Juuso Viljamaa

Valtiolliset kybervaikuttamisen keinot ja vaikutukset - case Kiina

Tietotekniikan kandidaatintutkielma

6. toukokuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Juuso Viljamaa

Yhteystiedot: juuso.j.viljamaa@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Valtiolliset kybervaikuttamisen keinot ja vaikutukset - case Kiina

Title in English: Cyber actions and effects by states - case China

Työ: Kandidaatintutkielma

Sivumäärä: 19+0

Tiivistelmä: Tässä tutkielmassa avataan valtiollisia kybervaikuttamisen keinoja sekä vaikutuksia globaalilla tasolla. Tarkoituksena on kuvailla yleisimpiä hyökkäyskeinoja ja erilaisia kybervaikuttamisen tapoja perehtyen hyökkääjän valtiosidonnaisuuteen ja motiiviin. Tutkielmassa avataan tekijöitä, jotka erottelevat kybersodankäynnin muista kybervaikuttamisen tavoista. Loppua kohden kuvaillaan reaalimaailman esimerkein 2000-luvun kybervaikuttamista lopussa keskittyen Kiinan kansantasavallan kybervaikuttamiseen ja vaikutuksiin.

Avainsanat: Kandidaatintutkielmat, Kyberturvallisuus, Kybervaikuttaminen, Kiina

Abstract: This thesis discusses the cyber actions of states and their global effects. The most used attack methods and different ways to effect are described concentrating on attackers motivations behind them as well as links to government. Factors that separate cyber warfare from other cyber actions are elaborated. Cyber actions from the 2000's are described with real world examples. The work is concluded by an overview of the cyber actions and effects of People's Republic of China.

Keywords: Bachelor's Theses, Cyber Security, Cyber actions, China

Sisällys

1 Johdanto

Yhteiskunnan tärkeiden toimintojen siirtyessä verkkoon myös haitalliseen vaikutukseen pyrkivä toiminta siirtyy yhä enenevissä määrin verkkoon. Viime aikoina yleistyneet hyökkäykset ovat vaatineet myös niiden torjumiseen liittyvää yleistä sääntelyä muutettavan, jotta niiden kontrolloiminen olisi helpompaa (Kumar ja Carley 2016). Puhuttaessa valtiollisesta kybervaikuttamisesta tässä tutkielmassa, puhutaan myös valtioon liitetyistä hyökkäyksistä. Vaikka hyökkääjä olisi yksityinen toimija, usein hyökkäys liitetään vahvasti alkuperämaahansa etenkin rajojen yli tapahtuvassa kybervaikuttamisessa. Hyökkääjä toimii aina jonkin maan lainsäädännön alla ja suorittaa toimiaan sen perusteella joko laillisesti tai laittomasti. Useimmiten kybervaikuttaminen tapahtuu teknisesti samoilla keinoilla tarkoituksesta riippumatta ja sen luokittelu on tulkinnanvaraista (Klimburg 2011), mutta tämän tutkielman myötä on tarkoitus myös perehtyä kybervaikuttamisen luokitteleviin tekijöihin.

Tutkielman toisessa luvussa käsitellään valtiollista kybervaikuttamista luokittelemalla se kybervakoiluun, kyberterrorismiin, yleiseen kyberrikollisuuteen sekä kybersodankäynnin määrittäviin tekijöihin. Tämä luku käsittelee vaikuttamista teknisestä sekä poliittisesta näkökulmasta. Luvun lopussa jatketaan kybervaikuttamisen käsittelyä keskittyen 2000-luvulla tapahtuneisiin merkittäviin valtiollisiin kyberhyökkäyksiin. Näitä hyökkäyksiä käsittelevässä alaluvussa esitetään aikaisemmin käsiteltyjä asioita reaalimaailman esimerkein, jotta 2000-luvun kybervaikuttamisen tilannekuvasta saadaan näkemys.

Toisen luvun alustuksella kolmas luku syventyy Kiinan kybervaikuttamiseen ja kuvailee reaalimaailman esimerkein Kiinan intressejä sekä valtion valmistautumista kybervaikuttamiseen. Luvussa kerrotaan myös saavutetuista vaikutuksista ja miten puolustava valtio on valmistautunut hyökkäyksiin. Viimeisessä kappaleessa kandidaatintutkielman sisältö koostetaan yhteen ja kirjallisuuskatsauksen tärkeimmät kohdat esitetään tiivistetysti.

2 Valtiollinen kybervaikuttaminen

Valtiollisella kybervaikuttamisella tarkoitetaan tässä kontekstissa valtioiden suorittamaa vaikuttamista, mutta myös eri valtioihin liitettyä vaikuttamista, joka voi olla esimerkiksi tietyn valtion kansalaisen itsenäisesti suoritettu hyökkäys toisessa valtiossa sijaitsevaa yritystä tai kriittistä järjestelmää kohtaan. Vuonna 2001 etelä-korealaislähtöinen kyberhyökkäys kohdistui Japanin opetusministeriön verkkosivustoa kohtaan, mikä myöhemmin paljastui eteläkorealaisten yliopisto-opiskelijoiden aikaansaannokseksi (Gandhi ym. 2011). Edellä mainittu on hyvä esimerkki siitä, miksi yksittäisten toimijoiden hyökkäyksiäkin voidaan käsitellä valtiollisesta näkökulmasta. Vaikuttamisen alkuperän selvitessä mainitaan lähes aina jokin valtio. Valtiollinen kybervaikuttaminen voi myös olla valtion sisäistä vaikuttamista kansalaisia kohtaan, mutta tämän tutkielman tarkoitus on keskittyä pääsääntöisesti valtakunnalliset rajat ylittävään toimintaan.

