Markus Lämsä

KYBERUHKIIN VALMISTAUTUMINEN: RISKIEN-HALLINTATYÖKALUJEN VERTAILU

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Lämsä, Markus
Kyberuhkiin valmistautuminen: Riskienhallintatyökalujen vertailu
Jyväskylä: Jyväskylän yliopisto, 2022, 40 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Marttiin, Pentti

Tässä kandidaatintutkielmassa käsitellään kyberuhkiin valmistautumista erilaisten riskienhallintamallien näkökulmasta. Kyberuhat ja hyökkäykset ovat nykyyhteiskunnassa näkyvillä yhä enemmän. Tutkielmassa vertaillaan eri riskienhallintamallien ominaisuuksia ja kyvykkyyksiä toimia kyberuhkien ehkäisemisen välineenä, keskittyen pääasiassa organisaation kokonaisvaltaisen riskienhallinnan (ERM) malleihin sekä kill chain-malleihin. Tutkielman tarkoituksena on tunnistaa se riskienhallinnan viitekehys, jota hyödyntämällä kyberuhkien torjunnalle tai lievittämiselle esitetyt vaatimukset täyttyvät todennäköisimmin. Lisäksi keskitytään havainnollistamaan mallin ominaisuuksia, kyvykkyyksiä sekä niiden vaikutusta mallin toimintaan. Tutkimusta tehokkaimman riskienhallintamallin tunnistamiseksi ei ole juurikaan saatavilla, etenkään kybermaailman ilmiöihin keskittyen ja tämän vuoksi olisikin tärkeää saada organisaatioiden tietoon varteenotettavimmat työkalut kyberuhkien vastaiseen työhön. Tutkimuksen tuloksena voidaan todeta, että nimenomaisesti kyberuhkien torjuntaan tehokkaampi valinta ovat kill chain-malliset viitekehykset. Etenkin kokonaisvaltaisemmat ATT&CK- ja Cyber Kill Chain-viitekehykset kykenevät täyttämään riskienhallinnalle asetetut vaatimukset lievitysorientoitunutta STRIDE-mallia paremmin.

Asiasanat: kyberuhka, kyberhyökkäys, riskienhallinta, kyberhyökkäysten tunnistaminen, kyberuhkiin valmistautuminen

ABSTRACT

Lämsä, Markus
Preparing for cyber threats: a comparison of risk management tools
Jyväskylä: University of Jyväskylä, 2022, 40 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Marttiin, Pentti

This bachelor's thesis inspects preparing for cyber threats from the perspective of risk management models. Cyber threats and attacks are on the rise in modern society. The dissertation compares the features and capabilities of different risk management models as a tool of preventing cyber threats, focusing mainly on the comprehensive enterprise risk management (ERM) models and Kill Chain models. The purpose of the research is to identify the risk management framework that is most likely to meet the requirements for the prevention or mitigation of cyber threats. In addition, the focus is on illustrating the features and capabilities of the models and their impact on the operating capability of the models. There is little research available to identify the most effective risk management model, especially focusing on cyber environment, and it would therefore be important to provide organizations with the most relevant tools for working against cyber threats. As a result of the study, it can be stated that Kill Chain-based reference frames are a more effective choice for combating cyber threats. In particular, the more comprehensive ATT&CK and Cyber Kill Chain-frameworks are better able to meet the requirements of risk management than the mitigation-oriented STRIDE model.

Keywords: cyber threat, cyber attack, risk management, detection of cyber attacks, cyber threat preparedness

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kuten vallitsevassa maailmantilanteessa olemme havainneet, ovat kybervaikuttaminen ja -uhat vaikuttaneet laajalti käynnissä olevassa konfliktissa. Tähän toimintaan on lisäksi osallistunut merkittävä määrä eri tahoja myös konfliktin ulkopuolelta, ja osa tahoista on jopa joutunut vaikuttamisen kohteeksi täysin haluamattaan. Näillä kyberympäristön tapahtumilla on täten eittämättä vaikutusta myös yksilön ja yksittäisen organisaation toimintaan.

