Nina Koivula

KIINAN SUORITTAMAN KYBERVAKOILUN AIHEUTTAMAT PITKÄAIKAISET HAITAT KIBS-YRITYKSILLE

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

TIIVISTELMÄ

Koivula, Nina
Kiinan suorittaman kybervakoilun aiheuttamat pitkäaikaiset haitat KIBS-yrityksille
Jyväskylä: Jyväskylän yliopisto, 2015, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Clements, Kati

Tämä kandidaatintutkielma käsittelee Kiinan suorittaman kybervakoilun aiheuttamia pitkäaikaisia haittoja KIBS-yrityksille. Tutkielma toteutettiin kirjallisuuskatsauksena teorialähtöisesti. Tutkielma selvittää, millaisia haittoja Kiinan suorittama kybervakoilu aiheuttaa KIBS-yrityksille, sekä lisäksi sen, kuinka vakavia nämä KIBS-yrityksille koituneet haitat ovat.

Aihetta on tärkeä tutkia, sillä Kiinan suorittamasta kybervakoilusta on saatu todisteita. Lisäksi kybervakoilusta koituvien haittojen on arvioitu olevan nousussa. Aihetta ei ole aiemmin tutkittu riittävästi, sillä sitä on hankala tutkia, koska yritykset eivät monesti tahdo tuoda julkisuuteen joutuneensa kyberhyökkäyksen uhriksi. Tutkimus myös vaatisi melko pitkällä aikavälillä suoritettua tutkimusta.

Tutkielman tuloksien perusteella voidaan sanoa, että kyberhyökkäyksen aiheuttamat pitkäaikaiset haitat KIBS-yritykselle ovat henkisen pääoman menetys, sekä maineen menetys ja asiakkaiden ja liikekumppanien luottamuksen menetys. Näistä arvioimme henkisen pääoman menetyksen olevan KIBS-yritykselle merkittävämpi haitta. Tutkielman aikana havaittiin myös, että KIBS-yrityksiä vastaan suoritetut kyberhyökkäykset vaikuttavat negatiivisesti länsimaiden talouteen. Tutkielman tulokset ovat kiinnostavia paitsi KIBS-yritysten näkökulmasta, myös länsimaisten valtioiden kannalta.

Avainsanat: kyberhyökkäys, kybervakoilu, henkinen pääoma, maineen menetys, Knowledge-based theory of the firm, tieto, KIBS-yritys, tietointensiiviset liike-elämän palvelut

ABSTRACT

Koivula, Nina
The long-term disadvantages to knowledge intensive business services caused by Chinese cyber espionage
Jyväskylä: University of Jyväskylä, 2015, 27 p.
Information Systems, bachelor's thesis
Supervisor(s): Clements, Kati

This bachelor's thesis covers the long-term disadvantages China's cyber espionage is causing to knowledge intensive business service companies. It was conducted as a literature review and by using a theoretical background. This study tries to find out, which kind of disadvantages cyber espionage conducted by China is causing to knowledge intensive business service companies and how severe these disadvantages are to them.

This is an important topic, since it has been proven that China is performing cyber espionage. Also the disadvantages caused by cyber espionage have been estimated to be on the increase. This topic has not yet been studied enough, mostly because companies do not seem to be willing to make it public knowledge that they have been under a cyber attack. The study would also require a long time to complete it, since the case has to be followed for several years to discover the long-term disadvantages caused by a cyber attack.

According to the results of this study we can say that the long-term disadvantages China's cyber espionage is causing to KIBS-companies are the loss of intellectual property and also losing face of the company and the trust of clients and business associates. We estimate the loss of intellectual property to be the most harmful of these disadvantages especially in the case of KIBS-companies. We also learned that the cyber attacks against KIBS-companies are causing western countries economical disadvantages. On this account, the results of this study are not only interesting to knowledge intensive business service companies, but also to western countries.

Keywords: cyber attack, cyber espionage, intellectual property, losing face, Knowledge-based theory of the firm, knowledge, knowledge intensive business service companies

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Viimeisen kahdenkymmenen vuoden aikana tietojenkäsittely ja tietoverkot ovat kehittäneet liike-elämää uuteen suuntaan, ja nykypäivänä sekä verkossa käytävä kauppa että vanhanaikainen, toimitiloissa käytävä kauppa, ovat riippuvaisia tietoverkoista (Andrijcic & Horowitz, 2006). Tekninen kehitys on avannut liike-elämälle paljon uusia mahdollisuuksia ja luonut kehitystä, mutta toisaalta tuoneet mukanaan uusia uhkia (Andrijcic & Horowitz, 2006).

Kyberrikollisuus on kehittynyt ja sitä käytetään esimerkiksi yritystoiminnan häiritsemiseen ja henkilötietojen varastamiseen (Andrijcic & Horowitz, 2006). Kyberrikollisuus johtaa monesti taloudellisiin tappioihin. Kyberhyökkäykset yrityksiä vastaan voivat aiheuttaa monenlaisia haittoja, hyökkäykset voivat esimerkiksi johtaa henkisen pääoman menetykseen, maineen menetykseen tai jopa oikeudellisiin toimiin yritystä vastaan. (Andrijcic & Horowitz, 2006).

Samaan aikaan Kiinan suorittamasta vakoilusta ja kybersodankäynnistä kirjoitetaan paljon (Inkster, 2013). Kiina onkin pyrkinyt ottamaan länsimaita kiinni teknologisessa kehityksessä, ja monesti se on käyttänyt epärehellisiä keinoja saavuttaakseen tavoitteensa (Wise, 2011; Inkster, 2013)

Esimerkiksi turvallisuusyritys McAfee arvioi, että kyberrikollisuus ja kybervakoilu aiheuttavat maailmanlaajuisesti jopa biljoonan Yhdysvaltain dollarin suuruiset tappiot (Iovan & Dinu, 2014). Tutkielma keskittyy erityisesti pitkäaikaisiin haittoihin, joita koituu kyberhyökkäyksistä, sillä makrotaloudellisesta näkökulmasta ne ovat erityisen haitallisia (Andrijcic & Horowitz, 2006).

Tutkielman tutkimuskysymykset ovat seuraavat:

- Millaisia haittoja Kiinan suorittama kybervakoilu aiheuttaa KIBS-yrityksille?
- Kuinka vakavia nämä KIBS-yrityksille koituneet haitat ovat?

Tutkielma pyrkii vastaamaan tutkimuskysymyksiin tutkielman lopussa. Tutkielma toteutettiin kirjallisuuskatsauksena (Okoli & Schabram, 2010) ja se suoritettiin teorialähtöisesti. Tutkielma pyrkii vastaamaan tutkimuskysymykseen käytetyn teorian pohjalta. Tutkielman viitekehyksenä käytetään esimerkiksi

Grantin (1996 ja 2002), Nonakan, Toyaman ja Nagatan (2000), Demsetzin (1991) ja Alavin ja Leidnerin (2001) teorioihin pohjautuvaa knowledge-based theory of the firm –teoriaa.

Kirjallisuuskatsauksen aineisto on pääasiassa haettu Google Scholar –hakupalvelulla. Lisäksi aineistoa ja taustalukemista on haettu JYKDOK –hakupalvelusta ja Jyväskylän yliopiston kirjastosta. Suurin osa lähdeaineistosta on löytynyt Google Scholar –hakupalvelua käyttämällä, mutta etenkin viitekehyksenä käytettyä teoriaa, knowledge-based theory of the firm –teoriaa, varten on käytetty JYKDOK –hakupalvelua. Haimme tietoa esimerkiksi sanoilla ”cyber attack” ja ”cyber espionage”, ”cyber attack definition” ja ”cyber espionage definition”. Haimme tietoa myös erilaisilla versiolla sanoista ”cyber attack China” ja ”cyber espionage China”, lisäksi ”cyber attack consequence” ja ”cyber attack result”. Lisäksi käytimme hakusanoja ”Chinese culture”, ”cyber espionage disadvantages” ja ”cyber espionage consequences for companies”. Neljättä lukua varten käytimme hyväksemme myös JYKDOK-hakupalvelua ja Jyväskylän yliopiston kirjastoa, josta haimme tietoa sanoilla ”knowledge intensive business services” ja ”knowledge-based theory of the firm”.”cyber espionage disadvantages” ja ”cyber espionage consequences for companies”.

