KYBERTERRORISMI JA SEN UHAT YHTEISKUNNAN TURVALLISUUDELLE

Antti Laurila

4/2017

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

Tiivistelmä

<table>
<tr><td>Tekijä

Antti Laurila</td><td colspan="2">Tutkinto/kurssi ja opinnäytetyö/nimike

Poliisi (AMK) / AMK20142</td></tr>
<tr><td>Julkaisun nimi

Kyberterrorismi ja sen uhat yhteiskunnan turvallisuudelle</td><td colspan="2">Julkisuusaste

Julkinen</td></tr>
<tr><td>Ohjaajat ja opintoaine/opetustiimi

Heli Jalander</td><td colspan="2">Opinnäytetyön muoto

Kirjallisuuskatsaus</td></tr>
<tr><td colspan="3">Tiivistelmä

Tämä opinnäytetyö käsittelee kyberterrorismia ja sen tuomia uhkia yhteiskunnan turvallisuudelle. Opinnäytetyössä tutkitaan mitä kyberterrorismi on ja miten tietoverkkojen käyttö tuo lisää haasteita mm. poliisille. Työ on toteutettu kirjallisuuskatsauksena.

Kyberterrorismi on kyberrikollisuutta, mutta sen tarkoitukset ovat perinteisen terrorismin kaltaiset. Terrori-iskun toteuttamista tietokoneyhteyden välityksellä ei voida sulkea pois. Tietotekniikka mahdollistaa monien toimintojen käytön jopa toiselta puolelta maailmaa, joten myös terroristeille tietotekniikan kehitys avaa uusia ovia. Lisäksi tietoverkkoihin murtautumisen avulla voidaan hyökätä mahdollisesti moneen kohteeseen yhtä aikaa.

Tekniikan kehittyessä yhä useampi prosessi käsitellään tietokoneiden avulla. Tietokoneiden tulo yhteiskuntamme jokapäiväisiksi työvälineiksi on tuonut myös rikollisille uuden mahdollisuuden toimia. Kyberrikollisuus on tuonut poliisille ja muille viranomaisille suuren joukon uusia tehtäviä, joten kyberturvallisuus on tärkeä asia kaikille.

Opinnäytetyssä on käsitelty myös terrorismia, koska se auttaa ymmärtämään missä aiheessa liikutaan. Kyberterrorismi on pohjimmiltaan kuitenkin terrorismia, johon kyberympäristö tuo vain vaihtoehtoja terrori-iskun toteuttamiselle.</td></tr>
<tr><td>Sivumäärä

44</td><td>Tarkastuskuukausi ja vuosi

Huhtikuu 2017</td><td>Opinnäytetyökoodi (OPS)

AMKkorkeakoulutetut</td></tr>
<tr><td colspan="3">Avainsanat

Terrorismi, kyberterrorismi, kyberrikollisuus, tietoverkko</td></tr>
</table>

SISÄLLYS

1 JOHDANTO

1.1 Taustaa

Terrorismi on noussut kansainvälisesti suureksi huolenaiheeksi. Terrorismi ei suoranaisesti kosketa jokaista ihmistä maan päällä, mutta sen vaikutus ulottuu laajalle sen julmuuden ja laajan uutisoinnin johdosta. 2000-luvulla terrorismin torjunta on noussut kansainvälisesti valtioiden turvallisuusviranomaisten keskeiseksi tehtäväksi ja nykypäivänä terrorismin torjuntaan käytetäänkin resursseja enemmän kuin koskaan aiemmin.

Terrorismi on globalisoituneessa maailmassa valtioiden rajoja rikkovaa kansainvälistä toimintaa, joten terrorismin uhka myös Suomessa on todellinen (Puistola & Herrala 2006, 9). Monelle sana terrori-isku herättää mielikuvia räjähteistä tai kidnappauksista. Terrorismi käsitteenä on kuitenkin laaja. Se on vaikutuskeino, jolla väkivaltaiset ryhmittymät pyrkivät tuomaan esille omaa tahtoaan (Puistola & Herrala 2006, 13). Terrorismi on joillekin tahoille äärimmäinen keino vaikuttaa asioihin. Myös terrorismi on mukautunut historiassa teknologisen kehityksen vauhdissa, mikä on tuonut terroristeille uusia tapoja toimia. Tämän työn tarkoituksena on tutkia tietoverkoissa ja niiden välityksellä tapahtuvaa terrorismia.

Tietotekniikka on kehittynyt 2000-luvulla nopeammin kuin koskaan. Tietotekniikan kehitys on tuonut myös rikollisuuteen uusia muotoja. Kyberrikollisuus, jolla tarkoitetaan tietotekniikkaan ja tietoverkkoihin kohdistuvia rikoksia sekä tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tapahtuvia rikoksia, on tullut jäädäkseen ja se on rikollisille entistä helpompaa ja nopeampaa. Tietotekniikkaan ja tietoverkkoihin kohdistuvia rikoksia ovat esimerkiksi tietomurrot, haittaohjelmien avulla tapahtuvat tietojen kaappaukset ja erilaiset verkkohyökkäykset. Käytännössä mitkä tahansa rikokset, joissa on käytetty tietotekniikkaa ja tietoverkkoja hyväksi, voivat olla kyberrikollisuutta. Yhteiskunnan palveluiden digitalisoiminen avaa myös rikollisuudelle aivan uudet mahdollisuudet. (Kyberrikollisuus, luettu 12.1.2017.)

Kyberterrorismi on tietoverkkoja hyväksi käyttämällä toteutettua toimintaa, jonka tarkoituksena on aiheuttaa pelkoa kohdeyleisössä. Tietoverkoissa kulkevaa tietoa on äärimmäisen paljon ja siihen puuttuminen terroristisissa tarkoituksissa voi saada aikaan suurtakin tuhoa. Nykypäivänä suuri osa tiedosta liikkuu verkoissa, joten tietoverkkoihin käsiksi pääsemällä on mahdollista tavoittaa suurikin yleisö.

Kyberterrorismi tarkoittaa tässä tutkimuksessa terroristisessa tarkoituksessa tehtyä toimintaa tietoverkkoja hyväksikäyttämällä. Kyberterrorismi voidaan laskea kyberrikollisuudeksi, mutta se eroaa kyberrikollisuudesta siinä mielessä, että kyberterrorismin tavoite on pohjimmiltaan aiheuttaa pelkoa ja pahimmassa tapauksessa laajaa tuhoa. Kyberrikollisuus tarkoittaa verkossa tapahtuvaa rikollisuutta, jonka tavoitteena on tietotekniikkaan ja tietoverkkoihin kohdistuvien rikosten tekeminen tai niitä hyväksikäyttämällä tapahtuvia rikoksia. Näitä voivat olla esimerkiksi pankkitunnusten kalastelu kansalaisilta ja niiden kautta tilien tyhjentäminen. Kyberterrorismin tulkinta ja määritteleminen ovat ongelmallisia, koska kyberympäristössä toimiminen on hankala todistaa kuten myös se, milloin toiminta ylittää terrorismin rajat rikoslain 34a §:n mukaan. Lisäksi terrori-iskun tapahtumat eivät välttämättä liity täysin tietoverkkoihin, vaan niitä käytetään vain osittain iskun toteuttamisessa. Rajanveto kyberterrorismille ja terrorismille on häilyvä.

Olen valinnut tutkimuksen kohteeksi tämän aiheen, koska terrorismi on mielenkiintoinen ja ajankohtainen kokonaisuus. Lisäksi terrorismin vaikutus yhteiskuntaan on maailmanlaajuisesti merkittävä. Kyberterrorismi on tulevaisuuden haaste niin viranomaisille kuin muillekin tahoille. Terroristiorganisaatiot voivat saada aikaan suurtakin tuhoa pelkästään tietokoneiden välityksellä, joten verkossa tapahtuvien iskujen toteuttaminen kiinnostaa terroristeja. Lisäksi tietoverkkojen käyttö ihmisten kaikessa toiminnassa lisääntyy kovaa vauhtia.

1.2 Tutkimustehtävä ja rajaukset

Tässä opinnäytetyössä tutkitaan mikä on kyberterrorismia sekä mitä uhkia se tuo yhteiskunnan turvallisuudelle. Lisäksi opinnäytetyössä tutkitaan mikä on poliisin rooli verkossa tapahtuvan terrorismin torjunnassa ja miten kyberturvallisuus vaikuttaa tietoverkkoja käyttävän yhteiskunnan arjessa.

Terrorismi on hyvin laaja käsite ja sitä on tutkittu todella paljon. Tässä tutkimuksessa keskitytään tietoverkoissa ja niiden välityksellä tapahtuvaan terrorismiin. Työ on rajattu kyberrikollisuuteen ja sen osana toimivaan kyberterrorismiin, mutta työssä käsitellään yleisesti myös terrorismin merkitystä ja sen ideologiaa, koska tällä tavalla lukijalle saadaan parempi kuva siitä, mikä kyberterrorismin pohjimmainen tarkoitus on. Tutkimuksessa sivutaan myös kyberrikollisuutta ja kybersotaa, koska näiden käsitteiden avaaminen auttaa lukijaa ymmärtämään millä alueella tutkimuksessa liikutaan. Lisäksi käsitellään poliisin ja

muiden viranomaisten tehtäviä kyberterrorismin torjunnan suhteen. Koska tietoverkot eivät noudata valtioiden rajoja, on myös kansainväliselle viranomaisyhteistyölle annettu sijaa. Teknologian kehityksen johdosta kyberterrorismi sijoittuu ajallisesti käytännössä vasta 2000-luvulle, joten tämä tutkimus on ajallisesti rajattu suurimmaksi osaksi Yhdysvalloissa syyskuussa 2001 tapahtuneiden terrori-iskujen jälkeiseen aikaan.

Tutkimuskysymyksenä on: ”Mitä on kyberterrorismi ja mitä uhkia se luo yhteiskunnan turvallisuudelle?” Tarkoituksena on tutkia terrorismia, joka tapahtuu tietoverkoissa ja niiden välityksellä. Tutkielmassa käsitellään myös mitä tietoverkot ovat ja mikä niiden merkitys yhteiskunnalle 2000-luvulla on. Alakysymyksenä on: ”Mitä uhkia kyberterrorismi luo yhteiskunnalle?” sekä ”miten kyberterrorismia torjutaan?” Näiden kysymysten pohjalta tutkielmassa käsitellään, miten poliisi pyrkii estämään verkossa tapahtuvaa rikollisuutta sekä mitä uhkia yhteiskunnalle kyberterrorismista voi olla.

1.3 Tutkimusmenetelmä

Työ on tutkimuksellinen opinnäytetyö, joka perustuu kirjallisuuskatsaukseen. Tarkoituksena on jo tutkitun tiedon perusteella selvittää, millaiset kyberterrorismin vaikutukset voivat yhteiskunnalle olla ja miten se mahdollisesti vaikuttaa yhteiskuntaan. Kirjallisuuskatsauksen tarkoituksena on selvittää, millaista tietoa käsiteltävästä aiheesta on jo olemassa ja sen tavoitteena on kehittää olemassa olevaa teoriaa. Kirjallisuuskatsaus on tutkimustekniikka, jonka avulla voidaan tutkia valmiita tutkimuksia ja koota niiden tulokset yhteen. Nämä tulokset ovat perustana uudelle tutkimukselle. Kirjallisuuskatsaus voidaan jakaa kolmeen tyyppiin: kuvailevaan kirjallisuuskatsaukseen, systemaattiseen kirjallisuuskatsaukseen sekä meta-analyysiin.

Kuvaileva kirjallisuuskatsaus on yleiskatsaus ilman tiukkoja ja tarkkoja sääntöjä. Siinä tutkittava ilmiö kyetään kuvaamaan laaja-alaisesti ja tarvittaessa luokittelemaan sen ominaisuuksia. Systemaattinen kirjallisuuskatsaus on tiivistelmä aiheen aiemmista tutkimuksista. Meta-analyysi käsittelee tiettyjä avainasioita ja vertailee niitä keskenään.

Tämä tutkimus on toteutettu systemaattisena kirjallisuuskatsauksena, joka on tiivistelmä aihepiirin aiempien tutkimusten keskeisimmästä sisällöstä. Työssä on käyty läpi tieteellistä materiaalia terrorismista ja kyberrikollisuudesta. (Salminen 2011, 3–10.)

Tässä tutkimuksessa lähteenä on kirjallisuus, joka on aiemmin tutkinut kyberterrorismia ja terrorismia. Tutkimus perustuu tietokirjallisuuteen, internetistä poimittuihin virallisiin lähteisiin, kuten Suomen poliisin ja Sisäministeriön internetsivuihin. Lisäksi aineistona on ympäri maailman tapahtuvien terrori-iskujen uutisointi painottuen kuitenkin Euroopan sisällä ja Lähi-idässä tapahtuneisiin terrori-iskuihin ja niiden uutisointiin. Tutkimuksessa on myös käytetty viranomaisten internetsivujen artikkeleita lähteinä.

2 TERRORISMI

2.1 Määritelmä

Terrorismin määritteleminen on moniulotteista ja eri lähteissä terrorismi on määritelty eri tavalla. Terrorismille ei ole toistaiseksi olemassa kansainvälisesti yhteisesti hyväksyttyä kattavaa määritelmää (Sisäministeriö, 2014). Vuonna 2004 Yhdistyneiden kansakuntien (YK) raportissa terrorismi määriteltiin toiminnaksi, jonka tavoitteena on tuottaa vakavaa ruumiillista väkivaltaa tai tappaa siviilejä sekä muita joukkoja, jotka eivät taistele, tai jonka tavoitteena on tuottaa pelkoa väestölle, tai saada valtion johto tai kansainvälinen organisaatio tekemään tai jättämään tekemättä tiettyjä toimia (Crenshaw 2011, 2). Pohjimmiltaan terrorismi on kuitenkin väkivaltaa, jonka tavoitteena on ajaa poliittisia ja/tai uskonnollisia päämääriä tuottaen psykologisia vaikutuksia laajalle yleisölle. Uskonnollinen terrorismi ja poliittinen terrorismi ovat useimmiten kuultuja terrorismin muotoja, mutta niiden raja voi kuitenkin olla hyvin häilyvä. (Laitinen 2007, 11.)

Terrori-iskun toteutus tapahtuu salassa, yllätyksellisesti, naamioidusti tai hämäämällä. Iskun tapahtuma-aika ja –paikka sekä niiden uhrien määrän on tarkoitus pelotella suurempaa joukkoa. Terrori-iskun psykologinen vaikutus on sen käyttäjien päällimmäinen tarkoitus. Valtaa vastustaville terrorismi on tehokas tapa vaikuttaa asioihin. Terrorismi ei kuitenkaan ole näin yksiselitteistä, koska sillä on kaksi puolta. Toisille isku on terrorismia ja toisille se on oikeutettua toimintaa omien intressien puolesta, jonka takia sen määritteleminen on haastavaa. Terrorismin ja muun poliittisen väkivallan väliin on vaikeaa vetää selvää rajaa. Ongelmana määrittelyssä on se, onko terrorismin kohde sotilaskohde, tai muu vastaava valtion hallitsema kohde, vai onko se siviilikohde. Mikäli sotilaskohteisiin tehdään isku, onko se terrori-isku vai muu sotaan liittyvä hyökkäys? Tämän takia on tärkeää määritellä iskun motiivi tai tarkoitus ennen kuin voidaan puhua terrori-iskusta. (Crenshaw 2011, 2–3.)

2000-luvulla terrorismi on laajentunut maailmanlaajuiseksi toiminnaksi, jonka tavoite ei enää pelkästään ole koskea paikallisen tason politiikkaa vaan terrorismilla voi olla maailmanlaajuisia tavoitteita. Kansainvälinen terrorismi ja sen uhkakuva on muuttunut entistä moninaisemmaksi. Euroopan maita merkittävimmin koskettavaa terrorismia 2010-luvulla on Suojelupoliisin mukaan radikaali-islamistinen terrorismi. (Suojelupoliisi, luettu 20.1.2017.)

