Veikka Rönkkö

KYBERUHKATIEDUSTELUN HYÖDYNTÄMINEN KYBERSODANKÄYNNIN UHKIA VASTAAN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Rönkkö, Veikka
Kyberuhkatiedustelun Hyödyntäminen Kybersodankäynnin Uhkia Vastaan
Jyväskylä: Jyväskylän yliopisto, 2023, 34 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Riekkinen, Janne

Valtioiden sisäisten palveluiden ja kriittisten infrastruktuurin digitalisoituessa niihin kohdistuu entistä vahvemmin kybersodankäynnin uhkat. Ukrainan sota on osoittanut, että kyberhyökkäyksillä on todellisen maailman vaikutuksia ja valtioiden on varauduttava niihin. Kybersodankäynnin uhkat ovat hyvin samanlaiset kuin mitä organisaatiot ja yritykset kokevat, mutta niiden aiheuttamat vauriot voivat ylittää valtameriä. Kyberuhkatiedustelussa organisaatiot ja yritykset keräävät ja jakavat kyberuhkadataa, -informaatiota ja -tietoa toistensa kanssa ennaltaehkäistäkseen uhkia ja vähentääkseen niiden aiheuttamaa vahinkoa. Tämän kandidaatintutkielman tarkoituksena oli kirjallisuuskatsauksella aiheeseen tutkia, kuinka unionit ja valtiot hyödyntävät kyberuhkatiedustelun toimintatapoja vahventaakseen omaa kyberresilienssiään. Tiedon jakamista tuetaan useiden eri yhteistyöorganisaatioiden kautta, jotka tukevat tiedon vaihtoa niin yksityisten kuin valtioiden organisaatioidenkin välillä. Kyberuhkien ennaltaehkäisyä toteutetaan direktiivein, lainsäädännöin ja säädösten avulla. Esimerkiksi Euroopan unioni uusi sen NIS-direktiivinsä toiseen versioon vuonna 2023, joka pakottaa sen jäsenvaltiot perustamaan omat tiedonvaihtoyhteistyöorganisaationsa. EU:lla on myös tulevaisuudessa tuloillaan kyberkestävyyssäädös digitaalisia elementtejä sisältävien tuotteiden ja palveluiden tietoturvallisuudesta.

Asiasanat: cyber threat intelligence, kyberuhkatiedustelu, kyberturvallisuus, kybersodankäynti

ABSTRACT

Rönkkö, Veikka
Leveraging Cyber Threat Intelligence Practices in Cyber Warfare Threat Prevention
Jyväskylä: University of Jyväskylä, 2023, 34 pp.
Information systems science, bachelor's thesis
Supervisor(s): Riekkinen, Janne

Digitalization of services and critical infrastructure has exposed them to the threats of cyberwarfare. The war in Ukraine has shown that cyber-attacks have a real-world impact and nation-states must be prepared to face them. In cyber threat intelligence, organizations collect and share cyber threat information with each other to prevent threats and to reduce the damage caused by them. Cyber threats of cyber warfare are very similar to what organizations experience, but the damage they cause can be multicontinental. The aim of this bachelors' thesis was as a literary review to study how unions and nation-states use the practices of cyber threat intelligence to strengthen their own cyber resilience. The information sharing is supported through several different cooperative organizations that support the exchange of information between both private and state organizations. The cyber threat prevention is supported and implemented through acts, directives, and legislation. For example, the European Union renewed their NIS directive in 2023, which forces its member states to establish their own information exchange cooperation organizations. The EU also has cyber resilience act on the way that regulates the cybersecurity of products and services with digital elements.

Keywords: cyber threat intelligence, cybersecurity, cyber warfare

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kyberuhkatiedustelu on uusi ajankohtainen aihe ja monen organisaation harkinnassa vastaiskuna kyberuhille (Abu ym., 2017). Se sisältää eri lähteistä kerättyä dataa, informaatiota ja tietoa, joiden pohjalta organisaatiot voivat tehdä päätöksiä kyberuhkien ennaltaehkäisyyn ja niiden vaikutusten minimoimiseen. Kyberuhkatiedustelun toimintatapojen pohjana on tiedon keräämisen ja ennaltaehkäisevien päätösten lisäksi tiedon jakaminen organisaatioille, jotka voivat olla samojen uhkien uhrina. Kyberuhkatiedustelu on käyttäjiensä toimesta todettu toimivaksi (Johnson ym., 2017, SANS, 2017, Zibak & Simpson, 2019), mutta silti sen toiminnassa on haasteita esimerkiksi eri osapuolten luottamuksen ja standardoimisen puutteen takia.

Valtioiden ja unionien kyberhyökkäyksien uhkat ovat usein samantapaisia, kuin mitä yksityisetkin organisaatiot kokevat. Esimerkiksi virukset, madot ja palvelunestohyökkäykset vaikeuttavat molempien toimintaa. Unionit ja valtiot tukevat direktiivein ja lainsäädännöin omia organisaatioitaan käyttämään kyberuhkatiedustelun toimintatapoja parantaakseen omaa resilienssiään kybersodankäynnin uhkia vastaan. Esimerkiksi Euroopan Unionin NIS-direktiivi ja sen 2023 päivitetty versio asettavat jäsenvaltioille vaatimuksia, kuten omien CERT-ryhmien perustamisen, joiden avulla parannetaan uhkilta varautumista ja niihin reagoimista.

Tämä kandidaatintutkielma toteutettiin kirjallisuuskatsauksena, jonka tavoitteena oli selvittää, miten kyberuhkatiedustelun toimintatapoja hyödynnetään kybersodankäynnin uhkia vastaan. Tutkielman tutkimusongelmaksi kehittyi:

- Miten kyberuhkatiedustelun toimintatapoja hyödynnetään kybersodankäynnin uhkia vastaan?

Palveluiden ja valtioiden kriittisen infrastruktuurin digitalisoituessa kybersodankäynnin uhkien vaikutus kasvaa. Ukrainan sodan ja siellä toteutettujen kyberhyökkäysten ollessa uutisissa, on hyökkäysten ennaltaehkäisyn tutkiminen aiheellista. Kyberuhkatiedustelu tuoreena kyberturvallisuuden aiheena voisi

olla yksi tapa parantaa ja tehostaa valtioiden ja sen sisäisten organisaatioiden puolustusta kyberhyökkäyksiä vastaan. Tutkimuksen löydökset auttavat ymmärtämään valtioiden ja unioneiden uhkamaisemaa, sekä selvittämään, kuinka varsinkin länsimaiset valtiot niiltä suojautuvat.

Kirjallisuuskatsaukseen aineistoa kerättiin suurimmaksi osaksi Google Scholar -hakukoneella sekä Jyväskylän yliopiston ja Maanpuolustuskorkeakoulun elektronisten kirjastojen avulla. Hakusanoina kyberuhkatiedusteluun olivat: Cyber Threat Intelligence, Threat Intelligence sekä Cyber Threat Intelligence sharing. Kybersodankäynnin hakusanoina toimivat: Cyber Warfare, Cyber threats sekä history of Cyber Warfare. Tutkielman lähteet ovat suurimmaksi osaksi artikkeleita alan lehdistä ja seminaareista, jotka ovat saaneet vähintään Julkaisufoorumin arvosanan yksi. Osa lähteistä eivät kuitenkaan ole julkaistu missään tieteellisissä julkaisualustoissa, esimerkiksi Yhdysvaltain puolustusministeriön sekä Suomen Liikenne- ja viestintäviraston raportit. Ne kuitenkin otettiin mukaan tutkielmaan niiden sisältämän relevantin valtiokohtaisen tiedon takia.

Tutkielma on jaettu kolmeen sisältölukuun. Ensimmäisessä sisältöluvussa määritellään kyberuhkatiedustelu ja kerrotaan kuinka organisaatiot sitä käyttävät. Luvussa kerrotaan myös sen tuomista hyödyistä sekä sen haasteista. Toisessa luvussa käsitellään kybersodankäyntiä, sen käyttöä lähimenneisyydessä sekä sen aiheuttamia ongelmia valtioille ja niiden organisaatioille. Viimeisessä luvussa kerrotaan kuinka kyberuhkatiedustelun tiedon jakamisen ja ennaltaehkäisyn toimintatapoja hyödynnetään valtioiden tukemana kybersodankäynnin uhkia vastaan. Tutkielman lähestymistapa on hyvin länsimainen, eikä viimeinen sisältöluku käsittele kuin Euroopan Unionin, Yhdysvaltojen sekä Suomen kyberuhkatiedustelun toimintatapojen tukemista ja käyttöä. Sisältölukujen jälkeen tutkielmassa on yhteenveto, jossa käydään läpi tutkimuksen sisältöä ja tuloksia. Yhteenvedossa ehdotetaan myös aiheita jatkotutkimuksiin.

2 KYBERUHKATIEDUSTELU

Tässä luvussa käsitellään Cyber Threat Inteligenceä, eli suomennettuna kyberuhkatiedustelua. Luvun alussa kerrotaan, minkä takia kyberuhkatiedustelua on alettu käyttämään kaupallisissa yrityksissä kyberrikollisuuden uhkia vastaan. Samassa alaluvussa kerrotaan, mitä kyberuhkatiedustelun määritelmää tutkielmassa käytetään. Käsitteen määrittelyn lisäksi tutkitaan, miten kyberuhkatiedustelu jakautuu alakäsitteisiinsä. Toisessa alaluvussa käsitellään, kuinka organisaatiot käyttävät kyberuhkatiedustelua. Miten sen tietoa saadaan ja kuinka sitä hyödynnetään ennaltaehkäisyssä sekä strategisessa päätöksenteossa? Kolmannessa alaluvussa kerrotaan, mitä kyberuhkatiedustelutiedon jakaminen on ja miten se tapahtuu organisaatioiden välillä. Samassa luvussa avataan myös hieman kyberuhkatiedustelutiedon jakamisen alustoja ja standardeja. Luvun lopuksi käydään läpi organisaatioiden saamat hyödyt kyberuhkatiedustelusta ja mitä haasteita aiheen kehittymisessä on havaittu.

2.1 Kyberrikollisuus ja kyberuhkatiedustelu sitä vastaan

Kyberrikollisuus on digitalisoitumisen tuoma tuore ilmiö. Se erottuu tavanomaisesta rikollisuudesta teknisyydellään ja on sen takia ollut puheenaiheena maailmanlaajuisesti. Mitä haasteita ja uhkia kyberrikollisuus luo, sekä kuinka niiltä vältytään, ovat olleet aiheen kirjallisuudessa usein esillä. (Sarwar, 2016).