Tutkielman rakenne on seuraava: johdantoa seuraavassa toisessa luvussa määritellään kyberhyökkäys ja kybervakoilu, kolmas luku keskittyy Kiinan ominaispiirteisiin kyberavaruudessa, neljäs luku käsittelee KIBS-yrityksiä ja tutkielman viitekehyksenä käytettyä knowledge-based theory of the firm –teoriaa, ja viides luku keskittyy esittelemään kyberhyökkäysten seurauksia KIBS-yrityksille. Tutkielman lopussa on pohdintaa ja yhteenveto tutkielmasta.

Tutkielman kontribuutio on tärkeimpien kybervakoilun aiheuttamien pitkäaikaisten haittojen tunnistaminen KIBS-yritysten tapauksessa ja haittojen yhteenveto, sekä niiden merkittävyyden arviointi. Tutkielma ei tarkastele erilaisia tapoja suorittaa kyberhyökkäyksiä teknisellä tasolla.

2 KYBERHYÖKKÄYKSEN MÄÄRITTELYÄ

Seuraavassa luvussa esitellään tutkielmassa usein esiintyvää kyberhyökkäykseen liittyvää sanastoa. Kuten Hunker (2010) toteaa, on alalla ongelmana se, että yhteisiä määritelmiä ei juurikaan ole.

2.1 Kyberhyökkäys

Kyberhyökkäykseksi lasketaan Hunkerin (2010) mukaan yritys käyttää hyväksi suojaamatonta kohdetta ilman lupaa. Kyberhyökkäys käynnistetään joukolla tietokonekäskyjä, ja se vaarantaa tietokoneen ja tietoverkkojen turvallisuuden (Madavi & Khandalkar).

Madavi ja Khandalkar toteavat, että hyökkäykset voidaan jakaa kahteen kategoriaan: suoriin ja älykkäisiin hyökkäyksiin. Suora hyökkäys voi olla esimerkiksi palvelunestohyökkäys, joka on lyhytaikainen. Älykäs hyökkäys taas on hyvin suunniteltu. Se voi olla esimerkiksi tunkeutuminen järjestelmään ja järjestelmän tietojen muokkaus. (Madavi & Khandalkar).

Colarik (2006) jakaa kyberhyökkäyksen erilaisiin vaiheisiin. Ensimmäinen vaihe on tiedustelu, jolloin hyökkääjä tekee havaintoja ja kerää tietoa kohteesta. Hyökkäyksen toinen vaihe on järjestelmään tunkeutuminen. Hyökkääjä ei juurikaan saa vahinkoa aikaiseksi ennen järjestelmään tunkeutumista. Ennen tunkeutumista hyökkääjä kykenee lähinnä häiritsemään palvelun saatavuutta. Kolmas vaihe on laajentaa valmiuksia, eli resurssien tarkastelua ja käyttöoikeuksien lisäämistä. Käyttöoikeuksia lisäämällä pyritään saamaan pääsy järjestelmän paremmin suojattuihin osiin. Neljännessä vaiheessa tunkeutuja vahingoittaa järjestelmää tai takavarikoi tietoa. Viimeisessä, eli viidennessä vaiheessa tunkeutuja pyrkii poistamaan todisteet tunkeutumisesta. Monesti tunkeutuja pyrkii suorittamaan kaikki viisi vaihetta, mutta tämä riippuu hyökkäyksestä. (Colarik, 2006).

Hunker (2010) taas jakaa kyberhyökkäykset passiivisiin ja vahingollisiin hyökkäyksiin. Passiivisessa hyökkäyksessä tunkeutuja kopioi ja mahdollisesti poistaa datan, mutta ei varsinaisesti vahingoita sitä. Vahingollisessa kyber-

hyökkäyksessä hyökkääjä saattaa vaihtaa tai muuttaa dataa, tai estää tietoverkkojen toiminnan. (Hunker, 2010).

2.2 Kybervakoilu

Kybervakoilulla tarkoitetaan tunkeutumista vastapuolen järjestelmään, jolloin tarkoituksena on varastaa suojattua tietoa (Rid, 2012). Hunkerin (2010) jaottelun mukaan kybervakoilu on osa passiivisia kyberhyökkäyksiä, jolloin tarkoitus on kopioida dataa. Vakoilu voi olla joko teknistä tai sosiaalista (Rid, 2012).

Fidlerin (2013) mukaan vakoilu voidaan jaotella perinteiseen vakoiluun, taloudelliseen vakoiluun ja teollisuusvakoiluun. Fidler (2013) toteaa, että perinteinen vakoilu ja taloudellinen vakoilu ovat yleensä valtio suorittamia, kun taas teollisuusvakoilu on monesti yrityksen suorittamaan. Perinteinen vakoilu tähtää suojatun tiedon keräämiseen toiselta valtiolta, taloudellisen vakoilun tarkoitus taas on esimerkiksi liikesalaisuuksien vieminen yksityiseltä yritykseltä. Teollisuusvakoilu on yrityksen suorittamaa, jolloin tarkoitus on laittomasti hankkia toisen yrityksen liikesalaisuuksia. (Fidler, 2013). Kybervakoilulla ei ole tarkkaa tavoitetta, vaan sen tarkoitus on kerätä tietoa, joita voidaan käyttää hyväksi (Rid, 2012).

Digitalisoitunut ympäristö lisää toimijoita kybervakoilun alalla, samoin se, että kyberalalla käytetään eniten valtioilta saatua rahaa juuri vakoiluun. Tästä johtuen suurin osa kyberturvallisuusuhkista onkin liittynyt vakoiluun. (Rid, 2012). On arvioitu, että jopa 140 eri maiden tiedustelupalvelua yrittää murtautua Yhdysvaltojen hallinnollisiin ja yksityisiin tietoverkkoihin (Hunker, 2010). Etenkin maiden hallintoa vastaan suunnatusta vakoilusta saadaan harvoin tietoa. Monesti tutkijat eivät myöskään onnistu analysoimaan vakoilun aiheuttamaan uhkaa. (Rid, 2012).

Fidlerin (2013) mukaan monet valtiot näkevät taloudellisen vakoilun olennaisena kansallisen turvallisuuden ja taloudellisen kehityksen kannalta. Suurista puolustusinvestoinneista huolimatta kybervakoilu tuleekin pysymään uhkana sekä yksityiselle että julkiselle sektorille (Rid, 2012).

3 KIINAN OMINAISPIIRTEET KYBERAVARUUDESSA

Seuraava luku käsittelee Kiinan kybertoiminnan historiaa ja esittelee Kiinasta lähtöisin oleville kyberhyökkäyksille ominaisia piirteitä. Luvussa esitellään lyhyesti tutkielman kannalta olennaisia piirteitä kiinalaisesta kulttuurista. Luku esittelee myös Kiinan motiiveja kybervakoilulle, samoin kuin mahdollisia hyötyjä, joita Kiina saa kybervakoilusta.

3.1 Kiinan kybervakoilun historiaa

Kiinassa aloitettiin käyttämään internetiä verrattain myöhään, mutta maan internetin käyttöaste on kasvanut vauhdilla, lisäksi internet on otettu laajasti myös armeijakäyttöön (Inkster, 2013).

Inkster (2013) kertoo, että Kiinan tiedustelusta ja tiedustelupalvelusta, etenkin ulkomaisiin kohteisiin kohdistuvasta tiedustelusta, on vain vähän tietoa. On kuitenkin yleisesti tiedossa, että Kiina harjoittaa kybertiedustelua laajalla alalla käyttäen myös epävirallisia tahoja (Inkster, 2013).

