Kristian Orpana

# HAKTIVISMI KYBERAKTIVISMIN VÄLINEENÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

# TIIVISTELMÄ

Orpana, Kristian
Haktivismi kyberaktivismin välineenä
Jyväskylä: Jyväskylän yliopisto, 2021, 31 s.
Tietojärjestelmätieteet, Kandidaatin tutkielma
Ohjaaja(t): Räisänen, Jaana

Haktivismiksi lueteltavia hyökkäyksiä tapahtuu paljon, mutta ilmiö on monelle täysin tuntematon. Haktivismin toimien kirjo on laaja, ja niiden vaikutukset voivat olla organisaatioille ja yritykselle merkittäviä. Haktivismi on kyberaktivismin kattotermin alle asettuva ilmiö, jolla tarkoitetaan hakkeroinniksi lueteltavien toimien hyödyntämistä kyberaktivismiin. Tutkimus on toteutettu kirjallisuuskatsauksena pyrkimyksenä tuottaa helposti ymmärrettävä katsaus haktivismiin. Kyberaktivismilla on tutkielmassa määritetty kyberympäristössä tapahtuvaksi aktivismiksi. Tämän kirjallisuuskatsauksen tavoitteena on koota eri lähteistä saatua tietoa haktivismista ja sen toteuttamistavoista sekä pyrkiä luomaan kuva haktivismin mahdollisista vaikutuksista.
Kirjallisuuskatsauksessa käytettiin laajasti eri tutkimusalojen tutkimuksia, jotta haktivismista ja sen ilmiöistä saatiin kasattua tarpeeksi kattava kuva. Tutkimuksen lähteenä toimivat aihepiiriä käsittelevät akateemiset tutkimukset sekä kyberturvatoimijoiden julkaisemat raportit toteutuneista iskuista.
Kirjallisuuskatsaus osoitti, että haktivismin vaikutukset voivat olla taloudellisesti merkittäviä kohteelle, mutta haktivismin tehoa kyberaktivismin keinona ei ole täysin pystytty määrittämään. Historiasta löytyy kuitenkin tapauksia, jossa haktivismilla on saatu aikaan jopa hallintoja kaataneita vaikutuksia.

Asiasanat: kyberaktivismi, haktivismi, aktivismi, internet-aktivismi

# ABSTRACT

Orpana, Kristian
Hacktivism as a form of cyberactivism
Jyväskylä: University of Jyväskylä, 2021, 31 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Räisänen, Jaana

Hacktivism is a phenomenon that is unknown to many even though there has been a lot of attacks which can be identified as a hacktivist attack. Hacktivism includes a myriad of unique means that can have major impact on organizations and enterprises. Hacktivism fits under the umbrella term of cyberactivism and can be defined as a combination of hacking and activism. The term cyberactivism is defined in this study as activism that takes place in the cyberspace. This study is conducted as a literature review aiming to provide a clear overview on hacktivism. This literature review attempts to combine information from different sources to form a summary of hacktivism and different ways it can be implemented. Based on this information a view of possible impacts hacktivism can have will be formed.
Source material from different fields of study were used to form a comprehensive perception of hacktivism. Academic articles about the subject matter and reports about past attacks from cyber security organizations were the main sources used in this literature review.
This study concludes that the impact hacktivism can have can be economically significant to the target of the attack. Researchers haven't been able to accurately determine the effect that hacktivism has as a means of cyberactivism. However there have even been events in history where hacktivism has been a factor in overthrowing a government.

Keywords: cyberactivism, hacktivism, activism, digital activism

# TAULUKOT

# SISÄLLYS

# 1 JOHDANTO

Internet on lisännyt kansalaisten vaikuttamismahdollisuuksia. Tämä on tehnyt kansalaisaktivismin toteuttamisesta helpompaa ja tuonut aivan uuden aktivismin tason – kyberaktivismin. Kyberaktivismi mahdollistaa ryhmien järjestäytymisen yli maantieteellisten rajojen eikä välttämätöntä tarvetta laajalle aktivismi-iskujen suunnittelulle enää ole. (Illia, 2003.) Yksi kyberaktivismin keinoista on haktivismi. Haktivismi on kyberavaruudessa tapahtuvaa aktivismia, jonka tavoitteena on aktivismin kohteeseen vaikuttaminen negatiivisessa mielessä. Näiden iskujen motiivi on yleensä poliittinen. (Domanski, 2015).

Haktivismin nimissä tehtyjä hyökkäyksiä esiintyi laajasti varsinkin 2010–luvun alussa. Näiden iskujen jälkeen moni niiden toteuttajista vangittiin, minkä takia iskujen määrä vähentyi. Haktivismi-iskut ovat kuitenkin viime vuosina lisääntyneet, mihin on vaikuttanut muun muassa Covid-19 –pandemia. Pandemian lieveilmiöinä on toteutettu esimerkiksi informaatio-operaatioita, joissa on pyritty vaikuttamaan muun muassa ihmisten mielipiteisiin yhteiskunnan toiminnan rajoituksista ja rokotteista. Haktivistisia toimia on lisännyt myös maiden kokema demokratian vähittäinen väistyminen. Esimerkki tällaisesta tapauksesta on Valko-Venäjän valtiota vastustaneet hakkerit, jotka keräsivät tietomurrossa dataa Valko-Venäjän kansalaisista sekä hallituksesta tavoitteenaan presidentti Aljaksandr Lukašenkan hallituksen häiritseminen (Halminen, 2021). Yritykset ovat kohdanneet haasteita ilmastonmuutokseen sekä eettiseen toimintaan liittyvissä kysymyksissä, mikä saa myös kuluttajat vaatimaan näitä toimia yrityksiltä. Näiden toimien huomiotta jättäminen voi altistaa suuremmalla todennäköisyydellä yrityksen kyberaktivismin ja haktivismin kohteeksi.

Kyberaktivismin sekä haktivismin aihepiiri on vielä laajasti tutkimatonta, mikä on todettu myös muiden tutkijoiden puolesta (mm. George & Leidner, 2019). Aihepiirin tutkimus on pirstaloitunut laajasti eri tutkimusalojen välille, eikä tietojärjestelmätieteen tieteenalan tutkimusta ole juurikaan. Georgen ja Leidnerin (2019) kirjallisuuskatsaus kyberaktivismista on ainoa tietojärjestelmätieteen alalla tehty laajempi katsaus kyberaktivismin aihepiiriin,

mutta sekään ei syvenny tarkemmin haktivismin käsitteeseen (George & Leidner, 2019).

Tämä kandidaatintutkielma on toteutettu kirjallisuuskatsauksena ja sen tarkoituksena on vastata näihin kolmeen tutkimuskysymykseen:

1. Millaisina eri keinoina kyberaktivismi ilmenee?
2. Mihin haktivismilla pyritään?
3. Millaisia vaikutuksia haktivismilla on saatu aikaan?

Tutkielma on toteutettu Brereton ym. (2007) esittämän systemaattisen kirjallisuuskatsauksen viitekehyksen mallia mukaillen (Brereton ym., 2007). Tutkimusprosessi aloitettiin määrittelemällä tutkimuskysymykset, jonka jälkeen lähdeaineistoa alettiin keräämään eri tietolähteistä. Pääosin lähdeaineisto on kerätty SCOPUS, Google Scholar sekä EBSCO tietokannoista. Hakusanoina käytettiin englanninkielisiä hakutermejä. Päähakutermeinä olivat ”cyberactivism”, ”hacktivism” sekä ”digital activism”. Lähteiden luotettavuus arvioitiin Julkaisufoorumin antaman luokituksen mukaan sekä lähteen viittausten määrän perusteella. Tieteellisten artikkelien lisäksi tutkielmaan on myös valittu kyberturvallisuustoimijoiden raportteja sekä uutisartikkeleita tukemaan esitettyjä aiheita. Näiden lähteiden luotettavuutta on arvioitu niiden julkaisijan tunnettavuuden mukaan. Tutkielmassa on pyritty käyttämään mahdollisimman tuoreita lähteitä, jotta uusimmat teknologian tuomat mahdollisuudet ovat saatu sisällytettyä mukaan. Lähdeaineiston niukkuuden takia tutkielmassa on kuitenkin jouduttu käyttämään myös hieman vanhempaa, vuosituhannen alussa kirjoitettua sisältöä.

Tutkielman rakenne on muodostettu niin, että lukijalle tulee selvä kuva aihepiirin tärkeimmistä yläkäsitteistä ennen alakäsitteiden määrittelemistä. Ensimmäinen luku koostuu kyberaktivismin käsitteen määrittelemisestä sekä ilmiön kehittymisestä ja sen eri muodoista. Toinen kappale pyrkii selittämään haktivismin käsitteen, minkä jälkeen se selittää miten haktivismia voidaan toteuttaa ja kenen toimesta. Kolmannen ja viimeisen sisältökappaleen tarkoituksena on esimerkkien avulla käsitellä haktivismin mahdollisia vaikutuksia. Lopuksi yhteenvetokappale kasaa tutkielman sisällön johtopäätökset yhteen sekä tarjoaa kuvan mahdollisista jatkotutkimusaiheista.