Kyberrikolliset ovat osaavampia, organisoidumpia ja paremmin rahoitettuja kuin ennen (Abu ym., 2018). Perinteinen staattinen puolustus ei sovi käytettäväksi vastassa ollessa uuden sukupolven dynaamiset kyberuhkat, joiden tiedetään olevan taitavasti välttteleviä, sitkeitä sekä monimutkaisia. Organisaatioiden täytyy kerätä ja jakaa reaaliaikaista informaatiota välttyäkseen niiltä tai vähintään minimoidakseen niiden tuottamat vauriot (Tounsi & Rais, 2018).

2.1.1 Kyberuhkatiedustelun määritelmä

Kyberuhkatiedustelu on uusi ajankohtainen aihe ja monen organisaation harkinnassa vastaiskuna kyberrikollisuuden uhille (Abu ym., 2017). Sitä käytetään terminä vaihtuvasti Threat Intelligencen kanssa. Kyberuhkatiedustelu on konseptina vaikea määritellä useiden eri lähteiden, kuten tutkijoiden ja alan ammattilaisten, käyttäessä termiä eri tavalla (Mavroeidis & Bromander, 2017; Tounsi & Rais, 2018). Mavroedisin ja Bromanderin (2017) mukaan kyberuhkatiedustelun ontologiassa on muitakin ongelmia, kuin määrittely. Jaottelun standardoitumisen puuttuminen on esimerkiksi heidän mielestään helposti korjattava ongelma kyberuhkatiedustelun kehittämisessä. Heidän löydöksistään kerrotaan myöhemmin tutkielmassa lisää.

Tounsin ja Raisin (2018) mukaan kyberuhkatiedustelutieto on mitä vain todisteisiin pohjautuvaa tietoa uhkista, jonka avulla voidaan informoida päätöksentekoa kyberhyökkäysten ennaltaehkäisyssä tai lyhentää vaarantumisen ja havaitsemisen väliä. Heidän mukaansa se voi myös olla tietoa, joka päätöksenteon auttamisen sijaan, auttaa ymmärtämään uhkamaisemaa paremmin. Tätä määritelmää kyberuhkatiedustelutiedosta käytetään tutkielmassa, sillä sitä käytetään kirjallisuudessa useiten. Kyberuhkatiedustelu on prosessi, jolla kyberuhkatiedustelutietoa kerätään ja jaetaan sekä sen pohjalta tehtävät ennaltaehkäisevät toimenpiteet.

Kyberuhkatiedustelutiedossa sisältyvän melun, kyberuhkadatan, -informaation ja -tiedustelutiedonvälillä on valtava ero. Eron ymmärtäminen on välttämätöntä parhaan hyödyn saamiseksi kyberuhkatiedustelusta (Abu ym., 2018). Datamelu voisi esimerkiksi olla kaikki organisaation palvelimeen liittyvä data. Uhkadata melusta eroteltu potentiaalisesti haitallinen data. Informaatio käsiteltyä uhkadataa, josta selviää, miten uhka toteutetaan. Ja tiedustelutieto turvallisuushenkilön ymmärrys hyökkäyksestä informaation pohjalta. Yhtenäisen tilannekuvan saavuttamiseksi tarvitaan erojen ymmärtämisen lisäksi pitkän aikavälin arviointia (Voutilainen & Kari, 2020).

2.1.2 Kyberuhkatiedustelutiedon jaottelu

Chismon ja Ruks (2015) jakavat kyberuhkatiedustelun sotilaskonteksteissa usein käytettyihin neljään alakategoriatasoon: strategiseen, taktiseen, operationaaliseen sekä tekniseen kyberuhkatiedusteluun. Eri tasoilla on omat ominaisuutensa, tarkoituksensa, sekä käyttäjäkuntansa organisaation sisällä (taulukko 1). Heidän jaotteluaan käytetään aiheen kirjallisuudessa usein, vaikka joidenkin tutkijoiden mielestä standardoiminen puuttuisikin (Mavroedis & Bromander, 2017).

TAULUKKO 1 Kyberuhkatiedustelun alajaottelu

Taso	Informaatioesimerkki	Yleisin käyttäjä
Strateginen	Kyberhyökkäyksen taloudellinen vaikutus	Korkeammat päätöksentekijät
Operaationaalinen	Organisaatiota lähestyvä uhka	Ylemmät turvallisuushenkilöt
Taktinen	Kuinka uhkatekijä toteuttaa hyökkäyksen	Uhkiin vastaavat henkilöt
Tekninen	IP-osoitelista uhkista	Uhkiin vastaavat henkilöt

Strateginen on kyberuhkatiedustelun korkein taso. Sen tiedon käyttäjiä ovat organisaatioiden korkeimmat päättäjät, joiden vastuulla on pitkän aikavälin päätökset organisaation päämääristä ja tavoitteista. Se sisältää informaatiota esimerkiksi hyökkäystrendeistä tai kyberhyökkäyksen taloudellisista vaikutuksista organisaatioon (Chismon & Ruks, 2015).

Operationaalisen tason kyberuhkatiedustelutieto on informaatiota organisaatiota jo lähestyvistä erilaisista uhista. Sitä käyttää hyödykseen organisaation ylemmän tason turvallisuushenkilöt. Chismonin ja Ruksin (2015) mukaan tällainen informaatio on hyvin harvassa, sillä yksityisillä organisaatioilla ei ole laillista oikeutta uhkatekijöiden tietoinfrastruktuuriin, kuten esimerkiksi kommunikaatiokanaviin. Vain jos hyökkääjät kommunikoivat avoimesti, voidaan hyvää operationaalista kyberuhkatiedustelutietoa kerätä. Tästä esimerkkinä haktivistiryhmät eli kyberuhkia toteuttavat aktivistiryhmät.

Taktinen kyberuhkatiedustelu sisältää informaatiota siitä, kuinka hyökkäyksiä toteutetaan. Siitä hyötyvät organisaation uhkiin vastaavat henkilöt. Taktisen tason informaatio saavutetaan usein lukemalla alan kirjallisuutta, kommunikoimalla muiden organisaatioiden saman tason työntekijöiden kanssa tai ostamalla sitä tarjoavilta tahoilta (Chismon & Ruks, 2015).

Teknisellä tasolla on dataa, joka on saatu teknisin tavoin. Esimerkki olisi lista IP-osoitteista, joiden uskotaan olevan vaarallisia. Tämän tason data on yleensä lyhytikäistä, sillä uhkatekijät voivat nopeasti esimerkiksi vaihtaa IP-osoitteitaan (Chismon & Ruks, 2015). Teknisen tason datan määrä on yleensä myös ylitsepääsemättömän valtava, joten monet turvallisuusvastaavat eivät pysty sitä tehokkaasti hyödyntämään (Tounsi & Rais, 2018). Joissain jaotteluissa neljäs tekninen taso jätetään jaottelun ulkopuolelle (Abu ym., 2017, Roberts & Brown, 2017).

2.2 Kyberuhkatiedustelun toimintatavat

Tässä luvussa käsitellään kyberuhkatiedustelun toimintatapoja. Aikaisemmin tutkielmassa määriteltiin ensimmäiseksi toimintatavaksi kyberuhkatiedustelutiedon keräämien, josta kerrotaan informaatiolähteet alaluvussa. Toiseksi tiedon

jakaminen sekä kolmanneksi tiedon pohjalta tehtävät ennaltaehkäisevät toimenpiteet ja päätökset.

2.2.1 Informaatiolähteet

Kyberuhkatiedustelua harjoittavat organisaatiot saavat informaationsa useista eri lähteistä. Yleisimmät ovat omasta sisäisestä tunnistusprosessista, luotettavilta vertaisiltaan, maksullisilta tilauspalveluilta, hallituksen virastoilta sekä avoimen lähteen yhteisöistä, blogeista ja internetfoorumeilta (Abu ym., 2018). Yleensä organisaatiolla ei ole käytössä vain yksi lähde (Sauerwein, Sillaber & Breu, 2018). Kyberuhkatiedustelulähteet voidaan jakaa kolmeen kategoriaan: sisäiseen, ulkoiseen ja yhteisölliseen.

Sisäisiä lähteitä voidaan käyttää organisaation päätapana kerätä dataa ja informaatiota, sillä se voi tarjota paremman näkymän organisaation omasta uhkaympäristöstä ja sen toiminnasta. Ymmärryksen kautta informaatiota ja työkaluja voidaan käyttää tehokkaammin hyödyksi. Muiden lähteiden hyödyntäminen sisäisen kanssa luo kuitenkin kattavamman kuvan yleisestä uhkamaisemasta. Sisäistä kyberuhkatiedusteludataa voidaan saada esimerkiksi sisäisestä verkosta ja organisaation käyttämästä Security Information and Event Management (SIEM) -järjestelmästä. Informaation muodot voivat olla sähköpostilokeja, hälytyslokeja, tapahtumaraportteja tai esimerkiksi palomuurilokeja (Abu ym., 2018).

Ulkoiset lähteet sisältävät suuren määrän erilaisia informaatioita. Ne vaativat organisaation sisäisen varmistuksen joltakulta, jolla on tietoa tämänhetkisestä uhkamaisemasta. Avoimien lähteiden informaatiota voi olla esimerkiksi turvallisuustutkijat ja julkisesti saatavilla olevat maine- ja estolistat. Niiden ongelmana on kuitenkin informaation laadun varmistus. Maksullisia ulkoisia lähteitä ovat yksityiset ja kaupalliset vaihtoehdot. Niiden informaatio voi olla uhkatiedustelusyötteitä sekä jäsenneltyjä ja jäsentämättömiä dataraportteja (Abu ym., 2018).

Yhteisöllisiä lähteitä yhdistää kiinnostus kyberuhkatiedustelua kohtaan. Akateemiset yhteisöt, kuten Information Sharing and Analysis Centers (ISACs) ja Research and Education Networking (REN-ISAC) tarjoavat aiheen tiedotusta, korkeampaa koulutusta ja esimerkiksi rahoituspalveluita (Abu ym., 2018).

