Aarne Takala

TALOUDELLINEN KYBERVAKOILU: MENETELMÄT JA TEKNIIKAT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Takala, Aarne
Taloudellinen kybervakoilu: Menetelmät ja tekniikat
Jyväskylä: Jyväskylän yliopisto, 2024, 29 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Halttunen, Veikko

Taloudellinen kybervakoilu on muodostunut merkittäväksi uhkaksi valtioille ja yrityksille, koska yhä suurempi osa liiketoiminnasta tapahtuu digitaalisessa ympäristössä. Tämä tutkielma käsittelee taloudellisessa kybervakoilussa käytettyjä menetelmiä ja tekniikoita. Tutkielman tarkoituksena oli selvittää, millaisia menetelmiä käytetään taloudellisen tiedon varastamiseen ja mitkä ovat näiden menetelmien taloudelliset vaikutukset. Tutkielma toteutettiin systemaattisena kirjallisuuskatsauksena ja aineisto kerättiin useista kansainvälisistä ja kotimaisista tietokannoista. Tutkielmassa havaittiin, että keskeisimpiä menetelmiä taloudellisen kybervakoilun näkökulmasta ovat APT-hyökkäykset (advanced persistent threat), haittaohjelmat (malware) ja käyttäjän manipulointi (social engineering). Näitä menetelmiä hyödyntämällä vakoilua suorittavat toimijat pääsevät käsiksi arkaluontoiseen taloudelliseen tietoon, mikä voi johtaa merkittäviin taloudellisiin menetyksiin ja kilpailuedun menetykseen yrityksille ja valtioille. Tutkielma osoitti myös, että taloudellisen vakoilun taustalla on usein päällekkäisiä taloudellisia, poliittisia ja sotilaallisia motiiveja. Lisäksi huomattiin, että uusien teknologioiden, kuten tekoälyn kehittyminen, laajentaa ja tehostaa kybervakoilu uhkia ja tekee niiden torjumisesta entistä haastavampaa. Tämän tutkielman tulokset korostavat kybervakoilun vakavuutta ja jatkuvan kehityksen tarvetta kyberturvallisuudessa yrityksien ja valtioiden kannalta.

Asiasanat: taloudellinen vakoilu, kybervakoilu, haittaohjelmat, APT-hyökkäykset, käyttäjän manipulointi

ABSTRACT

Takala, Aarne
Economic cyber espionage: Methods and techniques
Jyväskylä: University of Jyväskylä, 2024, 29 pp.
Information Systems, bachelor's thesis
Supervisor: Halttunen, Veikko

Economic cyber espionage has become a significant threat to states and companies as an increasing portion of business activities occurs in digital environments. This thesis examines the methods and techniques used in economic cyber espionage. The purpose of the study was to identify the methods used for stealing economic information and to assess the economic impact of these methods. The thesis was conducted as a systematic literature review, and the source material was collected from various international and domestic databases. The study found that the key methods in economic cyber espionage include APT attacks (advanced persistent threat), malware, and social engineering. By utilizing these methods, espionage actors can access sensitive economic information, leading to significant financial losses and loss of competitive advantage for companies and states. The study also revealed that economic espionage is often driven by overlapping economic, political, and military motives. Additionally, it was noted that the advancement of new technologies, such as artificial intelligence, expands and enhances cyber espionage threats, making them even more challenging to counteract. The findings of the study underscore the seriousness of cyber espionage and the ongoing need for development in cybersecurity for companies and states.

Keywords: economic espionage, cyber espionage, malware, APT, social engineering

TAULUKOT

TAULUKKO 1 Kybervakoilun ja -rikollisuuden erot..... 12

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT JA TAULUKOT

1 JOHDANTO 6

2 TALOUDELLINEN VAKOILU JA KYBERVAKOILU : KÄSITTEET JA TAUSTA 9
2.1 Taloudellinen ja teollinen vakoilu 9
2.2 Kybervakoilun määritelmä 11
2.3 Taloudellisen kybervakoilun historia 12

3 TALOUDELLISEN KYBERVAKOILUN MENETELMÄT 15
3.1 Vakoilumenetelmät ja -tekniikat 15
3.1.1 APT 16
3.1.2 Haitta- ja vakoiluohjelmat 18
3.1.3 Käyttäjän manipulointi ja tietojen kalastelu 20
3.2 Vakoilumenetelmien ja -tekniikoiden kehitys ja tulevaisuuden suuntaukset 22
3.3 Taloudellisen kybervakoilun kohteet 23

4 YHTEENVETO 25

LÄHTEET 27

1 JOHDANTO

Taloudellisesta kybervakoilusta on muodostunut merkittävä uhka valtioille ja yrityksille liiketoiminnan tapahtuessa yhä enemmän digitaalisissa ympäristöissä. Taloudellinen kybervakoilu viittaa kyberhyökkäysten käyttöön taloudellisesti arvokkaan tiedon hankkimiseksi laittomin keinoin (Snyder & Crescenzi, 2009). Ensimmäiset merkit taloudellisesta kybervakoilusta juontavat juurensa 1980-luvulle, jolloin tietokoneiden yleistyminen lisäsi tietoverkkojen kautta tapahtuvaa laitonta toimintaa. 1990-luvun lopulla ja 2000-luvun alussa internetin laajentuminen teki kybervakoilusta globaalin ilmiön, luoden pohjan nykyaikaiselle taloudelliselle kybervakoilulle (Rivera, 2014).

Yksi varoittava käytännön esimerkki taloudellisesta kybervakoilusta on APT1-ryhmän toiminta. Tämä Kiinan hallituksen tukema kybervakoiluryhmä on murtautunut yli 141 organisaatioon varastaen arvokasta taloudellista tietoa useilta teollisuudenaloilta. APT1-hyökkäykset osoittavat, miten kybervakoilu voi aiheuttaa merkittäviä taloudellisia ja kilpailuedun menetyksiä yrityksille ja valtioille (Wangen, 2015).

Tämä tutkielma keskittyy taloudellisen kybervakoilun menetelmiin ja tekniikoihin, tarkastellen, kuinka taloudellisesti motivoituneet vakoilijat hyödyntävät edistyneitä menetelmiä ja tekniikoita tiedon hankkimiseksi, ja mitkä ovat näiden menetelmien taloudelliset vaikutukset. Tutkielman taustalla on tarve ymmärtää paremmin taloudellista kybervakoilua, sen menetelmiä ja vaikutuksia, sillä näiden tietojen avulla voidaan kehittää tehokkaampia suojautumiskeinoja ja strategioita. Tutkielma pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

1) millaisia menetelmiä taloudellisessa kybervakoilussa käytetään?
2) mitkä ovat käytettyjen menetelmien mahdolliset vaikutukset taloudellisesta näkökulmasta?

Tutkimusmenetelmänä käytettiin systemaattista kirjallisuuskatsausta, jossa aineisto kerättiin useista kansainvälisistä ja kotimaisista tietokannoista. Suurin osa käytetyistä lähteistä on englanninkielisiä. Käytettyjä hakulausekkeita olivat

muun muassa "*Economic cyber espionage*," "*Financial espionage*," "*Cyber espionage cases*," ja "*Cyber espionage methods*." Kirjallisuuskatsauksessa keskityttiin erityisesti tapaustutkimuksiin ja yritysten tekemiin kyberturvallisuusraportteihin, jotka valottavat taloudellisen kybervakoilun käytännön toteutusta ja sen seurauksia. Tutkielmassa käytetty lähdemateriaali analysoitiin laadullisesti, pyrkien ymmärtämään ilmiön keskeisiä piirteitä ja vaikutuksia. Laadun varmistamiseksi suurin osa käytetystä kirjallisuudesta on tarkistettu julkaisufoorumin (JUFO) luokituksesta. Niissä tapauksissa, joissa artikkelin julkaisualustalla ei ollut JUFO-luokitusta, on pyritty arvioimaan kirjoittajan taustaa, julkaisijan pätevyyttä, ajankohtaisuutta sekä lähteen saamaa viitemäärää. Näin on varmistettu, että myös nämä lähteet ovat luotettavia ja relevanteilla kriteereillä arvioituja, vaikka JUFO-luokitusta ei olisikaan ollut saatavilla. Lähdemateriaalia kerättäessä tehtiin havainto, että valtaosa tämänhetkisestä tutkimuksesta ja kirjallisuudesta aiheen parissa kohdistuu kybervakoilulta ja -hyökkäyksiltä puolustautumiseen, eikä niinkään vakoilevan toimijan käyttämien keinojen tutkimiseen. Tämä osaltaan osoittaa tutkimuksen tarvetta aiheen parissa.

Tutkielmassa havaittiin, että keskeisimmät menetelmät taloudellisen kybervakoilun näkökulmasta ovat edistyneet pysyvät uhat (APT-hyökkäykset), haittaohjelmat (malware) ja käyttäjän manipulointi (social engineering), kuten tietojenkalastelu (phishing). Näitä menetelmiä hyödyntämällä vakoilevat toimijat pääsevät käsiksi arkaluontoiseen taloudelliseen tietoon, mikä voi johtaa merkittäviin taloudellisiin menetyksiin ja kilpailuedun menetykseen yrityksille ja valtioille (Solberg Søilen, 2016). Tutkielmassa korostui myös, että taloudellisen vakoilun taustalla on usein päällekkäisiä taloudellisia, poliittisia ja strategisia motiiveja.

Tutkielmasta saadut tulokset osoittavat, että kybervakoilu on monimutkainen ja jatkuvasti kehittyvä uhka, joka vaatii jatkuvaa kehitystä kyberturvallisuuden alalla. Esimerkiksi tekoälyn ja IoT-teknologioiden kehitys mahdollistaa kybervakoilun menetelmien kehittymisen, tehden niiden torjumisesta entistä haastavampaa (Akoto, 2022). Tutkielmassa tehdyt havainnot ja tulokset korostavat tarvetta panostaa entistä enemmän kyberturvallisuusresursseihin ja -menetelmiin taloudellisen tiedon suojaamiseksi.

