Tatu Suhonen

TIEDONLOUHINTA KYBERTERRORISMIN TORJUNTAKEINONA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Suhonen, Tatu Topi Sakari
Tiedonlouhinta kyberterrorismin torjuntakeinona
Jyväskylä: Jyväskylän yliopisto, 2017, 35s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaajat: Perälä, Piia & Taipalus, Toni

Terrorismi on teknologian kehittyessä siirtynyt kyberavaruuteen ja muuntautunut kyberterrorismiksi. Terrorismin uhka ei enää ole vain fyysinen, sillä kyberavaruus mahdollistaa tietoverkkojen monipuolisen käytön terroristisiin tarpeisiin. Kyberterrorismin uhka on synnyttänyt tarpeen luoda uudenlaisia torjuntakeinoja. Yksi kyberterrorismin torjuntaan käytetyistä menetelmistä on tiedonlouhinta, jonka avulla pystytään tehokkaasti löytämään ennestään tuntematonta tietoa suurista datamäärästä. Tässä tutkielmassa tutkitaan kyberterrorismia ilmiönä sekä tiedonlouhinnan menetelmiä ja sovelluksia kyberterrorismin torjuntaan. Tutkielma on kirjallisuuskatsaus, joka pohjautuu alan tieteelliseen tutkimukseen, sekä niitä tukeviin julkaisuihin. Tutkielman tuloksena voidaan todeta, että tiedonlouhinnan avulla voidaan pyrkiä estämään kyberterroristien iskuja sekä etsimään kyberterroristeja ja heidän toimintaansa verkosta. Tiedonlouhintaa voidaan hyödyntää kriittisen infrastruktuurin suojaamiseen tarkoitetuissa tunkeutumisen havainnointijärjestelmissä järjestelmien havainnointikyvyn parantamiseen. Verkossa tiedonlouhintaa voidaan hyödyntää kyberterroristien ja kyberterrorismiin viittaavan materiaalin etsimiseen. Tiedonlouhinta on kuitenkin ensisijaisesti vain päätöksentekoa edistävä työkalu, joka ei estä kyberiskuja tapahtumasta. Tiedonlouhinnalla voidaan silti saavuttaa ennaltaehkäisevä vaikutus ja vähentää kyberterrorismin riskejä. Datamäärien kasvaessa datan automaattisen käsittelyn ja analysoinnin merkitys korostuu, joten tiedonlouhinnalle löytyy tulevaisuudessa vielä enemmän käyttöä.

Asiasanat: kyber, terrorismi, kyberpuolustus, tiedonlouhinta

ABSTRACT

Suhonen, Tatu Topi Sakari
Data mining against cyberterrorism
Jyväskylä: University of Jyväskylä, 2017, 35p.
Information systems science, Bachelor's Thesis
Supervisor: Perälä, Piia & Taipalus, Toni

Due to technological advancements terrorism has moved to cyberspace and it has transformed into cyberterrorism. The threat of terrorism is no longer purely physical because cyberspace allows versatile use of networks for terrorist use. The threat has generated the need for new kinds of methods to fight against cyberterrorism. One of the used methods is data mining which allows the discovery of new knowledge from large datasets. The goal of this thesis is to examine cyberterrorism as a phenomenon and to discover the different methods and applications where data mining could be used against cyberterrorism. This thesis is a literature review and it is based on the scientific research and other supporting publications. The result of this thesis is that data mining is used to prevent cyberterrorist attacks and to find cyberterrorists and their activities on the web. Data mining can be used to enhance the detection capabilities of intrusion detection systems that are used to protect the nation's critical infrastructure. On the web data mining can be used to find cyberterrorists and cyberterrorist related content. However, data mining is primarily a tool for decision making and it does not prevent cyberterrorism from happening. Still it can reduce the risk of cyberterrorism acts and can give valuable information to prevent cyberterrorism. As the amount of data keeps on growing the automatic processing and analyzing of data will be more significant and therefore data mining will have lots of use in the future.

Keywords: cyber, terrorism, cyber defense, data mining

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Teknologian kehitys on muokannut ympäröivää maailmaamme. Terrorismi on seurannut samaa kehityspolkua ja sen seurauksena nykyisin myös terroristijärjestöt käyttävät informaatioteknologiaa olennaisena osana omaa toimintaansa (Last, 2005). Nykyisin kybermaailmassa tapahtuvasta terrorismista käytetään ilmaisua kyberterrorismi. Kyberterrorismia kuvaillaan terrorismin ja kybermaailman yhdentymänä, jossa informaatioteknologiaa hyödynnetään osana terroristista toimintaa (Ariely, 2007). Kyberterrorismi on yhä suurempi uhka valtioiden turvallisuudelle, sillä kyberterrorismin uhka on kyberterroristien kyvykkyyden parantuessa koko ajan kasvava (Curran, Concannon & McKeever, 2007). Julkinen infrastruktuuri sekä valtioiden kriittinen infrastruktuuri ovat entistä haavoittuvaisempia, sillä niiden tietoturvan taso ei pysy muun kehityksen mukana, mutta samalla kyberterrorismin luomat riskit kasvavat(Al Mazari, Anjariny, Habib & Nyakwende, 2016).

Vastatoimena kyberterrorismiin on alettu käyttää tiedonlouhintaa. Tiedonlouhinta on prosessi, jonka avulla pyritään löytämään uutta ja merkityksellistä tietoa suurista datamääristä (Han, Kamber & Pei, 2012). Aikakaudella, jossa datamäärät alkavat olla ihmisen käsiteltäväksi liian suuria, on aiheellista hyödyntää teknologioita, joilla tietokoneavusteisesti voidaan tutkia suuria datamääriä nopeasti ja tehokkaasti. Kyberterrorismin torjunnassa haasteena on muutosnopeus, joka pakottaa tutkijat jatkuvaan kehitystyöhön. Kyberterrorismiin ja tiedonlouhintaan liittyvää tutkimusta on tehty verrattain paljon, mutta tiedonlouhinnan käyttö kyberterrorismin torjunnassa on vielä ollut melko suppean tutkijajoukon mielenkiinnon kohteena. Tätä selittää varmasti se, että tiedonlouhinta on erittäin laaja tutkimusala ja tiedonlouhinnan menetelmiä voidaan käyttää moniin eri käyttötarkoituksiin. Kyberterrorismin uhka on kuitenkin todellinen ja monessa maassa siitä on tullut suuri turvallisuusuhka (Foltz, 2004), mikä motivoi myös tätä tutkimusta. Tutkimuksen tutkimusongelma on seuraava:

- Miten tiedonlouhintaa voidaan hyödyntää kyberterrorismin torjunnassa?

Varsinaisen tutkimusongelman selvittämiseksi ja tueksi käytetään kahta tarkentavaa tutkimuskysymystä, jotka selventävät aihepiiriä ja antavat lukijalle tarvittavan informaation tutkielman ymmärtämiseksi:

- Mitä on kyberterrorismi?
- Mitä on tiedonlouhinta?

Tutkielma toteutettiin kirjallisuuskatsauksena perustuen alan tieteellisiin julkaisuihin ja muihin tutkielman aihepiiriin liittyviin julkaisuihin. Tiedonhaussa hyödynnettiin enimmäkseen Jyväskylän Yliopiston kirjaston JYKDOK-hakupalvelua ja Googlen Scholar-palvelua. Tiedonhaussa käytettiin pääsääntöisesti hakusanoja ”cyberterrorism” ja ”data mining” ja niiden suomenkielisiä vastineita ”kyberterrorismi” ja ”tiedonlouhinta”. Lähteiden valinnassa painotettiin julkaisun viittausmäärää ja julkaisijan merkittävyyttä. Lähdemateriaalin valinnassa pyrittiin myös valitsemaan saatavilla olevista lähdemateriaaleista tuoreimmat ja ajankohtaisimmat.

Tutkielma koostuu johdannon lisäksi kolmesta sisältöluvusta. Johdantoa seuraavassa luvussa käsitellään kyberterrorismia määrittelemällä sen käsite ja tutkimalla kyberterrorismin viitekehystä. Luvun pyrkimyksenä on tuoda ilmi niitä erityispiirteitä, joita kyberterrorismiin ilmiönä liittyy. Luvussa kolme käsitellään tiedonlouhintaa määrittelemällä tiedonlouhinnan käsite ja tutkimalla tiedonlouhinnan prosessia ja käytössä olevia menetelmiä. Luku neljä käsittelee tiedonlouhinnan käyttöä kyberterrorismin torjunnassa. Neljännessä luvussa vastataan varsinaiseen tutkimuskysymykseen tutkimalla tiedonlouhinnan käyttöä kriittisen infrastruktuurin suojaamisessa ja verkon louhinnassa. Viimeinen, viides luku koostuu pohdinnasta ja yhteenvedosta.

2 KYBERTERRORISMI

Tässä luvussa määritellään kyberterrorismin käsite. Lisäksi luvussa syvennytään kyberterrorismiin hieman tarkemmin tutkimalla sitä Ahmadin ja Yunosin (2012) luoman viitekehyksen kautta. Luvun tavoitteena on tuottaa lukijalle yleiskäsitys kyberterrorismista, jotta lukija pystyy ymmärtämään kyberterrorismin yleisellä tasolla sekä tunnistamaan sen ominaispiirteitä.

2.1 Kyberterrorismin käsite

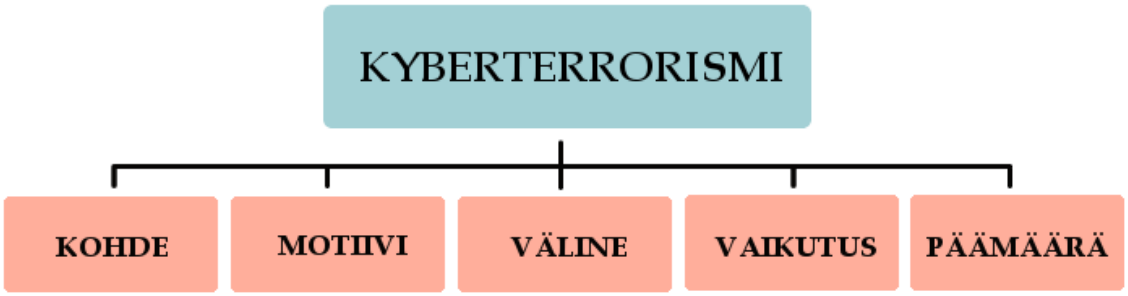
Terrorismin käsitteellä on monia selityksiä. Yksi usein käytetyistä terrorismikäsityksistä määrittää terrorismin henkilön tai organisoidun ryhmän suorittamana laittoman tai uhkaavan voiman tai väkivallan käyttönä, jonka päämääränä on pelotella tai pakottaa yksilöitä tai valtion hallintoa omien ideologisten tai poliittisten syiden takia (Bogdanoski & Petreski, 2013). Terrorismi on ajan saatossa muuntautunut perinteisestä terrorismista kybermuotoiseen terrorismiin, eli teknologian mahdollistamaan terrorismiin, joka tunnetaan nykyisin kyberterrorismina. Käsitteen on luonut ensimmäisenä vuonna 1982 Barry Collin, joka määritteli kyberterrorismin fyysisen maailman ja kybermaailman yhdentymäksi. (Samuel ym., 2014.)

Kyberterrorismista on tullut muodikas sana selittämään kybermaailmassa tapahtuvia kyberhyökkäyksiä. Käsitteelle ei kuitenkaan ole yleisesti vakiintunutta määritelmää, vaikka sitä runsaasti käytetään. Esimerkiksi monissa valtioissa kyberterrorismi mainitaan yhdeksi suurimmaksi uhaksi valtion turvallisuudelle. (Al Mazari ym., 2016.) Muun muassa FBI:n silloinen johtaja Robert Mueller totesi jo vuonna 2010 kyberterrorismin olevan todellinen uhka Yhdysvaltojen turvallisuudelle, sillä terroristit ovat hänen mukaansa osoittaneet selkeää kiinnostusta hakkerointiin ja kyberhyökkäysten tekemiseen (Chapmann, 2010). Silti keskustelua on käyty siitä, mitä kyberterrorismi oikeastaan todellisuudessa on ja onko sen luoma uhka aiheellinen (Foltz, 2004).

Nykyisin kyberterrorismin käsitteelle löytyy monia määritelmiä, jotka vaihtelevat hieman näkökulmasta, ajasta ja kirjoittajasta riippuen. Vaikka määritelmä ei ole vakiintunut, selkeitä ominaispiirteitä kyberterrorismin käsitteelle on löydettävissä. Denningin (2000a) mukaan kyberterrorismi tarkoittaa tietokoneita, tietoverkkoja ja säilöttyä informaatiota kohtaan tehtyjä laittomia hyökkäyksiä ja uhkauksia, joilla pyritään pelottelemaan tai pakottamaan valtion hallitusta tai kansalaisia omien poliittisten tai sosiaalisten tavoitteiden saavuttamiseksi. Denningin (2000a) mukaan hyökkäyksen luokittelu kyberterrorismiksi vaatii väkivaltaa ihmisiä tai omaisuutta kohtaan tai sen, että hyökkäys luo pelkoa kohdevaltion kansalaisissa.

