

Tunnistamme reaali maailman vaarat kohtuullisen hyvin, mutta jatkossa kansalaisten ymmärrystä verkon vaaroista tulee lisätä. Turhien pelkojen, ennakkoluulojen tai vaihtoehtoisesti liian huolettoman asenteen sijaan verkon vaarat tulisi tunnistaa asianmukaisesti ja sopeuttaa oman verkkokäyttäytyminen siihen. Tämä edellyttää mediakasvatusta ja kansalaisten informaatiolukutaidon kehittämistä entisestään kaikissa ikäryhmissä.

## LÄHTEET

Electronic Frontier of Finland. Ei päiväystä. EFFI Tor-verkossa. [Verkkosivu]. [Viitattu 18.8.2020]. Saatavana: <https://effi.org/effi-tor-verkossa/>

Ellonen, N., Fagerlund, M. & Haapakangas, K. 2019. Lapsiin kohdistuneiden seksuaalirikosten ilmoitukset kasvussa, uhrikokemukset eivät. [Verkkoartikkeli]. Helsinki: Tilastokeskus. Tieto&trendit 17.4.2019. [Viitattu 18.8.2020]. Saatavana: <https://www.stat.fi/tietotrendit/artikkelit/2019/lapsiin-kohdistuneiden-seksuaalirikosten-ilmoitukset-kasvussa-uhrikokemukset-eivat/>

Gehl, R. W. 2018. Weaving the dark web: legitimacy on freenet, Tor, and I2P. Cambridge, MA: The MIT Press.

Haasio, A. 2013. Netin pimeä puoli. Helsinki: Suomalaisen Kirjallisuuden Seura.

Haasio, A. 2017. Verkkorikokset. Helsinki: Avain.

Haasio, A. & Harviainen, J. T. 2019. Tor-verkko - mikä se on? Teoksessa: S. Päällysaho, A. Haasio, S. Saarikoski & S. Uusimäki (toim.) Seinäjoen ammattikorkeakoulu 2019: Moninaista osaamista. [Verkkojulkaisu]. Seinäjoki: Seinäjoen ammattikorkeakoulu. Seinäjoen ammattikorkeakoulun julkaisusarja A. Tutkimuksia 32, 66 - 74. [Viitattu 16.10.2020]. Saatavana: <http://urn.fi/URN:NBN:fi-fe2019121348144>

Haasio, A., Harviainen, J. T., & Savolainen, R. 2020. Information needs of drug users on a local dark web marketplace. Information processing & management 57 (2), 102080. doi: 10.1016/j.ipm.2019.102080

Harviainen, J. T., Haasio, A., & Hämäläinen, L. 2020. Drug traders on a local dark web marketplace. Teoksessa: Proceedings of the 23rd International Conference on Academic Mindtrek, 20 - 26. doi: 10.1145/3377290.3377293

Karhu, E. 2020. Lasten kokema seksuaalinen väkivalta ilmiönä. Teoksessa: M.-M. Oinas, M. Pietilä & V. Tuohino (toim.) Kysy, kohtaa ja kuuntele: Opas seksuaalisen houkuttelun ja seksuaalisen väkivallan ennaltaehkäisyyn nuorisotyössä. Verkkojulkaisu]. Oulu: Koordinaatti, Oulun kaupunki. [Viitattu 16.10.2020]. Saatavana: <https://koordinaatti.fi/system/files/2020-07/Kysyy%20kohtaa%20kuuntelee%20opas%20verkkoversio.pdf>

Korhonen, S. 2020. FBI: Verkkorikoksista 3 miljardin vahingot vuodessa – Kalastelu, huijaus ja kiristy tavallisimmat rikollisten keinot. [Verkkotietoliikenne]. Talouselämä 13.2.2020. sivu]. [Viitattu 18.8.2020]. Saatavana Alma Talent Ammattilaismediat -palvelusta. Vaatii käyttöoikeuden. L 19.12.1889/39. Rikoslaki.

Mattila, M. & Haasio, A. 2019. Kansallinen ja paikallinen vihapuhe digitaalisessa ympäristössä. Teoksessa: S. Päällysaho, A. Haasio, S. Saarikoski & S. Uusimäki (toim.) Seinäjoen ammattikorkeakoulu 2019: Moninaista osaamista. [Verkkojulkaisu]. Seinäjoki: Seinäjoen ammattikorkeakoulu. Seinäjoen ammattikorkeakoulun julkaisusarja A. Tutkimuksia 32, 289 - 296. [Viitattu 16.10.2020]. Saatavana: <http://urn.fi/URN:NBN:fi-fe2019121748537>

Miksi hakkerit haluavat henkilötietosi? Ei päiväystä. [Verkkosivu]. F-Secure. [Viitattu 18.8.2020]. Saatavana: <https://www.f-secure.com/fi/home/articles/why-do-hackers-want-your-personal-information>

Näin suojaudut tietomurroilta. 2020. [Verkkosivu]. Helsinki: Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. [Viitattu 18.8.2020]. Saatavana: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta>

Pelastakaa lapset. 2018. Lasten ja nuorten kokema seksuaalinen häirintä ja siihen liittyvä kiusaaminen digitaalisessa mediassa. [Verkkojulkaisu]. [Viitattu 18.8.2020]. Saatavana: [https://s3-eu-west-1.amazonaws.com/pelastakaalapset/main/2018/08/31131602/Sexting\\_raportti\\_web-002.pdf](https://s3-eu-west-1.amazonaws.com/pelastakaalapset/main/2018/08/31131602/Sexting_raportti_web-002.pdf)

Poliisi. 2020. Kyberrikollisuus. [Verkkosivu]. [Viitattu 18.8.2020]. Saatavana: <https://www.poliisi.fi/rikkokset/kyberrikollisuus>

Tietoverkkorikollisuus poliisin silmin. 2019. [Blogikirjoitus]. PoliisiBlogi 7.10.2019. Suomen Poliisi, KRP Kybertorjuntakeskus. [Viitattu 18.8.2020]. Saatavana: <https://blogi.poliisi.fi/tietoverkkorikollisuus-poliisin-silmin/>