2.2.2 Kyberuhkatiedustelutiedon jakaminen

Datan määrän kasvu digitalisoitumisen myötä on rakentanut kuilun datan määrän ja tietokoneiden laskentanopeuden välille. (Katal, Wazid, & Goudar, 2013). Se on vaikuttanut myös alalla toimivien organisaatioiden toimintaan. Yksittäiset toimijat eivät pysty käsittelemään kaikkea kyberuhkatiedusteluunkaan liittyvää dataa. Siksi organisaatiot ovat alkaneet jakamaan tiedustelutietoa toistensa kanssa pitääkseen itsensä yhden askeleen edellä uhkia vastaan (Sillaber ym., 2016, Sauerwein ym., 2017, Zibak & Simpson, 2019).

Perinteisten vastatoimien lisäksi yritykset vaihtavat informaatiota ja tietoa luotettujen organisaatioiden välillä auttaakseen haavoittuvuuksien ja uhkien

hallintaa sekä lieventääkseen tietoturvatapauksien vaikutuksia (Saurewein ym., 2017). Moni aiheen aiempi kirjallisuus on tutkinut tiedon jakamisen mahdollisia etuja. Tällaiset edut vaihtelevat uhkatilanteiden tuesta, kustannussäästöihin ja pelotesuojaan. Etujen tutkimisesta huolimatta, monilla organisaatiolla on vaikeuksia lähteä mukaan ja ylläpitää tiedusteluinformaation jakamista. Keskusteluissa aiheesta, syiksi nousevat usein konseptit kuten standardoiminen, kilpailu ja luottamus. Konseptien abstraktius ja kaiken kattavuus luovat esteen organisaatioiden miettiessä tiedustelutietojen vaihtamisen aloittamista (Zibak & Simpson, 2019).

Vaihdon tueksi aloitetut useat hallituksien tukemat hankkeet ovat saaneet vetoa viime vuosina. Esimerkiksi Hollannissa hallitus on ottanut käyttöön kansallisen havaitsemis-, vastaus ja asiantuntijaverkoston ja NATO on käynnistänyt Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) -hankkeen (Sillaber ym., 2016).

Kyberuhkatiedustelutiedon jakamiseen on kehitetty alustoja, ja niissä käytettäviä standardeja, joiden kautta organisaatiot voivat suorittaa tiedon vaihtoa. Perinteisesti kyberuhkatiedustelutietoa on vaihdettu ad-hoc ratkaisujen kautta, kuten esimerkiksi sähköposteilla tai puhelimitse. Viimeisen kymmenen vuoden aikana organisaatiot ovat siirtyneet kuitenkin enemmän käyttämään tiedon vaihtoon suunniteltuja alustoja (Sillaber ym., 2016). Sauerwein (ym., 2017) tutki tutkimuksessaan 22 eri kybertuhkatiedustelutiedon jakoalustaa, joiden vaatimukset olivat:

1. Helpottaa tiedon jakamista.
2. Antaa mahdollisuuden automaatiolle.
3. Helpottaa datan luomista, jalostusta ja tarkistamista.

Tutkimuksesta selvisi, että yleistä määritelmää jakoalustalle ei vielä ole. Useimmat alustat eivät hyödynnä täysin niiden kuvaavia ominaisuuksia, vaan keskittyvät ensisijaisesti jakamaan uhkatilanteiden indikaattoreita. Stojkovskin (ym., 2021) tuoreempi tutkimus kertoo uhkatietojakoalustojen käyttäjäkokemuksesta. Se sai selville, että niiden jyrkkä oppimiskäyrä sekä havaittu tuen tai yhteisön puute aloitteleville käyttäjille, tuo mahdollisia ongelmia sekä virheisiin että vajaakäyttöön.

Jakamisen tueksi on kehitetty useita tietotyyppistandardeja tiedonvaihdon automatisoinnin mahdollistamiseksi. Näitä ovat esimerkiksi:

- Open Incident of Compromise (OpenIOC)
- Cyber Observable eXpression (CybOX)
- Structured Threat Information eXpression (STIX)
- Incident Object Description Exchange Format (IODEF)
- Trusted Automated eXchange of Indicator Information (TAXII) (Abu ym., 2018, Saurewein ym., 2017).

Näistä STIX on tällä hetkellä eniten käytetty de-facto standardi strukturoidun uhkatietojen jakamiseen. Se on joustava ja laajennettava esityskieli, jota organisaatiot käyttävät kommunikoidessaan yleisiä uhkatietoja (Mavroeidis & Bromander, 2017).

2.2.3 Strateginen päätöksenteko

Korkein eli strateginen taso määrittelee laajan skaalan toiminnan. Strateginen päätöksenteon taso keskittyy organisaation mission ja suunnan määrittämiseen, tavoitteiden asettamiseen ja suunnitelmien laatimiseen (Mattern ym., 2014). Strateginen kyberuhkatiedustelu tarjoaa sille yleiskatsauksen uhkamaisemasta sekä ennakkovaroituksen kyberuhista (Voutilainen & Kari, 2020).

Strateginen päätöksenteko kyberuhkatiedustelun pohjalta korostaa ennaltaehkäisyä ja ennakointia. Se voi merkittävästi vähentää organisaation riskiä sen missiolle ja omaisuudelle sekä tukea sen liiketoimintaa (Borum ym., 2014). Jotta kyberuhkatiedustelusta johdettu strateginen päätöksenteko voisi ohjata organisaation kyberturvallisuutta, johtohenkilökunnan on oltava mukana tunnistamassa sen kriittisiä tietovaatimuksia. Kriittisiksi tietovaatimuksiksi määritellään usein tiedot, joita johtohenkilökunta tarvitsee strategisten päätösten tekemiseen. Tunnistuksen ja määritelmien ollessa kunnossa, kybertiedustelutoiminto on valmis arvioimaan yrityksen uhkia, haavoittuvuuksia ja mahdollisia vaikutuksia. Sekä neuvomaan johtajia riskejä ja resursseja koskevissa strategisissa päätöksissä (Borum ym., 2014).

Kyberuhkatiedustelun pohjalta johdettu strateginen päätöksenteko antaa myös lisäarvoa laajemmalle kyberturvallisuudentoiminnalle organisaatiossa, esimerkiksi tehostamalla liiketoimintariskien selittämistä ja kvantifiointia ylimmälle johdolle sekä muille sidosryhmille. Osoittamalla asianmukaista huolellisuutta tilintarkastajille sekä sääntelyviranomaisille, vähentää se myös yritysten altistumista oikeudellisille seuraamuksille. Sen avulla yritys voi käyttää omia turvallisuusresurssejaan tehokkaammin tietäessään, missä heidän riskikohtansa sijaitsevat (Borum ym., 2014).

2.3 Hyödyt organisaatioille

Kyberuhkatiedustelun ja sen tiedon jakamisen tavoitteena on hankkia monipuolista informaatiota, joka voi auttaa organisaation päätöksentekoa. Organisaation turvallisuustiimin taidot ja tiedonlähteet määrittelevät heidän kykynsä tuottaa tarkkaa ja toimivaa uhkatiedustelutietoa. Siksi kyberpuolustus on tehokkainta, kun organisaatiot tekevät yhteistyötä (Johnson ym., 2016, Tounsi & Rais, 2017). Uhkatietoja vaihtamalla organisaatiot voivat hyödyntää kollektiivista tietämystä saadakseen paremman käsityksen organisaation mahdollisesti kohtaamista uhista. Jakamalla, jonkun organisaation uhkan havaitsemisesta voi tulla toisen organisaation esto samana uhkaan (Mavroeidis & Bromander, 2017).

Johnsonin (ym., 2016) mukaan tiedon jaon hyötyjä on monia. Jakaminen antaa organisaatioille mahdollisuuden hyödyntää jakamiskumppaneidensa kollektiivista tietämystä, kokemusta ja analyyttisiä valmiuksia. Tämä parantaa useamman kuin yhden organisaatioiden puolustuskykyä. Organisaatiot ymmärtävät paremmin uhkamaisemaa ja voivat käyttää uhkatietoja kyberturvallisuus- ja riskienhallintakäytäntöihinsä. Jaetun tiedon avulla organisaatiot voivat tunnistaa vaikutuksen kohteena olevat alustat tai järjestelmät, toteuttaa suojatoimenpiteitä, parantaa havaitsemiskykyä ja reagoida tehokkaammin sekä toipua tapauksista uhkamaisemassa havaittujen muutosten perusteella. Jakamalla organisaatiot pääsevät paremmin perille dynaamisista ja nopeasti muuttuvista riskitekijöistä, tämä lisää puolustustehokkuutta ja vähentää onnistuneen hyökkäyksen todennäköisyyttä.

SANS instituutin tekemän kyselyn (Shackleford & Lee, 2017), mukaan: 78 % vastanneista kyberuhkatiedustelun käyttäjistä koki sen hyödyntäneen heidän turvallisuuttaan. Suurimmat turvallisuuden osa-alueet, joihin koettiin kyberuhkatiedustelusta olevan hyötyä, olivat: näkyvyyden parantaminen organisaatioon vaikuttaviin uhkiin ja hyökkäysmenetelmiin, turvatoimien parantuminen sekä tuntemattomien uhkien tunnistaminen.

Zibakin ja Simpsonin vuoden 2019 tutkimus kertoo, että tiedon jakamistakin hyödyntävät organisaatiot pitivät sen vaikutuksia positiivisina. Tutkimukseen osallistujat yhtyivät vahvimmin ajatuksiin, että uhkatiedon jakaminen tukee tietomurtojen havaitsemista ja palautusta, kehittää ja ylläpitää vahvoja ammatillisia suhteita sekä parantaa organisaation kestävyyttä.

2.4 Kyberuhkatiedustelun ja sen tiedon jakamisen haasteet

Moni aiheen aiempi kirjallisuus käsittelee kyberuhkatiedustelun haasteita. Kollektiivisen jakamisen ja jaetusta uhkatiedosta oppimisen edut ovat kiistattomat. Erilaiset esteet kuitenkin rajoittavat yhteistyömahdollisuuksia (Tounsi & Rais, 2017).

Mavroeidisin ja Bromanderin (2017) artikkeli käsittelee kyberuhkatiedustelun ontologian yhtenäisyyden puutetta. Heidän mukaansa epämääräisesti määritelty terminologia johtaa hämmennykseen asiantuntijoiden keskuudessa ja lisätyöhön aiheen laajentamisessa tai yhtenäistämisessä. Standardoinnin puute olennaisissa tiedoissa johtaa kirjallisuuteen, jossa ei ole kunnollista vakiomallia aiheelle.