Vaikka terrorismi on levinnyt laajalle, se voi silti vaikuttaa yksittäisillä iskuilla paikallisestikin. Islamistisella terrorismilla vaikutus saattaa olla länsimaisia valtioita sekä ”vääräuskoisia” kohtaan, mutta lisäksi sillä voidaan pyrkiä vaikuttamaan iskun kohteena olevan maan omaan sisäpolitiikkaan. Terrori-iskujen vaikutus on muuttunut entistä enemmän raaempaan suuntaan siten, että iskujen tarkoitus ei välttämättä ole enää tavoittaa mahdollisimman suurta yleisöä, vaan saada aikaan suurta tuhoa. Tästä johtuen länsimainen avoin yhteiskunta on erittäin haavoittuvainen. Esimerkkinä voidaan pitää vuonna 2001 Yhdysvalloissa tapahtuneita terrori-iskuja, joissa Al-Qaida–nimiseen terroristijärjestöön kuuluneet terroristit murhasivat useita tuhansia ihmisiä lentämällä kaapattuja matkustajalentokoneita New Yorkissa sijainneisiin World Trade Centerin kaksoistorneihin. Lisäksi iskujen kohteena oli Yhdysvaltain puolustusministeriön hallintorakennus Pentagon (CNN 8.9.2016). Yhdysvalloissa tapahtuneiden iskujen uhrimäärä oli hyvin suuri. Tästä johtuen valtiot käyttävät hyvin paljon resursseja terrorismin vastaiseen toimintaan, kun taas terrorismin kulut voivat olla hyvin pienet. Nykypäivänä terrori-iskuun voi liittyä toisistaan tietämättömiä tahoja sekä rahoittajia. (Laitinen 2007, 12.)

2.2 Terrorismin syyt

Terrorismin tarkoitus on välittää poliittista viestiä. Sen tarkoitusperä on syvemmällä kuin materiaalisten tappioiden tuottamisessa tai sivullisten ihmisten surmaamisessa. Iskun kohteelle koituneet tappiot eivät ole terroristiorganisaation syy iskuihin vaan todellinen syy on välittää viestiä suuremmalle yleisölle ja vaikuttaa heidän reagoimiseen terrorismia vastaan. (Crenshaw 2011, 34.)

Terrorismin taustalla voi olla kaksi syytä. Ensimmäisenä ovat mahdolliset tapahtumat, jotka ovat luoneet pidemmällä aikavälillä syitä mahdollisien terroristisen toimenpiteiden toteuttamiselle. Näitä voivat olla esimerkiksi pidempään kestänyt poliittinen painostus, joka pyritään lopettamaan, tai nopeat toimenpiteet, jotka voivat olla joidenkin tahojen mie-

lestä vastustamisen arvoisia. Esimerkki tällaisesta toimenpiteestä on tammikuussa 2015 tapahtunut terrori-isku Pariisissa Charlie Hebdo –nimisen satiirilehden toimitukseen. Iskun syynä oli lehden julkaisemat pilakuvat Muhammadista (MTV 7.1.2015). Toinen syy terrorismille on tekijät, jotka mahdollistavat ja sallivat sen toteuttamisen sekä tilanteet, jotka inspiroivat sekä motivoivat terroristisiin tekoihin. Nämä tekijät yhdessä voivat olla suoranaisesti terrorismin syitä. Ne eivät kuitenkaan ole ainoat syyt terrorismille, vaan jokaisen valtion sisä- ja ulkopolitiikka tuovat omat vaikuttavat tekijänsä mukaan yhtälöön. (Crenshaw 2011, 36.)

Erilaiset vähemmistöt ja niiden sortaminen saattavat johtaa väkivaltaisuuksiin ja kehittyä jopa terrorismiksi. On sanomattakin selvää, että kaikki sorretut vähemmistöt eivät tietenkään toteuta terrorismia. Sortaminen luo kuitenkin mahdollisuuden sellaisille yhteisöille ja organisaatioille, jotka ajattelevat, että heidän omien intressiensä johdosta on asioille tehtävä jotain. Mikäli valtion lait eivät mahdollista toimintaa ja siihen puututaan virkavallalla, on mahdollista, että myös omia etujaan ajavat yhteisöt ja organisaatiot vastaavat tilanteeseen väkivallalla. Lisäksi olosuhteet voivat olla sellaiset, että vähemmistöön kuuluvan ryhmän on mahdotonta edes vaikuttaa poliittisiin päätöksiin. Tämä luo tyytymättömyyttä vähemmistöryhmän kannattajia kohtaan, jolloin mahdolliset keinot päätösten vaikuttamiseen voivat olla väkivaltaiset. Terrorismi on looginen vaihtoehto, kun muu toiminta ei tuota tulosta. Vähemmistön kokema heikkous vaihtoehtojen rajoittamisessa voi aiheuttaa terrorismin houkuttelevaksi vaihtoehdoksi saada omalle tahdolle huomiota. (Crenshaw 2011, 38.)

Vaikka tiettyjä yhteisöjä sorretaan, se ei kuitenkaan tarkoita, että ne aloittaisivat vastarinnan nimenomaan terrorismia käyttämällä. Vaikka yhteisö ajattelisikin, että ajan mittaan tilanne tulisi muuttumaan yhteisön intressien suuntaan, voi olla mahdollista, että yhteisön jäsenistä osa ei kuitenkaan ole valmiita odottamaan muutosta. Muutoksen nopeuttamisen suhteen voidaan käyttää mahdollisia terroristisia toimenpiteitä omien tavoitteiden saavuttamiseksi lähes välittömästi. Syitä näiden yhteisöjen heikkouteen voi kuitenkin löytyä monesta eri asiasta, joten terrorismille on vaikeaa määrittää tarkkaa syytä.

Väkivallalla vaikuttaminen on nopea keino tavoittaa suuri yleisö. Kun terrori-isku tapahtuu, sen kohteena ovat uhrien lisäksi myös muu väestö. Useiden ihmisten surmaaminen tai kiduttaminen on julmaa ja ne saavat suurella osalla ihmiskuntaa tunteet nousemaan pintaan, jolloin psykologisesti katsottuna vaikuttaminen on vahvaa. Terrorismi vaikuttaa tun-

teisiin, jolloin ihmisen rationaalinen ajattelu ei välttämättä ole samalla tasolla kuin normaalisti. Mitä raaempi teko on, sitä enemmän se nostaa tunteita kohdeyleisössä ja näin ollen sitä suurempi teon vaikutus on. Tällöin syntyy vihaa sekä kostonhalua. Tämä antaa kansan tuen valtion johdolle tehdä poliittisia päätöksiä tilanteeseen reagoimisen suhteen. Näin esimerkiksi terrori-iskun kohteena ollut valtio voi hyökätä terroriteon tehneeseen valtioon, jolloin hyökkäykseen on kansan tuki, mikä on sodankäynnissä tärkeää. (Yli-Karjanmaa 2008, 37.)

Joillekin terroristijärjestöille huomion saaminen voi olla suurin tavoite. 2010-luvulla globalisaatio on tuonut myös terrorismiin uusia vaikutteita, joidenka takia se on levinnyt valtioiden rajojen ulkopuolelle eikä enää toimi pelkästään yhden valtion alueella. Tämä tarkoittaa terroristeille suurempaa yleisöä, joten iskujen suunnitteleminen ja toteuttaminen suuriin kaupunkeihin ja tapahtumiin, joissa on suuri määrä osallistujia, on tullut yleiseksi. Lisäksi yhteiskunnan infrastruktuuri edistää terrori-iskujen mahdollisuuksia ja samalla vaikeuttaa viranomaisten työtä iskuihin varautumiseen. Esimerkkinä voidaan pitää joukkoliikenteen kasvua, mikä on hyvinkin otollinen paikka mahdolliselle terrori-iskulle (Crenshaw 2011, 37). Lisäksi terrorismin toteuttaminen on hyvinkin vaihtelevaa aina pienemmistä itsemurhaiskuista suurimpiin, useita tuhansia uhreja vaativiin iskuihin.

Terrorismi on tehokas strategia erilaisen ideologian omaaville ryhmille, jotka ovat eri mieltä valtion päätöksistä. Se on yksinkertaista ja nopeaa toimintaa, joka saa välittömästi suuren huomion raakuudellaan. Terroristit havaitsevat mahdollisuuden toimia toisella tavalla ja käyttävät sitä hyväksi. Terroristeja yhdistäviä tekijöitä ei välttämä pystytä selvittämään tarkasti. Syy, minkä takia henkilö ajautuu terrorismin pariin voi olla monen eri tekijän summa. Ei ole olemassa yhtä ja samaa syytä, jonka takia henkilöt liittyvät terrorijärjestöihin. Sen lisäksi ei voida yhdistää tekijöitä, mitkä saavat henkilöt vielä jatkamaan toimintaa. Terrorismi on vähitellen kasvavan sitoutumisen ja vastustamisen yhdistävän ryhmän kehitys, johon myös valtion toimet vaikuttavat. Ryhmän kasvaessa yhteisten päämäärien ja tavoitteiden toteuttaminen on helpompaa, koska kanssa-ajattelijoita on useita. Terrorismin psykologinen vaikutus terroritekoja suorittaviin henkilöihin pienenee ryhmän koon kasvaessa. Tämän takia terroristiorganisaatioon kuuluvan henkilön käännyttäminen toisiin ajatuksiin on haastavaa. (Crenshaw 2011, 49–50.)

Valtioterrorismi tarkoittaa terrorismia, jota valtio tukee tai toteuttaa. Sitä voidaan toteuttaa myös toisen valtion toimesta, joko osittain tai kokonaan. Tällaisesta esimerkkinä on terro-

ristijärjestön toiminnan tukemista tai kokonaan valtion omilla resursseilla toteutettua terrori-iskua. Valtioiden roolia ei-valtiollisen terroritoiminnan tukemisessa on vaikea arvioida, koska sen todistaminen on usein hankalaa. Valtiot voivat tukea terrorismia esimerkiksi rahoittamisen avulla, tai sallia terroritoimintaan liittyviä toimenpiteitä. Valtiot voivat myös itsenäisesti toteuttaa terroritoimintaa, jolloin valtio itse tekee kokonaisuudessaan iskun. Tällaisessa tilanteessa voi kuitenkin olla mahdotonta selvittää teon alkuperää, koska valtiot eivät sitä yleensä tunnusta. Lisäksi on mahdollista, että iskun tehnyt valtio toimii jonkun toisen terroristijärjestön nimellä. Tällöin isku on toteutettu valtion toimesta, mutta se saadaan näyttämään siltä, että terroristijärjestö olisi sen toteuttanut. (Malkki & Paastela 2007, 72–77.)

2.3 Terrorismi 2000-luvulla

1900-luvun alkupuolella terroristiorganisaatiot käyttivät vielä hyvinkin perinteisiä armeijatyylisiä organisaatioita. Terrorismin kaltaisessa toiminnassa huomattiin hyvin nopeasti, että organisaatiokuviot, jotka sotavoimissa toimivat, olivat liian näkyviä ja helposti häirittäviä eivätkä välttämättä toimineet salassa pidettävän toiminnan kanssa. Tästä johtuen uusi joustavampi järjestelmä terroristeille on niin kutsuttu solujärjestelmä. Solujärjestelmässä organisaation rakenne on suojattu siten, että terroristi organisaatio toimii useana pienempänä soluna, joissa on jäseniä noin 12. Solun jäsenet eivät tiedä organisaatiostaan muuta kuin oman solunsa jäsenet. Tällöin solun johtaja on ainut henkilö, joka on tekemisissä organisaation ylemmän johdon kanssa. Solujen jäsenet eivät kykene tällä tavalla paljastamaan koko organisaatiota kiinni jäädessään, vaan voivat antaa ilmi pelkästään oman solunsa jäsenet. Tämä ei silloin kaada kerralla koko organisaatiota, mikäli yksi solun jäsen jää kiinni. (Neuman 2009, 17.)

Solujärjestelmän toinen ominaisuus on, että solut toimivat hyvin itsenäisinä. Itsenäiset solut ovat kuitenkin tiiviisti integroitu suurempaan organisaatioon, mutta toteuttavat niille annetut tehtävät itsenäisesti. Soluilla ei ole välttämättä tarkkaa ohjetta tai käskyä siitä, miten joku isku tulisi toteuttaa, vaan sillä on hyvin avoimet kädet toiminnan suhteen. Solujärjestelmä mahdollistaa terroristiorganisaation toiminnan myös laajemmilla alueilla. Tämän takia tietty organisaatio kykenee toimimaan ympäri maailman tarvittaessa. (Neuman 2009, 18–19.)

2000-luvun alkupuolella uskonnollinen terrorismi on yksi suurimpia uhkia yhteiskunnalle. Uskonto on ollut aina ihmisille tärkeää. Useille terroristiorganisaatioille uskonto on tärkein ja voimakkain liikkeellepaneva voima. Uskonnon avulla toiminta oikeutetaan ja sille määritetään haluttu lopputulos (Puistola & Herrala 2006, 105). Terrorismin suhteen merkittävin uskonto on islam. Radikaali-islamistinen terrorismi on tällä hetkellä huomattavin Euroopan maita uhkaava terrorismin muoto (Suojelupoliisi, luettu 18.4.2017). Uskonnollinen terrorismi voi olla toimenpiteiltään äärimmäistä, koska se perustuu uskontojen tulkintoihin ja niiden katsomuksien muovaamaan maailmankuvaan. 1900-luvun loppupuolella islamistinen Al-Qaida nousi yhdeksi vaikutusvaltaisimmaksi terroristiorganisaatioksi, joka tuli tunnetuksi iskujensa raakuudesta ja niiden suunnitelmallisuudesta. Al-Qaidan toiminnalle ominaista oli terrori-iskujen toteuttaminen useisiin kohteisiin yhtäaikaisesti sekä iskujen pitkäaikainen suunnittelu, operaatioiden salattu kommunikointi, iskujen mielikuvitteellisuus sekä niiden toteutus uusilla eri tavoilla. Lisäksi Al-Qaida oli poikkeuksellisen suuri terroristiorganisaatio. (Puistola & Herrala 2006, 104–105.)

Toinen merkittävä terroristiorganisaatio on ääri-islamilainen ISIL (Islamic State of Iraq and the Levant), jonka juuret ylettyvät 2000-luvun alkuun. ISIL tunnetaan myös nimillä ISIS (Islamic State in Irak and Syria) tai IS (Islamic State) ja on alun perin muodostunut Irakin Al-Qaidasta. ISIL on vaikuttanut Lähi-Idässä valtaamalla suuria osia Irakin ja Syyrian alueella vuonna 2013. Kesään 2015 mennessä ISIL oli vallannut jo puolet Syyriasta mukaan lukien kaikki suurimmat tieyhteydet Irakiin. ISIL omistaa oman armeijan ja vuonna 2013 sen vahvuudeksi on arvioitu 10 000–12 000 taistelijaa. ISIL rekrytoi menestyksekkäästi taistelijoita ulkomaisista henkilöistä sosiaalisen median (Facebook, Twitter) välityksellä. Vuonna 2014 esitettiin arvioita, että ISIL:n koko olisi jo 30 000–40 000 taistelijaa. ISIL on saanut mainetta median keskuudessa ympäri maailman lähinnä poikkeuksellisen raakojen toimintatapojen vuoksi (Lansford & Pauly 2016, 1–2.). ISIL ilmoitti vuonna 2014 perustaneensa kalifaatin hallitsemilleen alueille. ISIL tavoitteli Al-Qaidan asemaa maailmanlaajuisen islamilaisen aseellisen taistelun johdossa. Myös Suomesta on lähtenyt henkilöitä taistelemaan ISIL:n puolelle Syyriaan. Suomalaisia on myös kuollut taisteluissa. Ne henkilöt, jotka palaavat takaisin Suomeen ISIL:n riveistä, voivat olla vakava väkivallan uhka kansalliselle turvallisuudelle ja nämä henkilöt arvioidaan tapauskohtaisesti. (Suojelupoliisi, luettu 18.4.2017.)

2.4 Terrorismin uhkakuva Suomessa 2000-luvulla

Vuonna 2001 Yhdysvalloissa tehtyjen terrori-iskujen jälkeen terrorismista on tullut Suomessa aiempaa merkittävämpi poliittinen kysymys. Suomeen kohdistuva terrorismin uhka ei ole olennaisesti muuttunut 2000-luvun alussa, vaikka terrori-iskun mahdollisuutta ei voida sulkea pois. Suomessa mahdollisen terrori-iskun motiivi voisi olla vaikuttaminen muun Euroopan toimintaan. Lisäksi Suomessa vierailevat, varsinaisen iskun kohdemaan henkilöt, voivat aiheuttaa vaaran terrori-iskulle altistumiselle. (Malkki & Paastela 2007, 366–367.)