# 2 KYBERAKTIVISMI

Tässä kappaleessa esitellään kyberaktivismin käsite ja kyberaktivismin ilmiön kehittyminen internetin kehittymisen myötä. Kappaleessa analysoidaan myös, miten eri lähdekirjallisuudessa on kategorisoitu kyberaktivismi eri kategorioihin. Tämän kappaleen tarkoituksena on vastata tutkimuskysymykseen: millaisina eri keinoina kyberaktivismi ilmenee?

## 2.1 Mitä kyberaktivismi on?

Aktivistit ovat kautta aikojen pyrkineet hyödyntämään uusi teknologioita heidän toimissaan. Uusien viestintäteknologioiden ja median avulla toimijat ovat pystyneet saamaan oman äänensä kuuluviin yhä paremmin. (McCaughey & Ayers, 2003, s. 4.) Digitalisaation myötä mahdollisuudet kansalaisaktivismin toteuttamiseen ovat moninkertaistuneet. Uusien viestintä- ja informaatioteknologioiden myötä aktivismin toimintakenttä on muuttunut kohti laajempaa ja globaalimpaa alustaa, jossa eri toimijat yksilöistä laajoihin aktivismiryhmittymiin sekä aktivismin kohteisiin kohtaavat. (Illia, 2003.) Uusien teknologioiden mahdollistaman yhteisöllisyyden takia paine yrityksiä kohtaan on lisääntynyt ja kasvanut näkyvyys yli maantieteellisten rajojen on tehnyt samanmielisten toimijoiden suhteiden muodostamisen helpoksi. Internetin myötä aktivistiliikkeiden muodostumisen dynamiikka on muuttunut. Perinteisten aktivistiliikkeiden muodostuminen on laaja prosessi, joka vaatii resurssien keräämistä niin kannattajien kuin rahoituksenkin puolesta. Kyberaktivismin liikkeiden muodostuminen voi sen sijaan tapahtua välittömän toiminnan tuotoksena yhdistäen samaa aatetta ajavat kannattajat yhteen spontaanisti verkon välityksellä. (Illia, 2003; George & Leidner, 2019; Van Laer & Van Aelst, 2010.) Kyberaktivismi ei myöskään ole yhtä riippuvainen massamediasta kuin perinteinen aktivismi. Sosiaalisen median avulla liikkeet voivat saada näkyvyyttä tehokkaasti keräten lisää kannattajia, kun taas massamedian näkyvyys tuo liikkeen suuremman yleisön tietoon. Perinteisen

aktivismin tapauksessa ilman sosiaalista mediaa, liikkeiden suurempi näkyvyys jää median huomion vastuulle. Kyberaktivismia voidaan myös toteuttaa pienemmässä mittakaavassa; se ei vaadi laajoja kannattajamääriä, vaan jopa yksilöt voivat toteuttaa tehokkaita aktivismikampanjoita (Illia, 2003).

Kyberaktivismi määritellään pääosin digitaalisessa ympäristössä tapahtuvaksi aktivismiksi, jonka pyrkimyksenä on saada aikaan muutoksia poliittisessa ympäristössä. Kyberaktivismin taustalla voi olla toimijoina joko yksilö, ryhmä tai organisaatio. (George & Leidner, 2018; Vegh, 2003.) Näkemys siitä, että onko kyberaktivismi oma kokonaisuutensa, vai perinteisen aktivismin jatke, vaihtelee. Varsinkin vuosituhannen alun kirjallisuudessa kyberaktivismi kuvataan perinteisen aktivismin jatkeena, kun taas uudemmassa, vuosikymmenen vaihteen jälkeen toteutetuissa tutkimuksissa, kyberaktivismi kuvataan omana kokonaisuutenaan, joka sisältää omat, perinteisestä aktivismista eriytyvät ilmiöt (George & Leidner, 2019). Illia (2003) määrittelee kyberaktivismin kyberilmiöksi, jolla ei ole tarkkaa määritelmää. Se ei ole pelkästään ketterämpi ja nopeampi tapa toteuttaa aktivismia, vaan se sisältää myös laajemman kokonaisuuden, kuin pelkästään perinteisen aktivismin siirtymisen verkkoon. (Illia, 2003.) Vegh (2003) sekä Van Laer ja Van Aelst (2010) jakavat kyberaktivismin kahteen osa-alueeseen perustuen internetin rooliin aktivismissa: internet-tuettuun sekä internet-pohjaiseen aktivismiin. Internet-pohjainen aktivismi on kyberaktivismin ”uusi” muoto, koska sen olemassaolo perustuu internetin olemassaoloon. Internet-tuettu aktivismi pohjautuu perinteiseen aktivismiin, jonka toteuttamisessa hyödynnetään informaatioteknologiaa. (Van Laer & Van Aelst, 2010; Vegh, 2003.)

TAULUKKO 1 Esimerkkejä kyberaktivismia hyödyntäneistä liikkeistä

| **Vuosiluku** | **Tapahtuma** | **Kybertoimien rooli ja vaikutukset** |
|---|---|---|
| 1994 | Zapatistiliike | Sissiliike Meksikossa käytti hyväkseen internetiä ja sähköpostia raportoidessaan maailmalle liikkeen taistelusta Meksikon valtiota vastaan. (Halleck, 1994.) |
| 2006- | WikiLeaks | Kansainvälinen voittoa tavoittelematon yritys, joka pyrkii informaationvapauteen julkaisemalla muun muassa paljastavia uutisartikkeleita sekä salaisia dokumentteja (Karhula, 2011). WikiLeaks on ollut kyberhyökkäysten motivaattorina organisaation vastustajille sekä kannattajille (Dahan, 2013; Goode, 2015). |

| **Vuosiluku** | **Tapahtuma** | **Kybertoimien rooli ja vaikutukset** |
|---|---|---|
| 2007 | Viron patsaskiista | Viroon kohdistettiin kyberhyökkäyksiä useassa eri hyökkäysaallossa. Taustalla oli Viron päätös siirtää neuvostosotilaiden hautamuistomerkin paikkaa. Maailman ensimmäinen yhden maan kohdistama kyberhyökkäys toista maata vastaan. (Juurvee & Mattiisen, 2020.) Valtiosta erilliset patrioottihakkerit toteuttivat Viroon kohdistuneita kyberhyökkäyksiä monen eri vaikutuskanavan kautta. Hyökkäykset olivat laajamittaisia ja pyrkivät muun muassa vaikuttamaan ihmisten asenteisiin sosiaalisen median kautta sekä Viron valtion infrastruktuurin toimintaan hakkerointi-iskujen avulla. |
| 2010 | Arabikevät | Vastareaktio arabimaiden hallituksien valtaa vastaan. Sosiaalisen median kautta jaettiin kuvia ja videoita hallituksen sorrosta kansalaisia kohtaan. (Khamis, 2017.) Haktivistiryhmät toimivat aktivistien tukena mahdollistaen informaation jakamisen maailmalle (Jordan, 2015). |
| 2014 | ALS-haaste | Miljoonat ihmiset ympäri maailmaa kuvasivat ja jakoivat sosiaaliseen mediaan videoita kaataen jäävettä niskaansa tavoitteenaan kerätä varoja ALS-taudin tutkimiseen. Vuoden 2014 loppuun mennessä ALS-järjestö ALSA kertoi saaneensa yli 115 miljoonaa dollaria lahjoituksina. (Pressgrove, McKeever & Jang, 2018.) |

| Vuosiluku | Tapahtuma | Kybertoimien rooli ja vaikutukset |
|---|---|---|
| 2017 | #MeToo | Alun perin 2007 seksuaalisen hyökkäyksen kohteeksi joutuneille perustettu kampanja, joka levisi maailmanlaajuiseksi vuonna 2017 näyttelijä Alyssa Milanon käytettyä MeToo–hashtagia Twitterissä (Vagianos, 2017). Hashtagia käytettiin ensimmäisen kahden päivän aikana yli 800 000 kertaa Twitterissä ja yli 12 miljoonaa kertaa Facebookissa kannustaen seksuaalisen häirinnän sekä -väkivallan uhreja puhumaan kokemuksistaan (Cassandra & Criss, 2017). |

## 2.2 Kyberaktivismin kehitys ja Web 2.0

Internetin kehitystä voidaan kuvata jakamalla se eri versioihin. Yleisesti ensimmäisiä internetin vaiheita on kuvattu termillä Web 1.0 ja uudempaa kehitysversiota versioksi Web 2.0. Varsinkin termi Web 2.0 on yleistynyt käyttöön, vaikka termiä ei voi virallisesti yhdistää tiettyyn internetin kehitysvaiheeseen. Termi Web 2.0 rinnastetaan usein hieman virheellisesti synonyymiksi sosiaaliselle medialle. Todellisuudessa ”vanhan” internetin sivut voivat olla päivitetty niin, että sivu voidaan katsoa osaksi uutta versiota. Sivun tarkka määritys version mukaan ei aina ole aivan selkeää. Versionumerointi onkin käytännössä vain keino selittää internetin ja nettisivuissa käytetyn tekniikan kehityskulkua. Web 2.0 painottaa käyttäjää ensisijaisena toimijana verkossa kannustaen sisällön luontiin sekä sen muokkaamiseen (Cormode & Krishnamurthy, 2008).