2.1 Kyberhyökkäykset

Kyberhyökkäystapojen kirjo on laaja ja hyökkäystapa riippuu paljon hyökkääjän motiiveista, mutta myös ympäristöstä, jossa toiminta on tarkoitus suorittaa. Lähtökohtaisesti hyökkääjän täytyy olla tietoinen kohdejärjestelmistä ja laitteista etenkin yksityiskohtaisia hyökkäyksiä toteuttaessa. Karkeasti jaoteltuna hyökkäys on mahdollista toteuttaa joko verkon välityksellä tai fyysisesti järjestelmään kytkeytyneenä. Olemassa olevia ja tunnettuja hyökkäämistapoja on olemassa runsaasti, mutta valtiolliseen vaikuttamiseen liittyen tarkoituksena on tuoda esille kolme eri kategorian hyökkäystä mahdollisen haitallisen vaikutuksen ymmärtämiseksi.

Yksi tunnetuimmista ja yleisimmistä suuriin palveluihin kohdistuvista uhista on DDoS-hyökkäys (Distributed Denial of Service). DDoS-hyökkäyksen, eli hajautetun palvelunestohyökkäyksen, tarkoituksena on estää palvelun käyttäjiä pääsemästä hyökkäyksen kohteena olevaan palveluun (Zargar, Joshi ja Tipper 2013). Hyökkäys tapahtuu kohdistaen suuria määriä palvelupyyntöjä jatkuvalla toistolla eri laitteilta tarkoituksena hidastaa merkittävästi tai jopa kaataa kyseinen palvelu (Zargar, Joshi ja Tipper 2013). Strategisesta näkökulmasta DDoS-hyökkäyksellä on mahdollista vaikuttaa vakavin seurauksin käyttäen DDoS-hyökkäyksen

esimerkkiympäristönä vuosina 2020 ja 2021 COVID-19 viruksen vaikutuksen alaista poikkeuksellista toimintaympäristöä. Terveydenhuoltoon liittyvien tietojärjestelmien toimintakyvykkyys on elintärkeässä roolissa tiedon saatavuuteen liittyen, ja esimerkiksi potilastietojärjestelmän joutuessa DDoS-hyökkäyksen kohteeksi, seuraukset voivat olla kohtalokkaita tartuntojen lisääntyessä ja hoitopaikkojen kuormittuessa.

Toinen merkittävä sekä yrityksiä että valtioita koskettava kyberhyökkäys on tietojen kalastelu (phising). Tietojen kalastelulla voidaan tarkoittaa kohteena olevan käyttäjän harhaanjohtamista huijaussivustoille (Dhamija, Tygar ja Hearst 2006) tai haitallisen liitteiden lähettämistä vastaanottajalle (El Aassal ym. 2020). Tietojen kalastelun merkittäviä väyliä ovat viestintään tarkoitetut alustat. Tietojen kalastelussa hyökkääjän pyrkimyksenä voi esimerkiksi olla kohdekäyttäjän henkilökohtaisten tietojen kerääminen omiin tarkoituksiinsa ohjaamalla kohdekäyttäjä alkuperäistä sivustoa esittävälle valesivustolle. Valesivustojen avulla hyökkääjä pyrkii esimerkiksi siihen, että kohde luovuttaa käyttäjätunnuksensa ja salasanansa johonkin palveluun. Tietojen kalastelua voidaan pitää merkittävänä valtiollisena uhkana ja esimerkiksi Yhdysvalloissa tietojen kalastelusta johtuvien taloudellisten tappioiden määrä yrityksissä on arvioitu olevan vuosittain noin 100:sta miljoonasta kolmeen miljardiin Yhdysvaltain dollaria (Vayansky ja Kumar 2018). Arvion vaihteluväli on suuri, koska kaikkea taloudellisiin tappioihin liittyvää dataa ei ole saatavilla (Vayansky ja Kumar 2018). Yksityisiin yrityksiin kohdistuvat hyökkäykset eivät välttämättä ole suoraa valtiollista vaikuttamista, mutta yritysten taloudellisilla tappiolla on suora vaikutus maan talouteen ja esimerkiksi pörssiin. Yrityksiin kohdistuvat merkittävät hyökkäykset työllistävät valtiollisia toimijoita ja esimerkiksi tutkintaan käytetyt resurssit kuormittavat viranomaisia kuten poliisia ja rikostutkijoita. Näin ollen voidaan todeta, että valtiollinen näkökulma tulee esiin tämänkaltaisissa tapauksissa hyökkäysten seurauksien tutkinnassa ja jälkitoimien arvioinnissa.

Haittaohjelmia (malware) pidetään valtiollisina uhkina, koska niiden on koettu ajan kuluessa kykenevän suuriinkin vahinkoihin. Haittaohjelmien kategoriaan kuuluvat esimerkiksi kiristyshaittaohjelmat (ransomware), madot (computer worms) ja troijalaiset hevoset (trojan horses). Yksi yleisimmin mainittu on tietokonemato (worm) nimeltä Stuxnet, jonka avulla hyökättiin Iranin ydinvoimaloihin. Stuxnetin todettiin olevan ensimmäinen hyökkäys, jonka avulla on saavutettu fyysistä vahinkoa yli kansainvälisten rajojen ja sitä on myös pidet-

ty esimerkkinä uudesta sodankäynnin muodosta (Lindsay 2013). Stuxnetin oletetaan olleen Yhdysvaltojen ja Israelin yhteinen operaatio liittyen Yhdysvaltojen kyberkampanjaan Irania vastaan (Lindsay 2013).