Suojelupoliisi nosti terrorismin uhkatasoa kesäkuussa 2014 ja uudelleen marraskuussa 2015 (Sisäministeriö, luettu 14.2.2017). Suojelupoliisin 3.11.2015 antaman terrorismin uhka-arvion mukaan Suomeen kohdistuva terroriuhka on kohonnut viime vuosina. Edelleenkin terrorijärjestöjen suunnittelemien iskujen uhka on matala, mutta yksittäisten tekijöiden uhka on noussut vuoden 2014 jälkeen. Lisäksi suomalaisia kohtaan isku voi toteutua myös ulkomailla. Suomessa oleskelevien henkilöiden määrä, joilla on kytköksiä terroristijärjestöihin, on lisääntynyt. Osasyynä voidaan pitää erityisesti Syyriassa ja Irakissa aseelliseen toimintaan liittyneitä suomalaisia, joiden paluu Suomeen voi olla uhka kansalliselle turvallisuudelle. Suomesta peräisin olevien taistelijoiden johdosta myös ulkomaiset radikaali-islamistit tuntevat Suomen paremmin. Suojelupoliisin mukaan Suomessa on myös terrorismia tukevia ryhmiä, jotka ovat jatkaneet kasvuaan entisestään. Lisäksi Suomeen on saapunut viime vuosina huomattava määrä turvapaikanhakijoita, joista osalla on kytköksiä terroristiorganisaatioihin. (Suojelupoliisi 2015.)

2.5 Terrorismintorjunta

Terrorismintorjunnan tavoitteena on tunnistaa mahdolliset terroriuhat hyvissä ajoin sekä estää niiden toteutuminen. Terrorismintorjunta voidaan jaotella kahden näkemyksen mukaan. Ensimmäisen näkemyksen mukaan terroritekoja vastaan tulisi taistella keinoilla, joilla rangaistaan terroristeja ja ehkäistään tulevia iskuja. Toisen näkemyksen mukaan terrorismin torjunnassa tulisi keskittyä sen avaintekijöihin ja pyrkiä vaikuttamaan niihin seikkoihin, jotka radikalisoitumisen ylipäätään mahdollistavat. (Laitinen & Lumio 2009, 68.)

Suomessa terrorismintorjunta perustuu turvallisuusviranomaisten lisäksi myös yhteiskunnan muiden osapuolten toimivaan yhteistyöhön. Terrorismintorjunta on monen eri tahon

yhteinen tehtävä (Sisäministeriö, luettu 14.2.2017). Suojelupoliisin tehtävänä on terrorismiin liittyvien hankkeiden ja rikosten ennalta estäminen ja paljastaminen (Suojelupoliisi, luettu 17.2.2017). Keskusrikospoliisi vastaa terrorismirikosten esitutkinnasta. Viranomaisyhteistyö sekä yhteistyö muiden tahojen kuten koulujen ja sosiaalityöntekijöiden kanssa on tärkeää nimenomaan terrorismiin johtavien syiden ennakoinnissa ja niiden ehkäisemisessä sekä radikalisoitumisen tunnistamisessa. Suomessa pyritään rakentamaan jatkuvasti parempaa yhteyttä virkavallan ja muslimiyhteisöjen välille, koska radikaali-islamistinen terrorismi on edelleenkin suurin uhka. Näin kyetään saamaan mahdollisesti jo muslimiyhteisöiltä tietoja hankkeista, joilla voi olla yhteyksiä terroristiorganisaatioihin tai niiden toimintaan. (Laitinen & Lumio 2009, 70.)

3 KYBERTERRORISMI

Kyberterrorismi on yleisesti määritelty tietokoneiden käyttämiseksi kriittisten kansallisten infrastruktuurien, kuten energiatalouden, kulkuyhteyksien, tai valtion toimintojen, sabotoimiseksi. Koska suuri osa järjestelmistä on tietokoneriippuvaisia, on tietoverkot tuoneet uuden haavoittuvuuden yhteiskunnan haasteeksi. Kyberterrorismi juontaa juurensa jo 1990-luvulle, jolloin yhteiskunta alkoi kehittyä digitaalisesti. Tietoverkkojen yleistyessä huomattiin jo alusta asti, että mahdolliset väärinkäytökset voisivat olla kohtalokkaita. (Weimann 2015, 151.)

Tietotekniikan kehittyessä myös sen väärinkäyttö yleistyy. Kyberterrorismi (tai verkkoterrorismi) tarkoittaa terrorismia, jossa käytetään informaatiojärjestelmiä hyödyksi hyökkääjän tavoitteen saavuttamiseksi. Tällaisia voi olla esimerkiksi iskun tekeminen yhteiskunnan tai yritysten toiminnoille tärkeisiin tietoverkkoihin ja haitan aiheuttaminen vaikkapa vedenjakelujärjestelmiin (Malkki & Paastela 2007, 68). Kyberterrorismi on 2000-luvun alusta asti ollut uusi uhka kansalliselle ja kansainväliselle turvallisuudelle. Nykypäivänä lähes jokaisen yhteiskunnan palvelun toimintaan liittyy internet tavalla tai toisella ja uhka on vakava, koska yhteiskunta on hyvin riippuvainen tietokonejärjestelmistä ja internetistä (Council of Europe Publishing 2007, 7). Tämä mahdollistaa terroristeille uusia tapoja tehdä terrori-iskuja ja ennen kaikkea nopeasti ja laajasti. Mikäli terroristit pääsevät käsiksi yhteiskunnan tietoverkkoihin ja –järjestelmiin, voi terrori-iskujen aiheuttamat vahingot nousta äärimmäisen suuriksi. Lisäksi terroristien kaipaama julkisuusarvo nousee. Vuonna 1991 ilmestyneessä kirjassa ”*Computers at Risk*” väitettiin, että ”*tämän päivän terroristi kykenee*

aiheuttamaan enemmän haittaa näppäimistöllä kuin perinteisellä terroristipommilla". Tämä väite on esitetty yli 25 vuotta sitten, joten 2010-luvulla kyberterrorismi on hyvinkin varteenotettava vaihtoehto perinteisille terrori-iskuille. (Puistola & Herrala 2006, 147–148.)

Terroristijärjestöt kehittyvät, joten kyberympäristössä toimiminen on monista syistä uuden ajan terroristeille houkutteleva osa-alue. Kyberterrorismi on huomattavan halpaa ja terrori-iskun toteuttamiseen ei periaatteessa tarvita muuta kuin tietokone ja internetyhteys. Verkon välityksellä toteutettujen iskujen anonymiteetti on huomattavasti helpompi säilyttää kuin perinteisien pommi-iskujen toteuttamisessa. Vaikka tietoverkoissa tapahtuneista tapahtumista jää helposti jälki, jota viranomaiset voivat seurata, on se kuitenkin myöhäistä jo iskun tapahduttua. Jäljet ovat myös huomattavasti helpompi peittää kuin perinteisien terrori-iskujen toteuttamisessa.

Tietoverkkojen välityksellä tapahtuva toiminta mahdollistaa terrori-iskun toteuttamisen myös ilman välitöntä läsnäoloa. Terroristi voi tehdä iskun toiselta puolelta maapalloa pelkästään istuessaan tietokoneensa ääressä. Lisäksi tietokoneiden välityksellä tehdyn terrori-iskun kohteiden määrä voi olla erittäin suuri. Kyberterroristit voivat hyökätä esimerkiksi valtioiden, suurten yritysten tai vaikkapa yksityisten lentoyhtiöiden kimppuun. Vaikka tietojärjestelmät pyritään suojaamaan mahdollisimman hyvin, löytyy useiden kohteiden joukosta myös kohteita, joissa tietoturva ei ole ajan tasalla. Edellä mainittujen lisäksi kyberterrorismi voi nostaa uhrien määrän aivan uudelle tasolle, koska voidaan hyökätä moniin kohteisiin yhtäaikaisesti. Kyberterrorismilla pystytään luomaan myös huomiota herättäviä uhkakuvia. (Weimann 2015, 152–154.)

3.1 Informaatiosodankäynti ja kyberterrorismi

Informaatiosodankäynti ja kyberterrorismi ovat eri asioita. Kyberterrorismi voi olla informaatiosodankäyntiä, mutta informaatiosodankäynti ei välttämättä ole kyberterrorismia. Informaatiosodankäynnin tarkoituksena on sekoittaa perinteisiä fyysisiä sodankäynnin keinoja sekä virtuaalimaailmaa toisen valtion, organisaation tai muun tahon toimimiseksi halutulla tavalla ja samalla estää toiminta toisinpäin. Informaatiosodankäynti koostuu kuudesta osa-alueesta:

1. Psykologisista operaatioista, joiden tarkoituksena on vaikuttaa propagandalla vihollisen toimintaan ja tunteisiin.
2. Elektronisesta sodankäynnistä, jonka tarkoituksena on tuottaa informaatiota tai väärää informaatiota viholliselle. Voidaan käyttää myös perinteisen median kautta.
3. Sotilaallisesta harhauttamisesta, jonka tarkoitus on antaa vastapuolelle väärää tietoa sotilaallisesta toiminnasta.
4. Fyysisestä informaatiosodankäynnistä, jonka tarkoitus on fyysinen hyökkäys informaatiojärjestelmiä vastaan.
5. Turvallisuustoimenpiteistä, joilla varmistetaan omien järjestelmien toimiminen.
6. Informaatiohyökkäyksistä, joiden tarkoitus on tuhota vihollisen tietojärjestelmistä tietoa.

Kyberterrorismi on tarkkaan harkittu poliittisesti tai ideologiapohjaisesti perusteltu hyökkäys tai uhkaus hyökkäyksestä sellaisia tietojärjestelmiä, tietokonejärjestelmiä, tietokoneohjelmia tai dataa kohtaan, jolla voidaan aiheuttaa väkivaltaa siviilikohteita vastaan. (Taylor ym. 2006, 19–20.)

Kyberterrorismi voidaan jakaa neljään osa-alueeseen:

1. Infrastruktuuria kohtaan tehtyihin iskuihin, joiden tarkoitus on tuottaa tuhoa kriittistä infrastruktuuria vastaan.
2. Informaatiohyökkäyksiin, joiden tarkoitus on vaikuttaa kohteen tietojärjestelmiin muun muassa tuhoamalla niiden sisältämää tietoa.
3. Internetin käyttöön terrori-iskun suunnittelemiseen ja toteuttamiseen.
4. Terroristiorganisaation kehittämiseen, jonka tarkoituksena on rahoittaa, yhdistää ja rekrytoida terroristeja. (Taylor ym. 2006, 22–29.)

3.2 Infrastruktuuria kohtaan tehdyt terrori-iskut

Infrastruktuuri on 2000-luvun alusta alkaen ollut hyvin pitkälti tietokoneriippuvaista lähes kaikkialla maailmassa, sillä lähes jokainen järjestelmä toimii tietotekniikan varassa. Mikäli tietotekniikka jostain syystä lakkaa toimimasta, on todennäköistä, että koko järjestelmän toiminta kaatuu. Tällöin tietotekniikkainfrastruktuuria vastaan tehty isku voi olla houkutteleva kohde terroristeille. Onnistunut terrori-isku tietoinfrastruktuuria kohtaan aiheuttaisi

laajat taloudelliset tappiot, kun monet yhteiskunnan toiminnot lakkaisivat. Infrastruktuuri pitää sisällään monia elintärkeitä osa-alueita, kuten viestiliikennejärjestelmät, pankki- ja talousjärjestelmät, sähkön-, öljyn-, kaasunjakojärjestelmät, vedenjakelu- ja kuljetusjärjestelmät, hätäpalvelut ja valtion toiminnot. Näistä monet ovat vielä sidoksissa toisiinsa, joten yhden kaatuminen saattaa aiheuttaa myös muiden toimintojen kaatumisen. Lisäksi järjestelmien jatkuva kehitys tuo haasteita turvallisuusohjelmistoille ja niiden pysymiseen ajan tasalla. Tällöin löytyy jatkuvasti turvallisuusaukkoja, joita voidaan käyttää hyväksi. (Weimann 2015, 158.)

Pankki ja talousjärjestelmät sekä sosiaali- ja terveydenhuollon järjestelmät ovat haavoittuvaisia kyberterrori-iskuille, koska ne ovat pitkälti tietoverkkojen varassa ja tietoa liikkuu koko ajan huomattavia määriä. Näistä järjestelmistä useat ovat irrallisia muista järjestelmistä, mutta joka tapauksessa niiden kaatuminen aiheuttaisi suuria taloudellisia tappioita. Pahimmassa tapauksessa sosiaali- ja terveydenhuollon järjestelmien kaatuminen voi aiheuttaa uhkaa hengelle ja terveydelle. (Sisäministeriö 2017, 19.)

Sähkön- ja vedenjakelujärjestelmien kaatuminen vaikuttaisi välittömästi useisiin ihmisiin. Nämä järjestelmät toimivat pitkälti tietokoneilla ohjatun tekniikan, kuten esimerkiksi erilaisten sensoreiden ja mittareiden varassa. Näitä ohjaaviin tietokoneisiin käsiksi pääseminen verkkoyhteyden kautta on mahdollista ja on samalla riski järjestelmän toiminnan kannalta. Näiden tietokoneiden lamaannuttaminen voisi kaataa järjestelmät välittömästi. Hyvin toteutetun hyökkäyksen johdosta vian löytäminen saattaisi kestää pitkään. Vaikka tietokoneisiin ei päästäisikään käsiksi ulkopuolelta, riskin yhtälöön tuovat sellaiset työntekijät, joilla on ollut ennen mahdollisuus päästä käsiksi näihin järjestelmiin. Näiden työntekijöiden erikoisosaaminen ja manipulointi voivat antaa hyökkääjille lisää mahdollisuuksia.

Huoli liikenneinfrastruktuuria kohtaan toteutettuihin hyökkäysiin on kasvanut etenkin vuoden 2001 syyskuun 11. päivän tapahtumien johdosta. Lisääntynyt liikenne on saanut osakseen korkeatasoista tekniikkaa, jolla on kyetty parantamaan liikenneturvallisuutta. Etenkin ilmaliikenteessä tietokoneet ohjailevat monia turvallisuuden kannalta oleellisia järjestelmiä. Tietokoneiden tekemät virheet voivat olla kohtalokkaita usealle ihmiselle. Lentoliikennettä valvovia järjestelmiä vastaan hyökkääminen tietokoneiden avulla on mahdollista. Lentokoneille voidaan syöttää väärää tietoa muun muassa lentokorkeuksista ja muusta lentoliikenteestä. Toki nämä on pyritty ottamaan huomioon ja tämän takia on useita varajärjestelmiä, jotka toimivat itsenäisesti pääjärjestelmästä ja ovat hyvin suojattuja. Ongelmana

on kuitenkin näiden järjestelmien riippuvuus muusta infrastruktuurista, kuten sähköverkostosta ja viestiliikennejärjestelmistä. (Taylor ym. 2006, 22–23.)

Varsinkin Yhdysvalloissa edellä mainittuihin kohteisiin on tehty vuosien varrella useitakin iskuja, mutta mikään terroristiorganisaatio ei ole ilmoittautunut ottaneensa vastuuta iskuista. Iskut eivät ainakaan vielä ole tuottaneet suuria tappioita, mutta esimerkiksi vuonna 1997 teini-ikäinen hakkeri pääsi käsiksi Yhdysvalloissa sijaitsevan lentokentän puhelintoimintoihin ja sai kuudeksi tunniksi järjestelmän pois käytöstä. Isku ei aiheuttanut henkilövahinkoja, mutta useiden lentojen myöhästyminen aiheutti suuret taloudelliset tappiot useille lentoyhtiöille. Toinen esimerkki Yhdysvalloissa tehdystä iskusta on Chevron entisen työntekijän luvaton tunkeutuminen yhtiön tietojärjestelmiin, joka aiheutti tehtaan haitallisten kemikaalien pääsyn ilmastoon. Tapahtuma vaaransi miljoonien ihmisten terveyden Yhdysvaltojen länsiosissa ja Kanadassa. Edellä mainitut esimerkit ovat yksityisten toimijoiden aikaansaamia tapahtumia. Tällaisten tapahtumien takana voisi hyvinkin olla ideologiaan tai politiikkaan perustuva terrori-isku. (Taylor ym. 2006, 23–24.)