TAULUKKO 2 Kyberaktivismin erot Web 1.0:n ja Web 2.0:n välillä (Sandoval-Almazan & Ramon Gil-Garcia, 2014, s. 368)

| | Web 1.0 | Web 2.0 |
|---|---|---|
| Toiminta | Paikallista tai kansainvälistä | Globaalia ilman rajoja |
| Tiedon leviäminen | Perinteinen media, sähköpostit, nettisivut | Nettisivut, sosiaalinen media (mm. YouTube, Facebook, Twitter) |

| | | |
|---|---|---|
| Organisaation rakenne | Verkossa vertikaalinen, johtaja- tai organisaatiosidonnainen | Horisontaalista, itseohjautuvaa |
| Tiedon kehittyminen ja päivittyminen | Keskinopeaa | Välitöntä, jatkuva tiedon päivittyminen ja muokkaantuminen |
| Rekrytointi | Sähköpostien ja nettisivujen kautta | Online värvääminen sosiaalisen median kautta |
| Tiedon liikkuminen | Tieto järjestäjien kautta | Tiedon jatkuva liikkuminen jäsenten välillä |
| Kieli | Rajoittunut maahan tai alueeseen | Rajoittamatonta |
| Sitoutuminen | Reaalimaailma | Verkossa |
| Yhteys järjestön ulkopuolisiin henkilöihin | Pääosin reaalimaailmassa, osittain verkossa | Pääosin verkossa, osittain reaalimaailmassa |

Myös kyberaktivismin eri keinot ovat lisääntyneet internetin kehityksen myötä. Zapatisti-sissiliikettä, joka aloitti toimintansa vuonna 1994, pidetään yhtenä ensimmäisenä vallankumouksellisena liikkeenä, joka hyödynsi kyberaktivismin keinoja omien tavoitteidensa edistämiseen. Liike sai alkunsa 1. tammikuuta 1994 Meksikossa Chiapaksen osavaltiossa. 3000 paikallista työläistä aseistautui ja valtasi seitsemän kaupunkia tavoitteenaan taistella alueen alkuperäisasukkaiden kärsimää äärimmäistä köyhyyttä vastaan (Garrido & Halavais, 2003). Liikehdinnän kolmantena päivänä verkkoon ilmestyi teksti, jonka lopussa oli allekirjoitus *Subcomandante Marcos*. Kyseessä oli zapatistiliikkeen jäsen, joka halusi kertoa maailmalle toisen puolen konfliktista. Viesti julkaistiin paikallisessa lehdessä ja se käännettiin englannin kielelle. Näin tieto rohkeista vapaustaistelijoista levisi ympäri maailmaa verkon välityksellä keräten samalla suuren kannattajajoukon. (Halleck, 1994.) Kyberaktivismin keinojen avulla zapatistit pystyivät taistelemaan hallituksen levittämää disinformaatiota vastaan. Marcoksen kirjoitukset verkkoon toimivat sytykkeenä maailmanlaajuiselle tuelle zapatistiliikettä kohtaan. Liike sai maailmanlaajuista näkyvyyttä hyödyntämällä ainoastaan yksinkertaisia blogitekstejä ja sähköposteja.

Internet, ja tämän myötä myös kyberaktivismi ovat kehittyneet rutkasti vuoden 1994 takaisista tapahtumista. Web 2.0:n tuomien uusien mahdollisuuksien myötä aktivismin toteuttaminen on helpottunut ja yksittäisten toimijoiden vaikutusvalta on kasvanut. Näihin ovat vaikuttaneet muun muassa mobiililaitteiden yleistyminen sekä sosiaalinen media. Informaation leviäminen sosiaalisessa mediassa on nopeampaa ja aktivismin kohteille vaikeasti hallittavampaa. Web 2.0:ssa tapahtuva aktivismi on myös aikaisempaa enemmän vuorovaikutteista ja se kannustaa aktivisteja keskinäiseen kommunikaatioon. Näin ollen järjestöjen ja liikkeiden rakenne on muuttunut johtajasidonnaisesta liikehdinnästä enemmän horisontaaliseksi ja itseohjautuvaksi järjestäytymiseksi. (Sandoval-Almazan & Ramon Gil-Garcia, 2014.)

Web 2.0 on tehnyt aktivistien näkyvyyden suoremmaksi poistaen perinteisen median roolin tietojen välittäjänä. Tiedot liikkeiden ulkopuolisille toimijoille välittyvät suoraan nettisivujen sekä sosiaalisen median välityksellä.

Tämä on erityisen tärkeää maissa, joissa sananvapaus on rajoitettua ja media on valtion vallassa.

## 2.3 Kyberaktivismin eri muodot

Taulukossa 3 on jaettu kyberaktivismi kolmeen eri kategoriaan. Jako voidaan tehdä sen perusteella, miten suuri vaikutus aktivismin kokonaiskuvassa yhden toimijan teoilla on. Vegh (2003) painottaa aktivismin tasoa ja sen suuntaa suhteessa aktivismin toteuttajaan. Ensimmäisellä tasolla toimet perustuvat informaation vastaanottamiseen ja lähettämiseen. Keskitasolla on aktivismin joukkoistuminen joukkoihin liittymisen ja joukkojen muodostamisen muodossa. Viimeisellä tasolla on laajamittaisen liikehdinnän käynnistäminen ja siihen liittyminen. Nämä aktivismin tasot ovat progressiivisesti kasvavia. (Vegh, 2003.) George ja Leidner (2019) käyttävät hyväkseen Milbrathin (1965) poliittisen osallistumisen hierarkia –mallia, joka on myös kolmiportainen malli sisältäen matalan tason, keskitason sekä korkean tason aktivismin. Tämä malli ottaa huomioon Veghin (2003) kategorisointia paremmin myös kyberaktivismin perusluonteen; korkeamman tason aktivismiin osallistuva on myös yleisesti aktiivisesti mukana matalamman tason aktivistisissa toimissa (George & Leidner, 2019; Vegh, 2003).

TAULUKKO 3 Kyberaktivismin eri tasot ja näiden tasojen eri keinot (George & Leidner, 2019)

| **Matala taso** | **Keskitaso** | **Korkea taso** |
|---|---|---|
| Kliktivismi | Aloitteet | Haktivismi |
| Jakaminen/tykkääminen | Botivismi | Data-aktivismi |
| Sisällöntuotto | Digitaalinen kuluttajuus | Arkaluontoisten tietojen kalastelu ja paljastaminen |

### Matalan tason aktivismi

Matalan tason kyberaktivismi on yleisimmin esiintyvää verkossa tapahtuvaa aktivismia. Tutkimuksen mukaan jopa kaksi kolmasosaa amerikkalaisista sosiaalisen median käyttäjistä on osallistunut jollain tavalla tämän tason kyberaktivismiin (Rainie ym., 2012). Taso sisältää aktivismin kevyimmät muodot, jotka eivät vaadi toteuttajaltaan suuria ponnistuksia. Aktivismin keinoina tällä tasolla ovat muun muassa kliktivismi, sosiaalisessa mediassa poliittiseen keskusteluun osallistuminen esimerkiksi tykkäämällä ja jakamalla sekä sisällön tuottaminen. Vegh (2003) sisällyttää matalimman tason aktivismiin

myös yhteisöjen ja järjestöjen perustamisen digitaalisessa ympäristössä. Esimerkiksi Facebook-sivun tekeminen jonkin aatteen kannattamiseksi lasketaan tähän kategoriaan. Matalimman tason kyberaktivismin perustana on jakaa sekä vastaanottaa aktivismin aiheelle oleellista informaatiota (Vegh, 2003). Kyseessä voi olla esimerkiksi sellaisen informaation levittäminen, jota ei maan julkisen median lähteissä ole saatavilla, johtuen esimerkiksi diktatuurin vallan alla olemisesta.

Matalimman tason aktivismia on kritisoitu johtuen sen toteuttajalleen helposta luonteesta (katso esim. Gladwell, 2010). Tämän tason aktivismi ei vaadi suuria ponnistuksia, joten monelle se voi olla helppo tapa toteuttaa näennäisesti aktivismia, jonka vaikutukset jäävät kuitenkin kokonaiskuvassa vähäisiksi.

**Keskitason aktivismi**

Keskitason aktivismi on luonteeltaan enemmän osallistavaa toimintaa verrattuna matalan tason aktivismiin. Se vaatii enemmän resursseja ja on tätä myöten yleensä myös tehokkaampi aktivismin keino (George & Leidner, 2019). Keskitason aktivismissa pyritään vaikuttamaan omilla teoilla muihin toimijoihin esimerkiksi keräämällä joukkoja ja liikkeellepanemalla nämä edistääkseen ajettua asiaa. Keskitason aktivismi sisällyttää myös perinteisen offline-aktivismin toteuttamisen digitaalisin keinoin (Vegh, 2003).