2.1.1 Kybervakoilu

Kybervakoilun motiivi on sama kuin perinteisessä vakoilussa, eli hankkia tietoa salassa tiedustelemalla. Kybervakoilussa ympäristönä toimii verkko ja siihen liitetyt järjestelmät, mutta tiedustelu ei välttämättä ole aina laitonta. Vakoojat hyödyntävät internetistä löytyvää informaatiota suurimmaksi osaksi tiedonkeruuseen, mitä kutsutaan julkisten lähteiden tiedusteluksi (OSINT, Open Source Intelligence), mutta yleistä on hyödyntää hyökkäyksellisissä operaatioissa myös hakkerointikeinoja hankittaessa tietoja, joita ei ole julkisesti saatavilla verkosta (Geers 2009). Kybervakoilulla tarkoitetaan tässä kontekstissa kyberhyökkäysten avulla suoritettua vakoilua, kuten esimerkiksi tietojen kalastelua tai haittaohjelmien hyödyntämistä, minkä pyrkimyksenä on saada sensitiivistä informaatiota haltuun tai vaikuttaa johonkin.

Kybervakoiluun liitetään tyypillisiä työkaluja, joita on mahdollista hyödyntää esimerkiksi bottiverkkojen välityksellä. Bottiverkolla tarkoitetaan hyökkääjän haltuunottamia verkkolaiteita, jotka on kaapattu osaksi niin kutsuttua bottiverkkoa, ja jonka avulla on mahdollista toteuttaa suuren kapasiteetin hyökkäyksiä. Bederna ja Szadeczky (2019) mainitsevat monia esimerkkejä kybervakoiluun soveltuvista työkaluista, jotka yleisesti toimivat bottiverkkojen kanssa (Bederna ja Szadeczky 2019). Listaan kuuluu esimerkiksi keylogger ja troijalaiset hevoset (Bederna ja Szadeczky 2019).

Kybervakoilu liittyy olennaisesti valtiolliseen toimintaan ja on usein valtakunnalliset rajat ylittävää. Esimerkiksi Venäjän valtion tukemaksi tunnistettu vakoojaryhmä "The Dukes"on kohdistanut hyökkäyksiään länsimaita, politiikkaa ja muita organisaatioita kohtaan jo vuosien ajan (Limnéll 2015).

2.1.2 Kyberterrorismi

Digitalisaation kehittyessä ja palveluiden siirtyessä verkkoympäristöön, myös terroristiorganisaatioiden intressit kohdistuvat yhä enenevissä määrin verkkoon ja sen infrastruktuuriin. Kyberterrorismi voidaan määritellä pyrkimykseksi lamauttaa kriittistä kansallista infrastruktuuria ja aiheuttaa pelkoa valtioiden ja kansalaisten keskuudessa hyökkäystyökalujen avulla (Lewis 2002). Kyberterrorismi määritellään myös ei-valtiollisten toimijoiden suorittamaksi digitaaliseksi politiikaksi, jonka pyrkimys on poliittisessa, sosiaalisessa ja uskonnollisessa vaikuttamisessa (Kenney 2015).

Terroristiset teot yhdistetään usein terroristiorganisaatioihin ja niiden jäseniin. On kuitenkin havaintoja valtioiden suorasta osallistumisesta terroristisiin kyberhyökkäyksiin. Pohjois-Korean kyberjoukot suorittivat kyberhyökkäyksen vuonna 2009 Etelä-Korean kansalliseen ympäristötutkimuksen instituuttiin varastaen yli 2000 salaista dokumenttia sisältäen tietoja 700 yrityksestä, jotka käsittelevät myrkyllisiä kemikaaleja (Heickerö 2014). Varastettujen tietojen perusteella arvioitiin, että niitä olisi mahdollista hyödyntää terrori-iskussa, mikä luokitteli teon kyberterrorismiksi (Heickerö 2014).

Julkisuuteen ei ole tuotu ihmishenkiä vaatineita kyberterroristisia tekoja tähän päivään mennessä ja Kenneyn (2015) mukaan teot ovat olleet toimintaa häiritseviä, ei tuhoavia (Kenney 2015). Esimerkiksi vuonna 2008 Spanairin lentokoneen keskustietokone oli haavoittunut troijalaisesta hevosesta, minkä seurauksena lentäjät eivät saaneet tietoa lennonaikaisista varoituksista (Heickerö 2014). Lentokone putosi nousun jälkeen Madridin lentokentän läheisyydessä vaatien 154:n ihmisen hengen (Heickerö 2014). Alkuperää ei ole saatu selville ja näin ollen edellämainittua tapahtumaa on mahdotonta luokitella kyberterroristisista piirteistä huolimatta. Tapahtuma on kuitenkin luonteensa ansiosta esimerkki siitä, minkälaiseen kyberterrorismiin olisi syytä varautua tulevaisuudessa fyysisten vahinkojen minimoimiseksi.