Tutkielman avulla lukija pääsee tutustumaan taloudelliseen vakoiluun ja siihen, miten teknologiaa hyödynnetään tämän suorittamiseksi. Lisäksi syvennytään tarkemmin vakoilevan toimijan näkökulmaan ja tarjotaan näin uudenlaista katsausta kybervakoiluun.

Tutkielma rakentuu seuraavasti: Luvussa 2 esitellään ja määritellään tutkimuskysymysten kannalta tärkeimmät käsitteet, kuten taloudellinen ja teollinen vakoilu sekä kybervakoilu, jotta pystytään ymmärtämään taloudellisen kybervakoilun kokonaisuutta. Tämän jälkeen käydään läpi aiheen historiallinen tausta, jotta voidaan hahmottaa laajempi kokonaiskuva. Luvussa 3 käsitellään yleisimpiä keinoja taloudellisen kybervakoilun suorittamiseksi, minkä lisäksi esitellään tulevaisuuden kybervakoilun näkymiä ja pohditaan, miksi juuri tietyt valtiot tai yritykset näyttäytyvät houkuttelevina kohteina taloudelliselle

kybervakoilulle. Lopuksi yhteenvedossa, käsitellään tutkimusaihe, käytetyt menetelmät, tutkielman tulokset, johtopäätökset ja mahdolliset jatkotutkimusehdotukset.

2 TALOUDELLINEN VAKOILU JA KYBERVAKOILU : KÄSITTEET JA TAUSTA

Tämä luku tarjoaa perustan ymmärtää keskeisiä käsitteitä ja ilmiöitä, jotka liittyvät kybervakoiluun ja taloudelliseen vakoiluun. Taloudellisen vakoilun ja kybervakoilun merkitys on kasvanut merkittävästi digitaalisen talouden ja globaalien tietoverkkojen laajenemisen myötä. Tässä luvussa siis esitetään tutkielman kannalta olennaiset käsitteet: kybervakoilu, taloudellinen ja teollinen vakoilu sekä tarkastellaan niiden historiaa ja kehitystä.

Kybervakoilu voidaan nähdä modernina työkaluna taloudellisen vakoilun toteuttamisessa. Useimmat tietomurrot tehdäänkin taloudellisen hyödyn perässä (Verizon, 2020). Nykyään taloudellista vakoilua suoritetaan kybervakoilun keinoin, koska näin voidaan esimerkiksi vähentää riskiä kiinnijäämisestä (Solberg Søilen, 2016). Taloudellisen tiedon varastaminen teknologiaa hyödyntämällä on myös erittäin tehokasta (Solberg Søilen, 2016). Taloudellisella vakoilulla voi olla valtava vaikutus bruttokansantuotteeseen, kun kilpailija varastaa kehitystyöhön investoidun tiedon ja tuo markkinoille saman tai paremman tuotteen murto-osalla kustannuksista (Civuli ym., 2022). Seuraavaksi tarkastellaan taloudellisen vakoilun ja kybervakoilun käsitteitä yksityiskohtaisemmin.

2.1 Taloudellinen ja teollinen vakoilu

Kirjallisuudessa puhutaan hyvin usein joko taloudellisesta tai teollisesta vakoilusta ja on olennaista tunnistaa näiden kahden käsitteen välillä olevat eroavaisuudet, vaikka näistä kahdesta käsitteestä puhutaan kirjallisuudessa myös usein ristiin, eikä niin sanottua yhtenäistä linjausta käsitteiden erottamiseksi ole (Knickmeier, 2020). Taloudellinen ja teollinen vakoilu kattaa laajan joukon toimintoja, joita suoritetaan kilpailuetujen saavuttamiseksi (Hou & Wang, 2020). Se aiheuttaa valtavan määrän taloudellisia menetyksiä vuosittain (Jones, 2008). Historia osoittaa, että taloudellista vakoilua suorittavat tahot ovat

usein tieteellisesti ja taloudellisesti heikompia osapuolia, jotka pyrkivät saamaan kilpailijansa kiinni kehityksessä (Solberg Søilen, 2016)

Taloudellinen vakoilu voidaan määritellä laajaksi toiminnaksi, joka kattaa sekä valtiollisten, että yksityisten toimijoiden ja yritysten pyrkimykset hankkia taloudellista tietoa laittomin keinoin. Taloudellisen vakoilun käsite kattaa erilaisia toimia, jotka saattavat vaihdella perinteisestä vakoilusta kyberhyökkäyksiin, ja on usein kohdistettu yrityssalaisuuksien, kuten patenttien, kaupallisten strategioiden ja teknologian varastamiseen (Solberg Søilen, 2016). Toisin sanoen taloudellisen vakoilun kohteena on yrityksien tai valtiollisten tahojen henkinen pääoma. Suurimpana erona lailliselle liiketoiminnalle ja kilpailutiedolle taloudellisella vakoilulla on siinä, että sen harjoittajat varastavat tietoa sen sijaan, että nämä päättelisivät sen laillisista lähteistä (Snyder & Crescenzi, 2009). Snyder ja Crescenzi (2009) määrittelevätkin artikkelissaan taloudellisen vakoilun yhden maan kansalaisille kuuluvien liikesalaisuuksien väärinkäytöksi toisen maan hyödyksi, mukaan lukien luvattoman omistusoikeudellisten tietojen käytön sellaiselta taholta, jolla ei ole laillista oikeutta siihen. Taloudellisen vakoilun kohteet voivat kärsiä merkittävistä taloudellisista tappioista, mainehaitoista sekä kilpailuedun menetyksestä, siinä missä vakoilua suorittava osapuoli taas saa taloudellista ja strategista etua varastetun tiedon avulla (Solberg Søilen, 2016).

Teollinen vakoilu puolestaan keskittyy enemmän teknologisen ja teollisen tiedon varastamiseen, ja se onkin usein suunnattu yritysten tutkimus- ja kehitystyön tulosten, valmistusprosessien sekä muiden teknologisten innovaatioiden varastamiseen (Solberg Søilen, 2016). Olennaisimpina eroina taloudellisen ja teollisen vakoilun käsitteiden välillä on siis vakoilua suorittava taho, joka teollisen vakoilun tapauksessa käsitetään yksityisenä toimijana, kun taas taloudellista vakoilua suorittava taho saattaa olla valtiollinen tai valtion sponsoroima toimija. Ongelmana kuitenkin on se, että useammassa maassa termejä taloudellinen tai teollinen vakoilu ei sovelleta johdonmukaisesti tai näitä käsitteitä ei olla määritetty laissa, tehden näiden määrittämisestä ja ymmärtämisestä merkittävästi haastavampaa. (Knickmeier, 2020). Tässä kirjallisuuskatsauksessa käytetään termiä taloudellinen vakoilu viitattaessa kaikenlaiseen taloudellisesti motivoituneeseen vakoiluun, oli kyseessä yksityinen tai valtiollinen toimija, selkeyden säilyttämiseksi.

Jotta voidaan ymmärtää taloudellisen ja teollisen vakoilun käsitteitä, on olennaista tunnistaa näiden taustalla olevat motiivit. Knickmeier (2020) esittääkin tutkimuksessaan joukon erialisia mahdollisia motiiveja taloudellisen ja teollisen vakoilun taustalla. Ensimmäiseksi motiiviksi kerrotaan taloudellinen hyöty (financial gain), millä viitataan esimerkiksi yrityssalaisuuksien myymistä kilpailijoille tai niiden käyttöä oman liiketoiminnan edistämiseksi. Tämä käy ilmi myös siitä, miten nykyajan kyberhyökkäysten ensisijaiseksi tavoitteeksi on muodostunut juurikin taloudellisen hyödyn saavuttaminen (Neittaanmäki, Lehto, & Savonen, 2021, s.134-135). Toisena motiivina Knickmeier (2020) esittää kilpailuedun parantamisen, eli vakoilulla pyritään säästämään aikaa ja resursseja tuotekehityksessä, kun voidaan hyödyntää jo olemassa olevaa tietämystä.

Näiden lisäksi motiivina voi olla tyytymättömyys nykyiseen tai entiseen työnantajaan, joka on saattanut kohdella työntekijäänsä huonosti (Hou & Wang, 2020). Tämä voi johtaa arkaluontoisen taloudellisen tiedon vuotamiseen kilpailevalle taholle vanhan työntekijän halutessa kostaa tai varmistaakseen itselleen uusia mahdollisuuksia tulevaisuudessa (Knickmeier, 2020). Taloudellisen vakoilun taustalla olevat motiivit saattavat olla myös valtiollisia tai poliittisia. Valtiollinen toimija voi halutessaan tukea taloudellista vakoilua edistääkseen omia kansallisia etujaan, joko teollisessa tai strategisessa mielessä (Verizon, 2020). Tämä osoittaa osaltaan, miksi taloudellisesti, sotilaallisesti ja poliittisesti motivoituneen vakoilun erottaminen ei aina ole täysin yksiselitteistä; taloudellinen vakoilu voi olla samanaikaisesti poliittista, sotilaallista tai jopa molempia.

2.2 Kybervakoilun määritelmä

Kybervakoilusta on tullut tietynlainen standardi vakoilun maailmassa tänä päivänä. Tämä ilmenee esimerkiksi siinä, miten suuri osa taloudellisesta vakoilusta tapahtuu teknologiaa hyödyntämällä (Hou & Wang, 2020). Nykyään kybervakoilua käyttävät niin tiedusteluviranomaiset, kuin rikolliset ja se on osoittautunut hyödylliseksi, mutta uhkaavaksi strategiaksi tietojen keräämisessä, korruptiossa sekä teknologian ja patenttien varastamisessa (Civuli, Luma-Osmani, Rufati, & Arifi, 2022).