Zibakin ja Simpsonin vuoden 2019 tutkimus tunnisti kyberuhkatiedustelutiedon jakamisen ongelmiksi kaksi tekijää.

1. Organisaatiot ovat toisinaan varovaisia tai haluttomia liittymään tiedonjakamispyrkimyksiin.
2. Jakamisen ja sen työkalujen arviointimenetelmien puute estää niiden ongelmien tunnistamisen ja korjaamisen.

Organisaatioiden haluttomuus johtuu useista syistä, mukaan lukien kilpailusta, vastuusta ja odotetusta huonosta investoinnin takaisintuotosta. Osallistumista on vaikea kannustaa ilman empiiristä näyttöä kyberuhkatiedustelutiedon jakamisen arvosta osallistumista.

Abun (ym., 2018) artikkeli käsitteli kyberuhkatiedusteludataa sekä sen laadullisia ongelmia ja tunnisti useita haasteita. 1. Datan musertava määrä: kyberhyökkäyksiltä suojautumiseksi on erittäin tärkeää, että organisaatiolla on pääsy käyttökelpoisiin uhkien tiedustelutietoihin. Monet heistä kamppailevat kuitenkin edelleen valtavan uhkadatan määrän ja henkilöstön asiantuntemuksen puutteen kanssa. 2. Datan laadulliset haasteet: On yleinen käytäntö, että turvasyötteiden tarjoaja markkinoi uhkasyötteitä kyberuhkatiedustelutietona. 2015 vuoden Ponemon-instituutin tutkimus selvitti, että 70 % uhkasyötteiden datasta on kuitenkin ylimalkaista ja vaikeasti käytettävää. 3. Yksityisyys ja lailliset haasteet: kyberuhkatiedustelua käsiteltäessä on otettava huomioon tietosuoja- ja oikeudelliset kysymykset. Miten tietoja voidaan jakaa ja mitkä lait säätelevät tietojen jakamista? Monet organisaatiot ovat esimerkiksi varovaisia jakamasta tietoja, jotka voivat vaikuttaa negatiivisesti heidän brändiinsä (KPMG, 2013).

Tounsi ja Rais (2018) listasivat artikkelissaan enemmän syitä, joiden takia organisaatiot eivät jaa kyberuhkatiedustelutietoa. Negatiivisen julkisuuden pelko, lailliset säädökset ja yksityisyyshaasteet, laadulliset ongelmat sekä epäluotettavat osallistujat. Usko, että uhkatilanne ei ole tarpeeksi tärkeä jaettavaksi, budjettiongelmat, luonnollinen vaisto olla jakamatta, kyberhyökkäysten dynaaminen ja nopeasti muuttuva luonne, organisaation tietämättömyys uhkatilanteesta sekä usko, että tilanteelle ei tulla tekemään mitään.

Kyberuhkatiedustelulla on useita ongelmia sen perustassa, kuten käsitteiden määrittelyissä. Perustan ongelmat heijastuvat sen sovellettavuudessa. Organisaatioiden haluttomuus käyttää kyberuhkatiedustelua ja jakaa tuottamaansa tietoa vähentää niiden kykyä ennaltaehkäistä kyberuhkia sekä reagoida niiden vaikutuksiin. Osa näistä johtuu aiheen nuoruudesta ja sen tutkimuksen eteneminen vähentää ongelmien vakavuutta.

3 KYBERSODANKÄYNTI JA SEN UHKAT

Tässä luvussa käsitellään kybersodankäyntiä. Ensimmäisessä alaluvussa määritellään termi kybersodankäynti aiempaan aiheen kirjallisuuteen pohjaten ja tehdään oma tiivistelmä käsitteestä. Samassa luvussa käsitellään kyberhyökkäysten tekniikoita ja prosessia hyökkäyksen mahdollisesta etenemisestä. Toisessa alaluvussa kerrotaan mitä uhkia kybersodankäynti ja kyberhyökkäykset aiheuttavat valtioille ja sen kansalaisille. Lopuksi käsitellään kybersodankäynnin historiaa kertomalla esimerkkejä viimeisen viidentoista vuoden historian hyökkäyksistä Georgiaan, Iraniin, Ukrainaan ja Yhdysvaltoihin.

3.1 Kybersodankäynnin määritelmä

Tietotekniikat, joita esiteltiin 2000-luvun kansainvälisen kasvun ensisijaisena vektorina, näyttävät myös olevan pahimmillaan tietojärjestelmistä riippuvaisten yhteiskuntien akilleenkantapää. Niiden kautta ja kanssa vastustajamme sekä vihollisemme voivat hyökätä kimppuumme. Yleisesti ottaen huoli siitä, että kyberhyökkäykset voivat häiritä yrityksen tai kansakunnan taloutta tai jopa vaikuttaa maailmanlaajuiseen vakauteen, on tullut tietotekniikasta riippuvaisten maiden painajainen.

Kybersodankäyntiin kuuluu valtioiden rajojen puolelle organisoituneita yksiköitä, jotka käyttävät tietokoneita hyökätäkseen sähköisesti muita tietokoneita tai verkkoja vastaan. Hakkerit ja muut ohjelmointiin koulutetut henkilöt ovat näiden kyberhyökkäysten ensisijaisia toteuttajia. Nämä henkilöt toimivat usein valtioiden toimijoiden suojeluksessa ja mahdollisesti tuella (Billo & Chang, 2004).

Kyberhyökkäyksen tarkoitus voi olla esimerkiksi tietovakoilu, sabotaasi tai fyysinen vahinko. Tietovakoilulla tarkoitetaan arkaluonteisten, omistusoikeudellisten tai turvaluokiteltujen tietojen hankkimista. Fyysinen vahinko on seurausta kyberavaruushyökkäyksestä, jossa tarkoitus on vaikuttaa esimerkiksi

Supervisory Control and Data Acquisition eli SCADA-järjestelmiin niin, että teollisuus- tai infrastruktuuriprosessien ohjaus häiriintyy (Kärkkäinen, 2013).

Lehto (2020) käsitteli artikkelissaan kybersodankäynnin teoreettista taustaa:

> Kybersodankäynnissä ei ole rintamalinjoja vaan sodankäynti tapahtuu kaikkialla kybertilassa. Kyberhyökkäykset ja hyökkäysvektoreiden muutokset ovat hyvin nopeita. Sodankäynnissä on siirrytty päivä- ja tuntiluokasta minuutteihin ja sekunteihin. Kybersodankäynti korostaa oman tilannetietoisuuden merkitystä ja kykyä estää vastustajaa luomasta omaa tilannetietoisuuttaan. Kybersodankäynnissä korostuu periaate, jossa ihannetapauksessa vihollinen ei koskaan havaitse omaa toimintaamme ja se yllätetään täysin (Lehto, 2020, s. 67).

Tiivistettynä kybersodankäynti on organisoituja yksilöitä toteuttamassa kyberhyökkäyksiä toisen valtion suojeluksessa tai tuella. Kyberhyökkäykset ovat sähköisiä hyökkäyksiä organisaatioita tai valtioita vastaan, pyrkien aiheuttamaan häirintää kohteessa ja/tai saamaan omaa etua esimerkiksi informaation muodossa.

3.1.1 Kyberhyökkäystekniikat

Hyvin tunnetut kyberhyökkäystekniikat voidaan jakaa karkeasti neljään hyökkäyksen prosessin kategoriaan. Tiedustelu, hyökkäys, hyväksikäyttö ja käyttäjän manipulointi. Tiedustelussa hyökkääjä pyrkii saamaan kohteesta informaatiota, esimerkiksi sen heikkouksista tai järjestelmien liikenteestä (Andress & Winterfeld, 2014, s. 25). Tiedustelua voidaan suorittaa skannereilla tai ”sniffereillä” eli ohjelmilla, jotka tallentavat koneiden liikennettä.

Hyökkäyksessä löydettyjen heikkouksien kautta saastutetaan kohteen järjestelmät. Kooditasolla on esimerkiksi matoja tai viruksia, jotka voivat käyttää hyökkäysvektoreita asentaakseen rootkittejä tai troijalaisia hevosia, jotka toimivat takaovena järjestelmään ja jota voidaan käyttää hyökkäyksen levittämiseen (Liu & Cheng, 2009). Yksi matojen ja virusten käyttötarkoitus on botnet-armeijoiden rakentaminen. Jos joku rakentaa bottien armeijan, hän voi aiheuttaa hajautetun palveluneston, eli Distributed Denial of Service (DDoS), usuttaen kaikki botit muodostamaan yhteyden samana sivustoon tai järjestelmään samanaikaisesti (Andress & Winterfeld, 2014 s. 26).

Hyväksikäytössä hyökkääjät käyttävät hyödykseen hyökkäyksen kautta saatua hallintaa. On yleensä kolme tekijää, joita hyökkääjä voi järjestelmässä vaarantaa. Luottamuksellisuutta, eheyttä ja saatavuutta (Andress & Winterfeld, 2014 s. 27). Kun kohde on luottamuksellisuus, hyökkääjät vain varastavat salaisuuksia. Eheyshyökkäyksillä tarkoitetaan, kun hyökkääjät muuttavat järjestelmän tietoja. Käytettävyyshyökkäykset voidaan toteuttaa poistamalla järjestelmä tai ylittämällä sen kaistanleveys palvelunestolla.

Jos hyökkäysvektorina tekniset ratkaisut eivät toimi toinen vaihtoehto on käyttäjän manipulointi. Useiden järjestelmien suurin heikkous on sen käyttäjät (Andress & Winterfeld, 2014). Käyttäjän manipulointi voidaan ajatella toimenpiteenä, joka vaikuttaa jonkun käyttäytymiseen manipuloimalla hänen tuntei-

taan tai hankkimalla ja pettämällä heidän luottamustaan päästäkseen käsiksi järjestelmään (Liu & Cheng, 2009). Tämä voidaan tehdä henkilökohtaisesti, mutta usein se tehdään puhelimen tai muun etäviestimen yli, kuten sähköpostilla. Yleisin hyökkäys onkin nykyään sähköposti (Andress & Winterfeld, 2014 s. 27). Tällaista manipulointihyökkäystä kutsutaan tietojenkalasteluksi tai englanniksi phishing.