2.1.3 Yleinen kyberrikollisuus

Kyberrikollisuudella tarkoitetaan yleisesti tietotekniikan ja verkon välityksellä tehtyjä rikoksia. Kyberrikoksiksi luokitellaan myös kybervakoilu ja kyberterrorismi, mutta tässä kontekstissa kyberrikollisuudella tarkoitetaan yksilöiden ja järjestäytyneiden ryhmittymien tekemiä

yleisimpiä rikoksia, kuten petoksia, varastamista ja identiteettivarkauksia. Kyberrikollisuuteen liittyy olennaisesti erilaiset hyökkäystavat, joita käsiteltiin alaluvussa 2.1. Kybervakoiluun ja kyberterrorismiin liittyy vahvasti tekijän motiivi, mutta tämän alaluvun tarkoitus on käsitellä niin kutsuttuja yleisiä kyberrikoksia, joiden motiivi on yleensä vain esimerkiksi oman taloudellisen tai statuksellisen edun tavoittelu.

Kyberrikollisuudelle tunnuksenomaista on käyttää tietokonetta joko työkaluna rikoksiin, kohteena rikokselle tai molempia yhtä aikaa (Dashora 2011). Kyberrikollisuudesta käytetään myös termiä "kyber-riippuvainen rikollisuus"(McGuire ja Dowling 2013), joka kuvailee terminä hyvin rikosten luonnetta. Kyberrikoksia, joissa tietokonetta käytetään työvälineenä, ovat esimerkiksi talousrikokset, laittomat markkinat sekä immateriaali- ja tekijänoikeuksiin liittyvät rikokset (Dashora 2011). Yleisesti voidaan todeta, että kaikki rikokset, jotka täyttävät edellämainittuja tunnuspiirteet, voidaan luokitella enemmän tai vähemmän kyberrikollisen tekemiksi kyberrikoksiksi. Esimerkkeinä kohteen mukaan luokiteltavista kyberrikoksista mainitaan muun muassa "sähköposti pommitukset", järjestelmien anastukset sekä kohdejärjestelmän vahingoittamiset (Dashora 2011).

Kappaleessa käsiteltyjä kyberrikoksia ei välttämättä liitetä mihinkään valtioon, vaan tekijästä puhutaan joko yksilö- tai ryhmätasolla, mikäli tekijä on selvillä. Rikoksiin liittyen mainitaan usein esimerkiksi hyökkäyksen alkuperämaa tai tekijän kansalaisuus, mikäli nämä ovat selvillä. Tämä liittää rikoksen epäsuorasti johonkin tiettyyn valtioon. Hyvä esimerkki yksilön tekemästä laajasta kyberrikoksesta on kanadalaisen Michael Calcen vuonna 2000 toteuttama palvelunestohyökkäys yhdysvaltalaista verkkopalvelu-yritys Yahoota kohtaan (Deshmukh ja Devadkar 2015). Calce myös jatkoi hyökkäyksiään heikentäen CNN:n, eBayn, Dell:n ja Amazonin palvelimia osoittaen, kuinka helppoa suurien verkkosivustojen vahingoittaminen on (Deshmukh ja Devadkar 2015). Calcen hyökkäyksien perusteella on mahdollista päätellä, että kyberrikolliselle teon motiivi voi ainoastaan olla oman kyvykkyyden ja taitojen osoittaminen eikä rikokselle välttämättä löydy suoraa valtiosidonnaisuutta.

2.2 Kybersodankäynnin määrittävät tekijät

Kybersodankäyntiin liittyen todetaan, että olemassa ei ole laajalti hyväksyttyä määritelmää sekä termit kybersota (cyber war) ja kybersodankäynti (cyber warfare) eivät ole tarpeeksi selkeästi eroteltuja toisistaan (Robinson, Jones ja Janicke 2015). Parks ja Dugganin (2011) määritelmä määrittelee kybersodankäynnin tietoverkkohyökkäysten, puolustuksen ja erikoisten teknisten operaatioiden yhdistelmäksi (Parks ja Duggan 2011). Määritelmä ei kuitenkaan ota kantaa hyökkääjän motiiveihin ja tavoiteltuun päämäärään. Sodankäynnille tyypillistä on kuitenkin kahden tai useamman osapuolen läsnäolo sekä vaikuttaminen puolelta toiselle. Moderneihin valtioihin liittyen todetaan, että jokaisen tulisi olla varautunut olemaan kybersotaan liittyvän hyökkäyksen kohde sekä olemaan valmis suorittamaan vaikutuksellinen vastahyökkäys (Colarik ja Janczewski 2011).

Kybervaikuttamisen ja kybersodankäynnin rajaa ei voida määritellä yksiselitteisesti. Usein kybersodankäynti mielletään vahvasti valtiolliseksi toiminnaksi, kuten myös perinteinen sodankäynti. Robinson, Jones ja Janicke (2015) tuovat esille mallin kybervaikuttamisen määrittelemiseksi, mikä keskittyy tekijään ja sen vahingolliseen päämäärään (Robinson, Jones ja Janicke 2015). Kyberympäristön ulkopuolella sodankäynnin päämäärä on saavuttaa sotilaallisia tavoitteita, mutta esimerkiksi myös vakoilun tarkoitus voi olla tavoitella sotilaallista informaatiota salassa. Tekoon on helpompi liittää sodankäynnillinen intressi, mikäli tekijä on valtio yksilön sijaan. Jos tekijä on esimerkiksi terroristiorganisaatio, tekoon on luonnollisempaa liittää terrorismin intressi. Mikäli kyberhyökkäykseen liittyen tekijä on valtiollinen toimija tavoitteenaan sotilaallinen päämäärä, on teko mallin mukaan luokiteltavissa kybersodankäynniksi. Artikkelin tekijöiden mukaan kybersota määritellään valtion julistamaksi sodaksi, jossa tarkoituksena on käyttää vain kybersodankäynnin keinoja. (Robinson, Jones ja Janicke 2015)