Kybervakoilu tarkoittaa toimia, joilla pyritään hankkimaan arkaluontoista tai salaista tietoa yksityishenkilöiltä, kilpailijoilta, ryhmiltä ja hallituksilta laittomin keinoin, internetin, tietoverkkojen, ohjelmistojen tai tietokoneiden kautta (Neittaanmäki ym., 2021, s.134-135). Se on siis laitonta salaisen tiedon hankkimista teknologiaa hyödyntäen. Kybervakoilun tavoitteena on taloudellisen, poliittisen tai sotilaallisen edun saaminen ja on myös mahdollista, että kybervakoilulla pyritään saavuttamaan kaikkea näistä edellä mainituista samanaikaisesti (Wangen, 2015). Kybervakoilu on saanut erityistä huomiota viime vuosikymmeninä, kun internetin ja digitaalisen kommunikaation merkitys on kasvanut niin yksityisellä kuin julkisellakin sektorilla (Civuli ym., 2022). Kybervakoilun suorittamisessa hyödynnetään erilaisia tekniikoita, kuten haittaohjelmia (malware) ja tietojenkalastelua (phishing) (Wangen, 2015). Näitä menetelmiä ja tekniikoita käyttäen vakoileva taho pyrkii pääsemään käsiksi kohteen arkaluontoisiin tietoihin. Erityisesti haittaohjelmat mahdollistavat suuren osan kybervakoilusta (Wangen, 2015). Eri kybervakoilumenetelmistä ja -tekniikoista kerrotaan tarkemmin tutkielman seuraavissa luvuissa.

Kybervakoilu on eräänlainen kyberhyökkäys ja kirjallisuudessa vakoilutapauksia käsiteltäessä viitataan usein kyberhyökkäyksiin (Civuli ym., 2022). Kybervakoilun määritelmän ymmärtämiseksi on tärkeää pystyä tunnistamaan eroavaisuudet vakoilun ja suoran kyberhyökkäyksen välillä. Janssonin ja Sihvosen kirjoittamassa artikkelissa (2018) erottavaksi tekijäksi kybervakoilun ja kyberhyökkäyksen välillä kerrotaan olevan näiden

luonteet. ”Kybervakoilu on ei-tuhoava uhka, kun taas kyberhyökkäyksen tarkoitusperät ovat tuhoavia” (Jansson & Sihvonen, 2018). Kyberhyökkäys on siis kattokäsite ja ilmenee esimerkiksi kybervakoilun, -sabotaasin tai -sodankäynnin muodossa (Neittaanmäki ym., 2021, 134-135). Kirjallisuudessa ja myöhemmin tässä kirjallisuuskatsauksessa saatetaan siis kybervakoilun tapauksessa puhua kyberhyökkäyksistä.

Kybervakoilu on myös hyvä erotella kyberrikollisuudesta. Kybervakoilun ja kyberrikollisuuden olennaisin ero on niiden motiiveissa ja tavoitteissa (Neittaanmäki ym., 2021, s.134-135; Wangen, 2015). Kybervakoilu etsii tarkkaan määriteltyä tietoa monimutkaisemmilla menetelmillä, kun taas kyberrikollisuus tavoittelee taloudellista hyötyä yleisimmillä keinoilla. Kybervakoilun ja kyberrikollisuuden olennaisia piirteitä on eroteltu Wangenin (2015) tutkielmassa (taulukko 1).

Kyberrikollisuus voi siis kattaa sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tehtyjä rikoksia, kuten häirintää ja laittoman sisällön levittämistä (Neittaanmäki ym., 2021, s.134-135).

TAULUKKO 1 Kybervakoilun ja -rikollisuuden erot

	Kybervakoilu	**Kyberrikollisuus**
Päätavoitteet	Tiedonhankinta	Rahallinen voitto, vandalismi
Kohteet	Vähän	Useita
Haittaohjelma	Räätälöity	Yleinen
Vaadittu osaaminen	Toimialakohtainen, kyberturvallisuus, kieli ja kulttuuri	Kyberturvallisuus
Vaaditut resurssit	Paljon	Vähän
Tekninen monimutkaisuus	Korkea	Matala

Kybervakoilusta on vielä hyvä nostaa esiin yksi sen muista erottava tekijä. Kybervakoilussa on kaksi pääaspektia: inhimillinen ja tekninen (Rivera, Pazmiño, Becerra, & Barriga, 2022). Inhimillinen puoli sisältää aiemmin esitellyt motiivit, kuten taloudellisen tai poliittisen edun tavoittelun sekä käyttäjän manipuloinnin, jonka avulla ihmiset johdatetaan paljastamaan salaista ja arkaluontoista tietoa. Tekninen puoli taas käsittää edistyneiden ja monimutkaisten haittaohjelmien (malware) kehittämisen ja hyödyntämisen vakoilun toteuttamiseksi. Uusia tekniikoita kehitetään jatkuvasti, mutta nämä kaksi perusnäkökulmaa pysyvät keskeisinä (Rivera ym., 2022).

2.3 Taloudellisen kybervakoilun historia

Taloudellisen kybervakoilun historiallinen konteksti on olennaista ymmärtää, jotta voidaan hahmottaa sen vaikutuksia nykymaailmassa. Tässä luvussa

käydään tiivistetysti läpi taloudellisen kybervakoilun historiaa ja täydennetään teoreettista viitekehystä, tarjoten kontekstia tuleville luvuille.

Kybervakoilun varhaisimmat menetelmät ja tunnetut tapaukset voidaan liittää telekuunteluun (wiretapping) (Rivera, 2014). Jo 1800-luvulla kehittynyt wiretapping eli telekuuntelu oli ensimmäisiä teknologian ja vakoilun yhdistelmiä (Rivera, 2014). Kyseisellä menetelmällä kerättiin arkaluontoista tietoa, kun vakoileva taho pyrki yhdistämään itsensä puhelinlinjaan, ja näin salakuuntelemaan kohteen salaisia keskusteluja (Rivera, 2014). Kybervakoilun käsite kuitenkin muodostui ja vakiintui vasta 1900-luvun loppupuolella teknologian kehittyessä (Civuli ym., 2022).

1980-luvulla tietokoneiden yleistyminen lisäsi rahoitusmarkkinoiden ja verkkopetosten riskejä (Rivera, 2014). Tietokoneiden nopeus ja käytettävyys paranivat merkittävästi, mikä johti niiden laajaan käyttöön yksityisellä sektorilla (Gilani, Mujtaba, Zahoor, & AlMatrooshi, 2023). Pankit alkoivat hyödyntää laajoja tietokantoja, joissa säilytettiin tuhansien asiakkaiden taloustietoja, mikä lisäsi tietoverkkoihin liittyvää laitonta toimintaa kuten vakoilua, rikollisuutta ja ohjelmistopiratismia (Gilani ym., 2023). Tähän isona syynä oli se, miten teknologian kehittyminen tarjosi laitonta toimintaa harjoittavalle osapuolelle anonymiteetin ja näin tietynlaisen turvallisuuden tunteen (Gilani ym., 2023). Vuonna 1986 dokumentoitiin ensimmäinen kybervakoilutapaus, jossa länsisaksalainen hakkeri myi varastettuja tietoja Neuvostoliiton KGB:lle (Civuli ym., 2022). Tämä kybervakoilutapaus tapahtui ennen itse internetin syntyä.

1990-luvulla internetin laajentuminen teki kybervakoilusta ja -rikollisuudesta globaalin ilmiön, luoden pohjan nykyaikaiselle kybervakoilulle (Civuli ym., 2022). Teknologian myöhempi kehittyminen 90-luvulla ja 2000-luvun alkupuolella on mahdollistanut monimutkaisemmat kybervakoilutekniikat ja käyttäjän manipuloinnin kehityksen, joista esimerkkeinä tietojen kalastelu (phishing) (Gilani ym., 2023; Rivera, 2014). Entistä kehittyneempiä menetelmiä hyödyntämällä pystyttiin huijaamaan kohteilta henkilökohtaisia tietoja ja häiritä yritysverkkojen toimintaa (Gilani ym., 2023). Vuonna 1996 Kanadassa vakoilun kustannusten arvioitiin olevan jopa miljardi Kanadan dollaria kuukaudessa (Jones, 2008). Tämä osoittaa, miten kybervakoilusta oli muuttunut taloudellisesti erittäin merkittävä uhka valtioille.

2000-luvun alussa Kiina käynnisti Titan Rain-hyökkäykset länsimaita vastaan ja pyrki varastamaan arkaluontoista tietoa yrityksiltä kuten NASA ja Lockheed Martin (Jones, 2008). Nämä kyberhyökkäykset osoittivat, että kybervakoilu ei kohdistu enää pelkkiin valtioihin, vaan myös suuriin yrityksiin. 2000-luvun aikana kybervakoilun yleisimmiksi menetelmiksi vakioitui haitta- ja vakoiluohjelmat (Jones, 2008). Tämä käy myös ilmi Wangenin (2015) tekemästä tutkielmasta, jossa esitellään 2010-luvun alkupuolella raportoituja kybervakoilutapauksia. Vuosien 2010 ja 2014 välillä tapahtuneiden kybervakoilutapausten suorittamiseksi hyödynnettiin poikkeuksetta jonkinlaista haittaohjelmaa (malware) ja kohdennettua tietojenkalastelua (spear phishing) (Wangen, 2015).