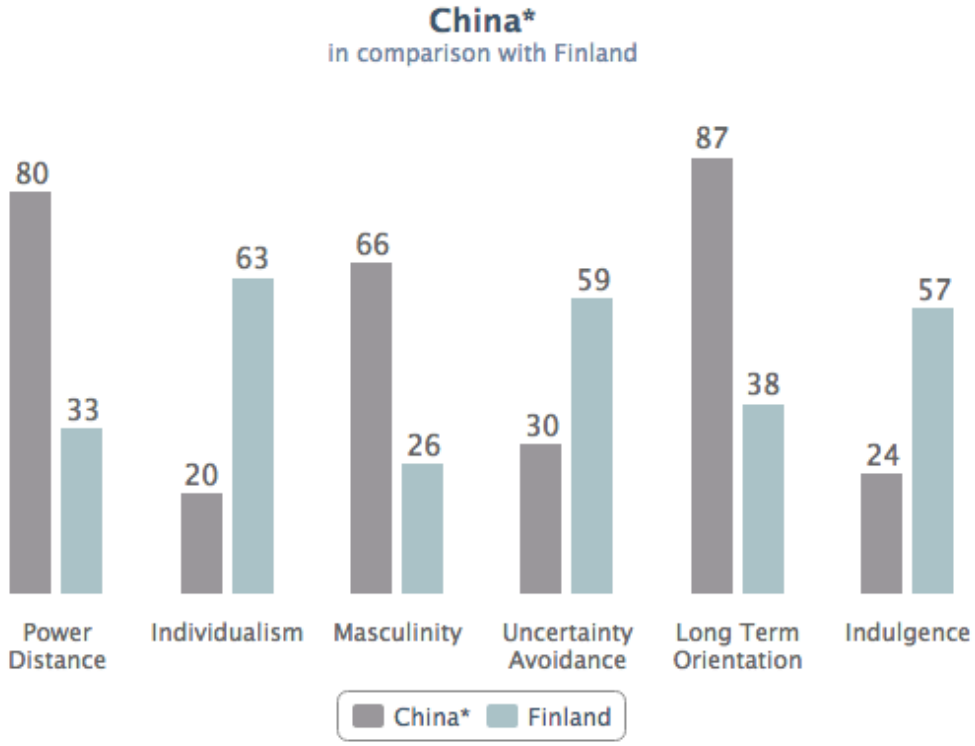
Feigenbaumin (2000) mukaan vuonna 1986 Kiinassa määritettiin etenkin tieteen ja teknologian alalle kohdistuvan ulkomaan tiedustelun olevan avainasemassa Kiinan taloudellisessa kehityksessä. Näin sai alkunsa Plan 863 – ohjelma, joka oli aluksi sotilaallinen, mutta muotoutui myöhemmin projektiksi, jonka tavoitteena oli vähentää Kiinan riippuvuutta ulkomaalaisesta teknologiasta (Feigenbaum, 2000). Wise (2011) kertoo, että ohjelman ulkomaille kohdistuvan tiedustelun aloittaminen sai alkusysäyksen ensimmäisessä Persianlahden sodassa, jossa kiinalaiset järkyttyivät amerikkalaisten tarkkuusaseiden kehittyneisyydestä. Kiina pyrki tämän jälkeen ottamaan länsimaita kiinni esimerkiksi teknologiassa (Wise, 2011).

Kiinan suorittamat laajamittaiset hyökkäykset alkoivat oletettavasti vuoden 2003 tunkeutumisilla Yhdysvaltain hallinnon tietoverkkoon (Inkster, 2013). Tämän jälkeen Kiinasta peräisin olevia hyökkäyksiä on Inksterin (2013) mukaan

havaittu esimerkiksi Yhdistyneessä Kuningaskunnassa, Saksassa ja Uudessa-Seelannissa. Yhdistyneet Kuningaskunnat jopa varoittivat yksityisellä sektorilla toimivia yrityksiä mahdollisista yrityksiin kohdistuvista kyberhyökkäyksistä, jotka ovat peräisin Kiinasta (Inkster, 2013).

3.2 Kiinalainen kulttuuri lyhyesti

Kiinassa vallitsee vahva kollektivistinen kulttuuri, joka tarkoittaa sitä, että ihmiset pyrkivät toimimaan ryhmän edun mukaan, ei niinkään yksilön etua ajatellen. Alla näkyvässä kuviossa näemme selvästi, että Kiinan saama luku individualismista on The Hofstede Centren suorittamassa vertailussa alhainen.



KUVIO 1 Kiinalainen kulttuuri verrattuna suomalaiseen kulttuuriin The Hofstede Centren mukaan

Vertailun vuoksi voimme sanoa, että esimerkiksi Suomen vastaava luku on 63. (The Hofstede Centre).

Kulttuurin Kiinassa voidaan sanoa olevan maskuliininen, joka tarkoittaa sitä, että yhteiskunta suosii kilpailua, saavutuksia ja menestystä. Kiinassa tämä näkyy etenkin vapaa-ajan ja perhesuhteiden uhraamisena. Kuten yllä olevasta kuviosta näkyy, sai Kiina tässä vertailussa korkean vertailuluvun maskuliini-

suudesta. (The Hofstede Centre).

Kiinan saama vertailuluku pitkän aikavälin orientaatiossa on korkea. Tämä tarkoittaa, että yhteiskunta on pragmaattinen ja täten pyrkii mukautumaan muutokseen. Monet pragmaattiset yhteiskunnat uskovat, että totuus riippuu tilanteesta, kontekstista ja ajasta. Pragmaattiselle yhteiskunnalle on tyypillistä säästäväisyys ja pitkäjänteinen tulosten tavoittelu. (The Hofstede Centre).

Kiinassa pitkään vallalla ollut kungfutselaisuus on myös vaikuttanut vahvasti kiinalaiseen käyttäytymiseen ja etiikkaan. Yksi kungfutselaisuuden ajatuksia oli käsitys siitä, että ihmisten tulisi oppia kopioimalla ja imitoimalla. (Yang, 2003). Tämän vaikutukset on edelleen nähtävissä Kiinassa, sillä Kiinasta löytyy maailman suurin määrä väärennettyjä tuotteita (Phillips, 2007).

3.3 Vakoilu ja hyökkäykset

Inkster (2013) toteaa, että Kiinan suorittamasta vakoilusta ja kybersodankäynnistä on kirjoitettu paljon, mutta siitä ei juurikaan ole pitäviä todisteita. Viimevuosina Kiinasta peräisin olevia kyberhyökkäyksiä ja –vakoilua on kuitenkin havaittua paljon (Inkster, 2013). Vakoilu ja hyökkäykset ovat kohdistuneet sekä kotimaahan että ulkomaille, kohteina ovat olleet sekä valtiot, merkittävät yritykset että oppositioryhmät (Inkster, 2013). Mattisin (2012) mukaan viimeaikoina todisteet Kiinan valmiudesta suorittaa operaatioita myös ulkomailla ovat tulleet selvemmiksi.

On löydetty merkkejä siitä, että Kiinan suorittamat kyberhyökkäykset ovat hyvin suunniteltuja (Inkster, 2013). Hyökkäyksissä on esimerkiksi pyritty ymmärtämään, miten kohteena olevat tietoverkot toimivat kyberhyökkäyksen alla (Krekel, Bakos & Barnett, 2009). Krekel ym. (2009) kertoo, että monesti hyökkäykset eivät ole kohdistuneet suoraan kohteeseen, vaan on pyritty esimerkiksi asentamaan troijalainen virus sähköpostin liitetiedostosta kohdetietoverkossa toimivaan tietokoneeseen. Tämä virus saadaan aktivoitua, jolloin päästään käsiksi varsinaiseen kohteeseen. Krekelin ym. (2009) mukaan kyseisessä kyberhyökkäyksessä käytetyt sähköpostit ovat tarkkaan suunniteltuja ja personoituja, joten vastaanottaja ei osaa aavistaa kyseessä olevan huijausviesti. Krekel ym. (2009) toteaa, että juuri hyökkäyksen tarkan ja yksityiskohtaisen suunnittelun vuoksi asiantuntijat ovat arvelleet, että hyökkäyksen takana ovat viralliset toimijat ja mahdollisesti myös johtavat hakkerit.

Wisen (2011) mukaan kiinalaiset ovat olleet tunnettuja siitä, että he ovat osanneet käyttää USA:n monitulkintaisia lakeja hyväkseen. Wise (2011) kertookin, että monet syytökset vakoilusta on pitänyt tämän vuoksi hylätä.

Inksterin (2013) mukaan hyökkäyksien jäljittämistä Kiinaan vaikeuttaa se, että Kiina käyttää tiedustelussa paljon epävirallisia toimijoita, esimerkiksi ulkomailla opiskelevia opiskelijoita, sekä lisäksi tutkijoita ja liikemiehiä.