Lewis (2002) määrittelee kyberterrorismin kyberhyökkäyksenä, joka johtaa valtion kriittisen infrastruktuurin tietojärjestelmien toimimattomuuteen. Lewisin (2002) mukaan kyberterrorismia voi myös olla tietoverkkojen ja niihin liittyvien teknologioiden käyttäminen siviilien tai valtion työntekijöiden pelottelemiseen. Pollit (1998) määrittelee kyberterrorismin informaatiota, dataa, tietokoneita tai tietokoneohjelmia vastaan ennalta suunniteltuna, poliittisesti motivoituneena hyökkäyksenä, joka johtaa väkivaltaan siviilejä kohtaan. Al Mazari ym. (2016) mukaan kyberterrorismi sisältää eri määritelmiä yhdessä tarkasteltuna usein toistuvia yhteneväisyyksiä: Tietoverkkoja ja teknologiaa käytetään hyökkäysten tekemiseen. Hyökkäysten kohteena on valtion infrastruktuuri tai valtion hallinto. Kyberterrorismin taustalla on psykologinen, sosiaalinen, poliittinen tai uskonnollinen motiivi ja iskujen tarkoitus on aiheuttaa vahinkoa yksilöille tai yhteisöille, tai fyysisesti aiheuttaa tuhoa valtion infrastruktuurille. Lisäksi hyökkäys voi olla ulkoisesta tai sisäisestä lähteestä. (Al Mazari ym., 2016.)

Al Mazari ym. (2016) jakavat kyberterrorismin käsitteen viiteen käsitettä kuvaavaan osaan: kohde, motiivi, väline, vaikutus ja päämäärä (ks. kuvio 1).



KUVIO 1 Kyberterrorismin käsitteen jaottelu (Al Mazari ym., 2016)

Ensimmäisenä mainittu kohde on esimerkiksi armeija, valtionhallinnon infrastruktuuri, valtion kriittinen infrastruktuuri, valtiollinen ja sosiaalinen identiteetti tai yksityinen sektori. Motiivi tekijällä voi olla sosiaalinen, poliittinen, us-

konnollinen tai ideologinen. Kolmantena mainittu väline tarkoittaa tietokoneita, kommunikointiteknologioita ja tietoverkkoja. Vaikutus voi olla väkivaltaa, tuhoa tai häiriöitä palveluissa, haittaa yksilöille tai yhteisöille sekä fyysisiä, operationaalisia tai informaationaalisia vaurioita. Päämäärä kyberterrorismissa tarkoittaa poliittisen, sosiaalisen, militaarisen tai ideologisen edun saamista. (Al Mazari ym., 2016.)

2.2 Kyberterrorismin viitekehys

Kyberterrorismin selittämiseksi on kehitetty erilaisia viitekehyksiä selittämään kyberterrorismin eri osa-alueita ja erityispiirteitä, jotka erottavat kyberterrorismin muusta verkossa tapahtuvasta rikollisesta toiminnasta. Ahmad ja Yunos (2012) jaottelevat kyberterrorismin viitekehyksen kuuteen osaan: kohde, vaikutus, motivaatio, hyökkäykseen käytettävä metodi, toimintaympäristö ja tekijän toiminta.

Kyberterrorismin ainutlaatuinen piirre Ackermanin ym. (2006) mukaan on se, että varsinaisen kohteen lisäksi hyökkäyksellä on paljon suurempi kohdeyleisö, johon vaikutukset ulottuvat. Sen vuoksi Rollinsin ja Wilsonin (2007) mukaan kyberterroristien pääkohde iskulle tulisi olemaan talous, jolloin onnistuneen hyökkäyksen seurauksena voisi syntyä fyysisiä ja taloudellisia tuhoja ja jopa kuolemantapauksia. Ahmad ja Yunos (2012) toteavat, että kyberterroristien kohteeksi valikoituu yleensä kriittinen infrastruktuuri, sillä kriittiseen infrastruktuuriin kohdistuvalla iskulla on yleensä muihin aloihin kohdistuvia sivuvaikutuksia. Syy tähän on valtion kriittisen infrastruktuurin merkitys yhteiskunnan toiminnan edellytyksenä. Jos kriittinen infrastruktuuri pettää, valtion toimintakyky voi lamaantua täysin. Monia tärkeitä kriittisen infrastruktuurin tietojärjestelmiä ohjataan valvomo-ohjelmistoilla (Supervisory Control and Data Acquisition, SCADA), jotka saattavat olla yhteydessä internetiin. Kriittistä infrastruktuuria valvoviin SCADA-järjestelmiin kohdistuvan iskun mahdollisuus on aikaisemmin ollut minimaalinen, mutta teknologian kehityksen myötä niistä on tullut kyberterrorismin tärkeimpiä kohteita. (Ahmad & Yunos, 2012.) Pollit (1998) käyttää esimerkkinä kohteen ja siihen kohdistuvan iskun vaikutusten laajemmasta vaikutuspiiristä murotehdasta, johon hyökkääjä pääsee käsiksi. Hyökkääjä lisää ohjausjärjestelmän kautta tehtaan työntekijöiden huomaamatta ravintolisää muroihin, jolloin niistä tulee myrkyllisiä. Murojen päätyessä markkinoille hyökkäyksen vaikutukset ulottuvat paljon kauemmas, vaikka itse iskun kohteena oli vain tehdas ja sen valvomo-ohjelmisto. (Pollit, 1998.)

Kyberterrorismissa tekijän motiivi katsotaan usein merkittäväksi määritteleväksi tekijäksi. Dunn Caveltyn (2007) mukaan vain sellaiset kyberhyökkäykset, joiden tekijöillä on poliittinen, ideologinen tai uskonnollinen motiivi, pitäisi laskea kyberterrorismiksi. Vaikka perimmäinen syy toiminnalle olisi jokin edellä mainittu, on toiminnan motiivina usein myös muita tekijöitä. Jalal (2013) ja-

kaa kyberterrorismin motivaatiotekijät neljään osaan. Ensimmäinen motivaatiotekijä liittyy vihollisen operationaalisen kyvyn tuhoamiseen. Kyberympäristö tarjoaa halvan ja tehokkaan työkalun vastapuolen vahingoittamiseen ja pahimmassa tapauksessa hyökkäyksen onnistuessa se saa kokonaisen valtion pysähdyksiin. Toinen motivaatiotekijä on organisaation, valtion tai allianssin maineen tuhoaminen, sillä monen suuren toimijan toiminta perustuu vahvaan maineeseen. Hyökkäyksen onnistuessa kohteen maine kärsii ja kyberterroristi saavuttaa oman motiivinsa. Kolmas motivaatiotekijä on saada hyökkäyksen kohde muuttamaan toimintaansa omien intressien mukaiseksi, esimerkiksi muuttamaan politiikkaansa. Neljäs motivaatiotekijä on halu näyttää omille tukijoille oma kyky tuottaa vahinkoa ja tappioita vihollisille. Tällöin hyökkääjän oma maine kasvaa tukijoidensa joukossa. (Jalal, 2013.)

Kyberterrorismin erilaiset hyökkäyksessä käytettävät metodit voivat vaihdella erilaisista tietoverkkojen välityksellä tehtävistä hyökkäyksistä psykologiseen vaikuttamiseen (Heickerö, 2007). Hyökkäyksen metodin kuitenkin määrittää hyökkääjän kyky suorittaa iskuja. Denningin (2000b) mukaan hyökkääjän kyvykkyyden tasot voidaan jakaa kolmeen osaan: yksinkertainen-epäjärjestelmällinen, edistynyt-epäjärjestelmällinen ja kompleksinen-koordinoitu. Yksinkertainen-epäjärjestelmällinen–taso tarkoittaa kykyä suorittaa yksinkertaisia iskuja yksittäisiin järjestelmiin jonkun muun luomilla työkaluilla. Hyökkääjä on huonosti organisoitu, eikä kykene oppimaan tai analysoimaan kohteitaan tehokkaasti. Edistynyt-epäjärjestelmällinen–tasolla hyökkääjä pystyy suorittamaan hyökkäyksiä useisiin järjestelmiin, pystyy muokkaamaan ja tekemään itse perustasoisia työkaluja hyökkäämiseen. Lisäksi hyökkääjä on jonkin verran organisoitu ja kykenee analysoimaan kohteitaan ja oppimaan. Korkeimmalla kompleksinen-koordinoitu–tasolla hyökkääjällä on kyky koordinoituihin ja hyvin organisoituihin hyökkäyksiin, joilla kyetään tuottamaan suurta tuhoa monimutkaisiin järjestelmiin. Lisäksi silloin hyökkääjällä on kyky itse luoda tehokkaita työkaluja, oppia ja analysoida erittäin tehokkaasti kohteitaan. (Denning, 2000b.)

Hyökkäyksissä käytettäviä metodeita on useita riippuen halutusta vaikutuksesta. Niitä ovat esimerkiksi tietojärjestelmiin tunkeutuminen ja sen seurauksena tiedon hankita ja tiedon muokkaus. Tietojärjestelmiin tunkeutumalla voidaan aiheuttaa suurempaa tuhoa organisaation operaatioihin, esimerkiksi ohjausjärjestelmien kautta. Kyberterroristit voivat myös käyttää palvelunestohyökkäyksiä (Denial of Service, Distributed Denial of Service), joilla voidaan lamauttaa palvelimen toiminta. Lamauttaminen tapahtuu lähettämällä palvelimelle niin paljon palvelupyyntöjä, että se ei pysty vastaamaan kaikkiin pyyntöihin tarpeeksi nopeasti ja näin ollen tukkeutuu. Lisäksi kyberterroristit voivat käyttää tietoverkkoja myös disinformaation levittämiseen tai kaapata verkkosivuja ja muokata niitä omien etujensa mukaiseksi. (Jalil, 2003.) Hyökkäyksen metodiin vaikuttaa se, kuka itse hyökkääjä on, sillä uhka voi tulla myös organisaation sisältä (Heickerö, 2007). Esimerkiksi tyytymätön tai närkästynyt työntekijä tai yhteistyökumppani voi olla suuri uhka, koska hänellä on tietotaitoa ja sisäpiirin tietoa organisaation asioista. Organisaation työntekijä voi myydä tie-

toa tai suorittaa iskun esimerkiksi lataamalla haittaohjelman organisaation järjestelmiin. (Ahmad & Yunos, 2012.)

Ahmadin ja Yunosin (2012) mukaan kyberterrorismin toimintaympäristö on kyberavaruus, jossa kyberhyökkäykset tapahtuvat. Kyberavaruuden merkitys sodankäynnissä ja vaikutuskanavana on kasvanut. Ahmad ja Yunos (2012) toteavat, että nykyisin kyberavaruus lasketaan viidentenä ulottuvuutena sodankäynnille maa-, meri-, ilma- ja avaruussodankäynnin lisäksi. Weimannin (2004) mukaan kyberterroristeille kyberavaruus on houkutteleva, sillä sinne on helppo pääsy ja se tarjoaa suuren kohdeyleisön, mutta verrattain vähän sensuuria. Lisäksi kyberavaruuden tarjoama nopea tiedonkulku, monet eri käytettävät mediat, anonymiteetti ja halpa käyttö tarjoavat erinomaisen alustan terroristien toimille (Weimann, 2004).

Tekijän toimet kyberterrorismissa ovat väkivaltaa virtuaalisessa maailmassa (Gordon & Ford, 2002). Informaatioteknologian kehittyminen ja nopeat muutokset kyberympäristössä ovat vaikuttaneet terroristien resursseihin ja mahdollisuuksiin (Ahmad & Yunos, 2012). Niiden myötä on syntynyt tapa jaotella kyberterrorismia tekijöiden toimien mukaan vaikutukseen ja aikomukseen perustuviin näkökulmiin (Rollins & Wilson, 2007). Vaikutusperusteinen näkökulma toteutuu silloin, kun kyberhyökkäyksistä koituu sellaisia vaikutuksia, jotka ovat niin haitallisia, että ne aiheuttavat yhtä paljon pelkoa kuin perinteiset terrori-iskut. Tällöin kyberterrorismi keskittyy määrittelyssä enemmän itse tekoon kuin tekijään. Aikomukseen perustuva näkökulma perustuu kyberterrorismin määrittelyssä enemmän tekijään. Aikomukseen perustuvan näkökulman mukaan tekijällä on aikomuksenaan laittomasti tai poliittisesti motivoituneilla kyberhyökkäyksillä pelotella tai pakottaa valtion hallitusta tai kansalaisia omien poliittisten tavoitteidensa saavuttamiseksi. (Rollins & Wilson, 2007.)