Kybersodankäynnin määritelmät voivat sisältää myös muita määrittäviä piirteitä, kuten esimerkiksi kineettisen vaikutuksen reaalimaailmaan (Parks ja Duggan 2011). Määritelmiä on olemassa runsaasti ja eroavaisuuksia niiden välillä ilmenee usein. Kuitenkin kybersodankäyntiin liittyen pääpiirteinä voidaan pitää valtion keskeistä roolia vaikuttamisessa hyökkäyksellisesti ja puolustuksellisesti sekä vaikuttamisen päämäärää kriittisissä ja strategisissa kohteissa. Kohde voi olla kirjaimellisesti esimerkiksi sotilaallinen tietojärjestelmä tai kom-

ponentti toisen valtion kriittisessä infrastruktuurissa.

2.3 Valtiollisia kyberhyökkäyksiä 2000-luvulla

Historiallisesti merkittäviä valtiollisia kyberhyökkäyksiä on tapahtunut 2000-luvun aikana useasti. Tässä luvussa on tarkoitus tuoda esille muutamia niistä. Kyberhyökkäyksistä on olemassa rajallisesti informaatiota, koska tarkkoja yksityiskohtia ei välttämättä tuoda julkisuuteen tapahtumien luonteen takia. Muutamien esimerkkien avulla on kuitenkin mahdollista saada näkemys 2000-luvun tapahtumista ja tilannekuvasta kybervaikuttamiseen liittyen. Kiina on ollut monien merkittävien kyberhyökkäysten takana ja Kiinan kybervaikuttamiseen keskitytään tarkemmin seuraavassa luvussa case-luontoisesti.

Vuonna 2007 Viroon kohdistuneita kyberhyökkäyksiä pidetään yhtenä merkittävimmistä kybersodankäynnin tapahtumista. Kyberhyökkäykset alkoivat, kun Viro päätti siirtää Neuvostoliiton toisen maailmansodan muistomonumentin keskeiseltä paikalta syrjäisemmälle, koska Viron venäläiset käyttivät tämän monumentin aluetta mielenosoitusten ja protestien paikkana Viron hallintoa kohtaan. Monumentin siirtäminen aiheutti suuria mellakoita Virossa, mutta myös laajoja kyberhyökkäyksiä Viroa kohtaan. Hyökkäykset olivat verkkosivujen vandalisointia sekä palvelunestohyökkäyksiä. Suurin hyökkäys sijoittui päivämäärälle 9.5.2007, jolloin Venäjällä juhlitaan toisen maailmansodan voittoa saksalaisista. Viro kuitenkin pystyi vastaamaan hyökkäyksiin tehokkaasti ja seuraukset olivat vain palveluiden hetkellisiä häiriöitä. Selvyyttä hyökkääjästä ei ole, mutta hyökkäyksistä epäillyn on arvioitu liittyvän Venäjään hyökkäyksen luonteen ja motiivien johdosta. (Ashmore 2009)

Sony Pictures Entertainmentiin (SPE) kohdistunut kybervakoilu ja kyberhyökkäys vuonna 2014 on esimerkki valtion kohdistamasta vaikuttamisesta yksityisen sektorin yritykseen. Vuoden 2014 loppupuolella SPE:n oli tarkoitus julkaista Pohjois-Koreaan liittyvä satiirielokuva "The Interview". Marraskuussa 2014 SPE:iin kohdistettiin kyberhyökkäys ryhmän "Guardians of Peace"toimesta, joka tyhjensi yrityksen kovalevyjä ja julkaisi yrityksen materiaalia ja tietoja julkisuuteen. "Guardians of Peace"kiristi yritystä jättämään elokuvan julkaisematta. Hyökkäys arvioitiin Sonyn ja Yhdysvaltain hallinnon tutkijoiden toimesta Pohjois-Korean aikaansaannokseksi, koska haittaohjelmassa oli havaittavissa samankaltaisuuksia ai-

emmin epäiltyihin Pohjois-Korean hyökkäyksiin yhdysvaltalaisia ja etelä-korealaisia kohteita kohtaan. Hyökkäyksen ajankohta kohdisti myös epäilyt Pohjois-Koreaan. (Haggard ja Lindsay 2015)

Yksi kaikkien aikojen suurimmista tietomurroista, joka ilmoitettiin julkisuuteen vuonna 2016, on yhdysvaltalaiseen yritykseen Yahoo kohdistunut tietomurto. Yahoon mukaan tietomurron kohteeksi joutui noin 500:n miljoonan käyttäjän henkilökohtaisia tietoja, mikä tapahtui vuoden 2014 lopussa (Trautman ja Ormerod 2016). Vuonna 2017 Yhdysvaltain oikeusministeriö kohdisti syytteet Venäjän valtion agentteihin (Trautman ja Ormerod 2016). Tämän tutkielman aiemman määritelmän mukaan tapahtuma voidaan luokitella yleiseksi kyberrikollisuudeksi, koska hyökkäyksen kohteena oli listautunut yhdysvaltalainen pörssiyhtiö, kybervaikuttaminen oli yksipuolista eikä hyökkäyksen motiiveista ole selkeää ymmärrystä.