Terrori-iskut infrastruktuuria kohtaan voivat olla vaikutuksiltaan vakavia. Lentoliikenteen valvontajärjestelmiä häiritsemisellä voidaan saada esimerkiksi kaksi konetta törmäämään toisiinsa aiheuttaen suuren onnettomuuden. Sairaalan sähköisiin järjestelmiin tunkeutuminen ja potilaille annettavien annoskokojen muuttaminen voisi aiheuttaa useita potilaskuolemia. Junaliikenteen tietokonejärjestelmien sekoittaminen voisi aiheuttaa junien törmäämisen, missä pahimmillaan kuolee satoja ihmisiä tai tulee suuria ympäristövahinkoja. Terroristien mahdollisuudet ovat melko laajat ja kyseessä ovat kuitenkin vain tietokoneilla tehtävät toimenpiteet. Yksi pelottavimpia ongelmia on myös se, että emme välttämättä edes tiedä, mitä kaikkea tietokoneilla voidaan tehdä. (Taylor ym. 2006, 23–24.)

3.3 Informaatiohyökkäykset

Tietoverkot mahdollistavat terroristeille myös terrori-iskujen toteuttamisen verkon välityksellä. Niiden välityksellä voidaan päästä käsiksi moniin tietokoneisiin, jotka ovat yhteydessä yhteiskunnan eri toimintoihin. Esimerkiksi kriittisen infrastruktuurin häiritseminen, pörssikurssien manipuloiminen tai valtioiden salaisuuksien paljastaminen ovat teoriassa mahdollista tehdä tietokoneiden välityksellä. Toistaiseksi kuitenkin terroristit ovat käyttäneet tietoverkkoja vain propagandansa levittämiseen sekä kommunikaatioon, mutta tieto-

verkkojen välityksellä tehtävät terrori-iskut voivat olla tulevaisuudessa terroristien uusi tapa toimia. (Weimann 2015, 23.)

Terrorismissa tietoverkkojen hyväksikäyttö on suhteellisen uutta. Tietoverkkojen käyttö vaatii ammattitaitoa, joita terroristeilla ei välttämättä ole. On kuitenkin tapauksia, jossa terroristiorganisaatiot ovat ostaneet hakkereilta palveluita, joiden pohjalle tulevia iskuja on suunniteltu. (Puistola & Herrala 2006, 157.)

3.3.1 Verkkohyökkäykset

Verkkohyökkäyksellä (tai kyberhyökkäyksellä) voidaan tuottaa huomattavia taloudellisia tappioita. Pelkästään tietokonevirukset aiheuttivat vuonna 2000 maailmanlaajuisesti noin 17 miljardin dollarin kustannukset. Taloudellinen vaikutus huomataan välittömästi, mikäli jotkut yhteiskunnan toiminnot ja palvelut eivät toimi. (Puistola & Herrala 2006, 152.)

Toteutustapoja verkkohyökkäyksille on monia. Tavallisimmin vahinkoa voidaan aiheuttaa muokkaamalla jo tallennettua tietoa eli dataa siten, että sitä ei voida välttämättä enää sellaisenaan käyttää. Data voidaan myös tuhota kokonaan tai muuttaa sellaiseksi, että alkuperäiset käyttäjät eivät voi sitä enää löytää. Tiedon saatavuus on nykyään edellytys lähes kaikille toiminnoille. (Puistola & Herrala 2006, 151–152.)

Tutkittaessa verkkohyökkäyksiä on huomattu, että ne tehdään yleensä viisivaiheisella toimintaperiaatteella. Ensimmäisessä vaiheessa kyse on kohteen tiedustelusta, jonka aikana kohteesta pyritään selvittämään heikkoja kohtia muun muassa kohteen järjestelmiin tunkeutuen. Ensimmäisen vaiheen tarkoitus on luoda pohjaa tulevalle hyökkäykselle. Toisessa vaiheessa on tarkoitus selvittää mitä ohjelmistoja kohteessa käytetään ja ohjelmistojen aukkojen avulla mahdollisuuksia tunkeutua järjestelmiin. Lisäksi voidaan pyrkiä murtautumaan kohteen langattomiin verkkoihin ja niitä kautta edetä tietokoneille. Kolmannessa vaiheessa hyökkääjä pyrkii luomaan oman tilin kohteen tietoverkkoihin tai asentamaan haittaohjelmistoja kohdejärjestelmään. Haittaohjelmat aktivoituvat erikseen, kun hyökkäys aloitetaan. Neljännessä vaiheessa hyökkääjä pyrkii asentamaan järjestelmiin takaportteja, joilla päästään järjestelmiin käsiksi koska tahansa. Tavoitteena hyökkääjällä on luoda itselleen järjestelmänvalvojan oikeudet. Tällöin voidaan jo saada aikaan huomattavaa vahinkoa. Viimeisessä vaiheessa hyökkääjä pyrkii peittämään omat jälkensä niin, että häntä ei

voida yhdistää tapahtuneeseen. Jälkien peittely mahdollistaa toiminnan jatkamisen myös tulevaisuudessa, mikäli niin halutaan. (Puistola & Herrala 2006, 162–164.)

Yhteiskunnan kriittisiä järjestelmiä, kuten puhelin- ja verkkojärjestelmiä voidaan myös häiritä verkkohyökkäyksillä. Varsinkin Yhdysvalloissa yleinen 911-hätäpuhelujärjestelmä on ollut usein verkkohyökkäyksien kohteena (Puistola & Herrala 2006, 153). Vuonna 2016 Lappeenrannassa verkkohyökkäyksellä katkaistiin kahdesta kerrostalosta lämmitys (Helsingin Sanomat 7.11.2016).

Pankkijärjestelmät ovat yleisiä verkkohyökkäyksen kohteita. Pankkien tileille on päästy tunkeutumaan ja niiden kautta on siirretty miljoonia dollareita. Useiden hyökkäysten selvittäminen on ollut haasteellista, eikä niiden tekijöitä ole pystytty selvittämään. (Puistola & Herrala 2006, 153–154.)

Monet järjestelmät toimivat nykypäivänä hyvin pitkälti tietokoneiden varassa. Tietotekniikka ohjaa jollain asteella lähes jokaista prosessia mitä ihmiskunta tarvitsee. Jokapäiväisiin toimintoihin saadaan nopeutta ja varmuutta hyödyntämällä tietotekniikkaa, jonka käytössä on myös riskinsä. Tietotekniikkaa vastaan voidaan hyökätä monella eri tavalla. Serverikeskukset ovat tietokoneiden keskittymiä ja niiden tuhoaminen voi lamaannuttaa hyvin monen järjestelmän toiminnan. Tietokoneiden lamaantumisen voi saada aikaan fyysisellä tuhoamisella tai sähkömagneettisella pulssilla, joka ylikuormittaa virtapiirin ja siten tuhoaa sen. Myös tietokoneiden ohjelmistokoodeja voidaan muuttaa tai sabotoida, jolloin tietokone tekee eri toimintoja mitä sen on alun perin tarkoitettu tehdä. Kyberterrorismissa kyse on yleensä siitä, että tietokoneen toimintatapaa muutetaan. (Weimann 2015, 155–156.)

3.3.2 Palvelunestohyökkäykset

Palvelunestohyökkäykset (Denial of Service, DoS) ovat yleinen kyberterrorismin menetelmä. Hyökkäyksen idea on lamaannuttaa palvelu niin, että sitä ei ole enää saatavilla. Muihin verkkohyökkäyksiin nähden palvelunestohyökkäyksen tarkoitus ei ole tunkeutua palveluun ja hakea sieltä luvattomasti tietoa, vaan häiritä palvelua ja sen toimintaa. Yleisiä tapoja tehdä palvelunestohyökkäyksiä on häiritä www-palvelun toimintaa niin paljon, etteivät asiakkaat voi käyttää palvelua. Toinen yleinen tapa on lähettää sähköpostiviestejä kohteelle niin paljon, ettei tämä voi käyttää sähköpostiaan enää levytilan loppumisen takia.

Palvelunestohyökkäys voidaan toteuttaa myös useista eri lähteistä samanaikaisesti. Tällöin kyseessä on hajautettu palvelunestohyökkäys (Distributed Denial of Service, DDoS). (Puistola & Herrala 2006, 161.)

Palvelunestohyökkäyksellä pyritään vaikuttamaan tietojen saatavuuteen, jolloin tietojen käyttö vaikeutuu tai niitä ei voida käyttää ollenkaan. Usein palvelunestohyökkäyksissä käytetään kaapattuja tietokoneita, heikosti suojattuja laitteita tai väärin määritettyjä palvelimia, jotka välittävät väärää liikennettä. Yleisin tapa tehdä palvelunestohyökkäys on kohdistaa verkkopalveluun huomattavan paljon liikennettä. Kun internetselaimeen kirjoitetaan haluttu osoite, lähettää tietokone tietoa kyseiselle palvelimelle. Palvelunestohyökkäyksessä tämä tehdään useita kertoja pienen ajan sisällä, jolloin tietoa vastaanottavan palvelimen rajoitettu kapasiteetti täyttyy ja palvelun käyttö estyy, koska se ei voi vastata palvelua käyttävän tietokoneen pyyntöihin. Tietokoneet hyökkääjä yleensä saa käyttöönsä kaappaamalla. Hajautetussa palvelunestohyökkäyksessä hyökkääjä on voinut saada tietokoneet käyttöönsä esimerkiksi saastuneiden sähköpostien välityksellä.

Palvelunestohyökkäyksen ja hajautetun palvelunestohyökkäyksen kohteeksi joutumista ei voi omalla toiminnallaan vaikuttaa. Kuitenkin oman tietokoneen joutumisen todennäköisyyttä yhdeksi hyökkääjän käyttämistä koneista voi vähentää pitämällä tietokoneen tietoturvaa käsittelevät ohjelmat ajan tasalla. Etenkin hajautetuissa palvelunestohyökkäyksissä yksittäisten tietokoneiden tietoturvan ylläpitäminen on keskeisessä asemassa. Palvelunestohyökkäyksen kohteeksi joutumista ei välttämättä huomaa mitenkään. Erilaisten palveluiden sivut voivat olla esimerkiksi huoltokatkon ajan pois käytöstä, joten kaikki katkokset eivät tietenkään johdu palvelunestohyökkäyksistä. Palvelunestohyökkäykseen viittaavia tekijöitä ovat poikkeuksellisen hidas internetyhteys sivulle, tietyn internetsivun toiminnan lakkaaminen tai sivulle pääsy on estynyt tai sitten huomattavasti lisääntynyt roskapostin saaminen sähköpostijärjestelmiin. (USA Department of Homeland Security 2013.)

Vuonna 2007 Viron hallituksen tietokoneet olivat laajan verkkohyökkäyksen kohteena. Hyökkäys toteutettiin palvelunestohyökkäyksenä, joka lamaannutti useita verkkopalveluita. Palvelunestohyökkäys nimensä mukaisesti estää hyökkäyksen kohteena olevan palvelun käytön. Viron hyökkäyksen kohteena olivat hallituksen sekä kahden suuren pankin internetsivustoja. Hyökkäyksen tekijästä ei ole tietoa. On esitetty spekulaatiota, että Venäjä olisi ollut hyökkäyksen takana, mutta mitään todisteita Venäjän osallisuudesta ei ole. (Weimann 2015, 155.)

3.3.3 Botnet

Botnet:lla tarkoitetaan joukkoa tietokoneita, jotka ovat kaapattu haittaohjelman avulla ja joita voidaan käyttää etänä verkon välityksellä. Kaapattuja tietokoneita voi olla tuhansia ja niitä voidaan käyttää samanaikaisesti kyberhyökkäyksessä tiettyä kohdetta vastaan häiritsemällä tai estämällä kohteen internetyhteyttä. Botnet-tietokoneita voidaan käyttää hajautetuissa palvelunestohyökkäyksissä, levitettäessä roskapostia, haittaohjelmia tai muun organisoidun rikollisuuden tai kyberterrorismin toiminnassa. Lisäksi kaapattuja tietokoneita voidaan käyttää kriittistä infrastruktuuria vastaan tehtyihin kyberhyökkäyksiin, jotka voidaan toteuttaa internetin välityksellä. Botnet-tietokoneet toimivat kyberterrorismissa myös propagandan levittämisessä. Ne ovat terroristeille helppo tapa toteuttaa kyberterrorismia, koska he voivat ostaa jo valmiiksi kaapattuja koneita kyberrikollisilta. Yhdysvaltain liittovaltion poliisin (Federal Byrou of Investigation, FBI) mukaan Botnet-hyökkäykset ovat maksaneet Yhdysvalloille miljoonia dollareita. (Weimann 2015, 156–157.)

3.3.4 SCADA-järjestelmät

SCADA (Supervisory Control And Data Aqcuisiton), eli valvontajärjestelmät, ovat potentiaalisia kyberterrorismin kohteita. SCADA-järjestelmät ovat tietokonejärjestelmiä, jotka valvovat ja hallitsevat teollisuus-, infrastruktuuri-, ja laitospohjaisia prosesseja. SCADA-järjestelmät valvovat esimerkiksi vedenjakelua, kaasunjakelua, jäteveden puhdistamisjärjestelmiä ja monia muita järjestelmiä, jotka toimivat yhteiskunnan eduksi. Mikäli näihin järjestelmiin päästään käsiksi, voidaan niiden toimintatapoja muuttaa. Tällöin SCADA-järjestelmien valvomiin kohteisiin voidaan päästä vaikuttamaan myös terroristisella tavalla ja niiden väärinkäyttö voi aiheuttaa vaaraa yhteiskunnalle esimerkiksi sähkönjakelun keskeytymisellä. (Weimann 2015, 157–158.)

3.4 Terrorismi ja internet

Ennen internetiä terroristiryhmät joutuivat järjestämään tapaamisiaan, rekrytointilaisuuksiaan ja iskujen valmisteluita erikseen valituissa paikoissa, esimerkiksi kouluissa. Syyskuun 11. päivän iskujen jälkeen terrorismin vastaiset toimenpiteet kohdistuvat hyvin tehokkaasti paikkoihin, joissa terroristeja uskottiin olevan. Tämä johti terroristien toiminnan salaamiseen ja internet tarjosi siihen hyvät keinot. (Weimann 2015, 128.)

Internet on mullistanut maailmaa alkuajoistaan lähtien. Internet tuo ihmiskunnalle hyviä työkaluja muun muassa tiedon etsimisen ja jakamisen suhteen. Myös terroristit ovat oppineet tämän ja käyttävät internetin luomia mahdollisuuksia häikäilemättömästi hyväkseen. Syyskuun 11. päivän iskujen tutkinta on osoittanut, että terroristit ovat hyödyntäneet internetiä muun muassa etsimällä tietoa yhdysvaltalaisista lentokouluista, lentojen aikatauluista ja käyttäneet internetin palveluita koordinoidakseen iskuja. Internet on mahdollistanut nopean tiedonsiirron sekä maailmanlaajuisen viestinnän.

Internet avaa terroristeille uusia mahdollisuuksia myös kommunikoinnin suhteen. Terroristit kommunikoivat verkon välityksellä toisilleen sekä myös muulle maailmalle (Council of Europe Publishing 2007, 35). Verkon välityksellä tapahtuvaa kommunikaatiota on oikeinsalattuna lähes mahdotonta seurata. Verkossa tapahtuvan toiminnan salaaminen on mahdollista yksinkertaisilla keinoilla ja salausten purkaminen vie aikaa. Tämä antaa verkkoa väärinkäyttäville tahoille mahdollisuuden toimia anonyymeinä pitkiäkin aikoja. Lisäksi terroristiorganisaatioilla on omia internetsivustoja, joilla ne pyrkivät levittämään propagandaansa sekä tiedottamaan jäseniään. Sivustot tarjoavat myös mahdollisuuden uusien iskujen suunnittelemiseen ja toteuttamiseen. Terrorismin suhteen internet tuo lukuisia etuja kommunikoinnin lisäksi. Internetissä on helppo esiintyä anonyyminä, jolloin kiinnijäämisen riski pienenee huomattavasti.