3.2 Kybersodankäynnin uhkat

Kyberhyökkäyksillä konfliktitilanteissa voi olla mahdollisesti erittäin vakavia seurauksia, erityisesti jos niiden vaikutus ei rajoitu kohteena olevaan tietojärjestelmään (Droege, 2013). Kybersodankäynnin historiasta löytyykin esimerkkejä, joissa kohdejärjestelmään käsiksi päästäkseen hyökkäykset ovat sivussa vaikuttaneet satoihin tuhansiin muihinkin tietojärjestelmiin. Kyberhyökkäykset voivat vaikuttaa mannerten välisellä skaalalla ja huolenaiheena on, että tarpeeksi kehittynyt haittaohjelma voisi kaataa koko maailmanlaajuisen verkon (Farwell & Rohonzinski, 2012).

Farwellin ja Rogonzinskin (2012) mukaan kyberaseet ovat eri luokkaa kuin ydinaseet, joilla on vain vähän käytännön hyötyä paitsi olla pelotteena. Kyberhyökkäysten tarkoituksena onkin yleensä vaikuttaa kybermaailmasta ”todelliseen maailmaan”. Esimerkiksi hyökkäämällä tukeviin tietojärjestelmiin voidaan manipuloida lennonjohtojärjestelmiä, öljyputkien virtausjärjestelmiä ja jopa ydinvoimaloita (Droege, 2013).

Valtiotasolla kyberhyökkäykset voivat aiheuttaa sotilaallisten järjestelmien kaatumisia, kommunikaatiovaikeuksia, salattujen tietojen joutumisia vääriin käsiin sekä kriittisen infrastruktuurin vaarantumisen. Kriittinen infrastruktuuri, kuten sähköverkot, liikenneverkot ja vesihuoltojärjestelmät ovat elintärkeitä kansantalouden ja vaurauden kannalta. Reaaliaikaisen seurannan ja valvonnan saavuttamiseksi, järjestelmät yhdistävät tietokoneet niiden fyysiseen prosessiin luoden kyberfyysisiä järjestelmiä. Niiden kyberfyysisyys altistaa ne kyberhyökkäyksille (Lewis, 2006). Kyberhyökkäys toisiinsa riippuvaisten järjestelmiä kohtaan voi aiheuttaa perättäisiä vaikutuksia, jotka voivat pahimmassa tapauksessa romuttaa koko kriittisen infrastruktuurin (Palleti, 2021).

3.3 Kybersodankäynnin historia

1980-luvun lopusta lähtien on ilmennyt uskomaton määrä kansallisen turvallisuuden uhkia, jotka ovat mahdollistettu verkossa toteutetuilla toimilla. Digitaaliset aseet ovat häirinneet kykyä rikastaa uraania ydinpommien valmistusta varten. Ne ovat aiheuttaneet sähköhäiriöitä Ukrainan sähköjärjestelmissä vaikuttaen satoihin tuhansiin. Kyberhyökkäykset ovat kohdistuneet propagandakampanjoiden tukemiseen Ja hakkereiden on nähty osallistuvan laaja-alaisiin

kampanjoihin varastaakseen kaupallisia sekä hallinnollisia salaisuuksia. Tässä luvussa kerrotaan muutaman esimerkin, miten kybersodankäyntiä on tuoreessa historiassa harjoitettu ja kuinka niihin on reagoitu.

3.3.1 Georgian sota

19. heinäkuuta 2008 tietoturvayritys ilmoitti hajautetusta palvelunestohyökkäyksestä verkkosivustoja vastaan Georgiassa. Kolme viikkoa myöhemmin, 8. elokuuta, turvallisuusasiantuntijat havaitsivat toisen, laajemman DDoS-hyökkäyskierroksen kohteena Georgian Web-sivustot. Nämä hyökkäykset näyttivät osuvan samaan aikaan Venäjän joukkojen siirtymisen Etelä-Ossetiaan kanssa. Georgia oli aloittanut alueella sotilasoperaatioita päivää aiemmin (Korns & Kastenberg, 2009).

Maahyökkäysten lisääntyessä myös kyberhyökkäykset lisääntyivät. Tämä oli ensimmäinen kerta, kun kyberhyökkäys tehtiin aseellisen konfliktin yhteydessä. Georgian ja Venäjän välinen kybersota keskittyi julkisen mielipiteen muokkaamiseen internetissä. Hyökkääjät tekivät esimerkiksi väärennettyjä verkkosivustoja hallitakseen kuinka heidän versionsa "totuudesta" toimitettiin yleisölle (Ashmore, 2009).

Hyökkäysten seurauksen Georgina hallitus oli kyberlukittu ja pystyi tuskin kommunikoimaan internetin välityksellä (Korns & Kastenberg, 2009). Georgia sai paljon apua kyberhyökkäysten torjumiseen sekä sisäiseen ja kansainväliseen viestintään. Esimerkiksi amerikkalainen yritys, jolla ei ollut selkeitä valtuuksia, eikä Yhdysvaltain hallituksen hyväksyntää, otti suoraan yhteyttä Georgian hallitukseen ja järjesti sen kyberomaisuuden siirtämisen Yhdysvaltojen alueelle (Korns & Kastenberg, 2009). Ulkopuolisten tutkijoiden mukaan Venäjän hallituksen osallisuudesta kyberhyökkäyksiin ei ole suoraa näyttöä. (Ashmore, 2009).

3.3.2 Stuxnet

17. kesäkuuta 2010 virustorjuntayritys Valko-Venäjällä sai sähköpostin iranilaiselta asiakkaaltaan: heidän koneensa oli jumissa käynnistyen uudelleen ja uudelleen. Tämä häiriö oli peräisin salaperäisestä haittaohjelmasta, jonka tutkijat nimesivät Stuxnetiksi koodissa olevan tiedostonimen perusteella (Lindsay 2013, Farwell & Rohonzinski 2011).

Ohjelma oli iskenyt Iranin Ydinlaitokseen Natanzissa. Stuxnet vaihtoi sentrifugien sähkövirtojen taajuutta, mikä sai ne vaihtamaan edestakaisin hitaan ja nopean välillä, johon niitä ei ollut suunniteltu. Natanzin ydinvoimalassa on suljettu tietokoneverkko, joten sillä ei ole yhteyttä Internetiin tai muihin verkkoihin. Siksi on erittäin todennäköistä, että Stuxnet tartutti verkon irrotettavan USB-aseman kautta. Stuxnetin löytäminen tapahtui Iranin ja Yhdysvaltojen välisten jännitteiden ollessa kireät. Uskotaan, että USA rakensi Stuxnetin Israelin tuella tavoitteenaan pysäyttää tai viivyttää Iranin ydinohjelmaa. (Baezner & Robin, 2017).

Stuxnet oli myös tartuttanut yli 100 000 tietokonetta, joista yli puolet on Iranissa, etsiessään oikeaa kohdettaan (Hyppönen, 2012). Ohjelma vaikutti Iranin lisäksi Intiassa, Indonesiassa, Kiinassa, Azerbaidzhanissa, Etelä-Koreassa, Malesiassa, Yhdysvaloissa, Iso-Britanniassa, Australiassa, Suomessa ja Saksassa (Farwell & Rohonzinski 2011). Kansainvälisellä tasolla Stuxnetin löytyminen aiheutti uusien kyberturvallisuusstrategioiden aallon, kun valtiot ymmärsivät, että kybertyökaluja voidaan käyttää kriittisiä infrastruktuureja vastaan. Valtiot pelkäsivät muunnettujen Stuxnet-versioiden kukoistavan kyberrikollisten keskuudessa (Baezner & Robin, 2017).

Tietoturvaasiantuntijat ovat kuvanneet Stuxnetin teknologisesti kehittyneimmäksi haittaohjelmaksi, joka oli siihen mennessä kehitetty kohdistettuun hyökkäykseen (Matrosov ym., 2012). Se on hienostunut haittaohjelma, joka on suunniteltu tunkeutumaan etäjärjestelmiin lähes itsenäisesti. Stuxnet edustaa 2010-luvun uuden sukupolven niin sanottuja laukaise ja unohda -haittaohjelmia, jotka voidaan kohdistaa valittuja kohteita vastaan (Farwell & Rohonzinski 2011).

3.3.3 Kiinan tiedustelu yhdysvalloissa

Tammikuun 2010 alussa Google ilmoitti, että Kiinasta peräisin oleva kyberhyökkäys oli tunkeutunut yrityksen infrastruktuuriin joulukuun puolivälissä ja varastanut tietoja, kuten Googlen lähdekoodia. Hakkerit pääsivät myös käsiksi ihmisoikeusaktivistien Gmail-tileihin ja 33 muun yrityksen verkkoihin. Mukaan lukien Yahoo, Adobe, Symantec, Juniper Networks, Disney, Sony, Johnson & Johnson, General Electric sekä General Dynamics olivat uhreina (Thomas, 2010, Segal, 2013). Segalin (2013) mukaan Google kommentoi, että hyökkäys oli erittäin kehittynyt ja kohdennettu, mikä johti immateriaalisen omaisuuden varkauteen. Tapauksen takia Google vetäytyi kaikesta internetsensuurista Kiinassa ja ilmoitti myöhemmin päätöksestään vetäytyä virallisesti Manner-Kiinasta. Sivuston Google.cn vierailijat ohjattiin osoitteeseen Google.com.hk (Tan & Tan, 2012, Hjortfal, 2011)

Yhdysvaltain henkilöstöhallinnon toimisto (U.S. Office of Personnel Management, OPM) paljasti 4. kesäkuuta 2015, että kyberhyökkäys oli vaikuttanut sen tietojärjestelmiin ja tietoihin. Hyökkäys oli vaarantanut noin 4,2 miljoonan nykyisen ja entisen liittovaltion työntekijän henkilötiedot. Myöhemmin samassa kuussa toimisto ilmoitti toisesta hyökkäyksestä, jossa tietomurron arvioitiin vaarantavan 21,5 miljoonan henkilön arkaluonteiset tiedot (Finklea ym., 2015). Hyökkäyksestä löytyi liitoksia kiinalaisiin hakkereihin, jotka olivat aiemmin olleet vastuussa kyberrikoksista. Ei kuitenkaan tiedetä, olivatko nämä henkilöt todella vastuussa varastetuista tiedoista (Gootman, 2015).