3 Case Kiina

Kiinaa pidetään yhtenä maailman suurvalloista, mutta myös yhtenä suurena globaalina kybervaikuttajana. Kiina on yksi maailman sulkeutuneimmista valtioista, joka seuraa aktiivisesti kansalaistensa liikkeitä. Kybertoiminnan osalta Kiina on ollut osallisena monessa merkittävässä hyökkäyksessä viime vuosikymmenten aikana. Kiinan kybertoimintaa voidaan ajatella myös idän pyrkimyksenä vaikuttaa länsimaihin sekä kerätä tietoa länsimaista. Edellä mainittua puoltaa se, että monen merkittävän kiinalais-lähtöisen hyökkäyksen kohteena on ollut länsimaa. Kiinasta tekee mielenkiintoisen kohdemaan tutkimuksen osalta se, että asioista tiedottaminen ei ole yhtä avointa kuin esimerkiksi Euroopan unionin sisällä ja tutkimustietoa Kiinan toimista on saatavilla rajallisesti. Tässä luvussa keskitytään Kiinan valtion rooliin maan kybervaikuttamisessa ja sen taustalla. Luvussa kuvataan esimerkein Kiinan toteuttamia hyökkäyksiä sekä niiden motiiveja, ja tuodaan esille esimerkki puolustajan näkökulmasta.

3.1 Valtiosidonnaisuus ja valmistautuminen

Kiinan valtion tiedetään aktiivisesti rahoittavan tietoverkko-operaatioihin liittyvää tutkimusta sekä hyökkäyksellisessä että puolustuksellisessa näkökulmassa, mikä kohdistuu Kiinan IT-yrityksiin sekä siviili- että asevoimien yliopistoihin. Päätösvalta käyttää tietoverkko-operaatioita kriiseihin liittyen on Kiinan armeijan ja valtion ylimmällä johdolla. Kuitenkin operaatioiden operatiivisen johdon väitetään olevan Kiinan armeijalla itsellään. Kiinan armeijan tiedetään olevan myös vahvasti riippuvainen kaupallisen sektorin yrityksistä armeijatason mikroelektroniikkan sekä tietoliikenteen tutkimukseen ja kehitykseen liittyen. (Krekel, Adams ja Bakos 2014)

Kiinassa on laaja yksilöllisesti ja verkkoryhmissä toimiva aktiivinen hakkeriyhteisö, joka koostuu ammattimaisista osaajista ja joka on kehittänyt monipuolista tietämystä keskuudessaan. Yhteisö koostuu esimerkiksi haittaohjelmatyökalujen kehittäjistä, tietoturvatutkijoista sekä yleisesti aloittelijoista ja ammattilaisista. Työkalut ja tekniikat, joita ryhmässä tuodaan esille, ovat olleet black hat -hakkereiden eli rikollisten suosiossa. (Krekel 2009)

2000-luvun alussa Kiinalle selvisi, että kiinalaiset hakkeriryhmät olivat olleet mukana siihen

aikaan käynnissä olleissa "hakkerisodissa", minkä seurauksena Kiina loppujen lopuksi tuomitsi hakkeroinnin laittomaksi, eikä tätä hyväksyttäisi (Krekel 2009). Tämän seurauksena monet hakkeriorganisaatiot loivat suhteita yrityksiin, jotka ovat läheisiä Kiinan turvallisuus organisaatioiden tai itse Kiinan hallinnon kanssa (Krekel 2009). Edellä mainitusta voidaan päätellä, että niin historiassa kuin tänä päivänäkin, Kiinan valtio on ollut sitoutunut ainakin jossain määrin Kiinasta lähtöisin olevaan kybervaikuttamiseen, tapahtui se laajemmin valtiollisten tietoverkko-operaatioiden tai yksittäisten hyökkäysten merkeissä.

3.2 Hyökkäykset, niiden motiivit ja puolustajan näkökulma

Kiinalaisten kyberrikollisten motiiveista todetaan, että hyökkäykset kohdistuvat Itä-Euroopan ja Venäjän kyberrikollisiin verrattuna osuudellisesti enemmän immateriaalioikeuksiin ja yrityssalaisuuksiin. 2000-luvulla esimerkiksi suuret yritykset, kuten Motorola, DuPont ja Ford Motor Company, ovat joutuneet tämänkaltaisen kyberrikollisuuden kohteeksi. Ford Motor Companyn tapauksessa Fordin tuotepäällikkö oli ottanut noin 4000 laitonta digitaalista kopiota Fordin dokumenteista, minkä tarkoituksena oli edesauttaa hänen pääsyään töihin kiinalaiseen autoalan yritykseen. Fordiin liittyvä tapaus on hyvä esimerkki kyberrikoksesta, jossa välikätenä toimi reaalimaailman ihminen eikä rikosta toteutettu verkon välityksellä. (Kshetri 2013)

Kybervakoiluun liittyen Kiinaan on jäljitetty tunnettu kyberoperaatio vuodelta 2003 koodinimeltään "Titan Rain", joka ilmoitettiin julkisuuteen vasta vuonna 2005. Yhdysvaltain ilmailu- ja avaruushallintovirasto Nasaan, sekä joihinkin muihin virastojen tietoverkkoihin Yhdysvalloissa kohdistettiin kyberhyökkäys, jonka seurauksena hyökkääjä sai haltuun informaatiota ilmailuspesifikaatioista sekä lentosuunnitelmajärjestelmistä. (Karatzogianni 2008) Vuonna 2009 tutkijat paljastivat kybervakoilutietoverkon nimeltään "GhostNet", jonka takana epäillään olleen Kiinan hallinnon. Hyökkäys luokitellaan taloudelliseksi ja poliittiseksi hyökkäykseksi, jonka kohteena oli Dalai Laman tietokone tarkoituksena saada haltuun informaatiota. Hyökkäyksen tutkinnan myötä haavoittuneita tietokoneita löydettiin myös muun muassa Iso-Britanniasta, Yhdysvalloista sekä Indonesiasta. (Gandhi ym. 2011)