Erilaisia internetissä olevia alustoja käyttämällä terroristit ovat saaneet levitettyään omaa propagandaansa myös niille, jotka eivät suoraan vieraile terroristiorganisaatioiden ylläpitämillä internetsivustoilla. Esimerkiksi sosiaalisen median sivustot, videonjakosivustot sekä verkkoyhteisöt ovat olleet paikkoja, jossa terroristit ovat saaneet houkuteltua sivullisia toimintaansa mukaan. (Weimann 2015, 19–20.)

Terrorismin psykologinen vaikutus on huomattava ja internetissä laajan yleisön huomion saaminen on helppoa. Terroristit voivat julkaista uhkauksen terrori-iskun suorittamisesta internetin välityksellä, jolloin uhkaus tavoittaa tuhansia ihmisiä välittömästi. Lisäksi internetissä voidaan julkaista raakoja kuvia tai videopätkiä terroristien toiminnasta. Al-Qaida on väittänyt jatkuvasti syyskuun 11. päivän iskujen vaikuttaneen myös Yhdysvaltain ekonomiaan muun muassa dollarin kurssin heikkenemisenä. Vaikka tämä ei pitäisikään paikkaansa, silti monet ihmiset ovat propagandan kohteena eivätkä välttämättä saa tietää totuutta koskaan. (Weimann 2015, 24.)

Terroristiorganisaatiot levittävät myös suuren määrän propagandastaan internetin välityksellä. Terroristit kertovat ideologiastaan ja perustelevat tekemänsä iskut poliittisilla tai uskonnollisilla syillä. Internetissä on mahdollista myös vaikuttaa tiettyyn yleisöön, jolloin saadaan kommunikoitua lähinnä sellaisten henkilöiden kanssa, kenelle viesti halutaan välittää. Tällöin terroristit voivat saada propagandansa lisäämään yleisön mielenkiintoa terrorismia kohtaan.

Internetin käyttö terroristien rekrytoinnissa ja koulutuksessa on arkipäivää. Moni Euroopassa, Pohjois-Afrikassa ja Lähi-Idässä tehdyn terrori-iskun tekijät ovat saaneet mielenkiintonsa ja koulutuksensa terrorismin suhteen internetin välityksellä. Al-Qaida on pyrkinyt radikalisoimaan lapsia muun muassa videopelien sekä piirrettyjen avulla. Tavoitteena on ollut kasvattaa pienestä asti lapsiin Al-Qaidan ideologiaa. (Weimann 2015, 28.)

Internetin palveluista on myös saatavana hyvin paljon tietoa eri kohteista. Terroristit käyttävät saamiaan tietoja iskujen suunnittelun apuna. Esimerkiksi palestiinalainen terroristijärjestö Hamas on käyttänyt Google Earth-palvelun tarjoamia satelliittikuvia raketti-iskujensa kohdentamiseen. (Weimann 2015, 29.)

Vaikka internetissä on mahdollista julkaista lähes mitä tahansa, on terroristienkin toimintaa kyetty vaikeuttamaan sulkemalla terroristisia internetsivustoja ja yhteisöjä. Tämän takia terroristit ovat pyrkineet siirtymään eteenpäin internetissä ja yrittävät löytää uusimpia alustoja joilla toimia. Näitä ovat tänä päivänä erilaiset sosiaalisen median palvelut. (Weimann 2015, 145.)

3.4.1 Sosiaalinen media terrorismin tukena

Sosiaalinen media koostuu palveluista, joissa ihmiset voivat jakaa kuvia, videoita, ideoita ja ajatuksia toistensa kanssa. Se on tehokas tapa pitää yhteyttä henkilöiden välillä, koska se rakentuu sellaiselle teknologialle, mitä voidaan käyttää tietokoneella sekä mobiililaitteilla kuten kännykällä ja tabletilla. Sosiaalinen media yhdistää ihmisiä entistä tehokkaammin ja lähes reaaliajassa. Yleisimpiä sosiaalisen median palveluita, joita terroristijärjestöt käyttävät, ovat Facebook ja YouTube. Perinteiseen mediaan verrattuna sosiaalinen media tavoittaa halutun yleisön nopeammin ja se antaa mahdollisuuden kelle tahansa julkaista lähes mitä tahansa. Terroristit ovat myös huomanneet tämän ja käyttävät sosiaalista mediaa hy-

väkseen, joten suunnitelmien ja iskujen paljastimen on suuren tietomäärän vuoksi haastavaa (Weimann 2015, 18).

Terroristit käyttävät sosiaalista mediaa kolmesta eri syystä. Ensinnäkin, se on ylivoimaisesti paras paikka saada huomiota. Toiseksi se tarjoaa ilmaiseksi palvelut, joiden kautta voidaan propagandaa levittää. Kolmanneksi se mahdollistaa yleisön tavoittamisen paremmin kuin perinteiset terroristiorganisaation omat internetsivustot. Lisäksi terroristit kohdistavat propagandansa mielellään nuoriin henkilöihin, joita sosiaalinen media enemmän koskettaa. Henkilöt, jotka ovat kiinnostuneet tietyistä asioista, kohtaavat helpommin toisensa sosiaalisen median välityksellä. Näin on myös laittomien asioiden kuten terrorismin suhteen. (Weimann 2015, 128.)

Yhdysvaltain kotimaan turvallisuusosaston (United States Department of Homeland Security) 2010 julkaiseman raportin mukaan terroristit käyttävät Facebook –palvelua seuraaviin tarkoituksiin:

- Operatiivisen ja taktisen tiedon, kuten pommiohjeiden, aseiden käsittelyn ja taktisen ammunnan, jakamiseen.
- Porttina ekstremismiin liittyvien internetsivujen ja muun radikaalin sisällön jakamiseen internetin välityksellä.
- Tiedustelutiedon jakamiseen.

Tiedustelutiedon jakamisen suhteen terroristit ovat muun muassa tarkkailleet yhdysvaltalaisia korkean tason sotilaita ja jakaneet näiden tietoja toisilleen. (Weimann 2015, 133.)

3.5 Vastatoimet

Kuten perinteisenkin terrorismin, niin myös kyberterrorismin torjunnassa, on kyse monen eri tahon yhteisestä tavoitteesta. Terrorismiin vastaaminen ei ole pelkästään poliisin tai puolustusvoimien tehtävä, vaan myös valtion muiden elimien sekä yksityisen sektorin panos on tärkeä. Terroristit hyökkäävät haavoittuvimpiin kohteisiin. Näin ollen myös kyberterrorismilta suojautuminen perustuu järjestelmien haavoittuvuuksien löytämiseen ja niiden tukkimiseen. Mikäli näiden järjestelmien käyttäjät eivät ole tietoisia järjestelmiensä haavoittuvuuksista, ei niitä myöskään kyetä korjaamaan. (Ozeren 2009, 30.)

Kyberterrorismin vastaiset toimet voidaan jakaa eri tavoilla. Ensimmäinen lähestymistapa on parantaa kansallisella tasolla koulutusta kyberturvallisuuden osalta, tarkastella ja arvioida muiden maiden toimintaa kyberympäristössä, pitämällä oma osaaminen ajan tasalla, kehittämällä tapoja torjua kyberhyökkäyksiä, vähentämällä järjestelmien riippuvuutta toisistaan ja rakentamalla enemmän itsenäisiä tietoverkkoja. Tällöin haasteena on yhtenevän ja globaalin teknologian käytön rajoittaminen vain kansalliselle tasolle. Hyvänä puolena on omavaraisuus ja riippumattomuus muiden maiden toiminnasta kyberterrorismin torjunnassa. Toinen lähestymistapa on yhteistyötä kannattava tapa, jolloin kansainvälinen yhteistyö on keskeisessä roolissa. Kansainvälisyys kuitenkin tuo myös terroristeille uusia mahdollisuuksia toimia. Vaikka yhteistyö on tehokas vaihtoehto terroristijärjestöjä vastaan, avaa se myös mahdollisuuden valtioiden harjoittamalle terrorismille. Tämän takia kansainvälinen yhteistyö on myös haastavaa. Lisäksi tilanne muuttuu epäedulliseksi niiden valtioiden kohdalla, joilla on enemmän menetettävää mahdollisen yhteistyön ja tiedon jakamisen väärinkäytön seurauksena. Kyberterrorismi on valtioiden rajat ylittävää toimintaa internetissä, joten kyberterrorismin torjunnan suhteen kansainvälinen yhteistyö on määritettävä tarkasti, koska kaikissa maissa ei päde samat lait. Kansainvälisen yhteistyön lisääminen tuo riskejä haavoittuvuuksien suhteen, mutta kustannukset ovat pienemmät. (Ozeren 2009, 53–55.)

Toisen näkökulman mukaan iskut pyritään estämään suojelemalla järjestelmiä ja pyrkimällä vaikuttamaan järjestelmien käyttöön terroristeilta. Järjestelmissä olevia haavoittuvuuksia voidaan myös vähentää, jolloin kyberhyökkäystä ei kyetä toteuttamaan. Kyberhyökkäykset voidaan estää myös tehokkaalla tutkinnalla ja viranomaistoiminnalla. Tällöin verkkoa on seurattava ja sieltä on löydettävä kyberterrorismiin viittaavaa materiaalia tai toimintaa, jonka perusteella vastatoimet voidaan toteuttaa. (Ozeren 2009, 55–56.)

Kyberhyökkäykseen vastaaminen on moniulotteinen ongelma. Tapa, jolla hyökkäys toteutetaan, määrittää sen, miten siihen vastataan. Kyberhyökkäys voitaisiin joissain tilanteissa rinnastaa sotilaalliseen hyökkäykseen, jolloin sotilaallisen voiman käyttäminen olisi perusteltua. Ongelmana on kuitenkin sotilaallisen voiman käytön perusteleminen kyberhyökkäyksen aiheuttamilla vaikutuksilla. Lisäksi kyberhyökkäyksen tehneen tahon jäljittäminen on vaikeaa, joten sotilaallisen voiman kohdistaminen oikeaan suuntaan olisi riskialtista. Mikäli hyökkäys kyettäisiin selvittämään tietyn tahon toimenpiteeksi, olisi sotilaallisen voiman käyttäminen ehkä jopa perusteltua. Tällaisissa tapauksissa täydellisen varmuuden saaminen hyökkääjästä olisi joka tapauksessa hankalaa, eikä välttämättä täysin perustuisi faktoihin. Esimerkiksi Venäjän on väitetty vaikuttaneen vuoden 2016 Yhdysvaltain presi-

dentinvaalien lopputulokseen, jonka johdosta kybersota on saanut entistä enemmän julkisuutta. Tällaisen hyökkäyksen tutkinta on kuitenkin vaikeaa.

Kyberiskujen vaikutus on kuitenkin täysin erilainen kuin perinteisten sotilaallisten iskujen. Isku vaikuttaisi tietoverkoissa tapahtuvaan informaatioon, jolloin sen tuomitseminen on hankalampaa kuin perinteisen sotilaallisen iskun. Vaikka kyberisku voitaisiin yhdistää johonkin tiettyyn valtioon, sen tekijästä ei silti voida olla vielä varmoja. Esimerkiksi Venäjä käyttää kolmansia osapuolia kyberhyökkäyksen toimeenpanemisessa ja tällöin Venäjän valtion hallinto voi jäädä hyökkäyksen ulkopuolelle.

Mikäli kyberhyökkäyksen tehnyt taho kyettäisiin tunnistamaan, voitaisiin kybervastahyökkäys toteuttaa aiheuttamalla samanlainen vaikutus hyökkäyksen tehneelle osapuolelle. Tässä on kuitenkin ongelmana se, että vastapuolella ei välttämättä ole sellaista infrastruktuuria, johon saadaan samanlainen vaikutus aikaiseksi. (Chivis & Dion-Schwarz 2017.)

3.6 Tulevaisuuden näkymät

Tulevaisuuden ennustaminen ei ole koskaan varmaa tietoa. Tietotekniikan kehittyessä huikeaa vauhtia, ei kovin kattavia ennusteita voida edes antaa. Terroristiryhmät voivat tulevaisuudessa käyttää entistä enemmän hyväkseen tietoverkkoja ja niiden tuomia mahdollisuuksia tavoitteidensa saavuttamiseksi. Internetin käyttö nopeuttaa rekrytointia, mahdollistaa salatut yhteydenpidot, auttaa iskujen koordinoimisessa ja helpottaa iskujen toteuttamista tietokoneiden välityksellä entistä tehokkaammin. Al-Qaidan väitetään parantavan jatkuvasti kykyään toimia virtuaalimaailmassa, ja sen pelätään myös pyrkivän tiedemiesten avulla parantamaan mahdollisuuksiaan kyberiskujen tekemiseen. (Weimann 2004, 10–11.)

Tavanomaisemmat terrori-iskut, kuten autopommit, salamurhat, itsemurhapommitukset kidnappaukset ja kaappaukset eivät välttämättä ikinä tule korvatuiksi kyberterrorismilla, mutta kyberhyökkäykset voivat yhtä aikaisesti toteutettuna tehostaa terrori-iskun vaikutusta. (Ozeren 2009, 37–38.)

4 KYBERTERRORISMIN UHAT YHTEISKUNNAN TURVALLISUUDELLE

Tietokoneiden merkitys 2010-luvulla on yhteiskunnalle suuri myös turvallisuuden näkökulmasta. Yli 12 tunnin mittaiset sähkökatkot ja tietokoneiden toimintahäiriöt ovat osoittaneet lisäävän ryöstelyä ja tottelemattomuutta suurilla väestöalueilla kuten kaupungeissa. Tällaisen sähkökatkoksen estäminen on tietokonejärjestelmien varassa.

Useat tavanomaisimpien terrori-iskujen kohteet ovat 2000-luvun alusta alkaen olleet jollain tavalla tietokoneohjattuja. Tietokoneohjatut järjestelmät parantavat mahdollisten terrori-iskujen kohteiden suojausta ja ovat tällä tavalla terroristeille vaikeammin saavutettavissa. Kuitenkin tietotekniikan tuomat ominaisuudet yhteiskunnalle voivat olla osaltaan myös terroristeille avain uusiin mahdollisuuksiin. Esimerkiksi lentokoneen pudottaminen perinteisellä pommilla voi olla tiukkojen turvajärjestelyiden johdosta hyvinkin vaikeaa. Kuitenkin lentokoneiden tietokoneisiin vaikuttaminen voi antaa lentäjille väärää informaatiota koneen toiminnasta, jolloin lentäjä saattaa tehdä virheen reagoidessaan saamansa informaation johdosta. Lentokoneen korkeuden arvioiminen väärin vuoristoisessa ympäristössä voi olla kohtalokasta. Toki tietokonejärjestelmiin murtautuminen on haastavaa, mutta sitä ei kuitenkaan voida sulkea kokonaan pois.

Lisääntynyt teknologia esimerkiksi rakennusten lämmitysjärjestelmissä mahdollistaa järjestelmän ohjaamisen rakennuksen ulkopuolelta. Järjestelmän kaataminen keskellä talvea voisi aiheuttaa asukkaille huomattavia ongelmia jo muutamassa tunnissa. Lämmitysjärjestelmien tietokoneohjattujen järjestelmien ylikuormittaminen voisi aiheuttaa tulipalon, tai sen kytkeminen kokonaan pois päältä laskisi asuntojen lämpötilaa nopeasti. (Kushner 1998, 196–197.)

4.1 Uhan aiheuttajat

Kyberterrorismin toteuttaminen vaatii suuret resurssit. Resurssien suhteen suurimmat toimijat ovat valtiot. Valtiot voivat toimia kyberympäristössä tehokkaasti, koska ne rakentavat jatkuvasti parempaa kyberpuolustusta. Tällöin myös kybersodankäynnin tavat kehittyvät. Pienempien iskujen toteuttaminen on mahdollista myös terroristijärjestöjen tai hakkereiden toimesta.