Taloudellisen kybervakoilun historia osoittaa, kuinka teknologian kehitys on jatkuvasti muuttanut ja monimutkaistanut vakoilun menetelmiä. Tietokoneiden ja internetin yleistyminen ovat luoneet kybervakoilusta globaalin ja taloudellisesti merkittävän uhan.

3 TALOUDELLISEN KYBERVAKOILUN MENETELMÄT

Taloudellinen kybervakoilu tarkoittaa siis kybervakoilua, jossa tavoitellaan taloudellisesti arvokasta tietoa. Se on monimutkainen ja jatkuvasti kehittyvä ilmiö, joka muovaa kansainvälistä kilpailua ja turvallisuutta. Yhä digitalisoituvammassa maailmassa taloudellisen tiedon varastaminen kyberhyökkäyksien ja -vakoilun kautta on muodostunut yhdeksi keskeisimmistä uhkista niin yrityksille kuin valtioille (Härting, Bühler, Winter, & Gugel, 2022). Tässä luvussa keskitytään kybervakoiluun taloudellisessa kontekstissa. Tarkastelussa ovat erityisesti eri vakoilumenetelmät ja -tekniikat, minkä lisäksi pyritään avaamaan vakoilun taustalla olevia motiiveja. Luvussa syvennytään kybervakoiluun ja -vaikuttamiseen, tutkitaan uudempia ja innovatiivisempia vakoilumenetelmiä ja niiden eroavaisuuksia sekä uusia uhkia suhteessa nykyisiin ja perinteisiin menetelmiin. Lopuksi esitellään taloudellisen kybervakoilun kohteita ja sitä, miksi juuri tietyt yritykset ja valtiot päätyvät vakoilun kohteeksi, ja mikä niistä tekee arvokkaita ja mielenkiintoisia vakoilukohteita.

3.1 Vakoilumenetelmät ja -tekniikat

Taloudellisen kybervakoilun suorittamisessa hyödynnetään erilaisia menetelmiä ja tekniikoita, joita ovat esimerkiksi erilaiset haittaohjelmat sekä käyttäjän manipulointi (social engineering). Näitä keinoja käyttämällä vakoileva taho pyrkii pääsemään käsiksi kohteen tietoihin ja järjestelmiin (Wangen, 2015). Tämä alaluku esittelee yleisimpiä kybervakoilumenetelmiä ja tekniikoita taloudellisesta näkökulmasta yksityiskohtaisemmin. Alaluvuissa selitetään, kuinka kukin menetelmä tai tekniikka toimii, minkä lisäksi niiden ymmärtämisen helpottamiseksi esitetään esimerkkejä vakoilutapauksista, pyrkien vastaamaan kysymyksiin: missä vakoilu tapahtui, kuinka se toteutettiin, mikä oli vakoilun alkuperä ja mitä tietoa haluttiin varastaa.

Taloudellinen kybervakoilu tapahtuu useimmissa tapauksissa APT:n, haittaohjelman (malware) tai käyttäjän manipuloinnin muodossa (Verizon, 2020). Seuraavissa alaluvuissa syvennymmekin näihin menetelmiin tarkemmin.

3.1.1 APT

Yksi merkittävimmistä uhkista nykyaikaisessa kybervakoiluympäristössä on APT (advanced persistant threat). APT:llä viitataan jatkuvaan ja kohdennettuun kyberhyökkäykseen, jossa vakoileva taho pyrkii saavuttamaan havaitsemattoman läsnäolon kohteen verkossa arkaluontoisen tiedon varastamiseksi pitkällä aikavälillä (Bodström & Hämäläinen, 2018). Jotta voidaan ymmärtää APT-hyökkäyksen käsitettä paremmin, on hyvä avata käsitettä hieman tarkemmin. Sanalla advanced viitataan siihen, miten hyökkääjä voi hyökkäyksessään käyttää laajasti eri keinoja ja tekniikoita (Neittaanmäki ym., 2021, s.141-142). Persistent taas viittaa hyökkääjän tai vakoilevan osapuolen sinnikkyyteen suorittaa tehtävä käyttäen valittuja toimintaohjeita ja tekniikoita, jotta hyökkäys saavuttaa sen tavoitteet. Sinnikkyydellä ei välttämättä tarkoiteta yksittäisen menetelmän tai tekniikan jatkuvaa käyttöä, vaan hyökkääjän jatkuvaa vuorovaikutusta kohteen kanssa, joka kestää niin pitkään kunnes tavoite saavutetaan (Neittaanmäki ym., 2021, s.141-142). Threat eli uhka viittaa hyökkääjän järjestäytyneisyyteen ja siihen, miten motivoituneita he ovat. Vaikka uhka mielletään usein käytettäväksi haittaohjelmaksi (malware), on todellinen uhka erityisesti hyökkäävä taho, jotka ovat hyökkäyksen konkreettinen uhka (Neittaanmäki ym., 2021, s.141-142).

APT-hyökkäysten tunnuspiirteisiin kuuluu siis niiden pitkäkestoisuus, korkea salaustaso sekä kohdennettu luonne, tehden niistä erityisen vaarallisia ja vaikeasti havaittavia (Cole, 2012). Koska APT-hyökkäyksen suunnittelu ja toteuttaminen vaatii paljon resursseja ja osaamista, on niiden takana usein valtiollisia toimijoita tai isompia organisaatioita, jotka omaavat edellytykset kuten rahoituksen hyökkäyksen suorittamiseen (Cole, 2012). Tero Bodströmin ja Timo Hämäläisen tutkimuksessa (2018) kerrotaan APT-hyökkäyksen yhdeksi olennaisimmaksi tunnuspiirteeksi olevan sen monimutkaisuus ja ulottuminen useille eri tasoille. Käynnissä oleva APT-hyökkäys käyttää useita eri tekniikoita naamioidakseen toimintansa kohteen verkossa tai tietojärjestelmissä. APT saattaa esimerkiksi soluttautua ja piiloutua kohteen verkkoon jäljittelemällä laillista tietoliikennettä ja muokkaamalla itseään hyökkäyksen aikana, tehden sen tunnistamisesta erittäin vaikeaa (Bodström & Hämäläinen, 2018). Kuten aiemmin jo esitettiin, APT-hyökkäykset myös useimmissa tapauksissa hyödyntävät muita vakoilumenetelmiä ja -tekniikoita, joita ovat esimerkiksi haittaohjelmat (malware), tietojenkalastelu (phishing) sekä käyttäjänmanipulointi (social engineering) (Wangen, 2015). Näitä vakoilumenetelmiä tarkastellaan tarkemmin myöhemmissä luvuissa.

Seuraavaksi tarkastellaan APT-hyökkäyksiä reaalimaailman esimerkkitapausten avulla ja selvitetään, miten tätä tekniikkaa hyödynnetään taloudellisen vakoilun suorittamisessa. APT1 on yksi tunnetuimmista

kybervakoiluryhmistä, joka erikoistuu taloustietojen ja henkisen pääoman varastamiseen taloudellisen hyödyn saavuttamiseksi. Se on yksi Kiinan hallituksen tukemista suurimmista kybervakoiluryhmistä, joka on toiminut vuodesta 2006 lähtien ja suorittanut useita kybervakoilukampanjoita lukuisiin kohteisiin (Wangen, 2015). Ryhmästä raportoineen yhdysvaltalaisen Mandiantin mukaan ryhmä operoi Shanghaista käsin ja on arviolta jopa tuhansien henkilöiden vahvuinen, kaikki ryhmään kuuluvat ovat tietoturvassa koulutettuja ja hallitsevat erinomaisesti englannin kielen (Ring, 2013). Raporttien mukaan APT1:llä on ollut kyky hakkeroida ainakin 141 organisaatiota yli 20 merkittävällä teollisuudenalalla (Wangen, 2015). APT1 kerää erityisesti taloudellisesti merkittävää henkistä pääomaa ja immateriaalioikeuksia, kuten teknologiasuunnitelmia (blueprints), valmistusprosesseja, testituloksia sekä yrityksien välisiä sopimuksia (Wangen, 2015). APT1 hyödyntää erittäin hienostunutta ja monitasoista vakoilumenetelmää, mikä käy ilmi sen toimintaperiaatteesta.

Mandiantin raportti osoittaa, että APT1 sisältää kahdeksan eri vaihetta, mikä kuvastaa hyökkäyksen monimutkaisuutta (Wangen, 2015). Käytännössä APT1 käyttää vaarallisia haittaohjelmia, joita kutsutaan Remote access trojans (RAT) murtautuakseen kohteensa tietojärjestelmiin. APT1 hyödyntää kahden tyyppisiä RAT-haittaohjelmia: yksinkertaisia ja monimutkaisia (Wangen, 2015). Yksinkertainen troijalainen antaa hyökkääjälle vakoilua suorittavalle toimijalle mahdollisuuden hallita tietokonetta etänä, suorittaa perustoimintoja kuten tiedostojen lataamista ja pitää itse haittaohjelman piilossa. Monimutkaisempi troijalainen puolestaan sisältää useita keinoja, joilla vakoileva osapuoli voi varastaa tietoa ja hiiren liikkeitä (Wangen, 2015). Tämä auttaa vakoilua suorittavaa tahoa saamaan täyden hallinnan uhrin tietokoneesta ja varastamaan heiltä arkaluontoista taloudellista tietoa.

Mandiantin raportista (2021) selviää, miten APT1-ryhmä murtautuu kohdeorganisaatioiden verkkoihin ja järjestelmiin lähettämällä huijausviestejä, joissa on haitallisia liitteitä tai linkkejä. Nämä viestit pyrkivät vaikuttamaan mahdollisimman aidoilta, sillä ne näyttävät tulevan jo entuudestaan tutuilta henkilöiltä, kuten työkavereilta tai yrityksen johdolta (Mandiant, 2021). Jos viestin saanut henkilö sattuu avaamaan tällaisen viestin, heidän tietokoneelleen latautuu haittaohjelma, joka antaa tässä tapauksessa APT1:lle pääsyn kohteen tietokoneeseen.