Keskitason aktivismin toimia ovat muun muassa kansalaisaloitteiden muodostaminen ja allekirjoittaminen, aktivismin toteutus botteja käyttäen eli botivismi sekä digitaalinen kuluttajuus, joka tarkoittaa oman kuluttamiskäyttäytymisen sovittamista aktivismin aatteen periaatteiden mukaisesti esimerkiksi boikotoimalla tiettyä yritystä tai toimijaa.

**Korkean tason aktivismi**

Korkean tason aktivismi on suoraa toimintaa, jossa toimijat pyrkivät toimillaan välittömään muutokseen. Korkean tason aktivismin vaikutukset ovat suoria ja suuria ja näillä pyritään vaikuttamaan yhteiskuntaan, valtioihin sekä organisaatioihin. Toimijat ovat yhdistyksiä tai yksittäisiä toimijoita, jotka toimivat omillaan. Korkean tason aktivismia voidaan kuvata oman käden oikeudeksi, jossa aktivistit toimivat lain rajamailla toimien ollessa usein laittomia. (George & Leidner, 2019; Samuel, 2004; Vegh, 2003.) Korkean tason laittomia toimia on kuvattu myös termillä digitaalinen kansalaistottelemattomuus (electronic civil disobedience) (mm. Taylor, 2005; Wray, 1999).

# 3 HAKTIVISMI

Tässä kappaleessa avataan, miten haktivismi on määritelty eri lähteissä. Tämän jälkeen käsitellään sitä, millaisia haktivistiryhmittymät ovat rakenteeltaan ja lopuksi selvitetään haktivismin eri keinoja, jotta lukijalle tulee selvä kuva siitä, minkälaisilla keinoilla haktivismia toteutetaan. Tämän kappaleen on tarkoitus vastata tutkimuskysymykseen: mihin haktivismilla pyritään?

## 3.1 Haktivismi yleisesti

Haktivismi on kyberaktivismin keino, joka asettuu edellisessä kappaleessa esitellyn kolmiportaisen kyberaktivismin kategorisoinnin korkeimmalle tasolle. Samuel (2004) määrittelee laajasti aihetta käsittelevässä ja useasti viitatussa väitöskirjassaan haktivismin poliittisen aktivismin ja tietokonehakkeroinnin yhdistelmäksi. Haktivismi on väkivallaton keino, joka käyttää hyväkseen laittomia tai lakisääteisesti monitulkintaisia, eli *transgressiivisia*, digitaalisia työkaluja poliittisten tavoitteiden saavuttamiseksi. (Samuel, 2004.) Peltomäki ja Norppa (2015) määrittelevät haktivismin kirjassaan ***Rikos meni verkkoon : näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen*** tietoverkossa tapahtuvaksi aktivismiksi, jonka tavoitteena on saada aikaan huomiota tai muutosta johonkin tiettyyn asiaan (Peltomäki & Norppa, 2015). Haktivismi on hakkeroinnista kasvanut liike, jonka tarkoituksena on teknologisia keinoja käyttäen pyrkiä edistämään poliittisia pyrkimyksiä. Termiä haktivismi käytettiin tiettävästi ensimmäisen kerran hakkerijärjestö Cult of the Dead Cow:n toimesta vuonna 1998 julkaisemassa ***Hacktivismo Declaration*** –manifestissa. Haktivismi on eroteltu useimmissa lähteissä väkivallattomaksi toimeksi, jonka tarkoituksena on oman aatteen edistäminen ilman merkittävää vahinkoa (Dahan, 2013; Denning, 2001; Samuel, 2004). Tämä määrittely erottaa haktivismin kyberterrorismista, jonka seurauksena voivat olla myös ihmisvahingot. George ja Leidner (2019) ovat kirjallisuuskatsauksessaan sisällyttäneet haktivismin käsitteeseen myös kyberterrorismin sekä isänmaallisten hakkereiden joukon.

Isänmaallisilla hakkereilla tarkoitetaan tässä tapauksessa nationalistisia hakkereita, jotka ovat valtiosta erillisiä toimijoita tehden hyökkäyksiä ulkopuolisiin valtioihin, jotka ovat konfliktissa hakkerin oman kotimaan kanssa (Dahan, 2013).

Haktivismi voidaan nähdä työkaluna, jota kansalaisoikeusjärjestöt käyttävät omien aatteidensa edistämiseksi. Haktivismin toimet ovat useimmiten suorempia ja välittömämpiä, kuin alemman tason kyberaktivistiset toimet. Tämä luo haktivisteille uskoa toimien paremmasta tehosta (Samuel, 2004). Toisin kuin hakkeroinnissa, haktivismissa teknologian rooli on olla taustatukena aatteen edistämisessä. Taylorin (2008) mukaan haktivismi sortuu kuitenkin usein hakkereiden tapaan liialliseen teknologian painottamiseen. Tämän takia ajatus digitaalisesti korrektista haktivismista on kerännyt suosiota. (Taylor, 2008.) Digitaalisesti korrekti haktivismi on haktivismin transgressiivinen muoto, joka vaatii tehokkaasti toimiakseen suuren määrän aktiivisia toimijoita. Tällainen massa-haktivismi on luonteeltaan lähellä perinteistä kansalaistottelemattomuutta, ja siitä onkin käytetty termiä digitaalinen kansalaistottelemattomuus (Dahan, 2013; Denning, 2001; Samuel, 2004). Digitaalisen kansalaistottelemattomuuden keinot ovat teknisesti alkeellisempia ja ne perustuvat suurten massojen osallistamiseen. Esimerkkinä kyberympäristössä tapahtuvaa verkkosivujen seisautusta voidaan verrata perinteisen aktivismin istumalakkoon. Digitaalisen kansalaistottelemattomuuden keinoja voidaan pitää suuremmalle massalle tavoitettavampana ja haluttavampana johtuen niiden transgressiivisyydestä sekä teknisestä yksinkertaisuudesta. Perinteisen kansalaistottelemattomuuden kaltaiset kriteerit täyttävä kyberaktivismi nähdäänkin suuremman yleisön näkökulmasta hyväksyttävämpänä haktivismin keinona (Delmas, 2018). Ns. kovemmat toimet, jotka vaativat myös enemmän teknistä osaamista, ovat yleensä selkeästi laittomaksi luokiteltavia, joka karkottaa näiden keinojen tukijoita.

## 3.2 Haktivismin järjestäytyneisyys

Vaikka haktivismia voidaan toteuttaa täysin itsenäisenä toimijana, toimivat haktivistit usein osana jotain suurempaa ryhmää tai ryhmittymää (Dahan, 2013; Samuel, 2004). Dahan (2013) kuvaa haktivisti-ryhmittymien rakennetta vapaaksi mutta vakaaksi ryhmäksi tai verkostoksi, jossa yhteisöllisyyden tunne on suurta. Ryhmittymien sisällä jäsenet toimivat usein anonyymisti nimimerkkejä käyttäen. Ryhmittymät itsessään pyrkivät median huomioon vahvistaakseen heidän omien toimiensa vaikutusta. Ryhmittymillä onkin usein oma mediastrategia, johon sisältyvät mediatapahtumat kuten lehdistötiedotteet sekä YouTube-videot, joissa ilmoitetaan tulevista hyökkäyksistä etukäteen. (Dahan, 2013.) Ryhmät ovat rakenteeltaan useimmiten horisontaalisia ja hajautettuja ilman konkreettista johtajuutta. Päätökset ryhmän sisällä perustuvat useimmiten yhteysymmärrykseen, mutta ryhmittymien vapaasta rakenteesta johtuen

toimijat voivat myös toimia omin päin ilman ryhmittymän varsinaista hyväksyntää. (Milan, 2015.)

Vuonna 2003 keskustelufoorumi 4chan:ista alkunsa saanut Anonymous on kenties kaikista tunnetuin haktivistiryhmittymä. 4chan on kuvalauta, joka perustuu vapaaseen keskusteluun ja äärimmäiseen sananvapauteen. Anonymous perustuukin perusidealtaan täysin rajoittamattoman sananvapauden mahdollistamiseen. Anonymous on kasvanut laajaksi ryhmittymäksi, joka hakkeroinnin lisäksi toteuttaa muun muassa offline-aktivismia sekä mediakampanjoita. (Goode, 2015.) Anonymous on toteuttanut suuren määrän iskuja suuryrityksiä sekä -organisaatioita vastaan. Kohteina ovat muun muassa olleet skientologiakirkko sekä useat Yhdysvaltalaiset suurpankit. Iskuja on usein tehty kostoiskuina reaktiona kohteen toimia vastaan. Iskujen motivaation pohjalla on Anonymouksen kyberlibertaristisiin sekä vasemmistolaisiin arvoliberaaleihin arvoihin kuten informaationvapauteen sekä ihmisoikeuksien parantamiseen perustuvat pyrkimykset.