4.1.1 Valtio ja kybervakoilu

Kyberympäristön merkitys kasvaa koko ajan ja kyberkeinoja voidaan käyttää poliittisten päämäärien saavuttamiseksi (Puolustusministeriö 2017). Toimiminen kyberympäristössä on osa monen valtion sotilaallista toimintaa. Vuosina 2005–2012 Yhdysvallat tekivät Israelin kanssa iskun Iranissa olleeseen ydinvoimalaan. Isku oli muista sotilasoperaatioista erillisenä toteutettu kyberhyökkäys ydinvoimalan hallintajärjestelmiin. Hyökkäys tehtiin Stuxnet-nimisellä haittaohjelmalla. Hyökkäyksen aikana tietokonevirus saastutti noin 100 000 tietokonetta yli 60 eri maassa. Viruksen tarkoitus oli tehdä fyysistä tuhoa Iranin Natanz:n ydinvoimalassa muuttamalla sen ohjausjärjestelmiä. Vaikka virus saastutti useita koneita, se ei kuitenkaan tehnyt mitään vahinkoa kuin vasta kohteessaan. Kohteessa se ohjelmoi järjestelmiä toimimaan sillä tavalla, että ne vahingoittuivat fyysisesti. Hyökkäyksen tarkoitus oli hidastaa Iranin ydinaseen rakentamista. Stuxnet on esimerkki siitä, miten valtiollinen toimija voi toteuttaa kyberhyökkäyksen. Tällaiset kyberhyökkäykset vaativat hyökkääjältä isot resurssit. Stuxnet:n toteuttaminen vaati laajamittaiset valmistelut muun muassa tiedustelun osalta, joita perinteinen terroristijärjestö ei olisi kyennyt tekemään. (Rid 2013, 43–46.)

Kybervakoilua toteuttavat sekä valtiot että yritykset. Kybervakoiluryhmät etsivät tietoa aineettomasta omaisuudesta, kansallisista salaisuuksista, liikesalaisuuksista, sotilaallisesta tiedosta sekä voivat vaikuttaa poliittisiin päätöksiin. Kybervakoilussa käytettävät keinot ja taidot kehittyvät jatkuvasti. Tästä johtuen puolustus myös kyberympäristöissä on pidettävä ajan tasalla. (Lehto ym. 2017, 19–20.)

4.1.2 Terroristijärjestöt

Stuxnet:n kaltaista iskua ei ole vielä toteutunut yhdenkään terroristijärjestön, kuten Al Qaida tai ISIL, toimesta. Kuitenkin kyberhyökkäykset kriittistä infrastruktuuria kohtaan voivat yleistyä terroristijärjestöjen kehittäessään omia tietoverkkotaitojaan. Mohammad Bin Ahmad As-Salim on julkaissut kirjan, joka kehottaa yksittäisiä tekijöitä aloittamaan ”*virtuaalisen jihadin*” eli virtuaalisen taistelun verkossa olevien keskustelualueiden kautta sekä tekemään verkkohyökkäyksiä erilaisia verkkosivuja vastaan. Lisäksi terroristijärjestöt ovat jatkuvasti kehittäneet kykyjään toimia kyberympäristössä. Toistaiseksi ihmishenkiä vaatinutta kyberterrori-iskua ei ole vielä tapahtunut. Onnistunut kyberhyökkäys voisi kuitenkin asettaa kansalaisten turvallisuuden kyseenalaiseksi. Esimerkiksi pankkijärjestelmän la-

maannuttaminen loisi yhteiskunnalle epävarmuuden tunnetta muun muassa lainojen epävarmuuden vuoksi, joka saattaisi luoda kaaosta. Tällöin arkisten raha-asioiden hoitaminen saattaisi pysähtyä kokonaan. (Taylor 2006, 322–323.)

ISIL käyttää teknologiaa hyödykseen sekä kehittää toimintaansa kybermaailmassa muun muassa viestinnässä ja rekrytoinnissa. Sen tiedetään myös yrittäneen palkata hakkereita ylläpitämään sosiaalisen verkostonsa infrastruktuuria. Kuitenkin asiantuntijoiden mukaan ISIL ei omista merkittäviä kyberterrorismin kykyjä. (Lehto ym. 2017, 19–20.)

4.1.3 Hakkerit, haktivistit, script kiddiet sekä yksinäiset sudet

Hakkerit ovat yleisnimitys henkilöistä, jotka ovat innokkaita tietokoneharrastajia. Hakkereita on niin yritysten, kuin myös valtioiden palveluksessa. Hakkerointi ei välttämättä ole laitonta, mutta mikäli se ylittää laillisen toiminnan rajat kutsutaan näitä henkilöitä krakkereiksi. Hakkerit voivat toimia omien intressiensä mukaisesti ja tehdä mahdollisesti pienempiä kyberiskuja, joko näyttääkseen omia taitojaan tai osoittaakseen mielipiteensä jostain asiasta. He voivat toteuttaa esimerkiksi palvelunestohyökkäyksiä, tai levittää haittaohjelmia, mutta mihinkään laajamittaisempiin operaatioihin heillä ei välttämättä ole resursseja eikä intressejä. Hakkereiden toiminnan motiivina ei yleensä ole terrorismi. (Taylor 2006, 62–64.)

Haktivistit pyrkivät hakkeroimaan sekä levittämään tietoja, jotka saattavat olla haitallisia organisaatioiden tai yksittäisten henkilöiden kohdalla. He toimivat sananvapauden puolesta ja puoltavat avointa internetiä. He ovat protestoineet tuomitsemistaan terroristien tavoin, mutta heidän tiedetään myös hyökänneen terroristeja vastaan. Haktivistit hyökkäsivät muun muassa ISIL:ä vastaan sulkemalla jihadistien verkkopalveluita ja paljastamalla useita Facebook- ja Twitter-tilejä, joiden uskottiin olevan kytköksissä terrorismiin. Script kiddiet ovat henkilöitä, jotka ovat hakkereita ja etsivät tietoja internetistä ja tekevät niiden avulla hyökkäyksiä. Tällaisten henkilöiden motiivina on usein hauskanpito.

Yksinäiset sudet ovat henkilöitä, joiden tarkoitus on valmistella ja toteuttaa väkivaltaisia tekoja yksinään. He toimivat ilman minkäänlaisten organisaatioiden apua. (Lehto ym. 2017, 19–20.)

4.2 Vaikutukset internetpalveluihin ja infrastruktuuriin

Yhteiskunnan palvelut ovat jatkuvasti enenevissä määrin siirtymässä internetin välityksellä toteutettaviksi. Suomessa esimerkiksi Kansaneläkelaitoksen ja pankkien palveluista suurin osa toimii internetissä. Näille sivuille toteutettu palvelunestohyökkäys voisi saada hyvin suuren mittakaavan nopeassakin ajassa, koska ne voivat vaikuttaa monen ihmisen päivittäiseen elämään. Vuonna 2015 uutisoitiin useista palvelunestohyökkäyksistä eri pankkien internetsivustoille. Pankkipalvelut olivat kuitenkin käytössä satunaisia katkoja lukuun ottamatta, mutta niiden toiminnassa oli havaittavissa ongelmia (Uusi Suomi 5.1.2015). Ruotsissa tehtiin vuonna 2012 suuri palvelunestohyökkäys viranomaisten internetsivuja kohtaan, jolloin useita palveluita oli poissa käytöstä tunteja. Iskun takana oli Anonymous-niminen hakkeriverkosto. (YLE-uutiset 5.10.2012.)

Palvelunestohyökkäys voi olla yksi tapa toteuttaa kyberterrorismia, mutta sen vaikutus on lyhytaikainen. Kuitenkin sillä voidaan aiheuttaa ongelmia palvelun käyttäjälle, vaikkakin varsinaisen terrori-iskun määritelmiä se ei täyttäisikään. Palvelun käyttäjät tietävät, että verkkosivut eivät aina toimi, jolloin terrorismin pohjimmainen tarkoitus, eli pelotteellinen vaikutus, jää toteutumatta.

Kyberterrorismin vaikutus palveluihin ja infrastruktuuriin voi olla monitasoinen. Kriittisen infrastruktuurin toimintahäiriöt ovat yleisiä, mutta vikojen korjaaminen ei yleensä kestä kauaa. Mikäli terrori-iskulla haluttaisiin vaikuttaa infrastruktuuriin tehokkaasti, pitäisi iskun olla kestoltaan pitkä. Kyberhyökkäyksellä aiheutettu pitkäkestoinen vaikutus on haastavaa. Verkossa toimiviin palveluihin on huomattavasti helpompi hyökätä esimerkiksi palvelunestohyökkäyksellä, mutta niiden vaikutukset voivat jäädä pieniksi, mikäli hyökkäystä ei kyetä pitämään yllä tarpeeksi pitkään. Terrori-iskun pitäisi olla laaja ja kohdistua moneen palveluun tai infrastruktuurin osaan yhtäaikaisesti, jotta sillä saataisiin aiheutettua haluttua vaikutusta eli pelkoa yhteiskunnalle. (Lewis 2002, 3.)

Yhdysvalloissa sähköverkko ja vedenjakelujärjestelmät ovat olleet jo pitkään kyberhyökkäysten kohteena. Hyökkäyksillä on tavoiteltu järjestelmien lamaantumista, mutta järjestelmät ovat useiden eri tahojen hallinnassa ja rakennettu toisistaan irrallisiksi siten, että mikäli pääjärjestelmä lakkaa toimimasta, voi varajärjestelmä vielä toimia. Tästä johtuen terrori-iskun tekijän olisi saatava lamaannutettua useita eri järjestelmiä samanaikaisesti.

Kyberiskun toteuttaminen yksinään ei välttämättä ole pienillä resursseilla tehokasta. Terroristeille kiehtovampaa voi olla perinteisen terrori-iskun vaikutusten tehostaminen kyberiskulla. Kuitenkin kyberiskuilla voidaan saada aikaan taloudellisia tappioita, mutta se ei välttämättä tavoita koskaan suurempaa yleisöä, eikä näin ollen ole terroristisessa tarkoituksessa kannattavaa.

Liikenneinfrastruktuurin kuten lentoliikenteen häiritseminen kyberhyökkäyksellä on mahdollista, mutta lentokoneen kaappaaminen ei onnistu niin kauan kuin lentokoneessa on hätätilanteita varten harjoitellut miehistö. Lisäksi lentoliikenne ei perustu pelkästään informaatioteknologiaan, joten lentoliikenne kyllä toimii kyberhyökkäyksenkin aikana. Taloudellisia tappioita kuitenkin voidaan saada myös tässä asiassa aikaiseksi. (Lewis 2002, 3.)

4.3 Psykologinen vaikutus

Terrorismi on usein käsitteellistetty psykologisen sodankäynnin välineeksi. Terrorismin psykologinen vaikutus on sen keskeinen tavoite. Terrori-iskulla pyritään vaikuttamaan kansalaisten turvallisuudentunteeseen ja aiheuttamaan paniikkia. Terrorismin pelko kasvaa entisestään sen arvaamattomuuden ja tuhovoiman mahdollisuuksien johdosta.

Kyberympäristön käyttäminen tuo terroristeille uusia mahdollisuuksia levittää uhkauksia tulevista terrori-iskuista nopeammin kuin millään muulla tavalla. Lisäksi internet mahdollistaa kuvien ja videoiden nopean levityksen. Etenkin ISIL on julkaissut erittäin raakoja teloitusvideoita, joissa muun muassa teloitetaan ISIL:n kaappaamia vankeja. Lisäksi ISIL pyrkii tehostamaan julmuuttaan julkaisemalla kuvia ja videoita lapsien käytöstä väkivallan toteuttajina. Näillä kaikilla on yhteinen tavoite, pyrkiä lisäämään pelkoa ja kauhua. (Weimann 2015, 24.)

Etenkin nuoret ovat haavoittuvaisia käyttäessään internetiä päivittäin. Nuoriin vaikuttaminen kuvamateriaalin avulla on tehokkaampaa kuin aikuiseen ihmiseen. Alle kouluikäinen lapsi ei vielä ymmärrä mikä on oikein ja mikä on väärin. Lapsille internetin välityksellä kehittyvä kuva saattaa olla hyvin vääristynyt kuva todellisuudesta. Nuorelle henkilölle internetin kautta välittyvä kuva terrorismista voi olla kovinkin ahdistavaa. (Salokoski & Mustonen 2007, 23.)

4.4 Kyberterrorismi ja poliisi

Poliisilain 1. luvun 1 §:ssä (22.7.2011/872) on lueteltu poliisin tehtävät ja niihin kuuluu rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. (PolL 1:1 §) Kyberrikollisuuden torjunta ja esitutkinta ovat näin myös poliisin tehtäviä. Keskusrikospoliisiin on perustettu Kyberrikollisuuskeskus vuonna 2015, jonka tehtävänä on tutkia vakavimpia tietoverkkorikoksia, pitää yllä tietoliikennerikosten tilannekuvaa, internet- ja verkkotiedustelu, tietotekninen tutkinta sekä tuottaa asiantuntijapalveluita poliisille ja muille viranomaisille esitutkintaan liittyen. Lisäksi Keskusrikospoliisi kouluttaa poliiseja kybertoimintaympäristössä tapahtuvien rikosten selvittämiseen. (Kyberrikollisuus, luettu 12.1.2017.)

Suojelupoliisin tehtäviin kuuluu muun muassa terrorismia tukevien hankkeiden ja rikosten ennalta estäminen ja paljastaminen. Keskusrikospoliisi vastaa terrorismirikosten esitutkinnasta, mutta Suojelupoliisi sekä muut viranomaiset voivat tarvittaessa avustaa tutkinnassa. (Sisäministeriö, luettu 14.2.2017.)

4.4.1 Kyberturvallisuuskeskus

Kyberturvallisuuskeskus palvelee viranomaisia, elinkeinoelämää sekä muita toimijoita kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. Keskeisin palvelu on kybertilannekuvan luominen, ylläpitäminen ja jakaminen yhteistyössä keskusta tukevan verkoston kanssa. Kyberturvallisuuskeskus voi tukea kyberhäiriötilanteen kohteena olleen viranomaisen tai yrityksen toimintaa, mutta aiheutuneiden vahinkojen rajaus kuuluu johtovastuussa olevalle viranomaiselle.

Kyberturvallisuuskeskus pitää yllä muodostamaansa kyberturvallisuuden kokonaistilannekuvaa ja arvioi kyberturvallisuuden yleistilannetta. Tämän yleistilanteen ymmärtäminen tukee muita aloja niiden kyberturvallisuuden yllä pitämisessä ja kehittämisessä. Lisäksi kyberturvallisuuskeskus seuraa kyberturvallisuusuhkia sekä analysoi ja tekee ennusteita tulevista kyberympäristön tapahtumista. Kyberturvallisuuskeskus varoittaa etukäteen Suomea uhkaavista kyberuhkan muodoista ja pyydettäessä avustaa niiden vastatoimissa. (Turvallisuuskomitea 2015.)

4.4.2 Kansainvälinen yhteistyö

Suomi on aktiivisesti mukana kansainvälisessä yhteistyössä terrorismintorjunnan suhteen. Suomen kannalta tärkeitä yhteistyökumppaneita ovat Euroopan Unioni (EU), Yhdistyneet kansakunnat (YK), Euroopan neuvosto (EN), Euroopan turvallisuus- ja yhteistyöjärjestö (Etyj), puolustusliitto NATO, Taloudellisen yhteistyön ja kehityksen järjestö (OECD) ja sen rahanpesun vastainen asiantuntijatyöryhmä (FATF). Suomi on myös mukana Euroopan yhteisessä terrorismintorjunnan poliisiyhteistyössä. Kansainvälistä yhteistyötä on pyritty edistämään tiedonvaihdolla, jakamalla käytäntöjä sekä kokemuksia ja asiantuntemusta eri valtioiden kesken. YK on tärkeä yhteistyökumppani terrorismintorjunnassa. Se ohjaa jäsenvaltioidensa terrorisminvastaista politiikkaa, tiedonvaihtoa ja yhteistyötä. Suojelupoliisi edustaa Suomea turvallisuusviranomaisten välisessä yhteistyössä. Lisäksi Suomen syyttäjäviranomaisella on edustaja EU:n terrorismirikosverkostossa. Terrorismin ylittäessä valtioiden rajat, on myös yhteistyö tärkeää terrorismin torjunnan laadun varmistamiseksi. (Sisäministeriö 2014.)