APT1-ryhmän toiminta on selkeä osoitus siitä, miten kybervakoilu mahdollistaa taloudellisten tietojen varastamisen ja tuottaa näin vakoilevalle taholle merkittävää taloudellista hyötyä. Tämänkaltainen kybervakoilu voi johtaa huomattaviin taloudellisiin menetyksiin niin yrityksille kuin valtioillekin, sillä tämä ei ainoastaan vahingoita kohdeyritysten ja -valtioiden taloudellista tilannetta, vaan voi myös merkittävästi heikentää niiden kilpailukykyä markkinoilla.

3.1.2 Haitta- ja vakoiluohjelmat

Haitta- ja vakoiluohjelmat ovat keskeisiä välineitä taloudellisessa kybervakoilussa ja ne mahdollistavat arkaluontoisen tiedon varastamisen ja järjestelmien sabotoimisen. Ne muodostavat merkittävän uhan kybervakoilussa, koska ne ovat muuttuneet yhä monimutkaisimmiksi ja niiden havaitseminen on vaikeutunut entisestään (Neittaanmäki ym., 2021, s.139-140). Tässä alaluvussa tarkastellaan erilaisia haitta- ja vakoiluohjelmia kuten troijalaisia ja haittakiristysohjelmia sekä esitetään, miten niiden avulla käytännössä toteutetaan taloudellisesti motivoitunutta kybervakoilua.

Haittaohjelma eli malware tarkoittaa tietokoneohjelmaa, joka on suunniteltu aiheuttamaan ei-toivottuja ja vahingollisia toimintoja tietokonejärjestelmässä (Wangen, 2015). Haittaohjelmia on monenlaisia, mutta kiristysohjelmat (ransomware), troijalaiset (trojan) sekä vakoiluohjelmat (spyware) ovat taloudellisen vakoilun näkökulmasta käytetyimpiä ja vaarallisimpia (Wangen, 2015). Haittaohjelmat voivat olla suunnattu erityisesti tiettyihin järjestelmiin tai toimia yleisinä, itseään toistavina ohjelmina, jotka pyrkivät iskemään kaikkiin saatavilla oleviin kohteisiin (Wangen, 2015). Kun kyseessä on erityisesti taloudellisesti motivoitunutta kybervakoilua, ovat käytetyt haittaohjelmat usein huomattavasti kohdennetumpia ja monimutkaisempia (Wangen, 2015). Haittaohjelma on lähtökohtaisesti suunniteltu varastamaan, salaamaan tai poistamaan arkaluontoista tietoa, mutta ne voivat myös muokata tai ottaa haltuunsa järjestelmien keskeisiä toimintoja ja salaa seurata kohteensa toimintaa (Agrawal, Singh, Gour, & Kumar, 2014; Wangen, 2015). Internetin ja laitteiden välisen riippuvuuden lisääntymisen myötä vakoilua suorittavan tahon on mahdollista levittää haittaohjelmia entistä nopeammin ja näin päästä käsiksi yhä useampaan tietokoneeseen lyhyessä ajassa (Agrawal ym., 2014). Pahimmillaan haittaohjelma pystyy pysyttelemään huomaamattomana jopa useita vuosia aiheuttaen kohteelleen merkittäviä ja vakavia taloudellisia menetyksiä (Neittaanmäki ym., 2021, s.139-140).

Kuten aiemmin jo todettiin, ns. troijalainen (trojan) on yksi yleisimmistä ja käytetyimmistä haittaohjelmatyypeistä ja sen toimintaperiaatteen ymmärtäminen on olennaista, kun tarkastellaan haittaohjelmia kybervakoilun välineenä. Troijalainen on haittaohjelmatyyppi, joka esiintyy kohteelleen hyödyllisenä ohjelmana saadakseen pääsyn käyttäjän tietojärjestelmään (Agrawal ym., 2014). Troijalaiselle tyypillinen piirre on sen kyky monistaa itseään ja varastaa arkaluontoista tai luottamuksellista tietoa käyttäjän laitteelta (Agrawal ym., 2014). Taloudellisen vakoilun tapauksessa troijalaiset siirtyvät kohteen järjestelmiin useimmiten sähköpostien ja niihin liitettyjen linkkien tai tiedostojen kautta (Wangen, 2015).

Jotta pystytään ymmärtämään paremmin haittaohjelmien vaikutusta ja merkitystä taloudellisen kybervakoilun välineenä, on hyvä tarkastella niitä reaalimaailman esimerkkitapausten kautta. Yksi tunnetuimmista haittaohjelmaa hyödyntävistä vakoilutapauksista on Stuxnet-niminen tietokonehaittaohjelma, joka kehitettiin erityisesti ohjaamaan ja haittaamaan teollisuuden ohjausjärjestelmiä (Civuli ym., 2022). Kyseinen haittaohjelma löydettiin vuonna

2010 (Wangen, 2015). Stuxnetin suunnittelusta vastasi Yhdysvallat ja Israel ja se luotiin vahingoittamaan Iranin ydinvoimaloita, vaikuttaen suoraan maan ydinmateriaalin tuotantoon ja energiaomavaraisuuteen (Civuli ym., 2022; Rivera ym., 2022). Stuxnet oli ensimmäinen laajalti tunnettu kyberhyökkäys, joka aiheutti vahinkoa fyysisellä tasolla digitaalisten järjestelmien lisäksi (Wangen, 2015). Vaikka Stuxnet ei varsinaisesti ollut vakoiluun luotu haittaohjelma, sen taloudelliset vaikutukset olivat merkittävät, ja se loi uudenlaisen muotin tuleville haittaohjelmille. Näistä yksi oli vuonna 2011 löydetty Duqu-haittaohjelma, joka erityisesti pohjautui Stuxnettiin (Bencsáth, Pék, Buttyán, & Félegyházi, 2012). Toisin kuin Stuxnet, Duqu oli suunniteltu kybervakoiluun ja varastamaan arkaluontoista tietoa, eikä aiheuttamaan fyysistä tuhoa ja sabotaasia (Bencsáth ym., 2012). Duqu levisi tarkasti teollisuusyrityksiin kohdennettujen sähköpostiviestien kautta, jotka sisälsivät itse haittaohjelman (Wangen, 2015). Haittaohjelman onnistuessa pääsemään käsiksi kohteen järjestelmiin, se pyrki varastamaan salasanoja, ottamaan näyttökuvia ja keräämään muuta arkaluontoista tietoa (Wangen, 2015). Duqu onnistui tartuttamaan noin 20 eri kohdetta, joista suurin osa oli Euroopassa ja Lähi-idän alueella (Bencsáth ym., 2012). Molemmat haittaohjelmat korostava kybervakoilun uhkaa ja osoittavat, että kybervakoilu voi aiheuttaa merkittäviä taloudellisia seurauksia sekä kansallisella että yksityisellä sektorilla.

Toinen taloudellisen vakoilun kannalta merkittävä haittaohjelmatyyppi ovat niin kutsutut vakoiluohjelmat (spyware). Vakoiluohjelma tarkoittaa haitallista ohjelmaa, joka tunkeutuu kohteen tietokoneeseen tai järjestelmiin keräämään tietoa käyttäjästä, pyrkien siirtämään sen kolmannelle osapuolelle ilman, että kohde havaitsee tätä (Qabalin, Naser, & Alkasassbeh, 2022). Vakoiluohjelma voidaan mieltää haittaohjelmien (malware) alalajiksi, mutta sillä on omat tekniset erityispiirteensä, jotka erottavat sen muista haittaohjelmista (Qabalin ym., 2022). Vakoiluohjelmien olennaisimpina tunnuspiirteinä voidaankin pitää niiden kykyä kerätä ja varastaa arkaluontoista tietoa (Civuli ym., 2022; Qabalin ym., 2022). Markkinoilla liikkuu monenlaisia vakoiluohjelmia, joista yksi esimerkki on näppäimistön painalluksia tallentava keylogging-ohjelma (Gilani ym., 2023). Tämänkaltainen vakoiluohjelma erikoistuu täsmällisesti tärkeiden ja arkaluontoisten tietojen kaappaamiseen ja niiden eteenpäin välittämiseen kolmansille osapuolille. Vakoiluohjelmat leviävät haittaohjelmille tyypilliseen tapaan internetin tai sähköpostiliitteiden kautta ja ne omaavat usein kyvyn levitä nopeasti toisiin laitteisiin (Gilani ym., 2023).

Viimeisenä taloudellisen vakoilun kannalta merkittävänä haittaohjelmana esitetään haittakiristysohjelmat eli ransomware. Ne kohdistuvat usein esimerkiksi pankki- ja rahoitussektorille sekä julkishallintoon, mutta lisääntyvissä määrin myös yrityksiin (Neittaanmäki ym., 2021, s.139-140). Kiristyshaittaohjelmat ovat haittaohjelmia, joiden tarkoituksena on uhkailla kohteitaan ja kiristää niiltä esimerkiksi rahaa tai arvokasta tietoa (Härting ym., 2022). Ne tunkeutuvat kohteen tietoliikenneverkkoihin eri keinoja käyttäen ja pahimmassa tapauksessa ne pystyvät esimerkiksi salaamaan kohteensa kaikki verkkolevyt ja pilvipalvelutiedostot, lamauttaen koko organisaation toiminnan

(Neittaanmäki ym., 2021, s.139-140). Yksi esimerkkitapaus kiristyshaittaohjelmien tehokkuudesta ja kyvystä tuottaa taloudellista vahinkoa on vuonna 2017 levinnyt WannaCry-kiristyshaittaohjelma. Kyseinen kiristyshaittaohjelma käytti hyväkseen Microsoft Windowsin haavoittuvuutta ja vaati kohteiltaan lunnaita bitcoinien muodossa (Neittaanmäki ym., 2021, s.139-140). Se onnistui tartuttamaan lyhyellä aikavälillä noin 200,000 tietokonetta ympäri maailman (Neittaanmäki ym., 2021, s.139).