Kiinan toteuttamilla ja tulevaisuudessa toteuttavilla kyberhyökkäyksillä on varmasti suuri merkitys sen armeijalle sekä Yhdysvaltojen pelotteelle. On todennäköistä, että Kiinan kehittyminen kybermaailmassa kehittyy. Kiinan kyberpelote on strategisesti älykäs ratkaisu, joka on melko halpa verrattuna täysimittaiseen tavanomaiseen armeijaan. (Hjortfal, 2011).

Washington ja Peking ilmoittivat 2013 perustavansa Yhdysvaltojen ja Kiinan kyberturvallisuustyöryhmän, joka piti ensimmäisen kokouksensa heinä-

kuussa 2013 (Segal, 2013). Turvallisuusryhmän tarkoitus on helpottaa Yhdysvaltojen ja Kiinan välisiä keskusteluja kyberkonfliktin riskeistä esimerkiksi kartoittamalla olemassa olevia ja uusia työkaluja niiden vähentämiseksi (Voo, 2019).

3.3.4 Ukrainan sota

Ukrainalainen alueellinen sähkönjakeluyhtiö Kyivoblenergo ilmoitti 23.12.2015 asiakkaille palvelukatkoksista. Katkot johtuivat kolmannen osapuolen laittomasta pääsystä yhtiön tietokone- ja SCADA-järjestelmiin (Lee, Assante & Conway, 2016). Kyberhyökkäys aiheutti kuuden tunnin sähkökatkon sadoille tuhansille asiakkaille Ukrainan pääkaupungissa Kiovassa ja sen ympäristössä. Se oli ensimmäinen dokumentoitu tapaus, jossa kyberhyökkääjät katkaisivat sähköverkon (Sullivan & Kamesnky, 2017).

Yrityksen ohjauskeskuksen operaattorit katselivat avuttomasti, kun hyökkääjät ottivat hallintaansa heidän tietokoneensa ja avasivat katkaisijat, joiden avulla vähintään kolmekymmentä sähköasemaa saatiin sammuksiin. Tekijät sammuttivat myös varavirtalähteet, jolloin operaattorit itse kompastuivat talvipimeässä. Haittaohjelmat pyyhkivät myös tärkeitä järjestelmätiedostoja, mikä aiheutti tietokoneiden kaatumisen. Puhelinkeskukset tulvivat näennäisesti Moskovasta soitetuista vääristä puheluita, jotta todelliset asiakkaat eivät päässeet läpi (Sullivan & Kamesnky, 2017).

Joulukuun 2015 hyökkäystä tutkivat huolellisesti muun muassa NATO, Yhdysvaltain turvallisuusministeriö ja Yhdysvaltain energiaministeriö (CISA, 2021a, Sullivan & Kamensky, 2017). Sekä ICS-CERT että SANS ovat antaneet suosituksia ja puolustusstrategioita Ukrainan sähkökatkostapaukseen liittyen, estääkseen vastaavia tapauksia tulevaisuudessa (Liang ym., 2017, CISA, 2021a, Lee ym., 2016).

Kesäkuussa 2017 kyberhyökkääjät käyttivät aikaisemmin keväällä asennettuja takaovia M.E.Docin asentamiin tietokoeisiin päästääkseen vapaaksi haittaohjelman nimeltä NotPetya. Haittaohjelma levisi automaattisesti, nopeasti ja satunnaisesti. Kun hakkerit pääsivät käsiksi tietokoneeseen, NotPentya saattoi poistaa salasanat RAM-muistista ja käyttää niitä hakkerointiin muihin koneisiin, joihin oli pääsy samoilla tunnistetiedoilla. Verkoissa, joissa on usean käyttäjän tietokoneita, se pystyi jopa sallimaan automaattisen hyökkäyksen ja siirtyä koneesta toiseen. Se salasi peruuttamattomasti tietokoneen Master Boot Recordsit, eli käynnistystietueet, ja vaati maksua tietueiden avaavaa avainta vastaan (Greenberg, 2018).

NotPenya lamautti leviämiselläämm monikansallisia yrityksiä, kuten Maerskin, lääkejätti Merckin, FedExin eurooppalaisen tytäryhtiön TNT Expressin, ranskalaisen rakennusyhtiön Saint-Gobainin, elintarviketuottaja Mondelēzin ja Reckitt Benckiserin. Kussakin tapauksessa aiheuttaen yhdeksännumeroisia kustannuksia. Se levisi jopa takaisin Venäjälle iskien valtion öljyyhtiöön Rosneftin. Seurauksena oli yli 10 miljardin dollarin kokonaisvahingot (Greenberg, 2018).

Ukrainan turvallisuuspalvelu on syyttänyt Venäjää tuhansista kyberhyökkäyksestä Ukrainan infrastruktuuria ja instituutioita vastaan, mukaan lukien 6 500 tapausta vain vuoden 2016 kahden viimeisen kuukauden aikana. Venäjä on toistuvasti kiistänyt hakkerointisyytökset (Sullivan & Kamensky, 2017).

4 KYBERUHKATIEDUSTELU VALTIOTASOLLA

Kybersodankäynnissä vaikuttavat usein samanlaiset kyberhyökkäykset kuin mitä kaupalliset yritykset joutuvat kestämään. Tietojen kalastelu, palvelunestot sekä haittaohjelmat ovat tuttuja valtio- sekä organisaatiotasolla. Yritysten niitä vastaan käyttämä kyberuhkatiedustelu voisi siis olla työkalu hyödynnettäväksi myös valtion uhkien ennaltaehkäisyssä. Valtiot tukevat ja antavat ohjeistustakin aiheesta. Esimerkiksi Yhdysvaltojen National Institute of Standards and Technology (Johnson ym., 2016) on antanut ohjeet kyberuhkatietojen jakamissuhteiden luomiseen ja niihin osallistumiseen. Ohje auttaa organisaatioita asettamaan tiedon jakamistavoitteita, tunnistamaan kyberuhkien tietolähteet, ottamaan yhteyttä kyberuhkatiedusteluyhteisöihin ja hyödyntämään uhkatietoja tehokkaasti organisaation toiminnan tukemiseksi.

Tässä luvussa käsitellään kyberuhkatiedustelutoimintatapojen hyödyntämistä valtiotasolla. Ensimmäisessä alaluvussa kerrotaan, kuinka kyberuhkatiedustelun toimintatapaa, tiedon jakamista, varmistetaan ja tuetaan valtiotasolla. Toisessa alaluvussa käsitellään, miten tiedon pohjalta valtiot tekevät ennaltaehkäiseviä toimia uhkia vastaan direktiivien, lakien ja säädösten avulla. Molemmissa luvuissa toimia tarkastellaan Euroopan Unionin, Yhdysvaltojen sekä Suomen näkökulmasta.

4.1 Tiedon jakaminen

Uhkatietojen jakaminen on ratkaiseva askel perusteellisen ymmärryksen hankkimisessa laajamittaisista kyberhyökkäystilanteista. Sekä eurooppalaiset että amerikkalaiset säännökset tietojen jakamisessa tähtäävät parempaan kyberresilienssiin, tehostamalla julkisen ja yksityisen sektorin yhteistyötä. (Skopik, Settanni & Fiedler, 2016).

European Union Agency for Cybersecurity (ENISA) on tukenut Euroopan Unionin jäsenvaltioita kansallisissa kyberturvallisuusstrategioissa yli kymmenen vuotta. Esimerkiksi sen edeltäjän Euroopan verkko- ja tietoruvaviraston

julkaisema opas (Ouzounis, 2009) kertoo päätavoitteekseen EU:n jäsenvaltioiden ja sidosryhmien tukemisen omien tiedonvaihto organisaatioiden perustamisessa ja ylläpitämisessä. EU on asettanut ENISA:n tehtäväksi lisätä operatiivista yhteistyötä EU:n tasolla auttamalla niitä EU:n jäsenvaltioita, jotka pyytävät sitä käsittelemään kyberhäiriötilanteita. Sekä tukea EU:n koordinointia laajamittaisissa, rajat ylittävissä, kyberhyökkäyksissä ja kriiseissä (Yhteyskomitea, 2020).

Voittoa tavoittelemattomat Information Sharing and Analysis Centers (ISAC) -tiedonvaihtoryhmät ovat yksi aiemmin mainitun sidosryhmän esimerkki. Niiden tarkoitus on olla keskeinen resurssi tiedon keräämiseen kyberuhkista sekä mahdollistaa kahdensuuntaisen tiedon jakamisen yksityisen ja julkisen sektorin välillä. Usein uhkatietojen keräämisen kohteena ovat kriittiseen infrastruktuuriin kohdistuvat uhkat. Monissa EU:n jäsenvaltioissa on olemassa ISAC-tiedonvaihtoryhmiä (ENISA, 2018).

Suomessakin ISAC-tiedonvaihtoryhmiä toimii aloilla, kuten elintarvike-, energia-, finanssi-, kemia-, logistiikka-, media-, terveydenhuolto- sekä vesihuoltoaloilla. (Kyberturvallisuuskeskus, 2023a). Kyberturvallisuuskeskuksen mukaan:

> ISAC-tiedonvaihtoryhmien jäsenet muodostavat laajan kansallisen verkoston, jolla on tärkeä rooli myös häiriötilanteiden hallinnassa. Häiriötilanteessa ryhmät ja niiden jäsenet tarjoavat verkoston hyväksi asiantuntemustaan, analyysiresursseja, tietolähteitä ja kansainvälisiä yhteyksiä. Yhteistyötä häiriötilanteissa harjoitellaan myös säännöllisesti (Kyberturvallisuuskeskus, 2023a).

Yhdysvalloissa Venäjän painostuksen takia Cybersecurity and Infrastructure Security Agency (CISA) julkaisi Joint Cyber Defence Collaborative (JCDC) yhteistyöorganisaation. ISAC:ien tapaan se tukee julkisen ja yksityisen puolen organisaatioiden kyberturvallisuustiedonvaihtoa. JCDC:n ydintoimintoja ovat:

1. kyberpuolustusoperaatioiden suunnitelmien kehittäminen ja koordinointi sekä suunnitelmien toteuttamisen tukeminen.
2. Ohjata operatiivista yhteistyötä ja kyberturvallisuustietojen yhdistämistä julkisen ja yksityisen sektorin välillä.
3. Kyberpuolustuksen ohjeiden tuottaminen ja levittäminen kaikissa sidosryhmissä (CISA, 2023).