Terrorisminvastainen toiminta on suuri osa kyberterrorismin torjuntaa. Kyberturvallisuuden osalta kansainvälinen yhteistyö on myös erittäin tärkeää. Suomella on tarkoitus vahvistaa kansallista kyberturvallisuutta osallistumalla kyberturvallisuuden osalta keskeisten kansainvälisten toimijoiden toimintaan. Tällöin edesautetaan tietojen ja kokemuksien siirtymistä taholta toiselle. Kyberuhat ylittävät terrorismin tavoin valtioiden rajat, joten yhteistyö on suuressa roolissa kyberturvallisuuden kehittämisessä. Euroopassa Suomen keskeisimmät kyberturvallisuuden yhteistyökumppanit ovat EU ja NATO, joiden kanssa yhteistyö on enimmäkseen tilannetiedon vaihtoa, koulutusta sekä yhteisen suorituskyvyn parantamista.

Kyberympäristön rajattomuuden johdosta tietoverkot ovat globaali toimintaympäristö. Kyberterrorismi voi toimia yhtäaikaisesti monen eri valtion alueella. Lakien ollessa eri valtioissa erilaiset, on yhteistyö suuressa roolissa. Lisäksi esitutkinta ja syyteharkinta voidaan joutua tekemään osittain myös toisessa maassa. Tällöin yhteistyön tekemisellä päästään huomattaviin etuihin pelkästään jo paikallisen lain ja toimintatapojen tuntemisen suhteen. (Council of Europe Publishing 2007, 47–48.)

4.5 Lainsäädäntö

Suomen rikoslaki ei ota suoranaisesti kantaa kyberympäristön käyttöön terroristisessa tarkoituksessa. Rikoslain 34a luku (24.1.2003/17) pitää sisällään terrorismirikokset. Luvussa ei käsitellä kyberympäristön käyttöä terroristisiin tarkoituksiin. Terroristisen teon toteutustavasta riippumatta, voidaan kuitenkin myös kyberympäristössä tehdyt terroristiset teot laskea terrorismiksi. (Council of Europe Publishing 2007, 167.)

Rikoslain 34a luku kriminalisoi terroristisessa tarkoituksessa tehdyt teot ja näitä tekoja voidaan myös toteuttaa kyberympäristössä (RL 34a 1 §). Terroristisen teon valmistelu on myös kriminalisoitu (RL 34a 2 §). Käytännössä terroristisen teon suunnittelu ja valmistelu voi tapahtua myös kyberympäristössä. Terroristiryhmän johtaminen ja terrori-iskun koordinoiminen voi tapahtua hyvin tietokoneiden tai puhelimien välityksellä, joten myös tällä tavalla voidaan kyberympäristöä käyttää terrori-iskun toteuttamisessa. Terroristiryhmän johtaminen on myös kriminalisoitu rikoslaissa (RL 34a 3 §). Rikoslain 34a luvun 4 §:n mukaan terroristiryhmän 1 tai 2 §:ssä tarkoitetun toiminnan edistäminen muun muassa kouluttamalla, kouluttautumalla ja värväämällä on myös kriminalisoitu (RL 34a 4 §). Lisäksi rikoslain 34a luvun 5 § kieltää terrorismin rahoittamisen (RL 34a 5 §). Terrorismin rahoittaminen ja edistäminen kyberympäristössä tietokoneiden ja internetin avulla on mahdollista. (Council of Europe Publishing 2007, 167-168.)

Terroristisen teon toteuttaminen, valmisteleminen, johtaminen sekä edistäminen voivat tapahtua monella eri tavalla. Kyberympäristöä voidaan hyödyntää, mutta varsinaiseen terrori-iskuun yhdistäminen voi olla hankala todistaa. Tällöin tarvitaan konkreettisia todisteita siitä, että esimerkiksi internetin käyttö on edesauttanut iskun toteuttamisessa. Muuten pelkästä internetin käytöstä ei voida tuomita. (Council of Europe Publishing 2007, 168.)

Rikoslain 38 luku käsittelee tieto- ja viestintärikoksia. Kyberrikollisuus on suhteellisen uusi ilmiö ja tämä vaatii myös lainsäätäjiltä tietojen päivittämistä aika-ajoin, jotta laki saadaan pysymään ajan tasalla. Rikoslain 38 luvun 3 § kriminalisoi tiedon hankkimisen oikeudettomasti toiselle osoitetusta kirjeestä tai muusta suljetusta viestistä. Lisäksi kyseinen pykälä kriminalisoi tiedon hankkimisen televerkossa tai tietojärjestelmässä välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällön taikka tällaisen viestin lähettämisen tai vastaanottamisen. (RL 38:3 §) Tällaisen toiminnan ei välttämättä voida katsoa olevan kyberterrorismia, mutta tällainen toiminta voi

sisältyä terrorismiin, jolloin rikoslain 34a luvun mukaan siitä voi tulla terrorismirikos. Rikoslain 38 luvun 5 § käsittelee tietoliikenteen häirintää. Pykälän mukaan tele-, radio- tai postiliikenteen häirintä on kriminalisoitu (RL 38:5 §). Rikoslain 38 luvun 7 § kriminalisoi toiselle aiheuttaman haitan tekemisen tai taloudellisen vahingon aiheuttamisen dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettoman tietojärjestelmän toiminnan estämisen tai sille vakavan häiriön aiheuttamisen (RL 38:7a §). Myös edellä mainittujen kaltaisia toimenpiteitä voitaisiin periaatteessa tehdä terroristisessa tarkoituksessa esimerkiksi palvelunestohyökkäyksenä. Tietomurto on suurimpia tietoturvallisuusriskejä. Se on kriminalisoitu rikoslain 38 luvun 8 §:ssä ja pitää sisällään oikeudettoman käyttäjätunnuksen käyttämisen, tunkeutumisen turvajärjestelyt murtamalla tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan (RL 38:8 §).

Rikoslain 38 luvussa kriminalisoidut teot voivat olla kyberrikollisuutta ja myös kyberterrorismia, mutta niiden osoittaminen terroristiseksi teoksi saattaa olla haastavaa. Koska internet menee valtion rajojen ulkopuolelle, on hyvinkin mahdollista, että epäilty rikos itsessään toteutetaan Suomen ulkopuolella, mutta vaikutukset ovat Suomessa. Tällöin epäilty rikos on myös Suomen rikoslain alainen rikos ja lakia voidaan täysin soveltaa epäiltyä rikosta kohtaan. (Council of Europe Publishing 2007, 170.)

4.6 Kyberturvallisuus

Kyberturvallisuus on noussut keskeiseen asemaan tietoliikenteen ja verkkopalveluiden lisäännyttyä. Suomi on riippuvainen tietoverkoista ja –järjestelmistä ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Kyberuhat ovat muuttuneet vaarallisemmiksi koko yhteiskunnan kannalta. (Turvallisuuskomitea 2015.)

Suomessa Viestintävirasto tuottaa tilannekuvaa tietoturvallisuuden ilmiöistä, tiedottaa niistä sekä toimii tietoliikenneturvallisuusviranomaisena. Viestintävirasto kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta (Viestintäviraston internetsivut). Kyberturvallisuus perustuu koko yhteiskunnan tietoturvan järjestelyihin. Kyberturvallisuus koskettaa kaikkia ja vaatii jokaisen kybertoimintaympäristössä toimivan tarvittavat ja riittävät turvallisuusratkaisut. Toimintamalli kyberturvallisuudessa perustuu

tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä monialaiseen yhteistyöhön. Tämän takia tietoturvatoiminnan kehittäminen on tärkeää.

4.6.1 Tietoturvallisuus

Tietoverkot ja tietokoneet ovat helpottaneet ihmiskunnan päivittäistä elämää, mutta niiden käyttö vaatii myös osaamista. Vaikka tietojärjestelmien käyttö helpottuu ja monipuolistuu koko ajan, on kuitenkin hyvä pitää mielessä tietoturvallisuus. Oikean tiedon saaminen oikeassa muodossa on tärkeässä asemassa järjestelmien toimivuuden kannalta. Tietojärjestelmien suojaamisessa on otettava huomioon monia asioita, esimerkiksi järjestelmien päivittäminen ja niiden oikeaoppinen käyttö. Suurimmaksi osaksi ne kyetään automatisoimaan, mutta viime kädessä ihminen on kuitenkin tietoturvallisuuden heikoin lenkki. Tietoturvassa on kyse tietojärjestelmien suojaamisesta niitä kohtaan, jotka tietojärjestelmiä käyttäisivät mahdollisesti väärin. Tämä on myös kaikkien kyberturvallisuusasiantuntijoiden tavoite. (Harrison & Herr 2016, 3.)

Tietoturvallisuusjärjestelyiden tavoitteena on palveluiden, tietojärjestelmien ja tietoaineistojen suojaus siten, että niiden luottamuksellisuus, eheys ja saatavuus varmistetaan. Lyhyesti sanottuna tämä tarkoittaa sitä, että tieto on saatavilla niille, ketkä sitä tarvitsee, mutta ei muille. Tiedon tulisi pysyä luotettavana, ajantasaisena ja oikeana. Lisäksi tietojen on oltava saatavilla silloin kun niitä tarvitaan. (Valtionvarainministeriö 2013, 17.)

Tietoturvallisuus on tärkeää, jotta voidaan turvata yksilön, yhteisön ja yhteiskunnan etuja. Se on yhteiskunnan toimintojen, sovellusten ja palveluiden sekä tietoteknisen infrastruktuurin perusedellytys. Jokainen organisaatiossa toimiva henkilö on vastuussa tietoturvallisuudesta omalta osaltaan. Tästä johtuen suurimmat tietoturvallisuuden ongelmat liittyvät ihmisten toimintaan. Puutteellinen tietoturvallisuus tuottaa lisäkustannuksia sekä vaarantaa valtion, kansalaisten, yhteisöjen ja asiakkaiden etuja. (Valtionvarainministeriö 2013, 18.)

4.6.2 Tietoturvallisuus vaikuttaa jokaisen yksilön toimintaan

Tietoturvallisuuskoulutus on suuressa osassa tietoturvallisuutta. Mitä paremmin ihmiset tietävät tietoturvallisuuteen liittyvät riskit, sitä helpompi järjestelmiä on suojata. Jokaisen

tulisi noudattaa tietoturvallisuusohjeita niin työpaikalla kuin vapaa-ajalla. Päätelaitteella on mahdollista käyttää lukemattomia palveluita päätelaitteen haltijan nimellä, joten sen suojaaminen on tärkeää. Käsiteltävä tieto voi olla arkaluonteista, joten sitä on suojeltava. Tieto voi myös olla suoraan salaiseksi luokiteltua, jolloin sitä ei saa käsitellä kuin erikseen luvan saanut henkilö. Tällöin tiedon haltijalla on vastuu tiedon suojaamisesta. Työpaikoilla on omat tietoturvaohjeensa, joten niitä noudattamalla tiedon pitäisi pysyä niillä käyttäjillä, joilla siihen on oikeus.

Tunnukset ja salasanat ovat tietoyhteiskunnassa päivittäin käytössä. Salasana on tehokas tapa pitää oikeudettomat henkilöt pois tiedon luota. Salasana on kuitenkin helppo murtaa, mikäli se on liian heikko. Lisäksi monet pitävät samoja salasanoja eri palveluissa. Tällöin yhden salasanan murtaminen saattaa antaa tilaisuuden päästä moniin eri järjestelmiin käsiksi. Käyttäjätunnukset ovat jonkun tietyn tahon tunnuksia, joilla järjestelmiin kirjaudutaan. Käyttäjätunnuksen käyttäminen yksilöi palvelun käyttäjän. Tämän takia käyttäjätunnuksien ja salasanojen suojaaminen on erittäin tärkeää.

Sosiaalinen media on päivittäin käytössä useilla henkilöillä. Sitä käyttäessä on syytä kuitenkin pitää mielessä, että palvelun tarjoajalla on mahdollisuus päästä käsiksi kaikkeen sisältöön mitä palvelu tarjoaa, myös yksityisiin keskusteluihin. Sosiaalinen media auttaa verkostoitumaan ja pitämään yhteyttä muihin ihmisiin, mutta sen käyttämisen suhteen kannattaa olla tarkka. Yksityisyyden suojaa koskevat asetukset on syytä tarkistaa. (Valtionvarainministeriö 2013, 11-15.)

5 JOHTOPÄÄTÖKSET

5.1 Terrorismin vaikutukset

Terrorismi on kautta historian ollut tehokas vaikutuskeino. Psykologiset vaikutukset ovat monesti laajat jo pienemmilläkin terrori-iskuilla, eikä terrori-iskun suoranaiset materiaaliset tappiot ole välttämättä pääasiallinen tarkoitus. Terrorismilla pyritään vaikuttamaan päätösten tekoon, joko valtiollisella tasolla tai mahdollisesti yksityisellä tasolla, esimerkiksi yritysten toimintaan liittyen.

Vaikka terrorismia on ollut maailman historiassa jo hyvin pitkään, on se kuitenkin 2000-luvulla muuttunut huomattavasti. Yksi suuri tekijä on median vaikutus väestöön. Media on

nykypäivänä läsnä jokaisessa pienemmässäkin tapahtumassa ja sen vaikutus siihen, miten tapahtumat nähdään kansalaisten silmissä, on erittäin suuri. Toinen ongelma on se, että media kirjoittaa terrori-iskuista tietynlaisen näkökulman, joka ei välttämättä ole viranomaisten kanssa samassa linjassa. Esitutkinnan käynnistyessä terrori-iskun jälkeen, ei viranomaiset voi vielä välttämättä antaa omia lausuntojaan, jolloin media on vain toimittajien saamien lähteiden varassa. Tällöin totuus voi vääristyä huomattavasti. Kuitenkin median esittäessä kansalaisille uutisten välityksellä oman kantansa, voi olla, että ensivaikutuksella on suuri merkitys, miten tapahtuma koetaan suuremman yleisön keskellä. Lisäksi media pyrkii saamaan julkisuutta mielenkiintoisilla kirjoituksilla, joten totuus voi vääristyä myös tästä syystä. Tämänkin johdosta terrorismi on saanut lisää vaikutusvaltaa.

Terrorismia vastaan taisteltaessa ja terrori-iskujen ennalta ehkäisemisellä terroriteon toteuttaminen muuttuu jatkuvasti hankalammaksi. Terroristiryhmät kehittyvät kuitenkin koko ajan ja pyrkivät parantamaan toimintaansa. Lähtökohtaisesti poliisi ja muut turvallisuusviranomaiset ovat aina askeleen jäljessä rikosten torjunnassa, joten näin on myös terrorismintorjunnan suhteen. Vaikka terrorismin torjunnan osalta tehdään paljon työtä, sen kokonaan pois kitkeminen on mahdotonta. Terrorismin kehittyessä on myös kehitettävä terrorismin torjuntaan liittyviä keinoja. Terrorismintorjunta on laaja käsite ja se ylettyy monen eri tahon ylle. Sen suhteen on otettava huomioon mitkä tekijät vaikuttavat terrorismin syntyyn ja mitkä sen ilmenemiseen. Terrorismia vastaan taisteltaessa niin kansallisella, kuin kansainväliselläkin yhteistyöllä on merkitystä. Varsinkin Suomen kokoisessa pienessä valtiossa, jossa resurssit ovat rajalliset, on viranomaisten ja yksityisen puolen toimijoiden yhteistyö suuressa roolissa. Kansainvälisellä yhteistyöllä on terrorismin vastaisessa toiminnassa suuri merkitys, koska terrorismi on nykypäivänä suurimmaksi osaksi valtioiden rajojen yli tapahtuvaa maailmanlaajuista toimintaa.