## 3.3 Haktivismin keinot

Haktivismin toimia voidaan kategorisoida niiden laillisuuden ja vaikutusten merkittävyyden mukaan. Samuel (2004) on kategorisoinut keinot transgressiivisiksi sekä lainsuojattomiksi toimiksi. Transgressiiviset toimet vaativat yleensä massojen osallistamista ja se on lakisääteisesti moniselitteistä, usein ns. lain harmaalla alueella. Lainsuojaton toiminta taas on selkeästi määriteltävissä laittomaksi toiminnaksi, jota yleensä toteutetaan teknisesti taitavien yksilöiden tai pienten ryhmittymien toimesta. (Samuel, 2004.) Ulkopuolisten haktivismin luokittelu laillisen aktivismin ja laittoman vandalismin välille riippuu jossain määrin henkilöstä; haktivismihyökkäykset suuryrityksiä kohtaan toteuttaen humoristisia, vahinkoa aiheuttamattomia keinoja saavat useimmiten aikaan positiivisia tunteita, mutta hyökkäykset internetin toimivuutta sekä yhteyksiä vastaan saavat usein negatiivisen vastaanoton (Taylor, 2008). Tämä voi olla yhtenä syynä siihen, miksi digitaalisesti korrekti haktivismi, eli teknisesti alkeellinen digitaalisen kansalaistottelemattomuuden muoto on laajemman yleisön silmissä hyväksyttävämpää ja tätä myöten myös kokonaiskuvassa tehokkaampaa.

**Virtuaalinen seisahdus**

Virtuaalinen seisahdus (engl. virtual sit-in) on transgressiiviseksi luokiteltava haktivismin keino, joka perustuu massojen voimaan. Hyökkääjät kuormittavat samanaikaisesti kohteena olevan verkkosivun palvelinta niin, että sen käyttö hidastuu tai estyy kokonaan. Virtuaalisen seisahduksen erottaa palvelunestohyökkäyksestä sen toteuttamistavan vuoksi; hyökkäys vaatii sen, että jokainen seisahdukseen osallistuva on konkreettisesti paikalla päivittämässä verkkosivua tai painamassa nappia seisahduksen toteuttavalla verkkosivulla

(Samuel, 2004). Hyökkäys voi palvelimesta riippuen vaatia jopa sadan tuhannen aktiivisen hyökkääjän kokoisen joukon, jotta haluttu lopputulos saavutetaan. Virtuaalinen seisahdus on periaatteeltaan saman tapainen kuin perinteisen aktivismin keinona käytetty sit-in tai istumalakko; kun reaalimaailmassa liikenteen kulku estetään tukkimalla kulkuväylät kohteeseen, kybermaailmassa verkkoliikenteen kulku estetään tukkimalla reitti verkkosivulle.

**Nettisivuväärennös**

Romagna ja van den Hout (2017) määrittelevät nettisivuväärennöksen jonkin verkossa olevan sijainnin turmelemiseksi ilman verkkosijainnin omistajan lupaa (Romagna & van den Hout, 2017). Samuel (2004) on omassa väitöskirjassaan määritellyt nettisivuväärennöksen verkkosivun sisällön luvattomaksi muutokseksi web-palvelimelle hakkeroitumalla (Samuel, 2004). Romagnan ja van den Houtin määritelmä ottaa nykyaikaisemmin huomioon myös verkossa olevien muiden sijaintien turmelemisen. Näihin sijainteihin voidaan luokitella esimerkiksi sosiaalisen median profiilien sisällön muuttaminen haktivistien motiivien mukaan. Väärennöksiä voidaan tehdä täsmäiskuna johonkin tiettyyn verkkosijaintiin tai suurissa määrin satunnaisiin sijainteihin haktivistien jakaman viestin mahdollisimman laajaksi levittämiseksi. Sivustoihin hakkeroituminen pyritään tekemään tietoturva-aukkojen avulla. Yleisin yksittäinen hyökkäyskeino sivustolle pääsemiseksi on sql-injektio, jossa palvelimelle tunkeudutaan verkkosivun tietokannan suojaamattomuuden kautta (Romagna & van den Hout, 2017).

**Uudelleenohjaus**

Verkkosivun uudelleenohjauksessa hakkerit ohjaavat verkkosivulle tulevan liikenteen heidän haluamalleen verkkosivulle. Haktivistien tapauksessa kohdesivu sisältää yleensä kritiikkiä alkuperäistä sivua kohtaan. (Samuel, 2004.)

**Palvelunestohyökkäys**

Palvelunestohyökkäyksen tavoitteena on estää verkossa olevan palvelun saavutettavuus. Se on yleinen ja tehokas kyberhyökkäyskeino, jonka tavoitteena ei ole palveluun murtautuminen vaan sen käytön estäminen (Samuel, 2004). Palvelunestohyökkäyksiä voidaan myös kohdistaa kohteeseen useasta eri lähteestä samaan aikaan, jolloin kyseessä on hajautettu palvelunestohyökkäys. Tällöin hyökkäyksestä saadaan tehokkaampi, koska verkkoa saadaan kuormitettua laajemmassa mittakaavassa ja useammasta eri lähteestä. Palvelunestohyökkäyksen toimesta sivuston käyttö voi hidastua tai sivusto voi kaatua kokonaan. Palvelunestohyökkäyksen toteuttamiseen on useita eri keinoja, yksinkertaisimmillaan hyökkäys voidaan toteuttaa ylikuormittamalla web-palvelin kutsuilla, jolloin palvelin ei pysty vastaamaan kutsuihin normaalilla nopeudella, tai ollenkaan. Hyökkäyksen tekemiseen on kehitetty myös useita

erilaisia työkaluja, joiden avulla hyökkäyksen voi toteuttaa ilman laajaa teknistä osaamista (Kang, Zhang & Ju, 2006). Palvelunestohyökkäys voi aiheuttaa merkittäviä taloudellisia menetyksiä johtuen palveluiden toiminnan keskeytymisestä, mutta hyökkäys ei kuitenkaan useimmiten aiheuta pysyviä vahinkoja laitteistoon tai dataan (Solomon, 2017).

**Informaatiovarkaus**

Informaatiovarkaudella tarkoitetaan yksityisen tiedon varastamista suojatusta verkosta tai yksittäisestä laitteesta. Teko on verrattavissa varkauteen, joten se on selkeästi laitonta toimintaa. (Hampson, 2012.) Haktivistien asenne informaatiovarkautta kohtaan voidaan nähdä myös yllättävän sallivana huolimatta sen laittomuudesta ja rangaistavuudesta. Hyökkäyksen tarkoituksena ei välttämättä ole hankitun tiedon käyttö, vaan näyttö hyökkäyksen kohteen heikosta tietoturvasta. Jossain tapauksissa haktivistit voivat kuitenkin käyttää saatua tietoa hyväkseen ja julkaista sitä. (Samuel, 2004.) Verizonin kyberturvallisuusraportissa (2012) todettiin haktivistien ja haktivistiryhmittymien olleen vastuussa 58 %:a tietomurroissa varastetusta tiedosta. Tästä huolimatta haktivistiryhmittymät olivat vastuussa vain 2 %:a tietomurroista, mikä vahvistaa käsitystä siitä, että haktivistit eivät välttämättä tavoittele iskuillaan taloudellista hyötyä, vaan keräävät mahdollisimman laajasti satunnaista informaatiota iskujen kohteista häiritäkseen kohteen normaalia toimintaa sekä paljastaakseen toimia julkisuuteen. (Verizon, 2012, 2016.)

**Digitaalinen vandalismi**

Digitaalisen vandalismin keinona käytetään tietokoneviruksia, matoja, troijalaisia sekä sähköpostipommeja, joiden tarkoituksena on kohteen informaatiojärjestelmien toiminnan häiritseminen. Virukset voivat myös esimerkiksi ottaa saastuttamansa tietokoneen haltuunsa näyttäen hyökkäyksen toimeenpanijan haluamaa viestiä tietokoneen ruudulla (Solomon, 2017). Taylor (2008) esittää digitaalisen vandalismin haktivismin tuhoisampana muotona.

**Web-sivuparodia**

Nettisivuparodiat ovat verkkosivuja, jotka on tehty muistuttamaan jotain tiettyä, jo olemassa ollutta verkkosivua (Samuel, 2004). Parodiasivulla voidaan esimerkiksi kritisoida kohdesivuston organisaatiota tai pilailla yrityksen kustannuksella. Parodiasivun osoite on yleensä lähellä alkuperäisen sivun osoitetta, jolloin kirjoitusvirheen tehdessään käyttäjä ohjataan parodiasivustolle.

**Ohjelmistokehitys**

Ohjelmistokehitystä on myös mahdollista toteuttaa haktivismin keinoin. Ohjelmistot ovat yleensä toteutettu käyttäen avointa lähdekoodia, jolloin ohjelmat ovat vapaasti muokattavissa. Haktivistien kehittämät ohjelmistot

pyrkivät helpottamaan haktivistien toimintaa; kyseessä voi olla esimerkiksi haktivisti-järjestölle kehitetty viestintäsovellus tai ohjelmisto, jonka avulla autoritäärisen valtion kansalaiset pystyvät kiertämään maan asettamat palomuurit, jotka estävät vierailun tietyillä verkkosivuilla (Samuel, 2004).