Tässä luvussa esiteltyjen haittaohjelmien avulla voidaan siis varastaa arkaluontoista tietoa ja sabotoida järjestelmiä, aiheuttaen yrityksille ja kansantalouksille merkittäviä taloudellisia menetyksiä. Esimerkkitapaukset, kuten Stuxnet, Duqu ja WannaCry osoittavat haittaohjelmien tuhoisuuden taloudellisesta näkökulmasta. Haittaohjelmien kehittyessä ja yleistyessä ne muodostavat yhä suuremman uhan sekä yksityisille että julkisille toimijoille.

3.1.3 Käyttäjän manipulointi ja tietojenkalastelu

Tässä alaluvussa esitellään tarkemmin käyttäjän manipuloinnin (social engineering) ja tietojen kalastelun (phishing) käsitteet sekä tarkastellaan, miten vakoilevat toimijat hyödyntävät näitä taloudellisen vakoilun välineinä.

Kybervakoilussa korostuvat niin tekniset kuin ihmisiin liittyvät näkökulmat. Tekninen näkökulma keskittyy aiemmin esiteltyjen haittaohjelmien käyttöön, kun taas ihmisten näkökulmassa hyödynnetään käyttäjän manipulointia ja esimerkiksi työntekijöiden tietotaidon puutetta organisaatiossa (Rivera ym., 2022). Ihmisten osuus kybervakoilussa on erittäin keskeinen, sillä haittaohjelmien siirtäminen kohteeseen ja sitä kautta arkaluontoisen tiedon varastaminen vaatii lähes poikkeuksetta käyttäjän manipulointia (Wangen, 2015). Tämä voidaan todeta aiempien lukujen esimerkkitapauksia tarkastelemalla, missä vakoilu on saanut alkunsa useimmiten esimerkiksi sähköpostiviestien tai haitallisten linkkien kautta. Jotta kyberhyökkäys pääsee alkamaan ja haittaohjelma saadaan siirrettyä kohteeseen, vaaditaan siis usein inhimillinen virhe. Termi käyttäjän manipulointi (social engineering) perustuu juuri siihen, että vakoileva taho käyttää jollain tapaa sosiaalista vuorovaikutusta suostutellakseen yksilöitä tai organisaatioita toimimaan haluamallaan tavalla (Neittaanmäki ym., 2021, s.140-141). Käyttäjän manipulointi eli social engineering on yksi keskeinen keino taloudellisessa vakoilussa, jossa ihmisten luottamusta, tietämättömyyttä ja muita inhimillisiä piirteitä hyväksikäytetään arkaluontoisten tietojen hankkimiseksi (Neittaanmäki ym., 2021, s.141).

Schaferin ja Karlinsin (2021) tekemässä tutkimuksessa pyrittiin osoittamaan, kuinka yksinkertaisilla välineillä, kuten mobiililaitteilla ja julkisesti saatavilla olevilla ohjelmistoilla sekä käyttäjän manipulaatiolla pystytään pääsemään yrityksen arkaluontoisiin tietoihin käsiksi. Aluksi henkilöstöä pyrittiin harhauttamaan soittamalla yrityksen eri osastoille ja esittämällä olevansa työntekijä tai ulkopuolinen avun tarpeessa oleva henkilö. Kohdeyrityksen henkilöstön avuliaisuutta ja tietämättömyyttä hyödyntämällä saatiin kerättyä pieniä, mutta tärkeitä tietoja, joita olivat esimerkiksi työntekijöiden nimet ja yhteystiedot. Tutkimuksesta kävi ilmi, kuinka helposti luottamuksen

rakentaminen tapahtui, eikä siihen vaadittu kuin kohteliaisuutta ja luovuutta. Kun vakoilija oli onnistunut keräämään tarpeeksi tietoa, tämä lähetti tekaistuja sähköposteja, jotka näyttivät tulevan luotettavasta lähteestä, yrityksen IT-osastolta. Vakoilija pyysi kohteitaan avaamaan sähköpostissa olevia liitteitä, jotka todellisuudessa sisälsivät eräänlaisen troijalaisen haittaohjelman. Haittaohjelman päästessä käsiksi kohteensa järjestelmiin, se pystyi varastamaan yritykseltä arkaluontoista taloudellista tietoa (Schafer & Karlins, 2021). Tämä esimerkkitapaus osoittaa, miten harmittomalta vaikuttavat tiedot saattavat koitua merkittäväksi uhkaksi yrityksille ja miten helposti ihmisten inhimillistä puolta pystytään hyväksikäyttämään taloudellisen vakoilun suorittamiseksi.

Kun tarkastellaan käyttäjän manipulointia (social engineering), on hyvä esitellä sen tyypillisimpiä esiintymismuotoja. Erityisesti tietojenkalastelu (phishing) on tyypillinen esimerkki käyttäjän manipuloinnista (Neittaanmäki ym., 2021, s.141). Tässä menetelmässä vakoileva taho pyrkii esiintymään luotettavana tahona ja yrittää päästä käsiksi kohteen henkilökohtaisiin tietoihin, kuten salasanoihin tai käyttäjätunnuksiin (Neittaanmäki ym., 2021, s.141). Aiemmassa kappaleessa esitetty tapaustutkimus yritysvakoilusta on esimerkki siitä, miten tietojenkalastelua voidaan hyödyntää taloudellisessa vakoilussa. Kirjallisuudessa esiintyy myös ns. kohdennettua tietojenkalastelua (spear phishing) ja on hyvä pystyä erottamaan tämänkaltainen käyttäjän manipulointi ”tavallisesta” tietojenkalastelusta. Tietojenkalastelun tapauksessa kyseessä on useimmiten laajamittaisesta hyökkäyksestä, jossa pyritään tavoittamaan mahdollisimman monta uhria samanaikaisesti (Koyun & Janabi, 2017; Wangen, 2015). Tietojenkalastelu (phishing) hyökkäykset eivät yleensä ole kohdennettuja, vaan vakoileva taho lähettää viestejä suurille ihmisjoukoille toivoen, että edes muutama heistä lankeaisi ansaan (Wangen, 2015). Esimerkiksi sähköpostitse lähetettävä huijausviesti, joka väittää olevansa pankilta ja pyytää päivittämään tilin tiedot, on tyypillinen esimerkki tietojenkalastelusta. Toisaalta taas kohdennettu tietojenkalastelu eli spear phishing on huomattavasti hienovaraisempaa ja tarkemmin suunniteltua (Koyun & Janabi, 2017). Tällaisen vakoilun tapauksessa vakoileva taho pyrkii keräämään kohteestaan tietoa esimerkiksi sosiaalisen median ja internetin kautta (Rivera ym., 2022). Näitä ennakkotietoja hyödyntämällä vakoileva taho pyrkii huijaamaan kohdettaan esimerkiksi tekeytymällä tämän työkaveriksi tai esimieheksi (Wangen, 2015). Erona ”tavalliseen” tietojenkalasteluun (phishing) on siis tarkempi kohdistuneisuus (Rivera ym., 2022).

Käyttäjän manipulointi on erittäin keskeinen keino taloudellisessa vakoilussa ja ilman sitä haittaohjelmien ja kyberhyökkäysten suorittaminen olisi huomattavasti haastavampaa, ellei jopa mahdotonta. Tällaiset käyttäjän manipulaatiota hyödyntävät kybervakoiluyritykset voivat johtaa merkittäviin taloudellisiin menetyksiin, niin yrityksien kuin kansantalouksienkin näkökulmasta. Käyttäjän manipulointi osoittaa myös, miten pelkästään teknologisen puolen kyberuhkilta suojautuminen ei riitä. On pystyttävä varautumaan myös inhimillisiin uhkiin.

3.2 Vakoilumenetelmien ja -tekniikoiden kehitys ja tulevaisuuden suuntaukset

Aiemmissa luvuissa on tarkasteltu, millaisia kybervakoilumenetelmiä lähihistoriassa ja nykyhetkessä hyödynnetään taloudellisen tiedon varastamiseen. Seuraavaksi tarkastellaan, miten uudet teknologiat, kuten tekoäly (AI), koneoppiminen ja IoT (internet of things) muokkaavat kybervakoilun kenttää ja tuovat mukanaan uusia haasteita sekä uhkia.

Tekoäly (AI) on tällä hetkellä yksi käsitellyimmistä aiheista useilla eri aloilla. Sen mahdollisia vaikutuksia ja käyttötarkoituksia on tutkittu myös kybervakoilun näkökulmasta. Tekoälyn kehittymisen uskotaan tuovan lisää haasteita kyberturvallisuuden näkökulmasta, kasvattaen kybervakoilun mahdollisuuksia (Gilani ym., 2023). Dr. Benjamin Jensenin (2023) antamassa todistuksessa kerrotaan, kuinka edistykset generatiivisessa tekoälyssä luovat uusia kohteita Kiinan vakoilukampanjoille. Lausunnossa kerrotaan, miten tekoäly mahdollistaa räätälöityjen haittaohjelmien kehittämisen immateriaalioikeuksien varastamiseen startup firmoilta (Jensen, 2023).