3 TIEDONLOUHINTA

Tässä luvussa määritellään tiedonlouhinnan käsite, jonka avulla tutkitaan tiedonlouhinnan perusteita ja tarkoitusta. Käsitteen määrittelyn lisäksi tutkitaan tiedonlouhintaprosessia, joka selventää tiedonlouhinnan toimintaperiaatteita. Luvun lopussa perehdytään muutamiin tiedonlouhinnassa käytettäviin menetelmiin. Luvun tarkoituksena on saada lukijalle yleiskäsitys tiedonlouhinnasta ja tiedonlouhintaprosessista, jotta lukija ymmärtää sen perusperiaatteet ja kykenee ymmärtämään tutkielman aihepiiriä.

3.1 Tiedonlouhinnan käsite

Datan määrä erilaisissa tietokannoissa on nykyisin valtava, koska dataa kerääntyy lähes kaikesta ihmisten jokapäiväisestä toiminnasta nopealla tahdilla. Datan joukkoon kertyy erittäin hyödyllistä tietoa, mutta siitä ei tiedetä, koska sitä ei osata etsiä. (Witten & Frank, 2005.) Ongelman seurauksena on syntynyt tarve tietokoneavusteisesti etsiä merkityksellistä tietoa säilötystä datasta, sillä ihminen ei enää yksin siihen kykene. Ongelman ratkaisemiseksi on alettu käyttää tiedonlouhintaa (data mining). Tiedonlouhinta koostuu monista eri tutkimusaloista, mutta niitä yhdistää pyrkimys luoda tärkeää tietoa suurista datamääristä (Fayyad, Piatetsky-Shapiro & Smyth, 1996.)

Tiedonlouhinnan käsite on nykyisin melko vakiintunut. Hanin ym. (2012) mukaan tiedonlouhinta on osa prosessia, jossa pyritään löytämään mielenkiintoisia malleja (pattern) ja hyödyllistä tietoa suurista datamääristä. Data voi olla säilöttynä moniin eri paikkoihin, kuten tietokantoihin, tietovarastoihin, internetiin tai muihin informaatiosäilöihin. (Han ym., 2012.) Witten ja Frank (2005) määrittelevät tiedonlouhinnan implisiittisen, ennestään tuntemattoman ja potentiaalisen informaation löytämiseksi datasta. Tiedonlouhinta perustuu automaattiseen tai puoliautomaattiseen prosessiin, jossa pyritään löytämään erilaisia malleja jo olemassa olevista suurista tietokannoista. Löytyneistä malleista

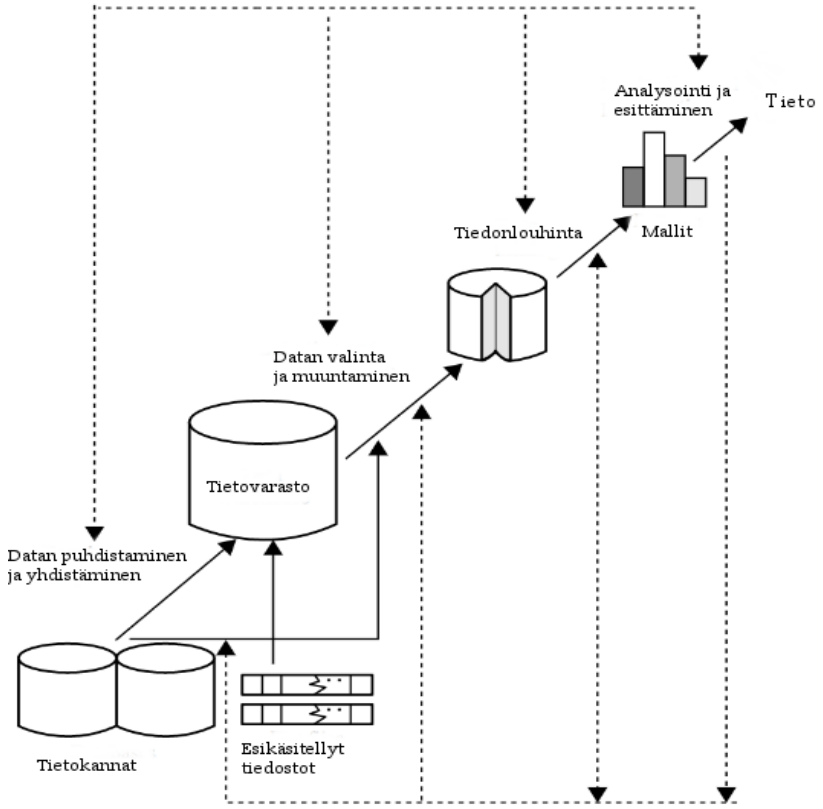
saadaan hyödyllistä tietoa, jota voidaan käyttää päätöksenteon tukena. (Witten & Frank, 2005.)

Tiedonlouhinnan juuret ovat pitkällä informaatioteknologian kehityksessä. Tietokannat ilmestyivät 1960-luvulla ja sen myötä niiden hallintaan kehitettiin erilaisia tietokannan hallintajärjestelmiä, joilla pystyttiin tekemään kyselyjä ja muokkauksia tietokantoihin. Tästä luonnollisena seurauksena 1980-luvulla laskentatehon kasvaessa syntyi datan kehittyneempi analysointi, kuten OLAP-työkalut. Kun 1990-luvulla datan määrän kasvu alkoi entisestään kiihtyä internetin yleistyttyä, alkoi tiedonlouhinnalle löytyä todellista tarvetta, sillä sen avulla kyettiin tekemään syvempiä ja tarkempia analyysejä tutkittavasta datasta. (Han ym., 2012.)

Käsitteen merkitys ei kuitenkaan aina ole ollut täysin vakiintunut, vaan siitä on ollut monia eri versioita käytössä. Tiedonlouhinnan lisäksi on käytetty muun muassa seuraavia käsitteitä kuvaamaan hyödyllisen tiedon etsimistä datasta: tiedon uuttaminen (knowledge extraction), informaation löytäminen (information discovery), informaationkorjuu (information harvesting), data-arkeologia (data archeology) ja datamallien prosessointi (data pattern processing) (Fayyad ym., 1996).

3.2 Tiedonlouhinnan prosessi

Hanin ym. (2012) mukaan tiedonlouhinta itsessään on osa prosessia, jota kutsutaan tiedon löytämiseksi tietokannoista (Knowledge Discovery in Databases, KDD). Suuret datamäärät ovat ihmiselle hankalia hahmottaa ja käsitellä, mutta KDD-prosessilla niitä saadaan tuotettua tietoa, joka on kompaktimpaa, abstraktimpaa tai hyödyllisempää (Fayyad ym., 1996). KDD-prosessi on iteratiivinen prosessi (ks. kuvio 2), joka pitää sisällään seitsemän vaihetta. Ensin data esikäsitellään kaksivaiheisesti. Data puhdistetaan, eli siitä poistetaan epäsäännöllisyydet ja selkeät virheet. Esikäsittelyn toisessa vaiheessa data integroidaan, eli yhdistetään useista lähteistä kerätty data yhdeksi aineistoksi tietovarastoon. Esikäsittelyn jälkeen valitaan analyysissä käytettävä data tietovarastosta ja muunnetaan se sellaiseen muotoon, että sitä voidaan käsitellä valitulla tiedonlouhintamenetelmällä. Datan muuntamisen jälkeen tapahtuu itse tiedonlouhinta, jossa valitulla menetelmällä etsitään datasta yhdenmukaisuuksia ja malleja. (Han ym., 2012.) Malli on yleinen nimitys tiedonlouhinnan tuloksesta, joka voi tapauksesta riippuen olla esimerkiksi sääntö, konsepti, assosiaatio, linkki tai ennustava malli. Mallin täytyy olla toistettavissa, jotta sitä voidaan pitää luotettavana. (Last, 2005.) Tiedonlouhinnan jälkeen tulokset analysoidaan ja tulosten joukosta etsitään kiinnostavimmat mallit. Louhintaprosessin lopussa uusi informaatio esitetään sellaisessa muodossa, että informaatiota hyödyntävä käyttäjä pystyy sitä ymmärtämään ja käsittelemään. (Han ym., 2012.)



KUVIO 2 KDD-prosessin kulku (Han ym., 2012)

Fayyad ym. (1996) korostavat iteraation ja silmukoiden merkitystä eri vaiheiden välillä osana KDD-prosessin onnistumista. Vaikka itse tiedonlouhinta on prosessin tärkeä vaihe, ei se onnistu ilman huolellista valmistelua ja datan esikäsittelyä. Myös tiedonlouhintavaihe on usein iteratiivinen, eli valittuja tiedonlouhinnan menetelmiä toistetaan useaan otteeseen valitulle aineistolle. (Fayyad ym, 1996.)

3.3 Tiedonlouhinnan menetelmät

Tiedonlouhinnan tavoitteet voidaan jakaa kahteen kategoriaan: varmentaminen (verification), jossa tarkoituksena on varmentaa käyttäjän hypoteesi, ja uuden tiedon löytäminen (discovery), jossa systeemi etsii autonomisesti uusia malleja datasta. Tavoitteisiin päästään erilaisilla tiedonlouhinnan menetelmillä, joista useimmat perustuvat muiden tutkimusalojen, kuten koneoppimisen, mallien tunnistamisen ja tilastotieteen tekniikkoihin. (Fayyad ym., 1996.) Varmentamisen menetelmät perustuvat usein perinteisiin tilastotieteen menetelmiin, kuten yhteensopivuustestiin tai varianssianalyysiin. Tiedonlouhinnassa ollaan kui-

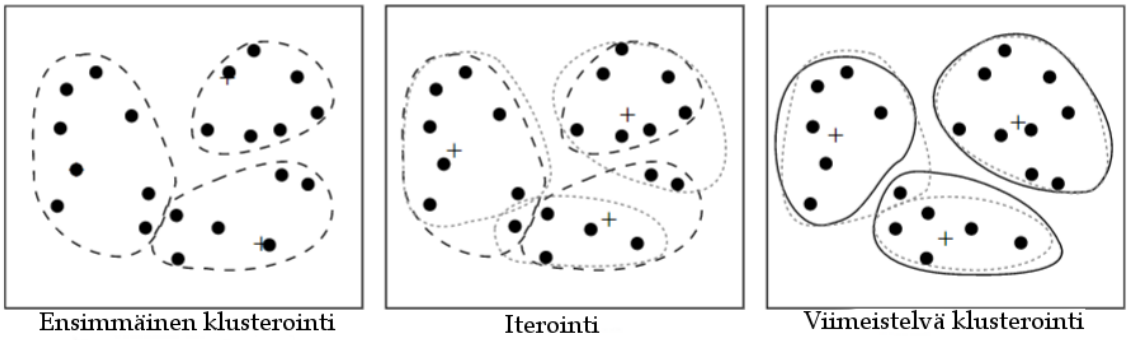
tenkin usein kiinnostuneempia uuden tiedon löytämisestä, sillä tosielämän tilanteissa on usein mielenkiintoisempaa löytää uusia malleja datasta kuin varmentaa jo tiedettyjä asioita. (Last, 2005.) Erilaisia menetelmiä tiedonlouhintaan on erittäin paljon. Menetelmät ovat myös kehittyneet hyvin monimutkaisiksi eri käyttötarkoituksia varten. Usein ne kuitenkin noudattavat muutamia perusperiaatteita, kuten matematiikan tunnettuja algoritmeja. (Fayyad ym., 1996.)

Yksi eniten käytetyistä menetelmistä on luokittelu (classification). Luokittelu on menetelmä, jossa dataa luokitellaan ennalta määrättyjen sääntöjen perusteella erilaisiin dataa kuvaaviin luokkiin. (Bramer, 2013.) Luokittelu tapahtuu antamalla algoritmille luokittelusäännöt harjoitussetillä. Harjoitussetti on tietokanta, jossa mahdolliset luokat ja niiden ominaisuudet on valmiiksi määritelty. Harjoitussetistä algoritmi oppii luokittelumallin (classifier), jonka perusteella algoritmi päättää mihin luokkaan käsiteltävä data-alkio kuuluu. (Han ym., 2012.) Luokittelua voidaan toteuttaa useilla erilaisilla tavoilla. Lähin naapuri – luokittelumenetelmä pyrkii luokittelumallin avulla etsimään lähimpänä käsiteltävän alkion arvoja olevan luokan. Naiivi Bayesilainenen luokittelumalli pyrkii todennäköisyysteorioiden avulla löytämään todennäköisimmän luokan käsiteltävälle alkiolle. Päätöspuissa luokittelusäännöistä luodaan päätöspuu, jonka mukaisesti algoritmi luokittelee käsiteltävät alkiot päätöspuun eri oksissa aloittaen sen juuresta ja päättyen johonkin puun oksien lehdistä. (Bramer, 2013.)