TAULUKKO 4 Haktivismin keinot ja niiden laillisuus (Samuel, 2004; Solomon, 2017)

| **Keino** | **Vaikutustapa** | **Laillisuus** |
|---|---|---|
| Virtuaalinen seisahdus | Verkkosivun kaataminen suurten massojen toimesta | Transgressiivinen |
| Nettisivuvääärennös | Verkkosivun sisällön muuttaminen ilman sivuston omistajan lupaa | Laiton |
| Uudelleenohjaus | Käyttäjän ohjaaminen toiselle verkkosivulle | Laiton |
| Palvelunestohyökkäys | Palvelun käytön estäminen | Laiton |
| Informaatiovarkaus | Arkaluontoisten salattujen tietojen varastaminen | Laiton |
| Digitaalinen vandalismi | Haittaohjelmien kehittäminen | Laiton |
| Web-sivuparodia | Parodia jostain verkkosivusta, käytetään hyväksi esimerkiksi kirjoitusvirhettä verkko-osoitteessa | Transgressiivinen |
| Ohjelmistokehitys | Aktivismissa ja haktivismissa apuna käytettyjen ohjelmistojen kehittäminen | Laillinen, transgressiivinen, laiton |

# 4 HAKTIVISMIN VAIKUTUSTEN ANALYSOINTI ESIMERKKITAPAUSTEN AVULLA

Tämän kappaleen tarkoituksena on käsitellä esimerkkitapausten avulla haktivistien toteuttamia hyökkäyksiä ja näiden hyökkäysten vaikutuksia laajemmalla tasolla. Kaikista tapauksista ei ole tutkimustietoa, joten niihin on viitattu käyttäen saatavilla olevaa tietoa. Näihin kuuluvat kyberturvallisuustoimijoiden raportit sekä uutiset tapahtumista. Tämän kappaleen on tarkoitus vastata tutkimuskysymykseen: millaisia vaikutuksia haktivismilla on saatu aikaan?

## 4.1 Tapaus 1 – Operation Tunisia

Arabikevät oli vallankumousten sarja, joka sai alkunsa 2010–luvun alussa Tunisiassa. Taustalla olivat köyhemmän kansanosan kokema valtiojohteinen sorto. Kapinoiden aikaan aktivistien Facebook–sivuja alettiin estämään ja heidän jakamaa sisältöä poistettiin. Myös internetin käyttöä rajoitettiin ja pääsy tietyille sivuille evättiin kokonaan. Esimerkiksi WikiLeaks–sivustolle pääsy estettiin, koska sivustolla esiintyi paljastuneita Yhdysvaltojen valtion dokumentteja, joissa esitettiin Tunisian valtionhallinnon epäkohtia. (Jordan, 2015.) Tunisian valtiolliset toimijat onnistuivat sisällyttämään pienen määrän koodia Facebook–sivuston salaamattomalle yhteydelle, minkä avulla valtio sai haltuunsa aktivistien kirjautumistietoja. Näiden tietojen avulla valtio toteutti aktivistien pidätyksiä (Anderson, 2011). Anonymous julkaisi viestin tukien aktivistien toimia ja aloitti Tunisian valtioon kohdistetut kyberhyökkäykset aktivistien tukemiseksi.

Anonymouksen jäsen kirjoitti lyhyen ohjelmakoodin, jonka aktivistit pystyivät kopioimaan Greasemonkey–selainlaajennukseen. Ohjelmakoodin avulla aktivistit pystyivät selaamaan verkkoa vapaasti, ilman valtion pääsyä heidän selaustietoihinsa. Koodin avulla pystyttiin myös kiertämään aiemmin kansalaisilta estetyt verkkosivut. (Olson, 2013, s. 142.) Haktivistit kohdistivat

palvelunestohyökkäyksiä Tunisian valtion virallisia verkkosivuja kohtaan kaataen ne. Tunisian pääministerin viralliselle verkkosivulle tehtiin nettisivuväärennös-hyökkäys, jossa sivuston sisällöksi vaihdettiin Anonymouksen kirjoittama viesti Tunisian valtiolle. Tässä viestissä vaadittiin internetin avaamista kansalaisille sekä kansalaisten sortamisen lopettamista. (Hill, 2011.) Haktivistiryhmän jäsenet jakoivat myös digitaalisia apupaketteja, jotka sisälsivät selainlaajennuksen lisäksi muun muassa viestintäohjelmia, jotka käyttivät hyväkseen suojattua Tor-verkkoa (Jordan, 2015). Näiden ohjelmien avulla aktivistit pystyivät viestimään keskenään suojassa valtiolta. Apupaketin työkalujen avulla aktivistit onnistuivat jakamaan informaatiota ja mediaa Tunisiassa tapahtuvasta liikehdinnästä muualle maailmaan.

Tässä haktivismihyökkäyksessä perinteiset aktivistit, alemman tason kyberaktivistit sekä haktivistit tekivät yhteistyötä mahdollistaen aktivismin toteutumisen monella eri tasolla. Anonymous onnistui omilla toimillaan kiertämään valtion asettamat rajoitukset informaatiovirran kulkemiseen. Tunisian konflikti levisi viiteen muuhun arabimaahan: Libyaan, Egyptiin, Jemeniin, Syyriaan sekä Bahrainiin. Arabikeväänä tunnettu vallankumouksellinen liikehdintä kesti vuoteen 2013 saakka (Encyclopaedia, 2021).

## 4.2 Tapaus 2 – Operation Ababil

Operation Ababil sai alkunsa syyskuussa 2012, kun nettisivusto Pastebiniin jaettiin englannin ja arabin kielellä ilmoitus hyökkäyksistä yhdysvaltalaisia pankkeja kohtaan. Viestissä ilmoitettiin, että nimellä Cyber fighters of Izz Ad-Din Al Qassam toimiva hakkerointiryhmä on tehnyt, ja tulee tekemään pankkeihin kohdistuvia hyökkäyksiä. Joulukuusta 2011 toukokuuhun 2013 46:a eri pankkia ja finanssialan yritystä kohtaan kohdistui ainakin 176 päivän ajan hajautettuja palvelunestohyökkäyksiä. Kohteina olivat muun muassa Bank of America, JPMorgan Chase sekä New Yorkin pörssi. Iskujen määrä muuttui satunnaisista iskuista viikoittaisiin ryhmittymän jakaman viestin jälkeen. Syyskuussa 2012, viestin jakamisen jälkeen suuria yhdysvaltalaisia finanssialan yrityksiä kohtaan kohdistettiin liikennettä, jonka määrä nousi pahimmillaan 120 gbps yltäneisiin siirtonopeuksiin. Suurin osa pankkien nettisivuista oli tehty kestämään vain noin kolmasosa tällaisesta kuormituksesta. Ryhmittymä käytti hyökkäyksessä muun muassa JS LOIC –työkalua, joka on JavaScript-pohjainen web-versio suositusta LOIC –palvelunestohyökkäysvälineestä. Ryhmittymän motiivina oli YouTube –videopalvelussa oleva Islaminvastainen elokuva, joka muun muassa esitti väitteitä, että jokainen teknologisesti aktiivinen Islaminuskoinen nuori tulee olemaan uhka länsimaille sekä sionistisille valtioille. Ryhmittymän mukaan sen jäsenet olivat vapaaehtoisia eri puolilta Lähi-Itää, mutta selvitysten mukaan hyökkäysliikenne oli aktiivista varsinkin Iranin sekä Palestiinan alueella. Hyökkäys on yhdistetty myös Iranin muodostamaan

kyberpuolustustiimiin, joka perustettiin Iranin ydinohjelmaan kohdistetun Stuxnet –viruksen paljastuttua. Hyökkäys on kyberturvallisuusasiantuntijoiden sekä EU Cyber Direct –ohjelman mukaan osa Iranin valtion tukemaa hyökkäystä Yhdysvaltoja kohtaan vastauksena Iraniin kohdistettuja pakotteita kohtaan. (Cyber Conflict Portal, 2020; *Deconstructing the Al-Qassam Cyber Fighters Assault on US Banks*, 2013.)

Yhdysvallat käynnisti yhdessä muiden maiden kyberturvallisuustoimijoiden, eli CERT-tiimien, välisen yhteystyön, jonka avulla hyökkäyksessä käytetyt laitteet saatiin suljettua pois verkosta ja näin ollen hyökkäykset saatiin lopulta estettyä (Nakashima, 2014). Hyökkäys aiheutti kymmenien miljoonien dollarien edestä kustannuksia yhdysvaltalaisille pankeille. Sadoilta tuhansilta asiakkailta evättiin pääsy pankkien palveluihin hyökkäysten aikana. Hyökkäyksen mahdollisti alimitoitetut turvallisuusjärjestelmät, jotka mahdollistivat bottiverkkoa hyödyntävien palvelunestohyökkäysten käytön (Cyber Conflict Portal, 2020).