3.4 Vapaat hakkerit

Inksterin (2013) mukaan kaikki Kiinasta peräisin olevat kyberhyökkäykset eivät ole Kiinan tiedustelupalvelun tuotoksia. Inkster (2013) kertoo, että Kiinassa on suuri hakkeriyhteisö, ja monet sen jäsenet ovat patrioottisia ja valmiita käyttämään kykyjään valtion hyväksi. Näitä hyökkäyksiä ei voida suoraan yhdistää Kiinan tiedustelupalveluun tai hallintoon (Inkster, 2013). Inkster (2013) toteaa, että on kuitenkin epäselvää, kuinka hyvin Kiinan hallinto on selvillä tiedustelupalveluidensa suorittamasta kybervakoilusta ja –hyökkäyksistä.

Hjortdalin (2011) mukaan monet amerikkalaisraportit ovat osoittaneet, että myöskään Kiinan hallinto ei kykene kontrolloimaan sitä, kuka suorittaa kyberhyökkäyksiä maassa. Kiina on lisäksi kiistänyt maassa olevan sotilastoiminnassa mukana olevia hakkereita, mutta on todennäköistä, että maa käyttää hakkereita vakoiluun (Hjortdal, 2011).

Julkisuuteen vuotaneen FBI –raportin mukaan Kiina on rakentamassa kyberarmeijaa, ja että se olisi värvännyt 30 000 sotilastaustan omaavaa kybervakoilijaa ja lisäksi 150 000 vakoojaa yksityiseltä sektorilta (Hjortdal, 2011).

Hjortdalin (2011) mukaan muitakin todisteita yksityisten hakkereiden ja hallinnon yhteistyöstä on löydetty. Hakkerit ovat esimerkiksi julkisesti maininneet toimivansa yhteistyössä hallinnon kanssa ja osallistuvansa hallinnon toimintaan, lisäksi tiedetään, että tiettyjä kiinalaisia yliopistoja, erityisesti informaatiosodankäynnin tutkimusta ja kehitystä on tuettu hallinnon toimesta (Hjortdal, 2011).

3.5 Syitä kyberhyökkäyksille ja mahdolliset hyödyt Kiinalle

Hjortdalin (2011) mukaan yleisesti ottaen voidaan sanoa, että kybervakoilulle on kolme syytä. Ensimmäinen syy on häiritä ja estää muiden valtioiden ja hallintojen toimintaa tunkeutumalla niiden julkisten infrastruktuurin kohteisiin. Toinen syy kybervakoilulle on kerätä tietoa, joka auttaa kehittämään valtion sotilaallista osaamista. Kolmas syy on teknologisen edistyksen muuntaminen taloudelliseksi hyödyksi kybervakoilua hyödyntäen (Hjortdal, 2011).

Inksterin (2013) mukaan Kiinan kyberhyväksikäytöstä ja sen toiminnasta tiedetään paljon, mutta paljon on edelleen myös epäselvää. Kiina on perinteisesti suunnannut kybertiedustelunsa tieteen ja teknologian alalle, mutta yhä enemmän kybertiedustelua on suunnattu myös poliittisiin ja taloudellisiin kiinnostuksen kohteisiin (Inkster, 2013). Kiinan harjoittaman kybervakoilun suurimmaksi syyksi nimetäänkin usein taloudellisen edun tavoittelu, mutta Kiina vakoilee myös esimerkiksi sotilaskohteita kerätäkseen sotilaallista tietoutta (Hjortdal, 2011). Hjortdalin (2011) mukaan Kiinan on lisäksi havaittu tunkeutuneen kriittisen infrastruktuurin kohteisiin.

Kiinan on todettu esimerkiksi hyökänneen valtionpäämiehiä ja valtioiden johtoa vastaan. Esimerkiksi kyberhyökkäys Saksan liittokansleri Angela Merke-

liä vastaan on onnistuttu jäljittämään Kiinaan. Kiinan vakavasta suhtautumisesta kybertiedusteluun kertoo sen kyky toteuttaa tämänlainen kyberhyökkäys valtion johtoa vastaan. (Hjortdal, 2011).

Kiina on ollut kiinnostuneempi kybervakoilun ja –tiedustelun käytöstä verrattuna muihin valtioihin etenkin siksi, että sen on mahdollista hyötyä vakoilusta ja tiedustelusta enemmän verrattuna muihin valtioihin (Hjortdal, 2011). Kiina hyötyy paljon länsimaista varastetusta tiedosta, sillä länsimaat ovat olleet Kiinaa edellä esimerkiksi teknologisessa kehityksessä (Inkster, 2013). Länsimaat taas eivät juurikaan ole kiinnostuneet vakoilemaan Kiinaa, sillä Kiinan vakoilu ei hyödyttäisi länsimaita yhtä paljon. (Hjortdal, 2011; Inkster, 2013). Kiinalla onkin pitkä historia tiede- ja teknologiavarkauksista länsimaista (Inkster, 2013).

Kiinan erityistä kiinnostusta kybervakoiluun ja kybertiedusteluun selittää myös se, että hyökkäyksiä on vaikea jäljittää verrattuna perinteiseen vakoiluun, joten hyökkäykset on helpompi kieltää kuin perinteinen vakoilu. Onkin vaikea määrittää hyökkäyksen alkuperää varmasti, mutta monia hyökkäyksiä on kuitenkin voitu jäljittää Kiinaan. (Inkster, 2013). Kyberhyökkäyksen suorittaminen on huomattavasti helpompaa kuin siltä puolustautuminen, joka myös puolestaan suosii hyökkääjää (Hjortdal, 2011).

Inksterin (2013) mukaan Kiinalla on paitsi kapasiteettia ja tietotaitoa suorittaa hyökkäykset, mutta myös kyky kestää Yhdysvaltojen painostus ja vastatoimet. Kiina on kuitenkin verrattain riippuvainen kybermaailmasta sekä sotilaallisella sektorilla että siviilikäytössä (Friedberg & Ross, 2009). Hjortdalin (2011) arvion mukaan Kiina pystyisi kuitenkin torjumaan mahdolliset hyökkäykset Yhdysvalloista.

Siitä, miten Kiina prosessoi ja käyttää keräämäänsä dataa ei juurikaan ole tietoa. On myös epäselvää, kuinka hyvin Kiinan on onnistunut hyödyntää keräämäänsä dataa. Lisäksi on vaikea arvioida, kuinka paljon Kiinan yritysmaailma on hyötynyt kybertiedustelusta. (Inkster, 2013)

Toistaiseksi on liian aikaista sanoa, millaisen uhkan Kiinan kybertiedustelu aiheuttaa länsimaille (Inkster, 2013). Kiinan on kuitenkin arveltu aiheuttavan tällä hetkellä yhden suurimmista uhkista esimerkiksi Yhdysvaltojen etulyöntiasemalle teknologiassa ja jopa uhkaavan Yhdysvaltojen kansallista turvallisuutta (Verton, 2008). Arvioiden mukaan Yhdysvaltoihin kohdistuva kybervakoilu aiheuttaa historian suurimman vaurauden siirron (Inkster, 2013).

3.6 Kritiikki

Kiinan suorittamiin kyberhyökkäyksiin liittyen on kuitenkin esitetty mielipiteitä myös siitä, että Kiina ei välttämättä olisikaan kaikkien maasta tulevien hyökkäysten takana. Tietoverkot Kiinassa ovat suojaamattomia, joten on mahdollista, että toinen valtio suorittaa kyberhyökkäyksiä Kiinan kautta, jolloin hyökkäys näyttää tulevan Kiinasta. Esimerkiksi Yhdysvaltojen on arveltu liioittelevan Kiinan kybervalmiuksia. Tämän taustalla voisi olla esimerkiksi suurempien budjettien tavoittelu (Hjortdal, 2011).

4 KIBS-YRITYKSET

Strambachin (2001) mukaan nimitys KIBS-yritykset tulee sanoista knowledge-intensive business services, eli vapaasti suomennettuna tietointensiiviset liike-elämän palvelut. Tietointensiiviset liike-elämän palvelut ovat siis tietointensiivisimpiä liiketoimintaan liittyvistä palveluista, eli KIBS ei sisällä esimerkiksi rutiinitoimia, kuten siivoamista tai huoltotöitä (Strambach, 2001).