Vaikka historian aikana Kiina on valtion tasolla keskittänyt kybervaikuttamista ulkomaita

kohtaan, Kiinan sisäistä kyberrikollisuutta tapahtuu myös. Kiinan kybertoimintaan liittyen tuodaan esille kiinalaisten kyberrikollisten kiinnostus maan sisäisiä toimialoja kohtaan, kuten esimerkiksi uhkapelialaa. Sisäiset markkinat nähdään rikollisten kohteena, joilla ei ole vahvaa organisaatiota toimintansa taustalla. Kiinan sisäisille kohteille on tyypllistä heikot puolustusmekanismit hyökkäyksiä vastaan. Valtion sisäisiin hyökkäyksiin liittyen mainitaan myös Kiinan valtion kohdistamat hyökkäykset niitä verkkosivuja kohtaan, jotka eivät noudata Kiinan sääntelyä. (Kshetri 2013)

Yhdysvallat tunnistetaan usein Kiinan kybervaikuttamisen kohteena ja tämän voi myös perustella kahden suurvallan, lännen ja idän, välisenä kanssakäymisenä. Kuitenkin kybersodankäyntiin liittyen Yhdysvallat ovat tietoisia ja varautuneita Kiinan kybervaikuttamiselle. Esimerkiksi tiedetään, että kiinalaiset tietävät Länsi-Tyynenmeren alueen tietoverkkojen olevan strategisesti ja kapasiteetin kannalta tärkeitä Yhdysvalloille ja niihin kohdistettu hyökkäys voisi johtaa konfliktiin (Gompert ja Libicki 2014). Yhdysvallat voivat olettaa Kiinan käyttävän kybersodankäynnin keinoja aseelliseen konfliktiin liittyen ja kohdistaen hyökkäyksiään myös ei-sotilaallisiin tietoverkkoihin. Todennäköisin kohde Kiinalle olisi kuitenkin järjestelmät, joilla mahdollistetaan Yhdysvaltain joukkojen toiminta Länsi-Tyynenmeren alueella. (Gompert ja Libicki 2014)

4 Yhteenveto

Valtiollisesta kybervaikuttamisesta voidaan todeta, että keinoja on olemassa monia, mutta teon motiivit ovat avainroolissa. Kyberhyökkäykset ovat teknisesti samantapaisia riippuen kuitenkin käytetystä hyökkäystavasta. Hyökkäyksen kohdistaminen oikeaan kohteeseen riippuu täysin hyökkääjän motiiveista. Valtion rooli hyökkäyksissä on vaihteleva ja se riippuu pitkälti siitä, onko kyseessä poliittista vaikuttamista vai onko hyökkäyksen tarkoituksena vain aiheuttaa ylimääräistä kuormitusta kohteelle. Kuten aikaisemmin tutkielmassa mainittiin, valtio liitetään usein yleisimpiinkin hyökkäyksiin alkuperämaana, jos esimerkiksi tarkempia tietoja kohteesta ei ole saatavilla tai hyökkäys on valtiolliset rajat ylittävä.

Kyberhyökkäykset ja vaikuttaminen on kehittynyt merkittävästi 2000-luvun alusta tähän päivään. On itsestään selvää, että merkittävien hyökkäysten myötä myös niihin varautuminen on kehittynyt. 2000-luvun alusta alkaen merkittäviin hyökkäyksiin liittyen mainitaan usein joko Yhdysvallat, Kiina tai Venäjä, mikä kertoo suurvaltojen panostuksesta kybertoimintaan. Valtioiden kyberjoukkojen vahvuudet ja sijainnit ovat pitkälti salaista tietoa, mistä kertoo myös se, että internetistä on erittäin haastavaa löytää luotettavaa informaatiota edellä mainittuihin liittyen. Kuitenkin tapahtuneiden hyökkäysten yhteydessä valtiot ovat saaneet merkittävää informaatiota valtioiden kybervaikuttamisesta ja yksittäisistä hyökkäyksistä, koska usein hyökkäyksiä ei ole pystytty pitämään täysin nimettöminä, vaikka tähän olisi pyritty.

Kiinan valtioon liittyen kybervaikuttaminen on merkittävässä roolissa. Valtiolla on vahvat resurssit ja kapasiteetti panostaa kybervaikuttamiseen liittyvään kehitykseen ja tutkimukseen. Esimerkiksi operaatiot "Titan Rain"ja "GhostNet"ovat hyviä esimerkkejä vahvasta kybervaikuttamisesta, joka kykenee esimerkiksi vaikuttamaan huomaamattomana toimijoiden järjestelmissä. Kiinan rooli vahvana kybervaltiona tarkoittaa myös ammattitaitoisia yksilöitä osana vaikuttamista. Kybertoimintaan liittyen valtion koko ei kuitenkaan suoranaisesti määritä, kuinka vahva kyky valtiolla on vaikuttaa kybermaailmassa. Valtiosta riippumatta on tärkeää olla valmis puolustautumaan kybervaikuttamisen haitoilta.