Hyökkäys on esimerkki haktivisti-iskusta, jonka taustalla on mahdollisesti valtiollinen toimija. Näin haktivismia voidaan käyttää peitetarinana valtioiden väliseen konfliktiin. Valtion roolia hyökkäyksissä on kuitenkin vaikeaa, ellei mahdotonta konkreettisesti todistaa, joten tässäkin hyökkäysten sarjassa julkiseen tietoon jää vain yhdysvaltalaisten virkamiesten asettamat syytökset ja väitökset Iranin valtiota kohtaan. Vuonna 2016 Yhdysvallat asetti syytteeseen seitsemän Iranin kansalaista syytettynä iskun toteuttamisesta (Brewster, 2016).

## 4.3 Hyökkäysten vaikutukset

Kahdesta tässä kappaleessa esitetystä haktivismioperaatiosta voidaan havaita, että haktivismilla voidaan saada niin välittömästi, kuin välillisestikin aiheutettua kohteelle monia erilaisia haittoja. Näihin haittoihin lukeutuvat muun muassa mainehaitat, taloudelliset haitat sekä yhteiskunnan toimintaa horjuttavat haitat. Mansfield-Devine (2011) esittää, että suurimmassa osassa hyökkäyksistä vaikutukset jäävät kokonaiskuvassa pienimuotoisiksi (Mansfield-Devine, 2011). Tässä tutkimuksessa esitetyistä esimerkeistä voidaan kuitenkin päätellä, että oikeaan paikkaan iskettäessä, voivat taloudelliset menetykset olla rahamäärässä mitattuna suuret. Nurmi ja Niemelä (2018) ovat käsitelleet haktivismia PESTEL–viitekehykseen sovitettuna. Viitekehys käsittää poliittisen, taloudellisen, sosio-kulttuurillisen, teknologisen, ympäristön sekä juridisen motivaation analyysin. 33:n eri haktivismioperaation analyysissa todettiin haktivismin mahdollisten kohteiden koskevan kaikkia viitekehyksen eri kategorioita. Nurmi ja Niemelä toteavat tutkimuksessaan, että haktivismin riskien määrittämiseen organisaatiotasolla ei löydy riittävästi dataa, joten tarkka riskien analysointi ei ole mahdollista. (Nurmi & Niemelä, 2018.) Tietoturvayhtiö Kasperskyn (2018) raportissa todetaan, että hajautetun palvelunestohyökkäyksen aiheuttamat kustannukset voivat nousta yli 120 tuhanteen dollariin per hyökkäys pienten ja

keskisuurten yritysten tapauksessa ja yli kahteen miljoonaan dollariin per hyökkäys suuryritysten tapauksessa. (Kaspersky, 2018).

Hyökkäysten vaikutusten arviointi vaihtelee sen mukaan, että arvioidaanko haktivismilla aikaan saatuja muutoksia, vai haktivismin vaikutuksia esimerkiksi yrityksen kokemiin taloudellisiin tappioihin. Suuryritykset voivat kokea rahamäärällisesti paljolta kuulostavalta tappioita, mutta iskujen vaikutukset jäävät lyhytaikaisiksi, eikä hyökkäysten toteuttajien toivomaa muutosta saada aikaan. Mansfield-Devinen (2011) mukaan tietoturva-ammattilaiset ovatkin kokeneet hyökkäyksissä positiivisen puolen; yritysjohto joutuu ottamaan huomioon haktivismi-hyökkäysten riskit, jotka on saatettu aiemmin sivuuttaa liian kalliina (Mansfield-Devine, 2011). Vaikutusten arviointia vaikeuttaakin se, että verkkosivuihin kohdistuneiden hyökkäysten kuten sivustoväärennösten sekä palvelunestohyökkäysten aiheuttamien menetysten ja mainehaittojen konkreettista rahallisen menetyksen arvoa on haastava arvottaa (Plachkinova & Vo, 2019).

# 5 YHTEENVETO

Tämän tutkimuksen tarkoituksena oli luoda kuva haktivismista kyberaktivismin osana käsitellen eri keinoja sen toteutukseen sekä sen mahdollisia vaikutuksia. Tutkimuksessa kerättiin tietoa eri tieteenalojen tutkimuksesta luoden tietojärjestelmätieteen tutkimukselle ominaisen poikkitieteellisen katsauksen tutkittavaan aiheeseen.

Vaikka haktivistisia tekoja on toteutettu jo yli kahdenkymmenen vuoden ajan 1990–luvulta saakka, on aihetta tutkittu varsin niukasti. Tästä kertoo myös haktivismin kattotermin, kyberaktivismin, melko suppea tutkimus. Varsinkin tietojärjestelmätieteen tutkimusalan tutkimusta aiheita ei ole paljoakaan olemassa. Haktivismia käsitteenä on tulkittu eri lähteissä eri tavoin, eikä tarkkarajaista määritelmää ole. Aiheen tutkimista voisi edistää aihepiirin käsitteiden ja ilmiöiden määrittely ja teorisointi. Tässä tutkimuksessakin viitattu McCaugheyn ja Ayersin (2003) toimittama kokoomateos kyberaktivismista ja haktivismista on vielä tänäkin päivänä osa usean aihepiirin tutkimuksen lähdekirjallisuutta. Kyseinen kirja on myöskin selvästi viitatuin teos Google Scholarin mukaan. Alan tutkimus vaatisikin päivityksen nykytietoon; kahdessakymmenessä vuodessa internet on muuttunut todella paljon tuoden laajoja, kyberaktivismin sekä haktivismin toimiin vaikuttaneita uudistuksia. Sosiaalista mediaa voidaan pitää yhtenä tärkeimpänä uudistuksena internetin kehityksessä. Tämä on tuonut kyberaktivismiin ja tätä myöten haktivismiin uuden ulottuvuuden lisäten toimijoiden mahdollisuuksia.

Kyberaktivismi on yhä useamman kansalaisen keino tuoda oma ääni kuuluville ja päästä mukaan demokraattiseen vaikuttamiseen. Merkitys on suuri varsinkin matalan demokratian maissa, joissa kansalaisten toimia ja mahdollisuuksia on sensuroitu valtiollisten toimijoiden puolesta. Kyberaktivismia on mahdollista toteuttaa monella eri tavalla, osa tavoista ei vaadi yksilöltä suuria ponnistuksia eikä käyttäjältään suurempaa vastuuta. Kyberaktivismi on kuitenkin mahdollista toteuttaa perinteisen aktivismin tapaan myös yksilöpainotteisena, suorana toimintana, joka pyrkii nopeisiin tuloksiin sekä vaikutuksiin. Haktivismi lukeutuu tällaiseksi suoran toiminnan kyberaktivismiksi. Toimia voidaan toteuttaa niin yksilö- kuin ryhmätasolla,

kohteiden vaihdellessa yksilöistä organisaatioihin sekä valtioihin. Haktivismin toteuttamiseen on useita eri keinoja, joiden määrä tulee varmasti myös lisääntymään internetin toimintojen sekä hakkerointitekniikoiden kehittyessä. Haktivismin teho kyberaktivismin keinona vaihtelee kohteen sekä iskun laajuuden mukaan. Joskus iskut jäävät vaikutuksiltaan pieniksi, jopa häirinnän tasolle, mutta ajoittain iskut onnistuvat aiheuttamaan kohteellensa merkittäviä ongelmia varsinkin silloin, kun iskut ovat laajempia haktivismi-operaatioita, jotka käyttävät hyväksi useita eri keinoja ja kyberaktivismin tasoja.

Yritysmaailmassa haktivismi-iskut ovat pakottaneet yritykset ottamaan kyberturvallisuuden paremmin huomioon (Mansfield-Devine, 2011). Tämä luo myös hankaluuksia yrityksen kyberriskien arvioimiseksi johtuen hyökkäysten vaikutusten vaikeasta arvioimisesta. Nurmen ja Niemelän (2018) käyttämä PESTEL-viitekehys pystyy analysoimaan hyökkääjien motiivien perusteella mahdollisia kohteita, mutta se ei ole yksinään riittävä analysoimaan sitä, minkälaiset vaikutukset yrityksen liiketoimintaan haktivismihyökkäyksillä on. Vaikutusten analysoimiseksi tarvittaisiin laajoja empiirisiä tutkimuksia, jossa saataisiin kerättyä dataa haktivismi-hyökkäyksistä. Haktivismin kohteeksi joutuminen tarkoittaa yleensä, että iskun kohteen toimet eivät ole eettisesti hyväksyttäviä, jonka takia yritykset eivät halua paljastaa joutuneensa hyökkäyksen kohteeksi mainehaittojen pelossa. Tämä hankaloittaa datan keräämistä ja näin ollen vaikutusten analysointia.