Tekoälyteknologian nopea kehitys luo uudenlaisia keinoja jo aiemmin esiteltyyn käyttäjän manipulointiin ja tietojenkalasteluun (Akoto, 2022). Sen avulla pystytään entistä tarkempaan kohdennukseen analysoimalla kohteen sähköpostiviestintää tai sosiaalisen median kommunikaatiota. Tekoäly oppii yksittäisten henkilöiden käyttäytymistä, kielenkäyttöä ja kirjoitustyyliä. Näitä tietoja voidaan sitten käyttää huijausviestien luomiseen, joita on entistä vaikeampaa erottaa aidoista viesteistä (Akoto, 2022). Tekoälyn ja kyberhyökkäysten yhdistyminen muokkaa kybertoimintoja kohti niin sanottuja hybridiuhkia, nostaen esimerkiksi kybervakoilun uhkatasoa ja kyvykkyyksiä (Gonçalves, 2019). Tekoälyllä siis pystytään lisäämään kybervakoilun vaikutusalaa, tiheyttä, nopeutta ja vaarallisuutta koneoppimisen tuomien synergiaetujen ansiosta (Gonçalves, 2019).

Tekoälyn lisäksi myös esimerkiksi 5G-verkot ja IoT (internet of things) luovat uusia uhkakuvia taloudellisen kybervakoilun kentälle. Uuden sukupolven verkkoteknologiat, kuten 5G tuovat mukanaan lisääntynyttä monimutkaisuutta ja hajautusta, mikä voi luoda uusia haavoittuvuuksia kybervakoilun näkökulmasta (Akoto, 2022). IoT-laitteiden lisääntyvä käyttö yrityksissä luo myös potentiaalisen kohteen kybervakoilulle (Hou & Wang, 2020). IoT-laitteiden monimuotoisuus ja usein puutteellinen tietoturva tekevät niistä alttiita väärinkäytölle (Rivera ym., 2022). Yhden laitteen murto voi mahdollistaa pääsyn koko laiteverkkoon, aiheuttaen ketjureaktion ja altistaen koko järjestelmän vakoilulle tai sabotaasille (Rivera ym., 2022).

Vaikka tekoälyä hyödyntävistä vakoiluyrityksistä tai -hyökkäyksistä ei ole vielä paljoa raportteja tai kirjallisuutta, on todennäköistä, että tulevaisuudessa

tekoäly ja IoT-ympäristöt tulevat olemaan keskeisiä kohteita ja välineitä taloudellisessa kybervakoilussa. Näiden teknologioiden tarjoamat mahdollisuudet tuovat uusia, ennennäkemättömiä uhkia, joita on tärkeää ennakoida ja torjua.

3.3 Taloudellisen kybervakoilun kohteet

Taloudellisella vakoilulla siis pyritään saamaan haltuun arvokasta henkistä pääomaa ja arkaluontoista taloudellisesti merkittävää tietoa. Tässä luvussa tarkastellaan taloudellisen kybervakoilun ensisijaisia kohteita, eli ketkä ovat suurimmassa vaarassa joutua vakoilun kohteeksi. Lisäksi analysoidaan teknisestä näkökulmasta, mitkä järjestelmät ja laitteet ovat vakoilijoille helpoimpia ja houkuttelevimpia kohteita.

Yleinen ajatus on, että taloudellinen vakoilu kohdistuisi ainoastaan isoimpiin ja taloudellisesti menestyneimpiin valtioihin, kuten Yhdysvaltoihin, Kiinaan ja Venäjään. Suuret valtiot, yritykset ja akateemiset laitokset ovat tyypillisiä kohteita niiden arvokkaan datan ja henkisen pääoman vuoksi (Civuli ym., 2022). Todellisuudessa taloudellista kybervakoilua kohdistuu myös pienempiin valtioihin ja yrityksiin (Härting ym., 2022).

Lähi-idän maat on nähty historian valossa erittäin houkuttelevina talousvakoilun kohteina, mikä osittain johtuu niiden heikoksi koetusta puolustuskyvystä, mutta taustalla on myös lähes poikkeuksetta sotilaallisia ja poliittisia syitä (Wangen, 2015). Jo aiemmin esitetty Stuxnet-haittaohjelma on yksi esimerkkitapaus Lähi-itään kohdistuneesta kybervakoilu ja -hyökkäys tapauksesta.

Toinen yleinen harhakuva on, että taloudellinen kybervakoilu rajoittuisi vain kilpailijamaihin; se ulottuu todellisuudessa myös liittolaismaihin, joita esimerkiksi Yhdysvaltojen tapauksessa ovat Ranska, Saksa ja Etelä-Korea (Akoto, 2022). Myös Kiinassa tämänkaltainen valtion sisäisten kilpailijoiden vakoilu on erityisen yleistä (Verizon, 2020). Tämä korostaa taloudellisen kybervakoilun monimutkaisia geopoliittisia ulottuvuuksia ja sitä, miten vakoilun kohde voi olla yhtä hyvin vihollinen kuin liittolainen (Solberg Søilen, 2016).

On selvää, että tietyt sektorit ja teollisuuden alat ovat taloudellisen vakoilun näkökulmasta erityisen alttiita ja houkuttelevia kohteita. Teknologia-, energia- ja finanssisektorit ovat jatkuvasti kybervakoilun kohteena niiden taloudellisesti strategisen merkityksen ja arkaluotoisen henkisen pääoman vuoksi (Rivera, 2014). Verizonin tekemästä raportista (2020) käy ilmi, miten vakoilluimmat sektorit ovat julkisen sektorin organisaatiot sekä tuotanto ja valmistus.

Vaikka taloudellisen ja teollisen kybervakoilun kohteina ovat usein suuret yritykset, kuten Apple tai Facebook, myös pienemmät yritykset voivat toimia houkuttelevina kohteina, sillä ne tarjoavat väylän päästä käsiksi laajempien ja suurempien yritysten tietoihin (Härting ym., 2022). Tämä tekee keskisuurista yrityksistä houkuttelevia kohteita vakoilutoimille (Akoto, 2022; Härting ym., 2022). Koska pienet ja keskisuuret yritykset (SME) toimivat usein

palveluntarjoajina suuremmille yrityksille, hakkerit ja vakoojat voivat pyrkiä tunkeutumaan suurempien yritysten järjestelmiin hyökkäämällä ensin pienempien yritysten heikommin suojattuihin järjestelmiin (Härting ym., 2022). Lisäksi, vakoilevaa tahoa voi houkutella pienempien ja keskisuurten yritysten kohdalla pienempi vaiva ja vakoiluun tarvittavat resurssit, eikä niinkään mahdollinen hyöty (Härting ym., 2022). Verizonin (2020) tekemä raportti toteaa, kuinka vakoiltavan yrityksen koolla ei niinkään ole väliä, olennaista on se, mitä kohdeyritys tuottaa ja onko vakoilevalla taholla intressejä tätä kohtaan. Esimerkiksi Kiina on osoittanut kybervakoilullaan kiinnostusta erityisesti pieniin startup-yrityksiin tekoälyn alalla (Jensen, 2023).

Taloudellisen kybervakoilun kohteet eivät rajoitu ainoastaan maantieteelliselle tasolle, tietyille sektoreille tai tiettyihin yrityksiin. Kybervakoilun kohteita on myös hyvä pystyä tarkastelemaan teknisellä tasolla. Käyttöjärjestelmien näkökulmasta Microsoft Windows ympäristöt ovat selkeästi yleisimpiä kohteita, mikä käy ilmi paljastuneista vakoilutapauksista (Wangen, 2015). Tämä johtuu varmasti suurimmilta osin siitä, että ne ovat yrityksien tapauksessa selvästi suositumpia, kuin Applen tai Linuxin käyttöjärjestelmät. Tämän takia vakoilevalla taholla on myös usein enemmän kokemusta näihin järjestelmiin tunkeutumisesta. Esimerkiksi vuonna 2012 paljastettu Gauss-haittaohjelma kohdistui erityisesti Windowsin eri käyttöjärjestelmäversioihin ja pyrki varastamaan tietoa kohteiden pankkijärjestelmistä (Bencsáth ym., 2012).

4 YHTEENVETO

Tässä tutkielmassa on tarkasteltu taloudellisen kybervakoilun menetelmiä ja tekniikoita, erityisesti keskittyen valtiollisten ja yksityisten toimijoiden käyttämiin menetelmiin. Tutkielman päätavoitteena oli selvittää, *millaisia menetelmiä taloudellisessa kybervakoilussa käytetään*? ja *mitkä ovat käytettyjen menetelmien mahdolliset vaikutukset taloudellisesta näkökulmasta*? Tutkielma toteutettiin systemaattisena kirjallisuuskatsauksena. Lähdeaineisto kerättiin useista eri tietokannoista, joita olivat JYKDOK, Google Scholar, Scopus, ScienceDirect ja ResearchGate. Tutkielmaan kerättiin tietoa niin kansainvälisistä kuin kotimaisista vertaisarvioiduista tutkimuksista ja kirjoista. Lisäksi lähdemateriaalina käytettiin erityisesti tapaustutkimuksia ja kyberturvallisuusyritysten tekemiä raportteja. Suurin osa valitusta lähdekirjallisuudesta oli kirjoitettu englannin kielellä. Lähteitä arvioitiin JUFO-luokitusten, julkaisijan ja sen luotettavuuden, viittausten määrän sekä ajankohtaisuuden perusteella. Näin pyrittiin varmistamaan aineiston korkea laatu ja relevanssi tutkimusaiheeseen.

Nykymaailmassa yhä suurempi osa liiketoiminnasta tapahtuu digitaalisessa ympäristössä, mikä on tehnyt tiedoista entistä arvokkaampia ja helpommin saatavilla olevia, lisäten samalla kybervakoilun uhkia (Härting ym., 2022). Kyberhyökkäykset ovat yhä monimutkaisempia ja vaikeammin havaittavissa, mikä korostaa tutkimuksen tarvetta ymmärtää kybervakoilun dynamiikkaa ja kehittää tehokkaampia suojautumiskeinoja.