4.1 KIBS-yritykset

Tietointensiivisten liike-elämän palveluiden nähdään tarjoavan tietointensiivistä panosta liiketoiminnan prosesseihin muille organisaatioille yksityisellä ja julkisella sektorilla (Muller & Doloreux, 2009). Yrityksistä huolimatta vielä ei ole saatu aikaiseksi yhtenäistä määritelmää yritykselle, joka tuottaa tietointensiivisiä liike-elämän palveluita (Strambach, 2001; Muller & Doloreux, 2009).

On kuitenkin määritelty, että tietointensiivisillä liike-elämän palveluilla on kolme ominaista piirrettä. Ensiksi, ne ovat riippuvaisia ammatillisesta tiedosta. Toiseksi, ne ovat joko itse pääasiallinen lähde tiedolle ja informaatiolle, tai ne käyttävät tietoa tuottaakseen keskitason palveluita asiakkaidensa tuotantoprosesseihin. Kolmanneksi, ne ovat kilpailun kannalta tärkeitä ja hyödyttävät pääasiassa liiketoimintaa. (Miles ym., 1995). Miles ym. (1995) myös määrittelee tietointensiiviset liike-elämän palvelut palveluiksi, joiden on tarkoitus johtaa tiedon luomiseen, kartuttamiseen tai levittämiseen. Toivonen (2006) taas määrittelee tietointensiiviset liike-elämän palvelut yrityksiksi, jotka tarjoavat palveluita muille yrityksille ja organisaatioille. Voidaan sanoa, että liike-elämän palvelut viittaavat siihen, että palvelut tuotetaan yrityksille ja esimerkiksi julkisille organisaatioille, mutta ei yksityiseen käyttöön. Tietointensiivisyys voi tarkoittaa esimerkiksi työn laatua. Tietointensiivinen yritys taas viittaa yrityksiin, jotka suorittavat haastavia toimintoja, jotka ovat luonteeltaan älykkäitä ja joissa henkinen pääoma on tärkeässä osassa. (Muller & Doloreux, 2009).

Tietointensiivisillä liike-elämän palveluilla voidaan viitata yritykseen, joka on tietointensiivinen. Tietointensiivisiä liike-elämän palveluita tarjoaviksi sektoreiksi voidaan laskea ainakin tietokoneisiin liittyvä toiminta, tutkimus ja kehitystyö ja muut liike-elämän palvelut. (Muller & Doloreux, 2009). O'Farrel ja Moffat (1995) taas määrittelivät tietointensiiviset liike-elämän palvelut palveluiksi, jotka tarjoavat asiakkaille strategista informaatiota ja asiantuntemusta, joka on suhteellisen aineetonta ja mahdollisesti pitkäkestoista, ollen samalla myös pikemminkin ongelmanratkaisua ja päätöksentekoa, kuin rutiininomaista työtä.

Tietointensiivisten liike-elämän palveluiden tuloksena syntyy usein aineetonta ja hiljaista tietoa. Tietointensiiviset liike-elämän palvelut voidaan nähdä rajapintana asiakkaiden hiljaisen tiedon ja kansantalouden laajemman tietokannan välillä. (Muller & Doloreux, 2009). Hertog (2000) yritti mukauttaa organisaation tiedon luomisen mallin tietointensiivisiin liike-elämän malleihin, ja hänen mukaansa hiljainen tieto on vähintään yhtä tärkeää tietointensiivisiä liike-elämän palveluita toteuttavan yrityksen ja asiakkaiden välisissä suhteissa, kuin kodifioitu tieto.

4.2 Knowledge-based theory of the firm

Grantin (1996) mukaan knowledge-based theory of the firm (KBTF), on seurausta kilpailevasta teoriasta, resursseihin perustuvasta näkemyksestä. Grantin (1996) mukaan resursseihin perustuva näkemys uskoo yrityksen koostuvan erilaisista uniikeista voimavaroista, jolloin johdon ensisijainen tehtävä on maksimoida arvoa käyttämällä resursseja optimaalisesti, kun taas KBTF näkee tiedon yrityksen strategisesti tärkeimpänä resurssina. Grantin (2002) mukaan tämä tietoon perustuva yrityksen teoria ei varsinaisesti kuulu yrityksen teorioihin, vaan se on pikemminkin joukko teorioita yrityksen luonteesta, joka painottaa tiedon tärkeyttä.

Grantin (2002) mukaan KBTF pohjaa niin sanottuun tietoon perustuvaan talouteen, jolloin tyypillistä on, että yritys tuottaa enemmän palveluita kuin tavaroita, ja että yrityksen kilpailuvaltit ovat pikemminkin aineettomia kuin esimerkiksi hyödykkeitä tai rahoitusvaroja. Alavi ja Leidner (2001) totesivat, että palvelut riippuvat siitä, miten aineellisia hyödykkeitä on käytetty ja miten niitä on yrityksen tietojen mukaan yhdistelty. Alavin ja Leidnerin (2001) mukaan tieto on sulautunut yritykseen, ja sitä toteutetaan esimerkiksi yrityksen yrityskulttuurin, identiteetin, rutiineiden, järjestelmien ja työntekijöiden kautta. Grantin (2002) mukaan yritys on monesti myös verkostoitunut, digitaalinen ja virtuaalinen ja lisäksi jatkuvassa muutoksessa.

Grantin (2002) mukaan teoria monesti jakaa tiedon puhutuksi ja hiljaiseksi tiedoksi. Puhuttu tieto on helppo kommunikoida eteenpäin, kun taas hiljainen tieto tarkoittaa esimerkiksi taitoa tehdä jotain, jolloin tieto voidaan siirtää eteenpäin esimerkiksi näyttämällä, miten tietoa käytetään. Grant (2002) myös toteaa, että hiljaista tietoa on kallista jakaa ja yhdistää. Puhuttu tieto taas kärsii

siitä, että tietoa ei voida käyttää yksinoikeudella. On esimerkiksi haastavaa tehdä sopimuksia, joissa ei paljasteta liikaa sen sisältämää tietoa. (Grant, 2002)

Demsetz (1991) totesi, että markkinat ovat tehokkaat vain silloin, kun tieto voidaan muuntaa tuotteeksi tai palveluksi niin, ettei tuotteen ostajan tarvitse päästä käsiksi tietoon, jota tarvitaan tuotteen tuottamiseksi. Kogut ja Zander (1992) täsmensivät organisaatioiden olevan sosiaalisia yhteisöjä, joissa yksilöllinen ja sosiaalinen osaaminen pyritään muuntamaan taloudellisesti kannattaviksi tuotteiksi ja palveluiksi.

Grantin (2002) mielestä yrityksen haaste tiedon yhdistämisessä on ylläpitää tehokkuus tiedon luomisessa ja tiedon hyväksikäyttämisessä. Grant (1996) näkeekin yrityksen tärkeimmäksi tehtäväksi integroida työntekijöiden hallussa olevan tiedon tavaroiksi ja palveluiksi. Lisäksi johdon tärkein tehtävä on mahdollistaa yhteistyö, jotta tietoa on mahdollista yhdistää. Grantin (2002) mukaan yrityksen tehtävä on mahdollistaa yhteistyö ja koordinointi, eli yhdistää yrityksen jäsenten erilaiset tavoitteet ja erilaiset aikaansaannokset. Jos tietoa ei yhdistetä ajoissa, on johtaminen haastavaa (Grant, 2002).

Grantin (2002) mukaan modulaarisuuden hyödyntäminen on ratkaisu tiedon yhdistämisen haasteeseen. Grant (2002) toteaakin, että jo Adam Smith totesi vuonna 1776 erikoistumisen olevan keino tehostaa työntekoa. Esimerkiksi tuotesuunnittelun voi jakaa osiksi ja osatekijöihin (Grant, 2002). Tietojärjestelmät ovat Grantin (2002) mukaan helpottaneet juuri tuotannon osittamista, sillä jopa hiljainen tieto on nykyään jossain määrin mahdollista kodifioida.