Lähteet

Ashmore, William C. 2009. *Impact of alleged Russian cyber attacks.* Tekninen raportti. Army Command ja General Staff College, Fort Leavenworth, KS, School of Advanced Military Studies.

Bederna, Zsolt, ja Tamas Szadeczky. 2019. “Cyber espionage through Botnets”. *Security Journal,* 1–20.

Colarik, A. M., ja L. J. Janczewski. 2011. “Developing a grand strategy for Cyber War”. Teoksessa *2011 7th International Conference on Information Assurance and Security (IAS),* 52–57. https://doi.org/10.1109/ISIAS.2011.6122794.

Dashora, Kamini. 2011. “Cyber crime in the society: Problems and preventions”. *Journal of Alternative Perspectives in the social sciences* 3 (1): 240–259.

Deshmukh, Rashmi V, ja Kailas K Devadkar. 2015. “Understanding DDoS attack & its effect in cloud environment”. *Procedia Computer Science* 49:202–210.

Dhamija, Rachna, J Doug Tygar ja Marti Hearst. 2006. “Why phishing works”. Teoksessa *Proceedings of the SIGCHI conference on Human Factors in computing systems,* 581–590. Association for Computing Machinery. https://doi.org/10.1145/1124772.1124861.

El Aassal, Ayman, Shahryar Baki, Avisha Das ja Rakesh M Verma. 2020. “An in-depth benchmarking and evaluation of phishing detection research for security needs”. *IEEE Access* 8:22170–22192. https://doi.org/10.1109/ACCESS.2020.2969780.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu ja Phillip Laplante. 2011. “Dimensions of cyber-attacks: Cultural, social, economic, and political”. *IEEE Technology and Society Magazine* 30 (1): 28–38. https://doi.org/10.1109/MTS.2011.940293.

Geers, Kenneth. 2009. “The Cyber Threat to National Critical Infrastructures: Beyond Theory”. *Information Security Journal: A Global Perspective* 18 (1): 1–7. https://doi.org/10.1080/19393550802676097.

Gompert, David C., ja Martin Libicki. 2014. “Cyber Warfare and Sino-American Crisis Instability”. *Survival* 56 (4): 7–22. https://doi.org/10.1080/00396338.2014.941543.

Haggard, Stephan, ja Jon R Lindsay. 2015. “North Korea and the Sony hack: Exporting instability through cyberspace”.

Heickerö, Roland. 2014. “Cyber Terrorism: Electronic Jihad”. *Strategic Analysis* 38 (4): 554–565. https://doi.org/10.1080/09700161.2014.918435.

Karatzogianni, Athina. 2008. *Cyber-conflict and global politics.* Routledge.

Kenney, Michael. 2015. “Cyber-terrorism in a post-stuxnet world”. *Orbis* 59 (1): 111–128. https://doi.org/10.1016/j.orbis.2014.11.009.

Klimburg, Alexander. 2011. “Mobilising Cyber Power”. *Survival* 53 (1): 41–60. https://doi.org/10.1080/00396338.2011.555595.

Krekel, Bryan. 2009. *Capability of the People’s Republic of China to conduct cyber warfare and computer network exploitation.* Tekninen raportti. Northrop Grumman Corporation, Mclean, VA.

Krekel, Bryan, Patton Adams ja George Bakos. 2014. “Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage”. *International Journal of Computer Research* 21 (4): 333.

Kshetri, Nir. 2013. “Cybercrime and cyber-security issues associated with China: some economic and institutional considerations”. *Electronic Commerce Research* 13 (1): 41–69.

Kumar, Sumeet, ja Kathleen M Carley. 2016. “Approaches to understanding the motivations behind cyber attacks”. Teoksessa *2016 IEEE Conference on Intelligence and Security Informatics (ISI),* 307–309. IEEE. https://doi.org/10.1109/ISI.2016.7745496.

Lewis, James Andrew. 2002. *Assessing the risks of cyber terrorism, cyber war and other cyber threats.* Center for Strategic & International Studies Washington, DC.

Limnéll, Jarno. 2015. “The exploitation of cyber domain as part of warfare: Russo-Ukrainian war”. *International Journal of Cyber-Security and Digital Forensics* 4 (4): 521–533.

Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare”. *Security Studies* 22 (3): 365–404. https://doi.org/10.1080/09636412.2013.816122.

McGuire, Mike, ja Samantha Dowling. 2013. “Cyber crime: A review of the evidence”. *Summary of key findings and implications. Home Office Research report* 75.

Parks, R. C., ja D. P. Duggan. 2011. “Principles of Cyberwarfare”. *IEEE Security Privacy* 9 (5): 30–35. https://doi.org/10.1109/MSP.2011.138.

Robinson, Michael, Kevin Jones ja Helge Janicke. 2015. “Cyber warfare: Issues and challenges”. *Computers & security* 49:70–94.

Trautman, Lawrence J, ja Peter C Ormerod. 2016. “Corporate Directors’ and Officers’ Cybersecurity Standard of Care: The Yahoo Data Breach”. *Am. UL Rev.* 66:1231.

Vayansky, Ike, ja Sathish Kumar. 2018. “Phishing–challenges and solutions”. *Computer Fraud & Security* 2018 (1): 15–20. https://doi.org/10.1016/S1361-3723(18)30007-1.

Zargar, Saman Taghavi, James Joshi ja David Tipper. 2013. “A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks”. *IEEE communications surveys & tutorials* 15 (4): 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127.