Tutkielma osoitti, että taloudellinen kybervakoilu on monimutkainen ja laaja-alainen ilmiö, joka hyödyntää erilaisia teknologisia ja inhimillisiä menetelmiä. Keskeisimpiä menetelmiä taloudellisen kybervakoilun näkökulmasta ovat APT-hyökkäykset (Advanced Persistent Threat), haittaohjelmat (malware) ja käyttäjän manipulointi (social engineering), kuten tietojenkalastelu (phishing). Näiden menetelmien avulla vakoilevat toimijat pyrkivät pääsemään käsiksi arkaluontoiseen taloudelliseen tietoon, mikä voi johtaa merkittäviin taloudellisiin menetyksiin ja kilpailuedun menetykseen yrityksille ja valtioille. Tutkielmassa myös huomattiin, miten vakoilu vaatii lähes

poikkeuksetta useamman menetelmän tai tekniikan hyödyntämistä vakoilun suorittamiseksi. Tutkielmassa havaittiin, että taloudellisen vakoilun taustalla on usein taloudellisia, poliittisia ja strategisia motiiveja, ja usein nämä motiivit ovat päällekkäisiä. Vakoilua suorittavat tahot pyrkivät hyötymään taloudellisesti tai saavuttamaan strategista etua kilpailijoistaan.

Tutkimusmenetelmät ja -tulokset tukevat aiempaa tutkimusta aiheen parissa, mutta tuovat esiin myös uusia näkökulmia, kuten tekoälyn ja IoT-teknologioiden (Internet of Things) roolin kybervakoilun kehittymisessä. Näiden uusien teknologioiden myötä kybervakoilun uhkat voivat monimuotoistua ja tehostua, mikä tekee ilmiön torjumisesta entistä haastavampaa.

Tutkielman rajoituksiin kuuluu se, että aineisto perustui pääasiassa julkisiin raportteihin ja aiempiin tutkimuksiin sekä kirjallisuuteen, mikä saattaa rajoittaa tulosten yleistettävyyttä. Suorasta taloudellisesta kybervakoilusta löytyi hyvin niukasti tutkimusta. Tutkielman aikana oli tarpeen yhdistellä eri lähteitä sekä etsiä tietoa ja selvittää, mitkä kybervakoilutapaukset kohdistuivat tarkasti ottaen taloudelliseen tietoon. Lähdemateriaalia kerättäessä tehtiin havainto, miten valtaosa tämänhetkisestä tutkimuksesta ja kirjallisuudesta aiheen parissa kohdistuu kybervakoilulta ja -hyökkäyksiltä puolustautumiseen, eikä niinkään vakoilevan toimijan käyttämien keinojen tutkimiseen. Myös kyberturvallisuusyritysten tekemiä raportteja tulee tarkastella kriittisesti. Niiden luotettavuutta voi kyseenalaistaa kaupallisten intressien ja tieteellisen vertaisarvion puutteen takia. Vaikka raportit ovat ajankohtaisia, nopeat julkaisut voivat sisältää liioiteltuja johtopäätöksiä. Lisäksi tutkielmassa ei voitu käsitellä kaikkia mahdollisia kybervakoilun menetelmiä yhtä syvällisesti.

Jatkotutkimuksessa olisi hyödyllistä keskittyä tarkemmin tiettyihin sektoreihin, kuten finanssi- ja teknologiasektoriin, ja selvittää, miten eri toimijat voivat parhaiten suojautua kybervakoilun uhkilta. Olisi tärkeää, että erityisesti taloudellisesta kybervakoilusta tehtäisiin yksityiskohtaisempaa ja tarkempaa tutkimusta, sillä tämän hetken kirjallisuus ja tutkimus ei tarjoa tarpeeksi laajaa kuvaa taloudellisesti motivoituneen kybervakoilun suorittamisesta. Lisäksi olisi tärkeää tutkia, miten uudet teknologiat, kuten tekoäly ja koneoppiminen vaikuttavat tulevaisuuden kybervakoilun menetelmiin ja niiden torjuntaan.

Tämän tutkielman tulokset korostavat kybervakoilun vakavuutta ja tarvetta jatkuvaan kehitykseen kyberturvallisuudessa. Taloudellisen tiedon suojaaminen on kriittistä, ja sekä yritysten että valtioiden on panostettava entistä enemmän resurssien ja tietoturvamenetelmien kehittämiseen, jotta ne voivat suojautua yhä monimutkaisimmilta kybervakoilun uhkilta.

LÄHTEET

Agrawal, M., Singh, H., Gour, N., & Kumar, M. A. (2014). *Evaluation on Malware Analysis*. *5*.

Akoto, W. (2022). Cyber economic espionage: A framework for future research. Teoksessa *A Research Agenda for International Political Economy* (ss. 159–170). Edward Elgar Publishing. Noudettu osoitteesta https://www.elgaronline.com/edcollchap/book/9781800884120/book-part-9781800884120-19.xml

APT1 | Exposing One of China's Cyber Espionage Units. (2021, joulukuuta 30). Noudettu 8. huhtikuuta 2024, osoitteesta Mandiant website: https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units

Bencsáth, B., Pék, G., Buttyán, L., & Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, *4*(4), 971–1003. https://doi.org/10.3390/fi4040971

Bodström, T., & Hämäläinen, T. (2018). A Novel Method for Detecting APT Attacks by Using OODA Loop and Black Swan Theory. Teoksessa X. Chen, A. Sen, W. W. Li, & M. T. Thai (Toim.), *Computational Data and Social Networks* (ss. 498–509). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-04648-4_42

Civuli, A., Luma-Osmani, S., Rufati, E., & Arifi, G. (2022). *Cyber Espionage Consequences as a Growing Threat*. *7*, 13–20.

Cole, E. (2012). *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. San Diego, UNITED STATES: Elsevier Science & Technology Books. Noudettu osoitteesta http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=1073020

Gilani, S. R. S., Mujtaba, B. G., Zahoor, S., & AlMatrooshi, A. M. (2023). Exploring cybercrime history through a typology of computer mediated offences: Applying Islamic principles to promote good and prevent harm. *Computing and Artificial Intelligence*, *1*(1), 321–321. https://doi.org/10.59400/cai.v1i1.321

Gonçalves, C. P. (2019). Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats. Teoksessa *Cyberspace*. IntechOpen. https://doi.org/10.5772/intechopen.88648

Hou, T., & Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). *Computers & Security*, *98*, 102019. https://doi.org/10.1016/j.cose.2020.102019

Härting, R.-C., Bühler, L., Winter, K., & Gugel, A. (2022). The threat of industrial espionage for SME in the age of digitalization. *Procedia Computer Science*, *207*, 2940–2949. https://doi.org/10.1016/j.procs.2022.09.352

Jansson, S., & Sihvonen, T. (2018). Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & viestintä*, *41*(1). Noudettu osoitteesta https://journal.fi/mediaviestinta/article/download/69950/31049

Jensen, B. (2023). *How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy*. Noudettu osoitteesta https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy

Jones, A. (2008). Industrial espionage in a hi-tech world. *Computer Fraud and Security*, *2008*(1), 7–13. Scopus. https://doi.org/10.1016/S1361-3723(08)70010-1

Knickmeier, S. (2020). Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries. *Security Journal*, *33*(1), 6–26. Scopus. https://doi.org/10.1057/s41284-019-00199-1

Koyun, A., & Janabi, E. A. (2017). *Social Engineering Attacks*. *4*(6).

Neittaanmäki, P., Lehto, M., & Savonen, M. (2021). *Yhteiskunnan digimurros*. Jyväskylän yliopiston IT-tiedekunta. Noudettu osoitteesta https://jyx.jyu.fi/handle/123456789/75328

Qabalin, M. K., Naser, M., & Alkasassbeh, M. (2022). Android Spyware Detection Using Machine Learning: A Novel Dataset. *Sensors*, *22*(15), 5765. https://doi.org/10.3390/s22155765

Ring, T. (2013). A breach too far? *Computer Fraud & Security*, *2013*(6), 5–9. https://doi.org/10.1016/S1361-3723(13)70052-6

Rivera, D. F. (2014). *Industrial Espionage: The Cyberspace War*. Noudettu osoitteesta https://prcrepository.org:443/xmlui/handle/20.500.12475/714

Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). An Analysis of Cyber Espionage Process. Teoksessa Á. Rocha, C. H. Fajardo-Toro, & J. M. R. Rodríguez (Toim.), *Developments and Advances in Defense and Security* (ss. 3–14). Singapore: Springer. https://doi.org/10.1007/978-981-16-4884-7_1

Schafer, J., & Karlins, M. (2021). Hacked by Bits and Pieces: What Can We Learn from an Example of Corporate Espionage? *Journal of Information Security*, *12*(03), 224–231. https://doi.org/10.4236/jis.2021.123012

Snyder, H., & Crescenzi, A. (2009). Intellectual capital and economic espionage: New crimes and new protections. *Journal of Financial Crime*, *16*(3), 245–254. Scopus. https://doi.org/10.1108/13590790910973089

Solberg Søilen, K. (2016). Economic and industrial espionage at the start of the 21st century – Status quaestionis. *Journal of Intelligence Studies in Business*, *6*(3), 51-. https://doi.org/10.37380/jisib.v6i3.196

Verizon: Cyber-Espionage Report. (2020). *Computer Fraud & Security*, *2020*(12), 4. https://doi.org/10.1016/S1361-3723(20)30125-1

Wangen, G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, *6*(2), 183–211. https://doi.org/10.3390/info6020183