Yhdysvallat julkaisi 2015 kyberturvallisuustiedon jakamistoimen. Se sisältää ohjeita, jotka auttavat muita kuin valtion tahoja jakamaan kyberuhkien merkkejä valtion hallituksen kanssa. Toimeen kuului myös menettelytapoja, jotka koskevat kyberuhkatietojen vastaanottamista ja käyttöä valtion tahoissa. Yksityisyyttä ja kansalaisvapauksia koskevia ohjeita näiden tietojen vaihdon yhteydessä sekä ohjeita valtion virastoille hallituksen hallussa olevien tietojen jakamisesta (CISA, 2021b).

Computer Emergency Response Teams (CERTs) ovat tietojärjestelmien hätätilanneryhmiä, jotka koostuvat eri alojen asiantuntijoista. CERT-ryhmät toi-

mivat useissa valtioissa ja niiden tehtävä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista (Kaufhold ym., 2022, Kyberturvallisuuskeskus, 2023b). Ryhmiä koordinoi Software Engineering Institute (SEI) Yhdysvalloista. CERT-asiantuntijat ovat monipuolinen ryhmä tutkijoita, ohjelmistokehittäjiä ja tietoturja-analyytikoita, jotka työskentelevät yhdessä kehittääkseen kyberturvallisuustietoa ja koulutusta parantaakseen kyberturvallisuuskäytänteitä. (Software Engineering Institute, 2023).

Valtiotasolla on siis monia valtioiden toimeksi panemia ja yksityisiä organisaatiota, jotka tukevat yksityisten ja valtiollisten organisaatioiden kyberuhkatiedustelutiedon keräämistä ja jakamista. Uhkatietojen jakaminen auttaa rakentamaan ja vahvistamaan organisaatioiden suhteita valtioiden virastoihin (Zibak & Simpson, 2019). Yhteistyö rakentaa vahvemman suojan valtiotasolla kohdattaviin uhkiin ja kehittää resilienssiä niitä vastaan.

4.2 Ennaltaehkäisy lainsäädännön ja säädösten avulla

Kyberuhkien ennaltaehkäisyä suunnitellaan ja toteutetaan paljon. kyberuhkatiedustelutiedon pohjalta eri valtiot, turvallisuus- ja poliittiset liitot ovat kehittäneet omia lakejaan ja direktiivejään parantaakseen omaa ja alaistensa kyberturvallisuuttaan. Euroopan unioni ja Yhdysvallat ovat yhä herkempiä kriittisen infrastruktuurin haavoittuvuudelle, mikä on johtanut uhkatietojen ja turvallisuusstrategioiden sekä direktiivien julkaisuun (Skopik, Settanni & Fiedler, 2016).

Euroopan komissio 2016 on yhdessä unionin ulkoasioiden ja turvallisuuspolitiikan edustajan kanssa julkaissut kyberturvallisuusstrategian sekä direktiiviehdotuksen, joilla varmistetaan verkko- ja tietoturvan (Network and Information Security, NIS-direktiivi) yhteinen korkea taso kaikkialla unionissa (Skopik, Settani & Fiedler, 2016).

NIS-direktiivi uusittiin NIS2-direktiiviin 2023. Se tarjoaa oikeudellisia toimenpiteitä kyberturvallisuuden yleisen tason parantamiseksi. Parannettu taso varmistetaan vaatimalla jäsenvaltioilta tarvittavat valmiudet ja asiamukainen varustus esimerkiksi valtion omalla pakollisella CERT-ryhmällä. NIS-yhteistyöryhmän perustamisella kaikkien jäsenvaltioiden kesken, tuetaan ja helpotetaan strategista yhteistyötä ja tiedonvaihtoa jäsenvaltioiden välillä. Kaikkien alojen turvallisuuskulttuurin kehityksellä varmistetaan yhteiskuntien kriittisten infrastruktuurien jatkumo (Euroopan Komissio, 2023a).

Euroopan unionissa ja sen jäsenvaltioissa on vuodesta 2019 ollut käytössä Euroopan unionin laajuinen kyberturvallisuuden sertifiointikehys tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille. Sertifikaatit tarvitsee sertifioida vain kerran ja ne tunnustetaan kaikkialla Euroopan Unionin sisällä, hyödyttäen siellä liiketoimintaa harjoittavia yrityksiä (Yhteyskomitea, 2020).

Euroopan komissiossa on valmisteilla asetusehdotus digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusvaatimuksista, joka tunnetaan nimellä Cyber Resilience Act eli Kyberkestävyyssäädös. Sen tarkoitus on vahvistaa Euroopan Unionissa käytettävien laitteisto- ja ohjelmistotuetteiden turvalli-

suutta. Suurin osa tämänhetkisistä laitteisto- ja ohjelmistotuotteista ei tällä hetkellä kuulu mihinkään kyberturvallisuutta koskevan Euroopan unionin lainsäädännön piiriin (Euroopan Komissio, 2023b). Isoin osa kyberturvallisuushyökkäyksistä kohdistuvat näiden tuotteiden haavoittuvuuksiin, mikä aiheuttaa merkittävää yhteiskunnallista ja taloudellista uhkaa.

Säädökselle asetettiin neljä konkreettista tavoitetta: 1. Valmistajien digitaalisia elementtejä sisältävien tuotteiden turvallisuuden parantamisen varmistaminen koko niiden elinkaaren aikana. 2. Johdonmukaisen kyberturvallisuuskehyksen varmistaminen. 3. Digitaalisia elementtejä sisältävien tuotteiden turvaominaisuuksien läpinäkyvyyden parantaminen. 4. Yritysten ja kuluttajien käyttämien digitaalisia elementtejä sisältävien tuotteiden turvallisuuden varmistaminen. (Euroopan Komissio, 2023b). Suomessa kyberkestävyyssäädökselle on asetettu oma liikenne- ja viestintäministeriön työryhmä.

Kyberturvallisuuskeskuksen (2020) mukaan Suomessa EU:n direktiivien lisäksi vaikuttavat EU:n yleiset tietoturva-asetukset sekä sähköisen viestinnän-, tietosuoja ja rikoslait. Sähköisen viestinnän palveluiden laki vaikuttaa teleyrityksiin, viestinnän välittäjiin, yhteisötilaajiin sekä verkkotunnusväittäjiin. Se koskee näissä organisaatioissa tietoturvaa ja luottamuksellisen viestinnän suojaa.

EU:n yleinen tietosuoja-asetus, jota suomen tietosuojalaki täydentää, asettaa vaatimuksia henkilötietojen keräämiseen, säilytykseen ja hallinnointiin. Se koskee EU:n sisäisiä ja ulkoisia organisaatioita. Suomen rikoslain mukaan kyberhyökkäysten suorittajat määritellään tietotekniikka- tai tietoverkkorikoksiksi. Rikoslain 38. luku sisältää niiden säätelyn (Kyberturvallisuuskeskus, 2020).

5 YHTEENVETO

Tämän tutkielman tavoitteena oli selvittää, miten kyberuhkatiedustelua hyödynnetään kybersodankäynnin uhkia vastaan. Sen ensimmäisessä sisältöluvussa selvitettiin mitä kyberuhkatiedustelu ja sen toimintatavat ovat. Kyberuhkatiedustelu on tiedon keräämisen ja jakamisen prosessi, sekä siitä saatava tieto. Kyberuhkatiedustelutieto on mitä vain todisteisiin pohjautuvaa tietoa uhkista, jonka avulla voidaan informoida päätöksentekoa kyberhyökkäysten ennaltaehkäisyssä tai lyhentää vaarantumisen ja havaitsemisen väliä. Se voi myös olla tietoa, joka päätöksenteon auttamisen sijaan, auttaa ymmärtämään uhkamaisemaa paremmin. Toimintatavoiksi tunnistettiin kyberuhkatiedustelutiedon kerääminen, jakaminen ja sen pohjalta tehtävät ennaltaehkäisevät päätökset.

Kyberuhkatiedustelusta on hyötyä organisaatioille esimerkiksi organisaatioon vaikuttavien uhkien ja hyökkäysmenetelmien näkyvyyden parantamisella, turvatoimien kehittämisellä sekä tuntemattomien uhkien tunnistamisella. Kyberuhkatiedustelun ongelmiksi tunnistettiin aiheen tuoreudesta johtuva standardoinnin puute sekä yritysten vastahakoisuus eri syistä jakaa oma tietoaan toisille yrityksille. Yritysten kyberuhkatiedustelutiedon jakamisen esteitä olivat esimerkiksi negatiivisen julkisuuden pelko, lailliset säädökset ja yksityisyyshaasteet sekä epäluotettavat toiset osapuolet.

Tutkimuksen toisessa sisältöluvussa tutkittiin kybersodankäyntiä, sen uhkia ja kuinka sitä on jo viime aikoina harjoitettu esimerkiksi Georgiassa ja Ukrainassa. Kybersodankäynti määriteltiin olevan organisoituja yksilöitä toteuttamassa kyberhyökkäyksiä toisen valtion suojeluksessa tai tuella. Kyberhyökkäykset ovat sähköisiä hyökkäyksiä organisaatioita tai valtioita kohtaan pyrkien aiheuttamaan häirintää kohteessa ja/tai saamaan omaa etua esimerkiksi informaation muodossa. Uhkien tunnistettiin olevan hyvin samanlaisia, kuin mihin yksityisetkin organisaatiot joutuvat varautumaan, kuten esimerkiksi madot ja virukset sekä palvelunestohyökkäykset. Vaikutukset kybersodankäynnin hyökkäyksillä voivat olla todella tuhoisia varsinkin, jos kohteena ovat valtioiden kriittiset infrastruktuurit. Esimerkiksi Ukrainan sodan alussa toteutetut hyökkäykset sähkölaitoksiin estivät sähkönsaannin kuudeksi tunniksi sadoille tuhansille asukkaille.