Alavin ja Leidnerin (2001) mukaan tietoon pohjaavat resurssit eivät ole helposti jäljiteltävissä, joten tietoon pohjaava teoria olettaa, että tietoon perustuva etu saattaa johtaa pitkäaikaiseen kilpailulliseen etuun. Nonakan, Toyaman ja Nagatan (2000) mukaan tieto ja taidot antavat yritykselle kilpailuedun, sillä uusien tuotteiden, prosessien ja palveluiden sekä olemassa olevien kehittäminen tapahtuu tietojen ja taitojen kautta. Alavin ja Leidner (2001) kuitenkin huomauttavat, että pelkkä olemassa oleva tieto ei vielä takaa yrityksen menestystä, vaan yrityksen kyvyllä käyttää hyväksi tietoa ja muodostaa uutta tietoa on suurempi merkitys.

5 KYBERHYÖKKÄYSTEN SEURAUKSET KIBS-YRITYKSILLE

Makrotaloudellisesta näkökulmasta tarkasteltuna etenkin kyberhyökkäykset, jotka ovat pitkävaikutteisia, ovat erityisen haitallisia (Andrijcic & Horowitz, 2006). Tämän vuoksi tarkastelemme tässä osiossa juuri pitkävaikutteisia haittoja, joita kyberhyökkäys aiheuttaa. On arvioitu, että Yhdysvalloissa menetetään 508 000 työpaikkaa vuosittain kybervakoilun vuoksi (Iovan & Dinu, 2014).

Lyhytaikaisempia haittoja ovat esimerkiksi palvelukatkoksista koituvat kustannukset, vakuutukset, mahdolliset sakot ja korvaukset sekä hyökkäyksestä toipumiseen kuluvat kustannukset (Iovan & Dinu, 2014).

5.1 Henkisen pääoman menetys

Henkisen pääoman kasvava merkitys on tehnyt yrityssalaisuuksien varastamisesta houkuttelevaa, lisäksi myös globalisaatio ja kasvava kilpailu markkinoilla on tehnyt yrityssalaisuuksien varastamisen houkuttelevammaksi (Andrijcic & Horowitz, 2006). Andrijcicin ja Horowitzin (2006) mukaan globalisaatio on samalla tehnyt henkisen pääoman ja yrityssalaisuuksien suojelemisesta entistä haastavampaa, sillä paljon henkistä pääomaa on varastoitu tietokoneelle ja tietoverkkoihin, jotta ne olisivat käytössä useilla toimijoilla sijainnista riippumatta.

CSI ja FBI julkaisivat vuonna 2005 raportin, jonka mukaan henkisen pääoman varastaminen on yleistymässä, samoin kuin henkisen pääoman menetyksestä koituvat taloudelliset menetykset (Lawrence, Loeb, Lucyshyn & Richardson, 2005). Whittle (2001) taas kertoo, että Pennsylvanian yliopistossa vuonna 2001 suoritetussa tutkimuksessa todetaan, että kuluneen kahden vuoden aikana henkisen pääoman varastamisen määrä on yli kaksinkertaistunut. Piazzan (2001) mukaan OMNI Consulting Group suoritti vuonna 2001 tutkimuksen, jonka mukaan henkisen pääoman menettäminen maksaisi yritykselle ainakin 5,57% yrityksen vuosittaisista bruttotuloista. Todellisuudessa summa saattaa olla jopa suurempi, riippuen yrityksen toimialasta ja koosta (Piazza, 2001).

Erityisen paljon kyberhyökkäyksiä henkisen pääoman varastamiseksi esiintyy esimerkiksi ilmailun-, bioteknologian-, elektroniikan-, televiestinnän- ja energia-alalla (Andrijcic & Horowitz, 2006). Voidaan kuitenkin sanoa, ettei mikään ala ole kyberhyökkäysten ja –vakoilun suhteen suojassa. Monesti henkisen pääoman menetyksiä ei kuitenkaan kirjata ylös tai raportoida, joten on vaikeaa arvioida, millaisia todellisia vaikutuksia henkisen pääoman menetyksellä on. (Andrijcic & Horowitz, 2006).

5.2 Maineen ja luottamuksen menetys

Kyberhyökkäyksen kohteeksi joutuneista yrityksistä suurin osa ei onnistu pitämään tietoa hyökkäyksestä luottamuksellisena, ja kun tieto hyökkäyksestä leviää, koituu siitä negatiivista julkisuutta ja täten haittaa yrityksen maineelle. Yritykset joutuvat ilmoittamaan hyökkäyksestä esimerkiksi asiakkaille, joita hyökkäys jollain tapaa koskee, sekä liikekumppaneille ja tavarantoimittajille. Monesti hyökkäyksissä menetetäänkin asiakkaiden ja liikekumppanien sensitiivistä dataa. (Iovan & Dinu, 2014).

Maineen menetys aiheuttaa monesti asiakkaiden ja liikekumppanien luottamuksen menetyksen (Gandhi ym., 2011). Luottamus on julkista tietoa, joka pohjaa ryhmän yleiseen mielipiteeseen. Luottamus on samalla subjektiivinen näkemys. (Yu, Shen, Miao, Leung & Niyato, 2010). Luottamuksen menetys saattaa johtaa asiakkaiden vaihtamiseen kilpailijoihin (Jackson, Jickling & Webel, 2004). Etenkin pankkialalla, terveydenhuollonalalla ja rahoituksen alalla hyökkäykset saattavat herättää epäluottamusta asiakkaissa (Gandhi ym., 2011).

Koska maineen ja asiakkaiden luottamuksen menetyksen hintaa on vaikea mitata, monet yrityksen aliarvioivat siitä koituvat kustannukset (Jackson, Jickling & Webel, 2004). Voidaan kuitenkin sanoa, että maineen menetys on yritykselle suurempi haitta, kuin pelkkä taloudellinen menetys (Hutton, Goodman, Alexander & Genest, 2001).

6 POHDINTA

Kuten aiemmin todettu, erityisesti pitkävaikutteisilla kyberhyökkäyksillä on suuria vaikutuksia makrotaloudellisesta näkökulmasta (Andrijcic & Horowitz, 2006). Tässä tutkielmassa on keskitytty pitkävaikutteisista haitoista henkisen pääoman menetykseen ja maineen ja luottamuksen menetykseen. Henkisen pääoman menetyksen on tutkittu aiheuttavan merkittäviä tappioita yrityksille. (Lawrence ym., 2005; Whittle 2001; Piazza 2001). Myös maineen ja asiakkaiden luottamuksen menetyksellä on suuria vaikutuksia, ja onkin arvioitu, että maineen ja luottamuksen menetyksestä koituu suurempi haitta kuin pelkästä taloudellisesta menetyksestä (Hutton, Goodman, Alexander & Genest, 2001).

Kiinan erityinen kiinnostuksen kohde kybervakoilussa on ollut taloudellisen hyödyn tavoittelu (Hjortdal, 2011). Kiinan kiinnostusta kybervakoiluun selittää erityisesti se, että maa hyötyy vakoilusta enemmän kuin esimerkiksi länsimaat hyötyisivät (Hjortdal, 2011).

Seuraavassa taulukossa on pyritty havainnollistamaan Kiinan suorittamasta kyberhyökkäyksestä koituvia henkisen pääoman menetykseen sekä maineen ja asiakkaiden luottamuksen menetykseen liittyviä vaikutuksia. Taulukko tarkastelee asiaa Kiinan, eli hyökkääjän, näkökulmasta, sekä lisäksi hyökkäyksen kohteena olevan KIBS-yrityksen näkökulmaa, KIBS-yrityksen kilpailijan näkökulmaa ja länsimaiden näkökulmaa. Lisäksi kullekin vaikutukselle on arvioitu sen merkittävyyttä kuvaava symboli, * kuvaa vähäisintä vaikutusta, *** kuvaa suurimmaksi arvioitua vaikutusta.