Tiedonlouhintaa voidaan toteuttaa myös ilman valmiita sääntöjä siitä miten dataa tulee jaotella. Yksi näistä menetelmistä on klusterointi, joka Kantardzicin (2011) mukaan perustuu datan lajittelemiseen erilaisiin ryhmiin, eli klustereihin niin, että samantyyppinen data laitetaan yhteen klusteriin. Klustereista muodostuu koko käsiteltävää aineistoa kuvaava kuvaaja. Klusterit muodostetaan algoritmilla, jolla etsitään samankaltaisuuksia tai eroavaisuuksia käsiteltävän data-aineiston alkioiden attribuuttien välillä. Samoja ominaisuuksia sisältävä data sijoittuu lähelle muita vastaavia ominaisuuksia sisältävää dataa ja vastaavasti poikkeukset ja erovaisuudet asettuvat kauemmaksi muista klustereista muodostaen omat klusterinsa. (Han ym., 2012.) Haluttu tarkkuus vaikuttaa klusteroinnin tulokseen. Tarkemmat vaatimukset yhteneväisyydelle synnyttävät useampia klustereita ja vastaavasti löysemmät vaatimukset mahdollistavat suuremmat klusterit, kun etäisyys klusterin keskuksesta voi olla suurempi (Kantardzic, 2011). Tapoja mitata etäisyyttä voi olla useita, mutta usein se toteutetaan laskemalla klusterin keskipisteen paikka ja mittaamalla tutkittavan arvon etäisyys klusterin keskipisteeseen (Bramer, 2013).

Klusterointia voidaan tehdä useilla eri tavoilla. Usein käytettyjä klusterointimenetelmiä ovat k-Means -klusterointi ja agglomeroiva hierarkkinen klusterointi. K-Means -klusteroinnissa valitaan klustereiden määrä *k* ja määritellään *k*-määrä klustereiden keskipisteitä. Sen jälkeen kaikki käsiteltävät arvot sijoitetaan etäisyysmittauksen perusteella lähimpään klusteriin. Klusterointi suoritetaan iteroivasti. Jokaisella iteraatiokierroksella kaikkien klustereiden keskipisteet päivitetään laskemalla klusterin sisällä olevien alkioiden avulla niiden keskikohta uudelleen (ks. kuvio 3). Klusterointiprosessi loppuu viimeistelevässä

klusteroinnissa. Tällöin klustereiden keskipisteet eivät enää muutu, vaikka iterointia jatkettaisiin. (Han ym., 2012.)



KUVIO 3 Klustereiden muodostaminen k-Means -klusteroinnilla (Han ym., 2012)

Agglomeroiva hierarkkinen klusterointi perustuu yhteen suureen klusteriin, joka koostuu sen sisällä olevista pienemmistä klustereista. Prosessi lähtee tilanteesta, jossa kaikki datasetin alkiot ovat yksittäisiä klustereita. Klustereita aletaan yhdistää niin, että kaksi lähimpänä toisistaan olevaa klusteria yhdistetään. Prosessia toistetaan, kunnes jäljellä on yksi klusteri, joka pitää sisällään kaikki muut klusterit. (Bramer, 2013.)

Tiedonlouhintaa voidaan tehdä myös assosiaatiosääntöjen avulla. Wittenin ja Frankin (2005) mukaan assosiaatiosäännöt ovat hyvin samankaltaisia kuin luokittelumenetelmät poiketen kuitenkin siten, että assosiaatiosäännöt perustuvat todennäköisyyksiin ja niillä voi ennustaa pelkkien luokkien sijaan myös mitä tahansa luokkien attribuutteja. Assosiaatiomenetelmät perustuvat matemaattiseen perusolettamukseen: jos tapahtuu tapahtumat A ja B, tapahtuma C tapahtuu todennäköisyydellä p (Hand, Mattila & Smyth, 2001). Assosiaatiomenetelmiä selitetään usein ostoskorianalyysillä, jossa analysoidaan asiakkaiden ostokäyttäytymistä heidän valitsemiensa tuotteiden perusteella. Jos asiakas yleensä ostaa maidon kanssa leipää, voidaan näiden kahden tuotteen välille muodostaa assosiaatio, jota voidaan hyödyntää päätöksenteossa. (Han ym., 2012.)

Verkossa tapahtuvaa tiedonlouhintaa voidaan tehdä joko verkon sisältöä, käyttöä tai rakennetta louhimalla (Kantardzic, 2011). Kantardzicin (2011) mukaan sisällön louhinnan tarkoituksena on louhia verkkosivujen sisältöä, kuten sanoja, kuvia, videoita. Lastin (2007) mukaan yksi yleisimpiä sisällön louhintaan käytettyjä menetelmiä on vektorimalli (vector-space-model), jossa verkkosivustojen sisältö pilkotaan pieniksi palasiksi, esimerkiksi sanoiksi tai lauseiksi. Näitä pieniä paloja eli vektoreita, käytetään verkon louhinnassa avuksi, kun halutaan etsiä verkosta vektorien kanssa yhtäläistä materiaalia (Last, 2007).

Verkon käytön louhinnan tarkoituksena on kerätä informaatiota verkon käyttäjistä ja luoda riippuvuussuhteita käyttäjien ja verkkosivujen välille sekä kuvata käyttäjän mielenkiinnon kohteita. Louhinta voidaan toteuttaa louhimalla käyttäjän sivuhistoriaa ja verkkosivujen vierailutilastoja, joiden perusteella

luodaan malli käyttäjän verkkokäyttäytymisestä. (Last, 2007.) Mallin luomisessa voidaan hyödyntää monia tiedonlouhinnan menetelmiä: Luokittelusääntöjä hyödyntäen voidaan luokitella verkon käyttäjä johonkin ennalta määriteltyyn luokkaan, klusteroinnilla voidaan jaotella verkon käyttäjiä yhteisten käyttäytymispiirteiden mukaan ja assosiaatiosääntöjen avulla voidaan havaita, jos käyttäjä usein vierailee saman istunnon aikana samoilla sivuilla, vaikka ne eivät olisi toisiinsa linkittyviä. (Kantardzic, 2011.)

Verkon rakenteen louhinta perustuu verkkosivujen keskinäisten riippuvuussuhteiden käsittelyyn. Louhinta voidaan toteuttaa esimerkiksi linkkianalyysillä, jossa tarkastellaan verkkosivujen välisiä riippuvuussuhteita niiden keskinäisen linkittyvyyden perusteella. (Last, 2007.) Thuraisinghamin (2004) mukaan linkkianalyysi on menetelmänä lähellä assosiaatioon perustuvia menetelmiä. Linkkianalyysissä käytetään myös graafiteorian menetelmiä mallien löytämiseksi datasta. Tuloksena syntyviä graafeja voivat olla erilaiset solmut ja linkit, joita pitkin seuraamalla voidaan löytää yhteyksiä datan eri osien välillä. (Thuraisingham, 2004.) Menan (2004) mukaan linkkianalyysillä ja informaation eristämistyökaluilla voidaan luoda linkkejä strukturoimattomista webdokumenteista esimerkiksi yksilöiden, organisaatioiden ja paikkojen välille. Thuraisinghamin (2004) mukaan linkkianalyysi on paljon käytetty ja tehokas tiedonlouhinnan menetelmä tietoverkkojen rakenteen louhintaan, sillä esimerkiksi internetin hakukoneet, kuten Google käyttävät sitä tietoverkon rakenteen analysoimiseen ja hakutulosten etsimiseen.

4 TIEDONLOUHINTA KYBERTERRORISMIN TORJUNNASSA

Kahdessa ensimmäisessä luvussa tutkittiin kyberterrorismia ja tiedonlouhintaa omina aihealueinaan. Tässä luvussa tutkitaan tiedonlouhinnan käyttötapoja ja menetelmiä kyberterrorismin torjuntaan. Ensin käsitellään tiedonlouhinnan hyödyntämistä kriittisen infrastruktuurin suojaamisessa, jossa tiedonlouhinnan menetelmiä hyödynnetään tunkeutumisen havainnointijärjestelmissä. Sen jälkeen perehdytään tiedonlouhinnan käyttöön verkossa, jossa tiedonlouhinnan menetelmillä voidaan suorittaan yhteiskunnan turvallisuuteen liittyviä operaatioita. Luvun tavoitteena on saada lukijalle kokonaiskuva tiedonlouhinnan käyttömahdollisuuksista ja menetelmistä kyberterrorismin torjunnassa.

4.1 Kriittisen infrastruktuurin suojaaminen

Tiedonlouhintaa voidaan hyödyntää monipuolisesti kyberterrorismin torjuntaan. Tiedonlouhinnalla voidaan joko edistää yhteiskunnan turvallisuutta pyrkimällä etsimään verkosta kyberterroristeja ja kyberterrorismiin kykeneviä organisaatioita, tai sillä voidaan pyrkiä edistämään kyberturvallisuutta parantamalla tietojärjestelmien tietoturvaa (Thuraisingham ym., 2008). Tietojärjestelmiä suojatessa tiedonlouhinnan menetelmillä voidaan rajoittaa kyberterroristien pääsyä suojeltavaan tietoon tai dataan ja auttaa pitämään tiedot niille kuuluvilla henkilöillä. Tiedonlouhintaa voidaan käyttää myös havainnoimaan ja estämään kyberhyökkäyksiä. (Kumar ym., 2016.)

Kyberterroristien hyökkäyksen kohteeksi valikoituu yleensä valtion kriittinen infrastruktuuri tai muu vastaava kohde (Al Mazari ym., 2016). Kumar ym. (2016) myös toteavat, että suurin osa kyberterrorismiksi luokiteltavista iskuista on tapahtunut tietojärjestelmiin tunkeutumalla. Rokachin ja Elovicin (2007) mukaan kriittisen infrastruktuurin toimintaa ohjataan ohjausjärjestelmillä, joten ne vaativat erityistä suojelua uhkia vastaan. Yksi tällainen suojakeino on tunkeutumisen havaitsemisjärjestelmä, eli Intrusion Detection System (IDS).

Rowlandin (2002) mukaan IDS on reaaliaikainen tunkeutumisen havainnointiin tarkoitettu järjestelmä, joka valvoo dataliikennettä. Valvonnan kohteena järjestelmällä voi olla tietokone, useat tietokoneet samassa verkossa tai verkko itse. Valvontaympäristössä tapahtuvan dataliikenteen perusteella IDS tekee päätöksiä siitä, mikä on normaalia ja mikä on mahdollisesti vaarallista ja ei haluttua dataliikennettä. Tarvittaessa IDS estää haitallisen liikenteen kulun ja varoittaa järjestelmän ylläpitäjää. (Rowland, 2002.) Ektefann Memarin, Sidin ja Affendeyn (2010) mukaan toimintatapoja tunkeutumisen havainnointiin IDS:ssä on kaksi: väärinkäytön havainnointi ja anomalioiden havainnointi. Horngin ym. (2011) mukaan väärinkäytön havainnoinnissa järjestelmän tapahtumia vertaillaan ennalta tunnettuihin hyökkäyksien ja väärinkäytöksien tunnusmerkkeihin. Jos järjestelmän tapahtuma vastaa jotain ennalta tunnettua tunkeutumismallia, aiheuttaa se hälytyksen. Anomalioiden havainnointi IDS:ssä perustuu erilaisiin profiileihin. Normaaleista tapahtumista luodaan profiilit, joissa määritellään niiden tunnusomaiset piirteet. Jos IDS huomaa, että valvottava tapahtuma poikkeaa liikaa normaaleista profiileista, hälyttää järjestelmä tunkeutumisesta. (Horng ym., 2011.) Näin ollen IDS voi havainnoida tunkeutumisen kahdella tavalla: joko entuudestaan tunnetun hyökkäysmallin perusteella tai poikkeavan toiminnan perusteella.

IDS ei ole toiminnassaan täysin aukoton, joten sen tehostamiseksi voidaan käyttää eri tiedonlouhinnan menetelmiä. Rockahin ja Elovicin (2007) mukaan tiedonlouhinnalla on neljä merkitystä IDS:ssä:

1. Variantit: Jos haittaohjelma naamioidaan näyttämään joltain toiselta ohjelmalta siten, että se täyttää IDS:n luotettavan mallin kriteerit, voidaan tiedonlouhinnalla havaita epäilyttävä toiminta etsimällä haittaohjelmasta anomalioita.
2. False Positive -ongelma: IDS tuottaa paljon turhia hälytyksiä tilanteissa, joissa todellista uhkaa ei ole. Tiedonlouhinnan avulla voidaan vähentää näiden hälytysten määrää analysoimalla vääriä hälytyksiä aiheuttavia tilanteita.
3. False Negative -ongelma: Tilanteessa, jossa IDS ei havaitsekaan hyökkäystä, voidaan tiedonlouhinnan avulla tutkia, poikkeaako toiminta liikaa normaalista toiminnasta, jolloin tapahtumasta aiheutuu hälytys.
4. Datan ylikuormittuminen: IDS:n tuottamat toimintolokit voivat kasvaa erittäin suuriksi. Tiedonlouhinnalla voidaan tutkia lokeja ja tuottaa hyödyllistä informaatiota järjestelmän toiminnasta ja kehittää IDS:n havainnointitarkkuutta.