Tämä kirjallisuuskatsaus antaa lähtökohdan haktivismin vaikutusten tarkemmalle tutkimiselle. Keräämällä ja analysoimalla haktivismi-iskuista saatua dataa olisi mahdollista ymmärtää haktivismin ja sen eri keinojen vaikutuksia niin organisaatiotasolla kuin myös laajemmalla, yhteiskunnallisella tasolla.

# LÄHTEET

Anderson, N. (2011, 14. tammikuuta). *Tweeting Tyrants Out of Tunisia: Global Internet at Its Best*. Wired. Haettu 4.8.2021 osoitteesta https://www.wired.com/2011/01/tunisia/

Brewster, T. (2016, 24. maaliskuuta). *U.S. Accuses 7 Iranians Of Cyberattacks On Banks And Dam*. Forbes. Haettu 4.8.2021 osoitteesta https://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/

Cormode, G., & Krishnamurthy, B. (2008). Key differences between Web 1.0 and Web 2.0. *First Monday*.

Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013, 51.

*Deconstructing the Al-Qassam Cyber Fighters Assault on US Banks*. (2013, 2. tammikuuta). Recorded Future. Haettu 4.8.2021 osoitteesta https://www.recordedfuture.com/deconstructing-the-al-qassam-cyber-fighters-assault-on-us-banks/

Delmas, C. (2018). Is Hacktivism the New Civil Disobedience?. *Raisons politiques*, (1), 63-81.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, *239*- 288.

Domanski, R. J. (2015). *Who Governs the Internet? : A Political Architecture*. Lexington Books.

Encyclopaedia, T. E. of. (2021). *Arab Spring*. Encyclopedia Britannica. Haettu 4.8.2021 osoitteesta https://www.britannica.com/event/Arab-Spring

EU Cyber Direct Cyber Conflict Portal. (2020). *DDOS ON US BANKS*. EU Cyber Direct. Haettu 4.8.2021 osoitteesta https://eucyberdirect.eu/wp-content/uploads/2020/11/2012-ddos-on-us-banks.pdf

Garrido, M., & Halavais, A. (2003). Mapping networks of support for the Zapatista movement. Teoksessa M. McCaughey & M. D. Ayers (toim.), *Cyberactivism: Online activism in theory and practice* (165–184). Routledge.

George, J., & Leidner, D. (2018). Digital activism: A hierarchy of political commitment. Teoksessa *Proceedings of the 51st Hawaii International Conference on System Sciences*.

George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3).

Gladwell, M. (2010). Small Change – Why the Revolution Will Not Be Tweeted. *The New Yorker*, *4*(2010), 42-49.

Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. *Popular Communication*, *13*(1), 74–86. https://doi.org/10.1080/15405702.2014.978000

Halleck, D. (1994). Zapatistas on-line. *NACLA Report on the Americas*, *28*(2), 30–32.

Halminen, L. (2021). Hallitusta vastustavien hakkerien epäillään saaneen haltuunsa Valko-Venäjällä koko kansan passitiedot ja poliisien dataa. *Helsingin Sanomat*. Haettu 15.8.2021 osoitteesta https://www.hs.fi/ulkomaat/art-2000008182226.html

Hampson, N. (2012). Hacktivism, Anonymous & a New Breed of Protest in a Networked World. *Boston College International and Comparative Law Review*, *35*(6), 511.

Hill, E. (2011, 3. tammikuuta). Hackers hit Tunisian websites. *Al Jazeera*. Haettu 4.8.2021 osoitteesta https://www.aljazeera.com/news/2011/1/3/hackers-hit-tunisian-websites

Illia, L. (2003). Passage to cyberactivism: how dynamics of activism change. *Journal of Public Affairs*, *3*(4), 326–337. https://doi.org/10.1002/pa.161

Jordan, T. (2015). Hacktivism: Operation Tunisia, Modular Tactics and Information Activism. Teoksessa *Information Politics* (176–191). Pluto Press. https://doi.org/10.2307/j.ctt183p2xf.14

Juurvee, I., & Mattiisen, M. (2020). The Bronze Soldier Crisis of 2007. Revisiting an Early Case of Hybrid Conflict. *International Centre for Defence and Security*.

Kang, J., Zhang, Y., & Ju, J.-B. (2006). Classifying DDoS attacks by hierarchical clustering based on similarity. *2006 International Conference on Machine Learning and Cybernetics*, 2712–2717.

Karhula, P. (2011). What is the effect of WikiLeaks for Freedom of Information? *FAIFE Spotlight [Online]*, *19*.

Kaspersky. (2018, 22. helmikuuta). *DDoS Breach Costs Rise to over $2M for Enterprises finds Kaspersky Lab Report*. Haettu 4.8.2021 osoitteesta https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report

Khamis, S. (2017). Revisiting Cyberactivism Six Years after the Arab Spring: Potentials, Limitations and Future Prospects. Teoksessa *Media in the Middle East* (3–19). Springer.

Mansfield-Devine, S. (2011). Hacktivism: assessing the damage. *Network Security*, *2011*(8), 5–13.

McCaughey, M., & Ayers, M. D. (toim.). (2003). Cyberactivism: Online activism in theory and practice. Routledge.

Milan, S. (2015). Hacktivism as a radical media practice. *Routledge Companion to Alternative and Community Media*, 550-560. Routledge.

Nakashima, E. (2014, 11. huhtikuuta). *U.S. rallied multinational response to 2012 cyberattack on American banks*. The Washington Post. Haettu 4.8.2021 osoitteesta https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html

Nurmi, J., & Niemelä, M. S. (2018). *PESTEL Analysis of Hacktivism Campaign Motivations.* Teoksessa *Nordic Conference on Secure IT Systems (323-335). Springer Verlag.*

Olson, P. (2013). We are Anonymous : inside the hacker world of Lulzsec, Anonymous, and the global cyber insurgency. Back Bay Books.

Peltomäki, J., & Norppa, K. (2015). Rikos meni verkkoon : näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Talentum.

Plachkinova, M., & Vo, A. (2019). Hacktivism and Its Impact on Society. 25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, *August 15-17, 2019*.

Pressgrove, G., McKeever, B. W., & Jang, S. M. (2018). What is Contagious? Exploring why content goes viral on Twitter: A case study of the ALS Ice Bucket Challenge. *International Journal of Nonprofit and Voluntary Sector Marketing*, *23*(1). https://doi.org/10.1002/nvsm.1586

Rainie, L., Smith, A., Schlozman, K. L., Brady, H., & Verba, S. (2012). Social media and political engagement. *Pew Internet & American Life Project*, *19*, 2–13.

Romagna, M., & van den Hout, N. J. (2017). Hacktivism and website defacement: motivations, capabilities and potential threats. *27th Virus Bulletin International Conference*, *1*, 1–10.

Samuel, A. W. (2004). Hacktivism and the future of political participation (Väitöskirja). Harvard University. Haettu 26.7.2021 osoitteesta https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

Sandoval-Almazan, R., & Ramon Gil-Garcia, J. (2014). Towards cyberactivism 2.0? Understanding the use of social media and other information technologies for political activism and social movements. *Government Information Quarterly*, *31*(3), 365–378. https://doi.org/10.1016/j.giq.2013.10.016

Santiago, C., & Criss, D. (2017, 17. lokakuuta). An activist, a little girl and the heartbreaking origin of 'Me too'. Haettu 15.8.2021 osoitteesta https://edition.cnn.com/2017/10/17/us/me-too-tarana-burke-origin-trnd/index.html

Solomon, R. (2017). Electronic protests: Hacktivism as a form of protest in Uganda. *Computer Law & Security Review*, *33*(5), 718–728. https://doi.org/10.1016/j.clsr.2017.03.024

Taylor, P. A. (2005). From hackers to hacktivists: speed bumps on the global superhighway? *New Media & Society*, *7*(5), 625–646. https://doi.org/10.1177/1461444805056009

Taylor, P. A. (2008). Hacktivism. In *The International Encyclopedia of Communication*. https://doi.org/10.1002/9781405186407.wbiech003

Vagianos, A. (2017, 17. lokakuuta). *The 'Me Too' Campaign Was Created By A Black Woman 10 Years Ago*. Haettu 6.8.2021 osoitteesta https://www.huffpost.com/entry/the-me-too-campaign-was-created-by-a-black-woman-10-years-ago_n_59e61a7fe4b02a215b336fee

Van Laer, J., & Van Aelst, P. (2010). INTERNET AND SOCIAL MOVEMENT ACTION REPERTOIRES. *Information, Communication & Society*, *13*(8), 1146–1171. https://doi.org/10.1080/13691181003628307

Vegh, S. (2003). Classifying forms of online activism: The case of cyberprotests against the World Bank. Teoksessa M. McCaughey & M. D. Ayers (toim.), *Cyberactivism* (81–106). Routledge.

Verizon. (2012). 2012 Data Breach Investigations Report. Haettu 29.7.2021 osoitteesta https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

Verizon. (2016). *Data breach digest*. Haettu 29.7.2021 osoitteesta https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

Wray, S. (1999). On electronic civil disobedience. *Peace Review*, *11*(1), 107–111.