Vaikka Suomessa terrorismin uhka on pieni verrattuna moneen muuhun Euroopan valtioon, ei pidä unohtaa sitä, että terrori-iskun mahdollisuus on kuitenkin olemassa. Suomen osallistuminen kansainvälisiin toimenpiteisiin, kuten esimerkiksi kriisinhallintaan, niin siviili- kuin sotilaspuolellakin, voi vaikuttaa maissa, joissa terroristijärjestöt pääsääntöisesti toimivat. Terrorismi voi olla vastalause valtioita vastaan, jotka toimivat terroristijärjestöjen hallitsemilla alueilla. Tällöin myös Suomi voi joutua terrori-iskun kohteeksi. Pelkästään kansainvälinen terrorismi ei ole ainoa ongelma, vaan myös kansallisella tasolla terrorismi on täysin mahdollista. Esimerkiksi kouluampumatapaukset ja pommi-iskut ostoskeskuksissa voivat olla yksittäisen henkilön toteuttamia. Tällöin ennalta estävä toiminta on isossa

roolissa, koska siihen pystymme omassa maassamme vaikuttamaan. Terrorismin vastainen työ Suomessakin on siis tärkeässä roolissa, jotta maan sisäinen turvallisuus voidaan pitää hyvällä tasolla.

Terrorismi ymmärretään helposti terroristijärjestöjen toteuttamiin terrori-iskuihin. Toinen huomioitava asia on valtiolliset toimijat, jolloin puhutaan valtiollisesta terrorismista. Tällöin iskun tekijä, toinen valtio, ei välttämättä ole varsinaisesti sotatoimissa iskun kohteena olevan valtion kanssa, mutta se saattaa vaikuttaa valtioiden välisiin suhteisiin hyvinkin paljon. Etenkin terrori-iskun esitutkinnassa tulisi pyrkiä selvittämään, kuka on teosta vastuussa. Yksittäiset toimijat ottavat usein vastuun tapahtuneista terrori-iskuista, mikä ei välttämättä tarkoita, että terrori-iskun tekijä ei olisi toinen valtio. Lisäksi esimerkiksi merkittävän kyberterrori-iskun tekeminen voi vaatia niin isot resurssit, että yksittäisen terroristijärjestön ei välttämättä ole mahdollista toteuttaa suurta kyberterrori-iskua. Suurilla valtioilla, kuten Venäjällä, Yhdysvalloilla ja Kiinalla, on suuri osaaminen kyberympäristössä, jolloin kyberterrori-isku on helpompi toteuttaa.

5.2 Kyberterrorismi osana terrorismia

Internetin kehittyminen on ollut 2000-luvulla nopeaa ja yhä enenevissä määrin useiden palveluiden, ainakin osittainen, siirtyminen internetiin on tapahtunut. Internetpalveluiden tietoturvaa kehitetään jatkuvasti, mutta kaikkea ei aina voida korjata. Moni haavoittuvuus saadaan korjattua vasta, kun sitä ollaan jo käytetty hyväksi. Palvelunestohyökkäykset ovat arkipäivää internetissä toimivien palveluiden osalta, vaikka niitä ei peruskäyttäjä välttämättä heti huomaakaan.

Kyberrikollisuuden lisääntyessä myös terrorismin siirtyminen kyberympäristöön on mahdollista. Terroristijärjestöt kehittävät omia kyberympäristön toimintamallejaan ja pyrkivät hyödyntämään teknologian kehityksen myös terroristisella tavalla. Terrori-iskun toteuttaminen tietoverkkojen välityksellä, esimerkiksi internetissä, on kuitenkin vaikeaa. Mikäli pelkästään internetin välityksellä toteutettaisiin terrori-isku, joka saisi sellaisen mittakaavan, kuin esimerkiksi Pariisin terrori-iskut saivat vuonna 2015, olisi sen oltava todella voimakas ja vaikuttavan suureen joukkoon ihmisiä. Lisäksi se pitäisi kertoa kansalaisille terrori-iskuna. Tähän ei kuitenkaan vielä palvelunestohyökkäys riitä, koska se ei todennäköisesti aiheuttaisi minkäänlaista kauhua. Kyberterrori-iskun tulisi olla esimerkiksi sellai-

nen, joka voisi lamaannuttaa sähkönjakelun tai vedenjakelun tai sen pitäisi saada esimerkiksi ydinvoimalan turvallisuusjärjestelyt pettämään ja näin synnyttää vaaran useille ihmisille. Tällöinkään ei välttämättä iskua uutisoitaisi terrori-iskuna, vaikka se vaikuttaisikin monen ihmisen elämään. Kuitenkin seurausten osalta voitaisiin jo puhua mahdollisesti terrori-iskusta. Tällaisen iskun toteuttaminen vaatisi resurssit, joita suuremmallakaan terrorijärjestöllä ei välttämättä vielä ole.

Määritelmää terroristille kyberympäristössä ei oikeastaan ole. Tietokoneita voidaan hyödyntää terroristien tekemien iskujen toteuttamisessa, mutta itse terroristia on vaikea määritellä tietokonemaailmassa. Terroriteon toteaminen on varsin helppoa tutkinnan myötä, mutta terroristin toimiminen internetissä on vaikea todistaa. Terrorismin raja kyberympäristössä on häilyvä, joten terroristin tunnistaminen ja määritteleminen ovat lähes mahdotonta ennen iskun tapahtumista.

Kyberterrori-iskun toteuttaminen vaatii huomattavasti tietoa ja taitoa, minkä saaminen voi olla terroristeille ongelma. On kuitenkin mahdollista, että terroristijärjestöt hankkivat tietotaitoa organisaation ulkopuolelta, jolloin raha on ratkaisevassa osassa. Ulkopuolisen kyberosaamisen ostaminen voi olla vaikeaa ja vaikka se onnistuisikin, on terrori-iskun salaaminen tärkeämpää, kuin iskun toteuttaminen uudella tavalla. Lisäksi terrorismi on toimintaa, joka on yleisesti paheksuttua ja sen salaaminen on vaikeaa jo pelkästään ilman organisaation ulkopuolisia toimijoitakin. Tällöin myös ulkopuolisen osaamisen hankkimisessa voi olla suuria riskejä iskun toteuttamisen kannalta.

Kyberturvallisuus paranee koko ajan ja sen avulla pyritään kehittämään kokonaisvaltaisesti kyberympäristön turvallisuutta. Kriittisen infrastruktuurin suojaaminen kyberhyökkäyksiltä on pyritty tekemään mahdollisimman kattavasti. Kyberturvallisuuskoulutusta on lisätty yrityksissä ja valtion työntekijöiden keskuudessa, mutta sen vakavuutta ei välttämättä oteta vielä tarpeeksi tosissaan. Tosiasia on se, että kyberturvallisuudesta löytyy aukkoja niin kauan, kuin ihminen on yhtälössä mukana.

Terrori-isku voidaan toteuttaa myös hybridi-iskuna, jolloin perinteisen terrori-iskun vaikutuksia pyritään lisäämään kyberhyökkäyksellä. Tämä saattaisi olla terroristijärjestöille helpompaa ja se saisi aikaan suuren huomion. Toistaiseksi kuitenkin on vielä helpompia tapoja tehdä terrori-isku kuin tietokoneiden kanssa, joten kyberterrorismin uhka terroristijärjestöjen osalta ei välttämättä vähään aikaan ole vielä ajankohtainen. Valtiollisen terrorismin

suhteen asia on kuitenkin toinen. Suurvalloilla on jo tarpeeksi kyberosaamista laajan kyberterrori-iskun toteuttamiseksi. Isku voidaan myös toteuttaa niin hyvin, että sen tekijästä ei jää jälkiä.

Kyberympäristössä viranomaiset toimivat jo rikollisuutta vastaan, mutta terroristien toiminta kybermaailmassa on vasta tulossa. Tällä hetkellä perinteisten terroritekojen riskin voidaan olettaa olevan suurempi kuin kyberterrori-iskun. On kuitenkin pidettävä mielessä, että maailma muuttuu ja tekniikan kehittyessä löytyy uusia vaihtoehtoja terrorismille. Esimerkiksi esineiden internet voisi tulevaisuudessa olla terroristien haluttuja kohteita. Tämän johdosta myös valtion taholta tulee entistä enemmän kiinnittää huomiota koulutuksen tärkeyteen kyberosaamisen lisäämisessä, koska osaajien määrä ja merkitys tulee entisestään korostumaan mentäessä yhä tietokonevaltaisempaa tulevaisuutta kohden.

LÄHTEET

Chivvis, Christopher, S. & Dion-Schwarz, Cynthia 2017: Why It's So Hard to Stop a Cyberattack – and Even Harder to Fight Back. RAND Corporation. Luettavissa: https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html
Luettu: 13.4.2017.

CNN-uutiset 8.9.2016: September 11, 2001: Background and timeline of the attacks. Luettavissa: http://edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/
Luettu: 8.2.2017.

Council of Europe Publishing 2007: Cyberterrorism – the use of the Internet for terrorist purposes. Ranska. Council of Europe Publishing.

Crenshaw, Martha 2011: Explaining Terrorism – Causes, Processes and Consequences. Yhdysvallat. Routledge.

Harrison, Richard M. & Herr, Trey 2016. Cyber Insecurity – Navigatin the Perils of the Next Information Age. Englanti. Rowman & Littlefield.

Helsingin Sanomat 7.11.2016: Verkkohyökkäys katkaisi kahdesta talosta lämmöt Lappeenrannassa – ”Laajuus ja voima on aika poikkeuksellinen”.
Luettavissa: http://www.hs.fi/kotimaa/art-2000002929144.html
Luettu: 20.2.2016.

Kushner, Harwey W. 1998: The Future of Terrorism: Violence in the New Millenium. Yhdysvallat. Sage Publications, Inc.

Kyberrikollisuus. Poliisin internetsivut. Luettavissa:
https://www.poliisi.fi/rikokset/kyberrikollisuus
Luettu 12.1.2017.

Laitinen, Kari 2007: Tuhat ja yksi uhkaa – tulkintoja terrorismista. Tampere. Poliisiammattikorkeakoulu.

Laitinen, Kari & Lumio, Milla 2009: Terroristin synty ja terrorismin torjunta. Tampere. Poliisiammattikorkeakoulu.

Lansford, Tom & Pauly, Robert J. Jr 2016: The New Islamic State – Ideology, Religion and Violent Extremism in the 21st Century. Yhdysvallat. Ashgate Publishing.

Lehto, Martti; Limnell, Jarno; Innola, Eeva; Pöyhönen, Jouni; Rusi, Tarja; Salminen, Mirva 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet sen saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminta. Luettavissa:
http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0
Luettu 13.4.2017.

Lewis, James A. 2002: Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Attacks. Yhdysvallat. Center of Strategic & International Studies. Luettavissa: https://csis-

prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
Luettu: 22.3.2017.

Malkki, Leena & Paastela, Jukka 2007: Terrorismin monet kasvot. Helsinki. WSOY Oppimateriaalit Oy.

MTV-uutiset 1.9.2016: 7.1.2015: Charlie Hebdo –isku on isku sananvapautta vastaan – pilapiirrokset nousevat keskusteluun. Luettavissa:
http://www.mtv.fi/uutiset/kotimaa/artikkeli/7-1-2015-charlie-hebdo-isku-on-isku-sananvapautta-vastaan-pilapiirrokset-nousevat-keskusteluun/6051506
Luettu: 9.2.2017.

Neuman, Peter 2009: Old & New terrorism. Englanti. Polity Press.

Ozeren, Suleyman 2009: Cyberterrorism and Cybercrime – Vulnerabilities and International Cooperation. Saksa. VDM VerlagDr. Müller Aktiengesellschaft & Co. KG.

Puistola, Juha-Antero & Herrala Janne 2006: Terrorismi Euroopassa. Juva. Ws Bookwell Oy.

Puolustusministeriö 2017. Valtioneuvoston puolustusselonteko 2017. Puolustusministeriön internetsivut. Luettavissa:
https://defmin.fi/files/3683/J05_2017_VN_puolustusselonteko_Su_PLM.pdf
Luettu: 12.4.2017.

Rid, Thomas 2013: Cyber War Will Not Take Place. Englanti. Oxford University Pess.

Salminen, Ari 2011: Mikä kirjallisuuskatsaus? Vaasan yliopisto. Luettavissa:
http://www.uva.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf
Luettu: 10.4.2017.

Salokoski, Tarja & Mustonen, Anu 2007: Median vaikutukset lapsiin ja nuoriin. Luettavissa: http://www.mediakasvatus.fi/publications/ISBN978-952-99964-2-1.pdf
Luettu 23.3.2017.

Sisäministeriö. Terrorismia torjutaan viranomaisten yhteistyöllä. Sisäministeriön internetsivut. Luettavissa: http://intermin.fi/poliisiasiat/terrorismin-torjunta
Luettu 14.2.2017.

Sisäministeriö 2014. Valtioneuvoston periaatepäätös kansalliseksi terrorismintorjunnan strategiaksi 2014-12017. Sisäministeriön internetsivut.
Luettavissa:
http://intermin.fi/documents/1410869/3723676/Kansallinen+terrorismin+torjunnan+strategia+2014-2017/9b549988-3c30-4ecb-ad7f-1f99053b131b
Luettu 14.2.2017.

Sisäministeriö 2016. Väliraportti: Kansallisen terrorismin torjunnan strategia 20142017. Luettavissa:
http://intermin.fi/documents/1410869/3723676/Terrorismin+torjunnan+strategia+väliraportti/41ed4a01-ec02-481b-900d-c350a83899e6

Luettu: 12.3.2017.
Sisäministeriö 2017. Väkivaltaisen ekstremismin tilannekatsaus 1/2007. Valtioneuvoston julkaisuarkisto. Luettavissa:
http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79235/03%202017_Vakivaltaisen%20ekstremismin%20tk%201_2017.pdf?sequence=1
Luettu: 12.4.2017.

Suojelupoliisi. Kansainvälinen terrorismi ja siihen liittyvät ilmiöt. Suojelupoliisin internet-sivut. Luettavissa: http://www.supo.fi/terrorismintorjunta/kansainvalinen_terrorismi
Luettu 18.4.2017.

Suojelupoliisi. Suojelupoliisin toimintaympäristö vuosina 2015-2016. Suojelupoliisin internetsivut. Luettavissa:
http://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/64088_Suojelupoliisin_toimintaymparisto_vuosina_2015-2016.pdf?63bfcddeb81cd388
Luettu: 20.1.2017.

Suojelupoliisi. Terrorismintorjunta. Suojelupoliisin internetsivut.
Luettavissa: http://www.supo.fi/terrorismintorjunta
Luettu 17.2.2017.

Suojelupoliisi 2015. Terrorismin uhka-arvio 3.11.2015. Suojelupoliisin internetsivut. Luettavissa: http://www.supo.fi/terrorismintorjunta/terrorismin_uhka-arvio
Luettu: 18.4.2017.

Taylor, Robert W.; Fritsch, Eric J.; Liederbach, John; Holt, Thomas J. 2006: Digital Crime and Digital Terrorism. Yhdysvallat. Pearcon Education.

Turvallisuuskomitea 2015. Suomen kyberturvallisuusstrategia. Turvallisuuskomitean internetsivut. Luettavissa:
http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia
Luettu 27.3.2017.

USA Department of Homeland Security. Understanding Denial of Service Attacks. 2013. Luettavissa: https://www.us-cert.gov/ncas/tips/ST04-015 Luettu: 16.2.2017.

Uusi Suomi 5.1.2015: Palvelunetsohyökkäyksistä ”uusia havaintoja”. Luettavissa:
https://www.uusisuomi.fi/kotimaa/76181-pankkihyokkayksista-uusia-havaintoja
Luettu: 22.3.2017.

Valtionvarainministeriö 2013. Henkilöstön tietoturvaohje 2013. Valtionhallinnon tietoturvallisuuden johtoryhmä. Luettavissa:
https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10128&groupId=10229
Luettu: 29.3.2017.

Weimann, Gabriel 2004: Cyberterrorism: How Real Is the Threat? Yhdysvallat. Luettavissa: https://www.usip.org/sites/default/files/sr119.pdf
Luettu 21.3.2017.

Weimann, Gabriel 2015: Terrorism in Cyberspace – The Next Generation. Yhdysvallat. Columbia University Press.

YLE-uutiset 5.10.2012: Ruotsi ”historian suurimman” nettihyökkäyksen kohteena. Luettavissa: http://yle.fi/uutiset/3-6323927
Luettu: 22.3.2017.

Yli-Karjanmaa, Hannu 2008: Valtiot ja terrorismi. Vaajakoski. Multikustannus Oy.