Tiedonlouhinnan menetelmillä voidaan siis tehostaa IDS:n toimintaa. Menetelmillä parannetaan IDS:n havainnointitarkkuutta ja vähennetään käytön aikana syntyvien virheiden määrää. Käytössä olevia tiedonlouhinnan menetelmiä ovat luokittelu-, klusterointi-, assosiaatio-, korrelaatio- ja fuusiomenetelmät. (Rokach & Elovici, 2007.)

Luokitteluun perustuvilla menetelmillä voidaan ratkaista suurin osa tunkeutumisen havainnointiin liittyvistä haasteista. IDS:ssä luokitteluun perustuvat menetelmät pyrkivät löytämään riippuvuuden syötettävien attribuuttien ja kohdeattribuuttien välillä. Riippuvuussuhteesta luodaan luokittelumalli. Luokittelumalleilla voidaan attribuutteihin perustuen luokitella erilaisia tapahtumia, kuten normaalitila, troijalaishyökkäys tai muu haitallinen tapahtuma. Lisäksi luokittelumenetelmien opein voidaan luoda oppiva malli, joka pystyy itsenäisesti luokittelemaan tapauksia, joita ei ole aikaisemmin tavattu. Mallille opetetaan säännöt, joiden perusteella datan attribuutteihin saa tehdä muutoksia. Jos pyynnöt attribuuttien muuttamiseen eivät täsmää mallille opetettuja sääntöjä, järjestelmä pystyy itsenäisesti luokittelemaan attribuutin muuntamisen vaaralliseksi ja varoittaa järjestelmää ja sen käyttäjää. (Rokach & Elovici, 2007.)

Klusterointia voidaan käyttää IDS:ssä anomalioiden havainnointiin vertaamalla tutkittavaa objektia tunnettuihin klustereihin (Elovici ym., 2004). Olettaen, että normaali toiminta on paljon yleisempää kuin järjestelmälle haitallinen toiminta, syntyy normaalista toiminnasta paljon suurempia klustereita kuin haitallisesta toiminnasta. Tällöin kun uusia tapahtumia analysoidaan, mitataan mitä klusteria lähimpänä ne ovat. Jos tapahtuma asettuu liian lähelle tunkeutumiseen viittavia klustereita tai liian kauas normaalin toiminnan klustereista, aiheuttaa tapahtuma hälytyksen järjestelmässä. (Portnoy, Eskin & Stolfo, 2001.)

Assosisaatiomenetelmiä voidaan hyödyntää IDS:n päätöksenteon kehittämiseksi. Niillä voidaan parantaa luokittelussa syntyvien luokittelumallien tarkkuutta esimerkiksi järjestelmän verkkoyhteyksiä tutkimalla. Verkkoyhteydet esikäsitellään ja niistä tehdään luettelo, joka sisältää verkkoyhteyksien perustiedot. Sen jälkeen verkkoyhteydet jaotellaan luokittelumenetelmällä normaaleihin ja tunkeutumisen tunnusmerkit täyttäviin ryhmiin. Tämän jälkeen algoritmi käsittelee verkkoyhteyksien tietoja. (Rokach & Elovici, 2007.) Algoritmi pyrkii etsimään kaikki mahdolliset usein toistuvat assosiaatiot käsiteltävästä datasta ja jaottelee ne löytyneiden assosiaatioiden mukaan (Zhang, Zulkernine, & Haque 2008). Jos normaalien yhteyksien ryhmästä löytyy samoja assosiaatioita kuin tunkeutumiseksi luokiteltujen yhteyksien ryhmästä, poistetaan havainnot haitallisen tunkeutumisen ryhmästä. Loput haitallisen ryhmän mallit identifioidaan. Tämän jälkeen luokittelumalli osaa identifioida paremmin haitalliset verkkoyhteydet, eikä turhia hälytyksiä synny niin paljon. (Rokach & Elovici, 2007.)

IDS keskittyy usein matalan tason, yksinkertaisiin hyökkäyksiin tai anomalioihin, joista syntyy yksittäisiä hälytyksiä. Tilanteessa, jossa IDS huomaa intensiivisen tunkeutumisen, syntyy usein paljon hälytyksiä. Hälytyksistä osalla voi olla yhteyttä toisiinsa osana isompaa hyökkäystä, kun taas jotkin hälytykset ovat täysin aiheettomia. Hälytysten määrä kasvaa usein hallitsemattoman suureksi ja tätä varten on kehitetty erilaisia korrelaatiomenetelmiä, joilla voidaan todentaa isompia hyökkäyksiä. (Rokach & Elovici, 2007.) Korrelaatiomenetelmiä voidaan jakaa kolmeen tyyppiin. Ensimmäinen tyyppi korreloi hälytyksiä niiden aiheuttamien samanlaisten attribuuttien perusteella. Toinen tyyppi korreloi hälytyksiä samanlaisten hyökkäyskenaarioiden mukaan, joita ihminen on

luokitellut, tai IDS on itse oppinut sille syötetyistä harjoitteludataseteistä. Kolmas tyyppi korreloi hyökkäyksiä niiden alku- ja lopputilanteiden perusteella. Jos jonkun myöhemmän hälytyksen alkutilanne vastaa aikaisemmasta hälytyksestä syntynyttä lopputilannetta, voidaan olettaa, että niiden välillä on jotain yhteyttä toisiinsa. Tällöin IDS osaa luokitella hälytykset osaksi isompaa ongelmaa. (Rokach & Elovici, 2007.)

IDS:t voivat käyttää useaa tiedonlouhinnan menetelmää yhdessä, jolloin se kykenee havaitsemaan ja oppimaan tunkeutumisia paremmin. Eri menetelmät sisältävät eri sääntöjä anomalioiden tunnistamiseen, jotka yhdessä parantavat tunnistustarkkuutta. Lisäksi järjestelmään on hankalampi tunkeutua IDS:n huomaamatta, jos se käyttää useita eri menetelmiä, sillä yhden menetelmän ohittaminen ilman hälytystä on luonnollisesti helpompaa kuin monia eri menetelmiä käyttävä IDS. Yksi tyypillinen IDS on ADAM (Audit Data and Mining), joka hyödyntää anomalioiden havainnointia ja luokittelusääntöjä. Se osaa muun muassa assosiaatiosääntöjen perusteella luoda todennäköisyyksiä tulevien yhteyksien tarkoituksesta ja oppii tunnistamaan tuntemattomia tapahtumia aiempien tapahtumien perusteella. (Rokach & Elovici, 2007.)

4.2 Verkon louhinta

Pelkkä kriittisen infrastruktuurin suojaaminen ei riitä kyberterrorismilta suojautumiseen. Kyberterrorismin toiminta ei rajoitu vain kyberhyökkäysten tekemiseen, vaan siihen liittyy oleellisesti toimiminen verkossa esimerkiksi propagandaa levittämällä tai rahoitusta hankkimalla (Al Mazari ym., 2016). Terroristien lisääntyneen verkon käytön vuoksi internetistä on tullut hyödyllinen informaation lähde terroristien löytämiseksi ja heidän aikeidensa selvittämiseksi (Last, 2005). Terroristisen verkkosivujen määrä on kuitenkin nykyisin niin suuri, että niitä ei enää manuaalisesti pystytä analysoimaan. Toisaalta turvallisuusviranomaisia kuitenkin kiinnostaa ketkä ovat verkkosivujen takana, ketkä ovat verkkosivujen kohdeyleisöä ja millaisia yhteyksiä heillä on terroristijärjestöihin (Last, 2007). Verkkoa louhimalla voidaan kyberterrorismin uhkaan vaikuttaa ennaltaehkäisevästi etsimällä sieltä kyberterrorismiin viittaavaa informaatiota (Last, 2005).

Verkosta, jolla tässä tutkielmassa viitataan englanninkieliseen tietoverkkoja kuvaavaan sanaan web, voidaan etsiä viitteitä kyberterrorismiin joko reaaliaikaisesti kerättävää dataa louhimalla, tai jo olemassa olevan datan perusteella. Reaaliaikaisessa tiedonlouhinnassa pyritään löytämään sellaista tietoa, jonka olemassaolosta ei vielä edes tiedetä. Reaaliaikaisen louhinnan haasteena on louhintaprosessiin kuluva aika, jonka vuoksi tiedonlouhintaa käytetään yleensä jo aikaisemmin kerätyn ja tuotetun datan käsittelyyn. Lisäksi reaaliaikaisen tiedonlouhinnan perustaksi tarvitaan simuloitua ja hypoteettista dataa, jotta voidaan reaaliaikaisesti etsiä sellaisia malleja, jotka saattavat olla kiinnostavia. (Thuraisingham, 2004.) Verkon nopeasti muuttuva sisältö vaikeuttaa sen lou-

hintaa. Sen vuoksi verkon reaaliaikaiseen louhintaan on kehitetty siihen paremmin toimivia menetelmiä, kuten inkrementaalisti oppivat algoritmit, erittäin nopeaksi optimoidut päätöspuut ja dynaamisesti muokkautuvat luokittelumenetelmät, jotka kykenevät hallitsemaan reaaliaikaisesti koko ajan muuttuvia ja jatkuvia datavirtoja. (Last, 2005.)

Kyberterrorismin havainnointiin on jo kehitetty useita verkon louhintaa hyödyntäviä järjestelmiä. Järjestelmien tehtävänä on louhitun tiedon perusteella antaa järjestelmän käyttäjälle ennakkovaroituksia ja siten aikaa reagoida tilanteeseen. (Best, 2010.) Järjestelmien käyttötarkoitus riippuu siitä, miten verkkoa halutaan louhia. Kantardzic (2011) jakaa verkon louhimisen kolmeen kategoriaan: verkon sisällön louhinta, verkon käytön louhinta ja verkon rakenteen louhinta. Kyberterrorismin torjunnassa eri verkon louhintamenetelmiä käytetään usein yhdessä, mutta niitä voidaan silti jaotella pääpiirteittäin eri tyyppeihin.

4.2.1 Sisällön louhinta

Verkon sisällön louhinta pyrkii löytämään verkon sisällöstä sellaista informaatiota, joka voi olla hyödyllistä kyberterroristien löytämiseksi ja kyberterrorismin ennaltaehkäisemiseksi. Wadhwan ja Bhatian (2013) mukaan verkosta voidaan etsiä kyberterrorismiin liittyvää materiaalia esimerkiksi sosiaalisen median aihetunnisteiden (hashtag) avulla. Kun aihetunnisteiden perusteella löytynyttä materiaalia käsitellään lisää esimerkiksi klusteroimalla, voidaan tuloksista erotella epäolennainen sisältö kuten uutiset ja muu tutkimuksen kannalta epäolennainen sisältö. Tällöin jäljelle jäävät viranomaisia kiinnostavat tulokset, joiden perusteella terroristeja voidaan paikantaa. (Wadhwa & Bhatia, 2013.)

Verkon sisältö muuttuu koko ajan ja nopeasti. Nopean muuttumistahdin vuoksi on kehitetty verkon sisällön louhintaan erikoistuneita työkaluja, joista yksi on älykäs informaatioagentti (intelligent software agent). (Last, 2007.) Älykäs informaatioagentti on itsenäinen ohjelma, joka on ohjelmoitu jäljittelemään ihmisten toimia verkossa. Niitä käytetään erityisesti filtteröimään ja organisoimaan hajanaista dataa, kuten suuria määriä strukturoimattomia web-dokumentteja. Älykkäiden informaatioagenttien toiminta perustuu hakukoneiden suurten indeksilistauksien läpikäymiseen vektorimallien avulla. Agentti lähettää saman pyynnön usealle eri hakukoneelle ja valikoi automaattisesti relevantit linkit analysoimalla niiden sisältöä. Agentti seuraa löytyneistä linkeistä parhaiten sopivia yhä pidemmälle ja jatkaa sisällön analysointiprosessiaan. Linkkejä seuraamalla pyritään löytämään vektorimallien mukaisia terrorismiin viittaavia sivuja ja jälkiä, joita muuten olisi vaikea löytää. Agentti lopettaa prosessin kun resurssit tai etsittävät sivut loppuvat, tai kun informaatioagentille asetetut tavoitteet saavutetaan. (Last, 2005.)