TAULUKKO 1 Kyberhyökkäyksen pitkäaikaiset haitat ja niiden merkitys

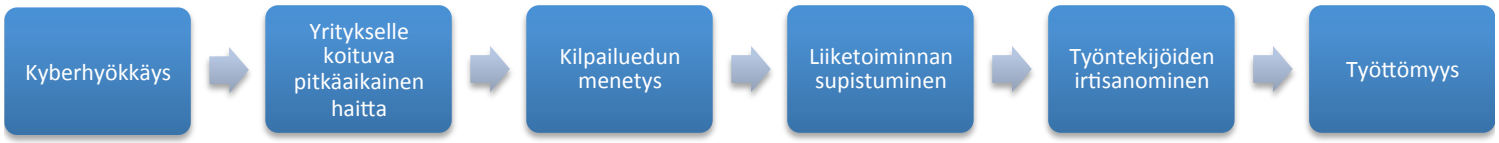
Kiinan suorittaman kyberhyökkäyksen pitkäaikaiset haitat KIBS-yrityksille	**Vaikutukset Kiinalle**	**Vaikutukset hyökkäyksen kohteena olevaan KIBS-yritykseen**	**Vaikutukset kilpailijoihin**	**Vaikutukset länsimaille**
Henkisen pääoman menetys	Kiina on pyrkinyt ottamaan kiinni Yhdysvaltojen teknologista etumatkaa (Wise, 2011). Kiinan taloudellinen kilpailukyky perustuukin osaksi länsimaista varastetun tiedon varaan. (Inkster, 2013). Kiina hyötyy kybervakoilusta, sillä länsimaat ovat sitä edellä teknologisessa kehityksessä (Hjortdal, 2011). **Merkitys Kiinalle: *****	Henkisen pääoman menetys kustantaa yritykselle arviolta 5,57% sen vuosittaisista bruttotuloista (Piazza, 2001). Tietoon pohjautuvat resurssit eivät ole helposti jäljiteltävissä (Alavi & Leidner 2001). Tieto ja taidot antavat yritykselle kilpailuedun, ja jos tieto joudutaan jakamaan muiden kanssa, jää kilpailuetu saavuttamatta (Nonaka, Toyama & Nagatan, 2000). **Merkitys KIBS-yritykselle: *****	Henkisen pääoman menetys vähentää yrityksen kilpailuetua (Nonaka, Toyama & Nagatan, 2000). Tämä luonnollisesti palvelee kilpailevia yrityksiä. Henkisen pääoman menetys kustantaa yritykselle suuria summia (Piazza, 2001), joten tämä raha on luonnollisesti pois esimerkiksi tuotekehityksestä. **Merkitys kilpailijalle: ***	Esimerkiksi Yhdysvalloissa menetetään 508 000 työpaikkaa vuosittain kybervakoilun vuoksi (Iovan & Dinu, 2014). On myös arvioitu, että Yhdysvaltoihin kohdistuva kybervakoilu aiheuttaa historian suurimman vaurauden siirron (Inkster, 2013). Kiinan suorittaman vakoilun voidaan siis sanoa haittaavan länsimaiden taloutta. **Merkitys länsimaille: *****
Maineen ja asiakkaiden luottamuksen menetys	Maineen ja luottamuksen menetys voi aiheuttaa asiakkaiden ja liikekumppanien vaihtamiseen kilpailijalle (Jackson, Jickling & Webel, 2004). Kiinalainen yritys saattaa olla potentiaalinen vaihtoehto asiakkaille ja liikekumppaneille. **Merkitys Kiinalle: ***	Maineen menetys on yritykselle suurempi haitta, kuin pelkkä taloudellinen menetys (Hutton, Goodman, Alexander & Genest, 2001). Tarkkaa hintaa maineen ja asiakkaiden luottamukselle on vaikea mitata (Jackson, Jickling & Webel, 2004). **Merkitys KIBS-yritykselle: ****	Luottamuksen menetys saattaa johtaa asiakkaiden vaihtamiseen kilpailijoihin (Jackson, Jickling & Webel, 2004). Kilpailijat siis saattavat hyötyä kyberhyökkäyksestä seuraavasta maineen menetyksestä. **Merkitys kilpailijalle: ***	Maineen menetys ja siitä seuraavan asiakkaiden luottamuksen menetys saattavat johtaa asiakkaiden vaihtamisen kilpailijoihin (Jackson, Jickling & Webel, 2004). Kilpailija saattaa olla länsimaiden ulkopuolella, jolloin seuraa taloudellinen menetys länsimaille. **Merkitys länsimaille: ***

Taulukosta on nähtävissä, että suurimmaksi arvioidut vaikutukset aiheutuu henkisen pääoman menetyksestä. Erityisesti KIBS-yrityksien henkisen pääoman menetyksestä hyötyy Kiina, joka on pyrkinyt ottamaan Yhdysvaltojen teknologista kehitystä kiinni jo Persianlahden sodasta saakka (Wise, 2011). Kiinan taloudellinen menestys perustuukin jossain määrin länsimaista varastetun tiedon varaan (Inkster, 2013). On kuitenkin epäselvää, kuinka hyvin Kiinan on onnistunut hyödyntää kybertiedustelusta saamaansa dataa, ja kuinka paljon se on hyödyttänyt Kiinan yritysmaailmaa (Inkster, 2013).

Taulukosta on myös nähtävissä, että henkisen pääoman menetyksestä kärsii eniten hyökkäyksen kohteena olevat KIBS-yritykset sekä länsimaiden talous. KIBS-yrityksille koituu kyberhyökkäyksestä suoraa taloudellista haittaa, sillä henkisen pääoman menetyksen on arvioitu kustantavan yritykselle ainakin 5,57% sen vuosittaisista bruttotuloista (Piazza, 2001). Kogut ja Zander (1992) totesivat, että organisaatioiden tehtävä on muuntaa osaamista taloudellisesti kannattaviksi tuotteiksi ja palveluiksi. Kybervakoilu vahingoittaa juuri tätä osaa yrityksen toiminnassa, ja lisäksi sen liiketoimintaprosesseja, sillä kybervakoiluun kuuluu olennaisesti tiedon varastaminen ja mahdollisesti myös jakaminen (Rid, 2012). Yritys siis menettää kilpailuedun, jonka sen hallussa yksinoikeudella olleet tiedot ja taidot loivat (Nonaka, Toyama & Nagatan, 2000). Kyberhyökkäyksen seurauksena yrityksen henkinen pääomaa ja yritykseen sulautunutta tietoa ei saada muunnetuksi taloudelliseksi eduksi kuten yleensä, sillä Grantin (2002) mukaan tieto kärsii siitä, että sitä ei voida käyttää yksinoikeudella. Kiinan suorittaessa kybervakoilua etu yksinoikeudesta menetetään. Länsimaille Kiinan suorittama vakoilu aiheuttaa työpaikkojen menetyksiä sekä vaurauden siirtoa (Iovan & Dinu, 2014: Inkster, 2013).

Taulukossa esitetyn arvion mukaan maineen ja asiakkaiden luottamuksen menetys aiheuttaa suurinta haittaa KIBS-yrityksille, jotka kärsivät maineen ja asiakkaiden ja liikekumppanien luottamuksen menetyksestä enemmän kuin pelkästä taloudellisesta menetyksestä (Hutton, Goodman, Alexander & Genest, 2001). On myös mahdollista, että hyökkäyksen kohteena olevan KIBS-yrityksen asiakkaat ja liikekumppanit vaihtavat liiketoimintansa pois kyseiseltä KIBS-yritykseltä maineen ja luottamuksen menetyksen seurauksena. Tarkkaa hintaa maineen sekä asiakkaiden ja liikekumppanien luottamuksen menetykselle on vaikea mitata. (Jackson, Jickling & Webel, 2004). Kyberhyökkäyksen kohteeksi joutuneen KIBS-yrityksen maineen menetyksestä ja asiakkaiden luottamuksen menetyksestä hyötyy eniten Kiina ja KIBS-yrityksen kilpailijat. Molemmissa tapauksissa on mahdollista, että luottamuksen menettäneet asiakkaat ja liikekumppanit päätyvät vaihtamaan liiketoimintansa joko kiinalaiselle yritykselle, jolla on kybervakoilun seurauksena samat tiedot ja taidot, tai kilpailevalle yritykselle, joka ei ole kärsinyt kyberhyökkäyksestä johtuvaa maineen menetystä.

Taulukosta käy siis ilmi, että KIBS-yrityksiin kohdistuva kybervakoilu aiheuttaa haittaa paitsi KIBS-yritykselle, myös länsimaiden taloudelle. Seuraavalla kuvalla pyritään havainnollistamaan, miten länsimaiden taloudellinen menetys tapahtuu .