Tutkielman tutkimusongelma oli, miten kyberuhkatiedustelun toimintatapoja hyödynnetään kybersodankäynnin uhkia vastaan. Kolmas sisältöluku vastasi siihen. Se selvitti, kuinka Euroopan Unioni, Suomi sekä Yhdysvallat tukevat kyberuhkatiedustelun toimintatapoja kybersodankäynnin uhkia vastaan. Kyberuhkatiedustelutiedon vaihtoa on tuettu perustamalla tiedonvaihto-organisaatioita, kuten ISAC-ryhmiä, jotka organisoivat tiedon vaihtoa. Tietoa vaihdetaan ryhmien avulla yritysten, mutta myös yritysten ja valtion organisaatioiden välillä. Ennaltaehkäisyä on tuettu direktiivein sekä lainsäädännöin. Niiden avulla varmistetaan, että kaikki valtioiden osaset ovat ajan tasalla kyberturvallisuudessa eikä haavoittuvuuskohteita toivon mukaan löydy. Esimerkiksi NIS-direktiivi pakottaa jokaisen Euroopan Unionin jäsenvaltion perustamaan oman CERT-tietojärjestelmähätätilanneryhmänsä. Tulevaisuudessa Euroopan Unionilla on tuloilla asetusehdotus digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusvaatimuksista. Sen tarkoitus on vahvistaa Euroopan Unionissa käytettävien laitteisto- ja ohjelmistotuetteiden turvallisuutta.

Tutkielmassa ongelmaksi kehittyi kyberuhkatiedustelutermin standardin puute. Eri lähteet ja tieteenalat puhuivat aiheesta eri tavoin ja siksi de-facto määritelmää oli vaikea hahmottaa ja kiteyttää. Vaikeuksia tuotti myös, että samasta asiasta puhuttiin eri termeillä. Esimerkiksi miten joissain lähteissä Cyber Threat Intelligence saattoi olla vain Threat Intelligence toisessa. Termin löysyys loi haasteen relevantin kirjallisuuden hakemisessa. Kyberuhkatiedustelun standardoimisessa olisi jatkotutkimismahdollisuuksia, kuten aiheen aiempi kirjallisuuskin on todennut. Kybersodankäyntiin liittyvät lähteet sen sijaan saattoivat sisältää vanhempia raportteja esimerkiksi Yhdysvaltojen puolustusministeriöltä ilman mitään julkaisufoorumiluokitusta.

Tämä tutkielma käsittelee aihetta hyvin länsimaisesta näkökulmasta ja keskittyikin vain Suomen, Euroopan Unionin ja Yhdysvaltojen lähestymistapoihin. Mahdollisia toisia lähestymistapoja jatkotutkimuksiin aiheesta voisivat olla enemmän idän valtioiden, kuten Venäjän, Kiinan, Koreoiden tai Japanin tutkiminen. Tutkielman viimeistelyn aikana Suomi liittyi NATO-jäseneksi. Sen kyberturvallisuuskäytänteissä on varmasti paljon tutkittavaa kyberuhkatiedustelun näkökulmasta.

LÄHTEET

Andress, J., & Wintefield, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* (2. painos) Syngress.

Ashmore, W. (2009). *Impact of Alleged Russian Cyber Attacks* (Accession Number ADA504991). School of Advanced Military Studies.

Baezner, M., & Robin, P. (2017). *Stuxnet.* Center for Security Studies.

Billo, C., & Chang, W. (2004). *Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States*. Institute for Security Technology Studies at Dartmouth College.

CISA. (2023) JCDC FAQs. Cybersecurity & Infrastructure Security Agency. Haettu 22.3.2023 osoitteesta https://www.dip.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs

CISA. (2021a, 20. heinäkuuta). Cyber-Attack Against Ukrainian Critical Infrastructure. Cybersecurity & Infrastructure Security Agency. Haettu 22.3.2023 osoitteesta https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA. (2021b, 15. lokakuuta). Cybersecurity Information Sharing Act of 2015 Procedures and Guidance. Cybersecurity & Infrastructure Security Agency. Haettu 22.3.2023 osoitteesta https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance

Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, *94*(886), 533–578.

ENISA. (2018). *Information Sharing and Analysis Center (ISACs) – Cooperative models.* ENISA.

Euroopan Komissio. (2022, 7. kesäkuuta). *The Cybersecurity Strategy*. Haettu 6.4.2023 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Euroopan Komissio. (2023a, 16. tammikuuta). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* Haettu 24.3.2023 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Euroopan Komissio. (2023b, 30. tammikuuta). *Cyber Resilience Act*. Haettu 24.3.2023 osoitteesta https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Farwell, J., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40.

Farwell, J., & Rohozinski, R. (2012). The New Reality of Cyber War. *Survival*, *54*(4), 107–120.

Finklea, K., Christensen, M., Fischer, E., Lawrence, S., & Theohary, C. (2015). *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*. (ADA623611) Library of Congress Washington DC Congressional Research Service.

Gootman, S. (2016). OPM Hack: The Most Dangerous Threat to the Federal Government Today. *Journal of Applied Security Research*, *11*(4), 517–525.

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Haettu 17.3.2023 osoitteesta https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

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

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing* (NIST SP 800-150). National Institute of Standards and Technology.

Katal, A., Wazid, M., & Goudar, R. H. (2013). Big data: Issues, challenges, tools and Good practices. Teoksessa M. Parshar, ym. (toim.), *Sixth International Conference on Contemporary Computing*, (404–409). Noida, India.

Kaufhold, M.-A., Stöttinger, M., & Reuter, C. (2022). Cyber Threat Observatory: Design And Evaluation of an Interactive Dashboard for Computer Emergency Response Teams. Teoksessa *Thirtieth European Conference on Information Systems,* Timişoara, Romania

Korns, S., & Kastenberg, J. (2009). *Georgia's Cyber Left Hook*. (ADA636632) Army War College Carlisle Barracks PA Strategic Studies Institute.

KPMG. (2013). *Cyber threat intelligence and the lessons from law enforcement*. KPMG International Cooperative.

Kyberturvallisuuskeskus. (2020). *Kyberturvallisuus ja yrityksen hallituksen vastuu*. Liikenne- ja viestintävirasto Traficom.

Kyberturvallisuuskeskus. (2023a, 13. maaliskuuta). *ISAC-tiedonvaihtoryhmät*. Haettu 22.3.2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

Kyberturvallisuuskeskus. (2023b, 3. maaliskuuta). *CERT*. Haettu 27.3.23 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert

Kärkkäinen, A. (2013). Computer Network Defence in Military Cognitive Networks. Teoksessa J. Vankka (toim.), *Cyber Warfare* (1-26). (Julkaisusarja 1, 34) Maanpuolustuskorekakoulu, Sotatekniikan laitos.

Lee, R., Assante, M., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. (Defense Use Case) E-ISAC SANS.

Lewis, J. (2006). *Cybersecurity and Critical Infrastructure Protection*. Center for Strategic and International Studies.

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Transactions on Power Systems*, *32*(4), 3317–3318.

Lindsay, J. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*, 365–404.

Liu, S. & Cheng, B. (2009) *Cyberattacks: Why, What, Who, and How*. IEEE Xplore

Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). *Stuxnet Under the Microscope*. (Revision 1.31) ESET LLC.

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational Levels of Cyber Intelligence. *International Journal of Intelligence and Counterintelligence*, *27*(4), 702–719.

Mavroeidis, V., & Bromander, S. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. Teoksessa J. Brynielsson. (toim.) *2017 European Intelligence and Security Informatics Conference*, (91–98). Athens, Greece.

Ouzounis, V. (2009). *Good Practice Guide on Information Sharing*. ENISA, Symantec Inc., Landitd Ltd.

Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, *4*(1), 8.

Ponemon. (2015.). *The Cost of Malware Containment*. Ponemon Institute LLC.

Sahrom Abu, M., Rahayu Selamat, S., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371.

Sarwar, T. B. (2016). Analyzing the Challenges of Cybercrime in the Global Context: Need for A Cross –Border Response. *Society & Change*, *2*.

Sauerwein, C., Sillaber, C., & Breu, R. (2018). Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes. Teoksessa P. Drews, B. Funk, P. Niemeyer & P. Xie. (toim.) *Multikonferenz Wirtschaftsinformatik 2018 Data driven X – Turning Data into Value,* (1333-1344) Lüneburg, Germany.

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. Teoksessa J. Leimester & W. Brenner. (toim.) *Wirtschaftsinformatik 2017 Proceedings*, (837-851). St.Gallen, Switzerland.

Segal, A. (2013). The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists*, *69*(5), 38–45.

Shackleford, D., & Lee, R. (2017). *Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey*. SANS, LookingGlass Cyber Solutions.

Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016). Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. Teoksessa S. Katzenbeisser & E. Weippl. (toim.) *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, (65–70). Vienna, Austria.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176.

Software Engineering Institute. (2023). *The CERT Division*. Haettu 27.3.2023 osoitteesta https://www.sei.cmu.edu/about/divisions/cert/index.cfm

Stojkovski, B., Lenzini, G., Koenig, V., & Rivas, S. (2021). What's in a Cyber Threat Intelligence sharing platform?: A mixed-methods user experience investigation of MISP. Teoksessa *37th Annual Computer Security Applications Conference*, (385–398). Austin, Texas, Yhdyvallat.

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal*, *30*(3), 30–35.

Tan, J., & Tan, A. E. (2012). Business Under Threat, Technology Under Attack, Ethics Under Fire: The Experience of Google in China. *Journal of Business Ethics*, *110*(4), 469–479.

Thomas, T. L. (2010). Google Confronts China's "Three Warfares". *The US Army War College Quarterly: Parameters*, *40*(2), 101-113.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233.

Voo, J. (2019). U.S.-China Cybersecurity Group Explores Mutual Interests, Goals. *Belfer Center for Science and International Affairs*. Haettu 20.3.2023 osoitteesta https://www.belfercenter.org/publication/us-china-cybersecurity-group-explores-mutual-interests-goals

Voutilainen, J., & Kari, M. J. (2020). Strategic Cyber Threat Intelligence: Building the Situational Picture with Emerging Technologies. Teoksessa T. Eze, L. Speakman & C. Onwubiko. (toim.) *Proceedings of the 19th European Conference on Cyber Warfare*, (545-553) Chester, UK.

Yhteyskomitea. (2020) *Kyberturvallisuus EU:ssa ja sen jäsenvaltioissa*. EU Contact Commitee.

Zibak, A., & Simpson, A. (2019). Cyber Threat Information Sharing: Perceived Benefits and Barriers. Teoksessa S. Furnell, ym. (toim.) *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 1–9. Canterbury, UK.