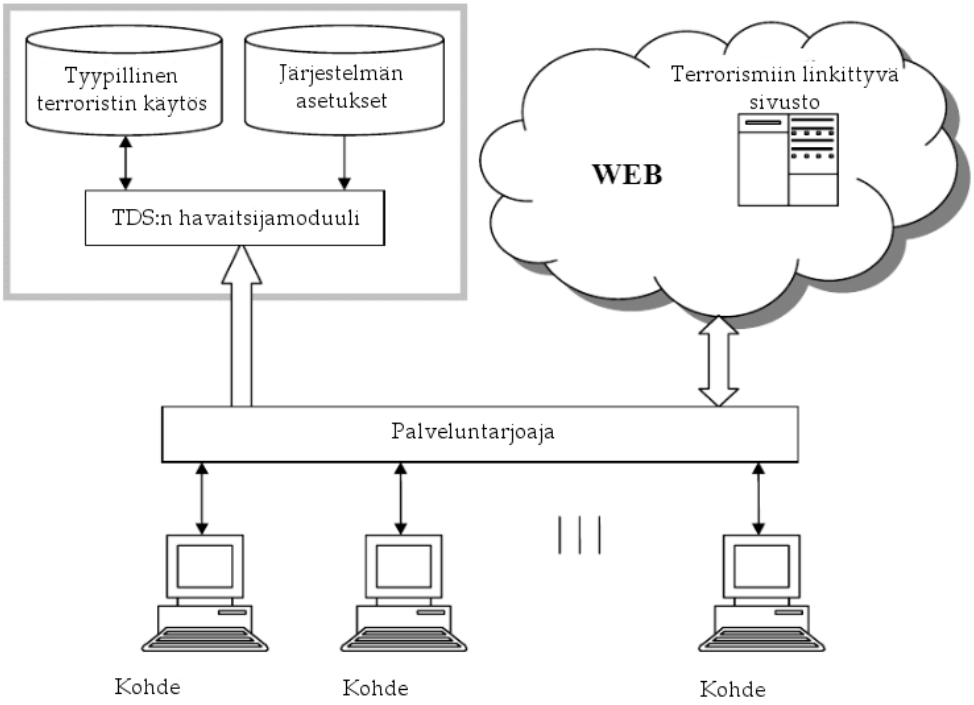
Verkon pitkäaikaiseen valvontaan tarvitaan työkaluja, jotka pystyvät huomioimaan verkon sisällössä tapahtuvia trendimuutoksia (Last, 2005). Älykkäitä informaatioagentteja voidaan verkon sisällön louhinnassa käyttää myös tähän tarkoitukseen. Mendez-Torreblanca, Montes y Gomez ja Lopez-Lopez (2002) ovat kehittäneet menetelmän, jossa informaatioagentti vertailee eri aika-

leimalla olevia versioita samoista sivustoista. Informaatioagentti pyrkii etsimään tutkittavista sivustoista eri aikaväleillä tapahtuvia trendimuutoksia ennalta määriteltyjen sanojen toistuvuuden muutoksia tarkkailemalla (Mendez-Torreblanca ym., 2002). Trendien havainnointi on kuitenkin hankalaa, sillä trendin määrittely on pitkälti subjektiivinen asia. Ihminen on usein paljon tehokkaampi määrittelemään trendimuutoksia kuin tilastojen ja matemaattisten algoritmien varassa oleva tietokone. Ihmisillä on kyky kontekstisidonnaiseen ajatteluun ja kyky ymmärtää kielellisiä merkityksiä, joita algoritmi ei välttämättä osaa ottaa huomioon. (Last, 2005.) Last (2005) korostaa kuitenkin sitä, että pitkäaikaisessa valvonnassa informaatioagenteilla voidaan tehokkaasti huomata tärkeitä muutoksia valvottavien sivustojen sisällössä.

4.2.2 Käytön louhinta

Kyberterroristeja voidaan etsiä verkosta myös verkkoliikennettä louhimalla. Verkon käytön louhinnalla voidaan kerätä informaatiota verkon käyttäjistä ja luoda riippuvuussuhteita käyttäjien ja vierailtujen verkkosivujen välille (Last, 2007). Reaaliaikainen valvonta mahdollistaa terroristien tunnistamisen ja heidän toimiensa ennaltaehkäisyn (Elovici, 2005).

Terrorist Detection System, eli TDS, on anomalioiden havainnointiin perustuva tiedonlouhintajärjestelmä, joilla pyritään etsimään terroristeja seuraamalla heidän verkkoliikennettään. (Elovici, 2005.) TDS:n hyödyntää toiminnassaan sisältöpohjaisen havainnoinnin teoriaa, joka perustuu harjoittelu- ja havaitsemismoodiin (Last ym., 2003). Harjoittelumoodissa järjestelmälle syötetään verkkosivuja, joissa on terrorismiin liittyvää sisältöä. Verkkosivujen tekstisisällön perusteella suoritetaan klusteroimalla analyysi, jonka tuloksena saadaan tyypillinen terroristin käyttäytymistä ja kiinnostuksen kohteita kuvaava vektorimalli. Havainnointimoodissa TDS havainnoi reaaliaikaisesti verkkoliikennettä ja analysoi tutkittavan henkilön vierailemien sivujen sisältöä (ks. kuvio 4). Jos sisällön perusteella tehtävä vektorimalli on toistuvasti tarpeeksi lähellä harjoittelumoodissa luotua vektorimallia, syntyy siitä hälytys järjestelmässä. Tällöin tutkittava henkilö voidaan tarvittaessa koittaa paikantaa henkilökohtaisen IP:n perusteella. (Elovici, 2005.) Paikantaminen ei kuitenkaan nykyisin enää ole täysin yksinkertaista ja helppoa. Terroristit ovat ottaneet käyttöönsä VPN-yhteydet (Virtual Private Network), jotka kierrättävät käyttäjän verkkoliikenteen usean palvelimen kautta, jolloin käyttäjän jäljittäminen on hyvin hankalaa (Kahn & Kellner, 2004). Ongelma voidaan kiertää liittämällä järjestelmä suoraan palveluntarjoajan infrastruktuuriin, jolloin palveluntarjoaja voi tarvittaessa antaa käyttäjän tarkan IP-osoitteen (Elovici, 2005).



KUVIO 4 TDS-järjestelmän toiminta (Elovici ym., 2004)

Thuraisingham ym. (2008) ovat kehittäneet bottiverkkojen havainnointiin käytettävän tiedonlouhintajärjestelmän. Bottiverkkojen havainnointi on tärkeää, sillä bottiverkkoja voidaan käyttää monien eri kyberrikosten, kuten palvelunestohyökkäysten tekemiseen. Kyberterroristeille palvelunestohyökkäys on hyvä ja tehokas tapa toteuttaa iskuja, sillä pahimmillaan se voi aiheuttaa miljoonien dollarien vahingot (Jalil 2003). Bottiverkkojen havainnointi perustuu bottiverkon jatkuvan sisäisen viestinnän havainnointiin kaapattujen tietokoneiden ja niitä hallitsevan botmasterin välillä. Havainnoinnissa hyödynnetään klusterointia, luokittelua ja anomalioiden havainnointia (Thuraisingham ym., 2008.)

4.2.3 Rakenteen louhinta

Vuonna 2010 verkossa arvioitiin olevan yli 100 000 terroristista verkkosivustoa, joista suurin osa syvässä verkossa, eli dark webissä. Verkon syvemmät osat ovat otollisia kyberterroristeille, sillä niitä on vaikeampi valvoa ja niistä on vaikeampaa löytää yksittäisiä käyttäjiä. Syvä verkko ei näy tavanomaisten hakukoneiden indeksilistauksissa, joten sen louhinta on vaikeampaa. Syvän verkon louhintaan täytyy käyttää erikoistuneita louhintamenetelmiä, jotka kykenevät löytämään piilossa olevan sisällön. Louhintaan voidaan käyttää muun muassa linkkianalyysiä terroristisen sisällön linkittämiseen, sisällön louhintaa terrorismiin liittyvän datan löytämiseen ja klusterointia datan sekä verkkosivujen jaottelemiseen. (Chen, 2012.) Chenin (2012) mukaan terrorismi on siirtymässä syvään verkkoon yhä enemmän ja sen vuoksi syvän verkon louhinnan merkitys kasvaa tulevaisuudessa.

Rakenteen louhinnassa etenkin linkkianalyysi on osoittautunut yksinkertaiseksi ja tehokkaaksi välineeksi kyberterrorismin torjunnassa. Julkisista tietokannoista tai muista suurista datakeskittymistä voidaan helposti etsiä linkkejä etsittävien asioiden välillä. Louhinnalla voidaan löytää esimerkiksi epäilty, katuosoite tai muuta tutkimuksen kannalta tärkeää tietoa. Löytyneistä tiedoista voidaan linkkejä seuraamalla löytää muita ihmisiä, paikkoja tai asioita, jotka voivat olla tutkimuksen kannalta tärkeitä. (DeRosa, 2004.) Esimerkkinä linkkianalyysin tehokkuudesta DeRosa (2004) käyttää syyskuun 11. päivän terroriiskuja vuodelta 2001. Yhdysvaltain epäiltyjen terroristien seurantalistan, lentolippujen varaustilastojen ja julkisen tallennetun datan avulla tehty linkkianalyysi olisi tunnistanut ja linkittänyt toisiinsa kaikki iskuun osallistuneet 19 terroristia muun muassa yhteisten katuosoitteiden ja lentojen varaustietojen kautta.

4.3 Haasteet

Tiedonlouhintaan ja sen käyttöön kyberterrorismin torjunnassa liittyy vielä useita ratkaisemattomia haasteita. Yangin ja Wun (2006) mukaan useat tiedonlouhinnan haasteet liittyvät skaalautuvuuteen datamäärien kasvaessa nopeaa vauhtia. Kasvun kiihtyessä myös datan muodot muuttuvat entistä kompleksisemmaksi. Tiedonlouhinnan avulla olisi kyettävä entistä nopeammin ja tehokkaammin muodostamaan monipuolisempaa informaatiota entistä kompleksisemmista data-aineistoista. (Yang & Wu, 2006.)

Datan määrä tai monimutkaisuus ei kuitenkaan ole ainoa ongelma. Yksi suurista haasteista liittyy tiedonlouhinnan käyttäjään, eli ihmiseen. Abbas, Mustafa ja Ibrahim (2015) toteavat, että tiedonlouhintaprosessissa syntyvän informaation arvottaminen ja ymmärtäminen jää aina ihmisen tehtäväksi, vaikka tiedonlouhinta pystyykin löytämään data-aineistoista selkeitä yhteyksiä ja malleja. Ihmisen päätöksenteko ei aina ole täysin rationaalista, sillä päätöksentekoon voi vaikuttaa monia muita tekijöitä kuin pelkkä tiedonlouhinnan tulos. Terrorismin vastaisessa työssä ei ole varaa virhearviointeihin, joten ihmisen päätöksenteon merkitys on suuri kyberterrorismin vastaisessa toiminnassa. Toinen haaste Abbasin ym. (2015) mukaan on tulosten oikeellisuuteen liittyvät ongelmat, sillä tiedonlouhintaprosessin tulokset eivät välttämättä muodosta kausaliteettia reaalitodellisuudessa. Kolmantena yleisenä haasteena tiedonlouhinnassa nähdään käytettävissä olevan datan tyyppiin, laatuun ja yhtenäisyyteen liittyvät ongelmat (Abbas ym., 2015; Thuraisingham, 2004). Data-aineisto saattaa koostua monista alun perin eri käyttötarkoituksiin tarkoitetusta datasta, jolloin erityyppisten datojen käyttö yhdessä saattaa aiheuttaa vääristymiä. Data-aineiston laatu voi olla heikko, jos siitä puuttuu osia tai se ei ole tarpeeksi tarkkaa. (Abbas ym. 2015.) Lisäksi osittainen informaatio, eli esimerkiksi louhittavan datan eri osien jakautuminen eri turvallisuusviranomaisten välille, saattaa aiheuttaa vääristyneitä tuloksia ja vaikeuttaa johtopäätösten tekemistä (Thuraisingham, 2004).

Tunkeutumisen havainnointijärjestelmiin liittyvät haasteet liittyvät suurilta osin järjestelmien luotettavuuteen. IDS:t ovat kustannuksiltaan kalliita, mutta niiden havainnointitarkkuus ja suoritusteho eivät ole kehittyneet erityisen hyviksi. Järjestelmillä on vaikeuksia käsitellä suuria ja nopeita datavirtoja ja tunnistaa salauksella suojattua dataa. Lisäksi IDS:t aiheuttavat edelleen paljon vääriä hälytyksiä ja oikean hyökkäyksen tapahtuessa niiden kyky estää hyökkäys on monesti puutteellinen. (Garcia-Teodoro, Diaz-Verdejo, Maciá-Fernández & Vázquez, 2009.)