KUVIO 2 Kyberhyökkäyksen vaikutukset länsimaiden talouteen

Kuvasta näkyy, kuinka kyberhyökkäyksen seurauksena koituvasta pitkäaikaisesta haitasta johtuva yrityksen kilpailuedun menetys johtaa liiketoiminnan supistumiseen ja sen seurauksena työntekijöiden irtisanomiseen. Työntekijöiden irtisanominen taas johtaa työttömyyteen, joka on valtioille ongelmallista.

7 YHTEENVETO

Tutkielman tutkimuskysymykset olivat seuraavat:

- Millaisia haittoja Kiinan suorittama kybervakoilu aiheuttaa KIBS-yrityksille?
- Kuinka vakavia nämä KIBS-yrityksille koituneet haitat ovat?

Tutkielman pohjalta voimme nyt vastata, että kyberhyökkäyksen aiheuttamat pitkäaikaiset haitat KIBS-yritykselle ovat henkisen pääoman menetys sekä maineen menetys ja asiakkaiden luottamuksen menetys. Näistä arvioimme henkisen pääoman menetyksen olevan KIBS-yritykselle merkittävämpi haitta.

Tutkielmassa ilmi tulleiden haittojen valossa olisi suositeltavaa, että yritykset kiinnittäisivät tulevaisuudessa enemmän huomiota tietoturvallisuuteensa. Mahdollisesti myös valtioiden tulisi länsimaissa valvoa riittävän tietoturvan toteutumista yrityksissä, sillä tutkielmassa kävi ilmi, että kybervakoilun haitat koskevat lopulta myös valtion taloutta.

Yksi mahdollinen tapa suojautua Kiinan kybervakoilulta on kiinnittää KIBS-yrityksissä huomiota siihen, miten tietoa jaetaan kiinalaisten liikekumppanien kanssa, tai miten tietoa esimerkiksi jaetaan Kiinassa toimivalle tavaranvalmistajalle. Kiinassa on pitkään ollut vallalla kulttuuri, jonka mukaan kopioiminen ja imitoiminen ovat parhaita tapoja oppia (Yang, 2003). Tästä johtuen käsitys kopioimisesta ja tiedon varastamisesta saattaa olla länsimaisilla ja kiinalaisilla yrityksillä erilainen.

Tulevaisuuden tutkimusehdotukseksi ehdotamme tutkimusta siitä, kuinka paljon Kiinan yritysmaailma on hyötynyt kybervakoilusta, eli kuinka suuren taloudellisen edun Kiina on saanut verrattuna länsimaiden kokemiin taloudellisiin menetyksiin. Olisi myös tarpeen kehittää numeerinen menetelmä kyberhyökkäysten haittojen arvioimiseen, jolloin esimerkiksi yrityksien tietoturvaan käyttämien varojen tarpeellisuuden arvioiminen olisi helpompaa.

Tutkielman tuloksia tarkasteltaessa tulisi huomata, että suurin osa käytetyistä lähteistä on länsimaisten kirjoittajien tuotoksia. Tämä saattaa johtaa jossakin määrin puutteelliseen ja rajoitettuun näkemykseen.

LÄHTEET

Alavi, M. & Leidner, D. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. *MIS Quarterly, 25*(1), 107-136.

Andrijcic, E. & Horowitz, B. (2006). A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. *Risk Analysis*, *26*(4), 907-923.

Colarik, A. (2006). *Cyber Terrorism: Political and Economic Implications.* Hershey: Idea Group Inc.

Demsetz, H. (1991). *The Nature of the Firm*. New York: Oxford University Press. 159-178.

Feigenbaum, E. A. (2000). *China's Techno-warriors: National Security and Strategic Competition from the Nuclear to the Information Age.* Palo Alto: Stanford University Press.

Fidler, D. P. (2013). Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. *ASIL Insights*, *17*(10).

Friedberg, A. L. & Ross, R. S. (2009). Here Be Dragons: Is China a Military Threat?. *National Interest 103*.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *Technology and Society Magazine, IEEE*, *30*(1), 28-38.

Grant, R. (1996). Toward a Knowledge-based theory of the firm. *Strategic Management Journal 17,* 109-122.

Grant, R. (2002). *The Strategic Management of Intellectual Capital and Organizational Knowledge.* New York: Oxford University Press, Inc.

Hertog, P. D. (2000). Knowledge-intensive business services as co-producers of innovation. *International Journal of Innovation Management*, *4*(04), 491-528.

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security 4(2)*, 1-24.

Hunker, J. (2010). Cyber war and cyber power: Issues for NATO doctrine. *Research Paper 62*, 1-12.

Hutton, J. G., Goodman, M. B., Alexander, J. B. & Genest, C. M. (2001). Reputation management: the new face of corporate public relations?. *Public Relations Review, 27(3)*, 247-261.

Inkster, N. (2013). Chinese Intelligence in the Cyber Age. *Survival: Global Politics and Strategy 55(1*), 45-66.

Iovan, S. & Dinu, M.B. (2014). Impact of the loss and theft of electronic data on companies. *Fiability & Durability/Fiabilitate si Durabilitate 1*, 39-45.

Jackson, W. D., Jickling, M. & Webel, B. (2004). The economic impact of cyber-attacks. *Congressional Research Service, Library of Congress*.

Kogut, B. & Zander, U. (1992). Knowledge of the firm, combinative capabilities, and the replication of technology. *Organization Science, 3*, 383-397.

Krekel, B., Bakos, G. & Barnett, C. (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. McLean: Northrop Grumman Corporation.

Lawrence, A. G., Loeb, M. P., Lucyshyn, W. & Richardson, R. (2005). CSI/FBI computer crime and security survey. *Computer Security Institute*.

Madavi, T. J., & Khandalkar, A. V. Cyber Attack & Security. *International Journal For Engineering Applications and Technology.*

Mattis, P. (2012). Beyond Spy vs. Spy: the Analytical Challenge of Understanding Chinese Intelligence Services. *Studies in Intelligence, 56(3).*

Miles, I., Kastrinos, N., Bilderbeek, R., den Hertog, P., Flanagan, K., Huntink, W. & Bouman, M. (1995). Knowledge-Intensive Business Services: users, carriers and sources of innovation. *European Innovation Monitoring System, EIMS Publication, 15.*

Muller, E. & Doloreux, D. (2009). What we should know about knowledge-intensive business services. *Technology in Society*, *31*(1), 64-72.

Nonaka, I., Toyama, R. & Nagata, A. (2000). A firm as a knowledge-creating entity: a new perspective on the theory of the firm. *Industrial and corporate change*, *9*(1), 1-20.

O'Farrell, P. N. & Moffat, L. A. (1995). Business services and their impact upon client performance: an exploratory interregional analysis. *Regional Studies*, *29*(2), 111-124.

Okoli, C. & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Available at SSRN 1954824*.

Phillips, T. (2007). *Knockoff: The deadly trade in counterfeit goods: The true story of the world's fastest growing crime wave*. Kogan Page Publishers.

Piazza, P. (2001). Economic leaks can sink a business. *Security Management, 36*.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35(1)*, 5-32.

Strambach, S. (2001). *Innovation Networks: Concepts and Challenges in the European Perspective*. Springer Science & Business Media, 53-68.

The Hofstede Centre. Country Comparison: China in comparison with Finland. Haettu 1.9.2015 osoitteesta http://geert-hofstede.com/china.html

Toivonen, M. (2006). Future Prospects of Knowledge Intensive Business Services (KIBS) and Implications to Regional Economies. *ICFAI Journal of Knowledge Management*, *4*(3).

Verton, D. (2008). The Evolution of Espionage: Beijing's Red Spider Web. *China Brief*, *8*(15), 4.

Whittle, S. (2001). Management—Intellectual theft is on the increase. *Computing, 19*.

Wise, D. (2011). *Tiger Trap: America's Secret Spy War with China*. Boston: Houghton Mifflin Harcourt.

Yang, D. (2003). The development of intellectual property in China. *World Patent Information*, *25*(2), 131-142.

Yu, H., Shen, Z., Miao, C., Leung, C. & Niyato, D. (2010). A survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE, 98(10)*, 1755-1772.