Verkon louhinnan kohdalla haasteet ovat hyvin erilaisia riippuen tutkittavasta verkon louhinnan osa-alueesta. Syynä erilaisiin haasteisiin on osa-alueiden toisistaan poikkeavat toimintatavat ja tavoitteet. Yksilöllisten haasteiden lisäksi myös tiedonlouhinnan yleiset haasteet vaikuttavat verkon louhintaan. Verkon louhinnan pääpiirteet ja haasteet on esitelty kootusti taulukossa (ks. taulukko 1).

Turvallisuusviranomaisten näkökulmasta sisällön louhinnan suurimmat haasteet liittyvät verkon muutosnopeuteen, joka mahdollistaa kyberterroristien piiloutumisen. Terroristit voivat julkaista informaatiota internetissä milloin vain, missä muodossa tahansa ja millä kielellä tahansa sekä poistaa tiedot yhtä nopeasti kuin julkaisivat ne (Last, 2007). Tarkan ja ajankohtaisen sisällön louhinnan tekeminen on näin ollen erittäin hankalaa.

Verkon käytön louhinnan suurimmat haasteet ovat yksityisyydensuojaan liittyvät lainsäädännölliset ongelmat. Soloven (2008) mukaan suuret tiedonlouhintaoperaatiot eivät vain loukkaa ihmisten yksityisyyttä, vaan samalla vievät yksilöltä mahdollisuuden tietää varmuudella kuinka omia henkilötietoja käsitellään. Vasta-argumenttina ongelmaan esitetään usein kansallinen turvallisuus, joka on myös Suomessa herättänyt keskustelua. Muun muassa puolustusvoimien tiedustelulaitoksen apulaisjohtaja Martti J. Karin mukaan Suomen uusi valmisteilla oleva tiedustelulainsäädäntö uhkaa jäädä riittämättömäksi, jos terrorismin uhka ei ole riittävä peruste verkkotiedustelun kohdentamiseen (Suihkonen, 2015).

Rakenteen louhinnan haasteet ovat louhintaprosessin aikana tai sen tuloksista syntyviä päätöksentekoon liittyviä haasteita. Thuraisingham (2004) mukaan esimerkiksi linkkianalyysi muodostaa tiedonlouhintaprosessissa erittäin suuren määrän linkkejä, joista relevanttien linkkien valitseminen automaattisesti on vielä haasteellista. Lisäksi Thuraisingham (2004) huomauttaa osittaisen informaation aiheuttamista ongelmista, joissa eri viranomaiset käsittelevät eri osia käsiteltävästä datasta. Osittainen informaatio voi aiheuttaa hyvin erilaisia tuloksia ja hankaloittaa päätöksentekoa, koska tulosten yhdistely voi olla vaikeaa (Thuraisingham, 2004). Rakenteen louhinnassa haasteita tuottaa myös se, miten materiaaliin päästään käsiksi. Syvä verkko tarjoaa tehokaan suojan kyberterroristeille, sillä syvä verkko on erittäin laaja ja sen louhiminen nykyisillä menetelmillä on vielä melko hankalaa ja hidasta. Samalla kuitenkin suurin osa kyberterroristisesta materiaalista on jo syvässä verkossa. (Chen, 2012). Näin ollen syvän verkon louhinta vaatii vielä parempia menetelmiä ja lisää valvontaa, jotta kyberterrorismia voidaan tehokkaasti verkosta etsiä.

TAULUKKO 1 Verkon louhinnan käyttö ja haasteet

Osa-alue	**Tarkoitus**	**Sovellusesimerkki**	**Haasteet**
Sisällön louhinta	Kyberterrorismiin viittaavan sisällön ja niihin liittyvien henkilöiden etsintä, trendien havainnointi	Älykkäät informaatioagentit	Verkossa koko ajan tapahtuvat sisältömuutokset
Käytön louhinta	Kyberterroristien etsintä epäiltyjen verkkoliikennettä valvomalla	TDS – Terrorist Detection System	Rajoittava lainsäädäntö ja yksityisyydensuoja
Rakenteen louhinta	Kyberterroristien ja kyberterrorismiin liittyvän materiaalin linkittäminen verkosta löytyvän materiaalin perusteella	Linkkianalyysi	Relevanttien yhteyksien löytäminen lukuisista assosiaatioista, kyberterrorismin piiloutuminen syvään verkkoon

Kyberterrorismin torjunnassa haasteita tiedonlouhille aiheuttavat niin yleiset tiedonlouhinnan haasteet kuin myös kyberterrorismin aiheuttamat haasteet. Thuraisinghamin (2004) mukaan tiedonlouhinnan menetelmät vaativat vielä runsaasti kehittämistä, jotta ne olisivat tarpeeksi luotettavia havaitsemaan ja estämään kyberterrorismia tehokkaasti. Tulevaisuudennäkymiä tarkastellessa voidaan tiedonlouhinnan merkityksen kuitenkin nähdä korostuvan. Kyberterrorismin torjunnassa tärkeää on havaita ja estää iskut. Siihen tehtävään tiedonlouhinta ja verkon louhinta tarjoavat ratkaisuja ja työkaluja. Kehitykseen tarvitaan kuitenkin maailmanlaajuista rajat ylittävää yhteistyötä, sillä terrorismi ei tunne valtionrajoja. (Thuraisingham, 2004.)

5 YHTEENVETO JA POHDINTA

Tässä tutkielmassa tutkittiin tiedonlouhinnan käyttöä kyberterrorismin torjuntakeinona. Tutkielma toteutettiin kirjallisuuskatsauksena perustuen alan tieteellisiin julkaisuihin. Tutkielman aihepiiriä lähestyttiin määrittelemällä kyberterrorismin käsite ja tutkimalla kyberterrorismin viitekehystä. Sen jälkeen määriteltiin tiedonlouhinnan käsite ja tutkittiin tiedonlouhinnan prosessia ja muutamia käytössä olevia menetelmiä. Tutkielman varsinainen tutkimuskysymys oli: miten tiedonlouhintaa voidaan hyödyntää kyberterrorismin torjunnassa? Tutkimusongelmaa lähestyttiin tutkimalla kyberterrorismin torjuntaan käytettyjä tiedonlouhinnan menetelmiä ja sovelluksia, sekä pyrittiin löytämään haasteita, joita kyberterrorismi aiheuttaa tiedonlouhinnassa.

Tutkielman lähdekirjallisuuden perusteella tutkimuksen tulokseksi voidaan todeta, että kyberterrorismin torjunnassa tiedonlouhintaa voidaan hyödyntää joko valtion kriittisen infrastruktuurin suojaamiseen tai verkon louhintaan. Tiedonlouhinnalla voidaan parantaa kriittisen infrastruktuurin suojaksi tarkoitettujen tunkeutumisen havainnointijärjestelmien havainnointitarkkuutta. Tunkeutumisen havainnoimisjärjestelmissä tiedonlouhinnan menetelmillä voidaan huomata poikkeavia tapahtumia eli anomalioita. Lisäksi eri menetelmillä voidaan vähentää väärien hälytysten määrää ja vastaavasti hälyttää silloin kuin järjestelmä ei ilman tiedonlouhintaa huomaa tunkeutumista. Tiedonlouhinnan avulla järjestelmän havainnointitarkkuutta voidaan kehittää paremmaksi myös tutkimalla kertyneitä toimintolokeja. (Rokach & Elovici, 2007.)

Tutkielman lähdekirjallisuus osoittaa, että tiedonlouhintaa voidaan käyttää kyberterrorismin torjuntaan louhimalla verkkoa. Verkon louhinnan avulla verkosta voidaan löytää kyberterroristeja, heidän toiminnastaan kiinnostuneita henkilöitä ja kyberterroristista materiaalia sekä muodostaa riippuvuussuhteita löytyneiden tulosten välille (Last, 2005). Verkon louhinta jakaantuu kolmeen osaan: sisällön, käytön ja rakenteen louhintaan (Kantardzic, 2011). Niillä kaikilla on hieman toisistaan eroavat tavoitteet ja toimintatavat, mutta usein niitä käytetään yhdessä. Sisällön louhinnassa esimerkiksi vektorimallilla voidaan etsiä verkosta kyberterroristista materiaalia ja selvittää materiaalin perusteella ketkä ovat materiaalin takana. Sisällön louhinnalla voidaan myös selvittää terroristien

aikeita ja pyrkiä ennaltaehkäisemään niitä. (Last, 2007.) Käytön louhinta on verkkoliikenteen seurantaa, jossa pyritään löytämään terroristeja seuraamalla verkon käyttäjien verkkoliikennettä ja tutkimalla käyttäjien verkkokäyttäytymistä (Last, 2007). Verkon rakenteen louhinta pyrkii luomaan riippuvuussuhteita tutkittavien asioiden välille tutkimalla verkosta löytyvän materiaalin välisiä riippuvuussuhteita (Last, 2007). Riippuvuussuhteita voivat olla esimerkiksi yhteydet paikkojen, henkilöiden ja tapahtumien välillä. Muun muassa linkkianalyysillä voidaan verkosta löytyvän datan perusteella etsiä terroriverkostoja ja terrori-iskujen tekijöitä. (DeRosa, 2004.) Viime aikoina rakenteen louhinnan kehitys on suuntautunut yhä enemmän syvän verkon louhintaan, sillä kyberterrorismi on siirtymässä syvään verkkoon parempien suojausten taakse (Chen, 2012).

Täysin ongelmatonta tiedonlouhinnan käyttö kyberterrorismin torjunnassa ei ole, sillä useat haasteet vaikeuttavat tiedonlouhinnan tehokasta hyödyntämistä. Osa haasteista on kaikkea tiedonlouhintaa yleisesti koskevia. Rajallinen laskentateho yhdistettynä nopeaan datamäärien ja datan kompleksisuuden kasvuun tuottaa skaalautumiseen liittyviä ongelmia (Yang & Wu, 2006). Tulevaisuudessa täytyy kehittää entistä tehokkaampia ja monipuolisempia tiedonlouhinnan menetelmiä, jotka pystyvät hallitsemaan suurempia datamääriä entistä nopeammin, joissain tapauksissa jopa reaaliaikaisesti (Thuraisingham, 2004). Tiedonlouhinnan haasteena voidaan nähdä myös sitä hyödyntävä ihminen, sillä ihminen ei ole päätöksenteossaan täysin rationaalisesti toimiva kone. Lisäksi ihminen voi ymmärtää väärin tiedonlouhinnan tulokset tai tehdä huonoja valintoja niiden pohjalta (Abbas ym., 2015.) Siitä herääkin kysymys, voidaanko tiedonlouhinnan tuloksiin aina edes luottaa, jos koko tiedonlouhintaprosessin takana on erehtyväisyyteen taipuvainen ihminen? Tiedonlouhinnan tulokset voivat olla vääriä ja epäluotettavia. Käytettävä algoritmi voi olla huonosti tehty tai käytössä oleva data epätarkkaa, jolloin tiedonlouhinnan tuloksia ja niiden merkitystä päätöksentekoon on syytä kyseenalaistaa. Esimerkiksi tunkeutumisen havainnointijärjestelmissä tapahtuvan virhearvion seurauksena järjestelmä voisi oppia huonoja toimintamalleja, jolloin pahimmassa tapauksessa järjestelmä ei hälyttäisi tunkeutumisen tapahtuessa.

Myös verkon louhintaan liittyy monia haasteita. Verkko on laaja ja se muuttuu nopeasti. Tietoverkko tarjoaa runsaasti piilopaikkoja, mutta samalla myös suuren kohdeyleisön sekä tehokkaan, helpon ja edullisen vaikuttamiskanavan. Verkon sisällön nopea muuntautumistahti vaikeuttaa terroristien löytämistä, sillä terroristinen materiaali voi syntyä milloin ja missä vain, millä kielellä tahansa ja toisaalta myös kadota erittäin nopeasti. (Last, 2007.) Verkon reaaliaikainen valvonta vaatii paljon resursseja ja nykyistä tehokkaampia louhintamenetelmiä, jotka kykenevät hallitsemaan kiihtyvällä tahdilla kasvavia datavirtoja (Thuraisingham, 2004). Verkkoliikenteen valvonta on hankalaa lainsäädännöllisten esteiden vuoksi, sillä verkon käytön louhinta nähdään usein yksityisyydensuojaa loukkaavana (Solove, 2008). Verkon rakenteen louhintaa vaikeuttaa verkon valtava koko. Louhintaprosessissa syntyvien linkkien määrä kasvaa hyvin nopeasti erittäin suureksi. Löytyneistä linkeistä tulisi löytää tutkimuksen

kannalta relevantit ja jättää epäolennaiset pois. Lisäksi ei voida olla varmoja, että kaikki mahdolliset linkit löytyvät. (Thuraisingham, 2004.) Esimerkiksi syvä verkko kätkee suurimman osan internetistä, mutta juuri sen louhinta osoittautuu tällä hetkellä vielä haasteelliseksi (Chen, 2012).

Haasteista huolimatta tiedonlouhinnalle kuitenkin löytyy todellista tarvetta kyberterrorismin torjunnassa. Kyberterrorismin uhka on olemassa ja mahdollisen iskun toteutuessa sen seuraukset voivat olla vakavat (Ahmad & Yunos, 2012). Datamäärät alkavat olla niin suuria, että ihminen ei niitä manuaalisesti mitenkään voi niiden vaatimalla tehokkuudella käsitellä (Witten & Frank, 2005). Näin ollen kyberterrorismin torjunnassa joudutaan entistä enemmän tukeutumaan automaattiseen datan käsittelyyn. Käyttökohteita tiedonlouhinnalle on kyberterrorismin torjunnassa useita ja saavutettavissa olevat tulokset rohkaisevat sen käyttämiseen. Selkeää kuitenkin on, että perinteistä terrorismintorjuntaa tullaan edelleen tarvitsemaan, mutta tiedonlouhinta voi toimia erinomaisena apuvälineenä kyberterrorismin torjunnassa. Erityisesti se, että tiedonlouhinnalla voidaan ennakoida tulevaa ja edistää päätöksentekoa (Thuraisingham, 2004), on tärkeää. Ennakointi ja hyvä päätöksenteko voivat parantaa yhteiskunnan varautumisen ja kokonaispuolustuksen tasoa. Terrorismin vastaisessa työssä ennakoinnin ja varautumisen merkitystä ei voi liikaa korostaa. Terroristille yksikin onnistuminen riittää, mutta puolustusviranomaisille yksikin epäonnistuminen voi olla katastrofaalinen.

Tutkielman tuloksia on kuitenkin jossain määrin syytä kyseenalaistaa. Aihepiiriä tutkii suhteellisen pieni määrä tutkijoita. Sen seurauksena tutkielmaa leimaa lähdemateriaalien välisen diskurssin vähyys, mikä rajoittaa tutkielman tulosten yleistettävyyttä. Tutkimusalalle on ominaista nopea kehitystahti, joten jotkin tässä tutkielmassa mainitut tiedot saattavat jo olla tällä hetkellä tai pian tulevaisuudessa vanhentunutta tietoa. Myös se tosiasia, että kyberterrorismi käsitteenä on vielä kiistelty, vaikeuttaa koko tiedonlouhinnan tehokkuuden arviointia. Jos koko ilmiön määrittely on vielä hankalaa, kuinka voidaan järkevästi mitata sen torjumisessa onnistumista?

Jatkotutkimusaiheita tiedonlouhinnan käyttämiseen kyberterrorismin torjunnassa voidaan nähdä monia. Kyberterrorismiin liittyen jatkotutkimusta tiedonlouhinnan saralla tarvitaan erityisesti reaaliaikaisten tiedonlouhintamenetelmien kehittämiseen paremman reaaliaikaisen puolustuskyvyn saavuttamiseksi. Verkon louhinnan alalla syvän verkon louhintaan tarvitaan tehokkaampia louhintamenetelmiä ja -sovelluksia, joilla syvän verkon tarjoama suoja saadaan poistettua. Lisäksi tutkimusta tarvitaan kyberterroristien todellisen suorituskyvyn selvittämiseksi, sillä tällä hetkellä arviot iskujen ja niiden vaarallisuuden todennäköisyyksistä perustuvat suurelta osin arvailujen varaan.

LÄHTEET

Abbas, O., Mustafa, M., E., Ibrahim, S., B. (2015). The Role of Data Mining in Information Security. *International Journal of Computer (IJC), 17(1),* 1-20.

Ackerman, G., Abhayaratne, P., Bale, J., Bhattacharjee, A., Blair, C., Hansell, L., Jayne, A., Kosal, M., Lucas, S., Moran, K., Seroki, L. & Vadlamudi, S. (2006). *Assessing terrorist motivations for attacking critical infrastructure*. Monterey: Monterey Institute of International Studies.

Ahmad, R., & Yunos, Z. (2012). A dynamic cyber terrorism framework. *International Journal of Computer Science and Information Security, 10(2)*, 149-158.

Al Mazari, A., Anjariny, A., Habib, S. & Nyakwende, E. (2016). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. *International Journal of Cyber Warfare and Terrorism (IJCWT), 6(1),* 1-12.

Ariely, G. (2007). Knowledge Management, Terrorism, and Cyber Terrorism. Teoksessa L. Janczewski & A. Colarik (toim.), *Cyber Warfare and Cyber Terrorism* (s.7-16). Lontoo: Information Science Reference

Best, C. (2010). Threat Early Mining through Web Mining. Teoksessa M. Last & A. Kandel (toim.) *Web intelligence and security: Advances in data and text mining techniques for detecting and preventing terrorist activities on the Web* (s.55-65). Washington D.C.: IOS Press.

Bogdanoski, M., Petreski, D. (2013). Cyber Terrorism – Global Security Threat. *International Scientific Defense, Security and Peace Journal, 13 (24)*, 59-73.

Bramer, M. (2013). *Principles of Data Mining* (2nd ed. 2013.). London: Springer London.

Chapmann, G. (2010, 5. maaliskuuta). Cyber terrorism a real and growing threat : FBI. Haettu 5.12.2016 osoitteesta http://phys.org/news/2010-03-cyber-terrorism-real-threat-fbi.html

Chen, H. (2012). *Dark Web, Exploring and Data Mining the Dark Side of the Web*. New York: Springer Science+Business Media.

Curran, K., Concannon, K., & McKeever, S. (2007). Cyber Terrorism Attacks. Teoksessa L. Janczewski & A. Colarik (toim.), *Cyber Warfare and Cyber Terrorism* (s.1-6). Lontoo: Information Science Reference

Denning, D. E. (2000a). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *The Computer Security Journal, 16(3)*, 15-35.

Denning, D. E. (2000b). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. Teoksessa Linden, E. V. (toim.), *Focus On Terrorism, Volume 9* (s. 71-76). New York: Nova Science Publishers, Inc.

DeRosa, M. (2004). *Data Mining and Data Analysis for Counterterrorism*. Washington, D.C.: The CSIS Press.

Dunn Cavelty, M. (2007). Critical information infrastructure: vulnerabilities, threats and responses. *Disarmament Forum, 2007 (3),* 15-22.

Ektefa, M., Memar, S., Sidi, F., & Affendey, L. S. (2010, March). Intrusion detection using data mining techniques. Teoksessa *2010 International Conference on Information Retrieval & Knowledge Management,(CAMP),* (pp. 200-203). IEEE.

Elovici, Y. (2005). TDS – An Innovative Terrorist Detection System. Teoksessa M. Last & A. Kandel (toim.) *Fighting terror in cyberspace*. (75-90). Hackensack, N.J.: World Scientific.

Elovici, Y., Kandel, A., Last, M., Shapira, B., & Zaafrany, O. (2004). Using data mining techniques for detecting terror-related activities on the web. *Journal of Information Warfare, 3(1)*, 17-29.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine, 17(3)*, 37-54.

Foltz, C., B. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security, 12(2),* 154-166.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, *28*(1), 18-28.

Gordon, S. & Ford, R. (2002). Cyberterrorism?. *Computers & Security, 21(7)*, 636-647.

Han, J., Kamber, M. & Pei, J. (2012). *Data mining : Concepts and techniques* (3rd ed). Amsterdam ; Boston: Elsevier.

Hand, D. J., Mannila, H., & Smyth, P. (2001). *Principles of data mining*. MIT press.

Heickerö, R. (2007) *Terrorism Online and the Change of Modus Operandi* Tukholma: Swedish Defence Research Agency.

Horng, S., Su, M., Chen, Y., Kao, T., Chen, R., Lai, J. & Perkasa, C. D. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. *Expert Systems with Applications, 38*(1), 306-313.

Jalil, S. A. (2003). *Countering Cyber Terrorism Effectively: Are We Ready To Rumble?*. Bethesda: System Administration, Networking, and Security Institute (SANS).

Kahn, R., & Kellner, D. (2004). New media and internet activism: from the 'Battle of Seattle'to blogging. *New media & society*, *6*(1), 87-95.

Kantardzic, M. (2011). *Data mining: Concepts, models, methods, and algorithms* (2nd ed.). Hoboken, New Jersey: John Wiley.

Kumar, S. R., Jassi, J. S., Yadav, S. A. & Sharma, R. (2016). Data-mining a mechanism against cyber threats: A review. Teoksessa *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)* (s. 45-48). Greater Noida: IEEE.

Last, M., Shapira, B., Elovici, Y., Zaafrany, O., & Kandel, A. (2003). Content-based methodology for anomaly detection on the web. Teoksessa *International Atlantic Web Intelligence Conference* (pp. 113-123). Springer Berlin Heidelberg.

Last, M. (2005). Using Data Mining Technology for Terrorist Detection on the Web. Teoksessa M. Last & A. Kandel (toim.) *Fighting terror in cyberspace*. (41-62). Hackensack, N.J.: World Scientific.

Last, M. (2007). Data Mining. Teoksessa L. Janczewski & A. Colarik (toim.), *Cyber Warfare and Cyber Terrorism* (s.358-365). Lontoo: Information Science Reference

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Center for Strategic and International Studies.

Mena, J. (2004). *Homeland security techniques and technologies*. Charles River Media.

Mendez-Torreblanca, A., Montes y Gomez, M., & Lopez-Lopez, A. (2002). A Trend Discovery System for Dynamic Web Content Mining. Teoksessa *Proceedings of the 11th International Conference on Computing CIC-2002*, Mexico City, Mexico, November 2002.

Pollit, M. M. (1998). Cyberterrorism – Fact or Fancy. *Computer Fraud and Security, 1998(2)*, 8-10.

Portnoy, L., Eskin, E., & Stolfo, S. (2001). Intrusion detection with unlabeled data using clustering. Teoksessa *Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001)*.

Rockah, L & Elovici, Y. (2007). An Overview of IDS Using Anomaly Detection. Teoksessa L. Janczewski & A. Colarik (toim.), *Cyber Warfare and Cyber Terrorism* (s.327-337). Lontoo: Information Science Reference

Rollins, J. & Wilson, C. (2007). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues* CSR Report For Congress (Order Code RL33123). Washington, DC: Congressional Research Service (CRS)

Rowland, C. H. (2002). *U.S. Patent No. 6,405,318*. Washington, DC: U.S. Patent and Trademark Office.

Samuel, K., Osman, W., Al-Khasawneh, Y., & Duhaim, S. (2014). Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. *International Journal of Computer Science and Mobile Computing, 3(5)*, 1082–1090.

Solove, D. (2008). Data Mining and the Security-Liberty Debate. *The University of Chicago Law Review, 75*(1), 343-362.

Suihkonen, R. (2015, 15. marraskuuta). Puolustusvoimien asiantuntija terrorismin tiedustelusta: "Suomessa ollaan sokeita" Haettu 27.2.2017 osoitteesta
http://www.ksml.fi/kotimaa/Eversti-terrorismin-tiedustelusta-Suomessa-ollaan-sokeita/381395

Thuraisingham, B. (2004). Data mining for counter-terrorism. Teoksessa H. Kargupta, A. Joshi, K. Sivakumar & Y. Yesha (toim.), *Data Mining: Next Generation Challenges and Future Directions* (s. 157-183). AAAI Press.

Thuraisingham, B., Khan, L., Masud, M. M., & Hamlen, K. W. (2008, December). Data mining for security applications. Teoksessa M. Guo, Z. Wang, F. Tang, C-Z. Xu (toim.), *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008. EUC'08. Vol. 2* (s. 585-589). IEEE.

Wadhwa, P., & Bhatia, M. P. S. (2013, February). Tracking on-line radicalization using investigative data mining. Teoksessa *2013 National Conference on Communications (NCC),* (pp. 1-5). IEEE.

Weimann, G. (2004). *www.terror.net: How modern terrorism uses the Internet*. (Special Report 116). Washington, DC: United States Institute of Peace.

Witten, I. H., & Frank, E. (2005). *Data Mining: Practical machine learning tools and techniques*. San Francisco: Morgan Kaufmann.

Yang, Q., & Wu, X. (2006). 10 challenging problems in data mining research. *International Journal of Information Technology & Decision Making*, *5*(04), 597-604.

Zhang, J., Zulkernine, M., & Haque, A. (2008). Random-forests-based network intrusion detection systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38(5),* 649-659.