Lehto (2021) käsittelee Euroopan komission pohdinta-asiakirjassa (2017) analysoitua tulevaisuuden uhkamaailmaa. Keskeisimpinä havaintoina asiakirjan sisällöstä hän esittää muun muassa teknologian kehityksen ja uusien teknologioiden sekä laitteiden käyttämisen kyberrikollisuudessa ja muussa haitallisessa toiminnassa, millä on suora vaikutus nyky-yhteiskunnan rakenteisiin turvallisuuden ja puolustuksen näkökulmasta. Internetin helppokäyttöisyys ja sen käyttäjien määrän nopea kasvu on tuonut mukanaan kyberrikollisten ja erilaisten kyberuhkien määrän kasvun, jonka johdosta digitaalinen toimintaympäristömme on kokenut merkittäviä muutoksia. Oman turvallisuutensa tähden kyberuhilta puolustautuminen on nyt erittäin tärkeä toimi organisaatioille, varsinkin kriittiseen infrastruktuuriin kuuluvien sellaisten.

Kybermaailman uhilta voidaan pyrkiä suojautumaan monin keinoin. Yksi keino valmistautumiseen, puolustautumiseen ja vaikutusten minimointiin on käyttää erilaisia riskienhallintamenetelmiä puolustustoimien viitekehyksenä.

Tässä tutkielmassa vertaillaan keskenään erilaisia riskienhallintamalleja, pääasiassa kill chain-pohjaisia malleja. Lisäksi arvioidaan mallien kyvykkyyttä toimia kyberuhkien ehkäisyn tai torjunnan välineinä näiden ominaisuuksien, hyötyjen, vajavaisuuksien sekä haasteiden avulla.

Kill Chain -mallit ovat kyberuhkien tunnistamiseen ja ehkäisemiseen kehitettyjä malleja (Lockheed Martin, 2015). Ne perustuvat Yhdysvaltain asevoimien kehittämään kill chain -taktiikkaan, mistä nimi myös juontuu (Kiwia, ym. 2017). Näiden lisäksi vertailussa mukana on COSO-ERM-viitekehys, joka on kokonaisvaltaisen organisaation riskienhallinnan viitekehys (Leino ym., 2005).

Vaikka näitä viitekehyksiä käytetään kyberuhkien torjunnassa, on niiden käytännön toiminnasta tehtyä tutkimusta haastavaa löytää, eikä vertailevaa

tutkimusta viitekehyksistä ole juurikaan tehty. Yhtenä haasteena organisaatiolle voidaan nähdä viitekehysten runsaus ja samanaikaisesti laaja pohjautuvuus Lockheed Martinin kehittämään Cyber Kill Chain -viitekehykseen. Viime aikoina kasvaneen kyberuhkien uhkapotentiaalin johdosta olisikin tärkeää tunnistaa niitä malleja, joiden avulla organisaatiot pystyisivät sekä ehkäisemään että torjumaan kyberuhkia tehokkaasti.

Tutkimuskysymyksenä tässä tutkielmassa toimii seuraava:

1) *Mitkä ovat vertailtavien riskienhallintamallien tai kill chain-mallien ominaisuudet ja eroavaisuudet, sekä mitä mallia hyödyntämällä kyberuhkien torjunnalle asetetut tavoitteet todennäköisimmin täyttyvät?*

Kandidaatintutkielma on toteutettu kuvailevana kirjallisuuskatsauksena. Kirjallisuushaut on tehty valikoituja kandidaattiseminaarissa esiteltyjä tietokantoja hyödyntäen, joita ovat pääasiassa IEEE Xplore, Scopus ja ProQuest, Springer sekä lisäksi Google Scholar. Joitakin hakuja on myös tehty JYX-julkaisuarkistoa apuna käyttäen. Hakusanoina on käytetty ensisijaisesti valittujen riskienhallintamallien nimiä, ”Cyber Kill Chain”, ”ATT&CK”, ”STRIDE” ja ”COSO-ERM-2017”. Näiden lisäksi käytettiin myös hakusanoina ”risk management” ja ”cyber threats” käsitteiden määrittelyn yhteydessä. Tavoitteena mallien nimien hakusanakäytössä oli löytää mallikohtaisia tapaustutkimuksia niiden käytöstä.

Lähteinä on käytetty kirjoja, akateemisia artikkeleita, konferenssijulkaisuja, virastojen asiakirjoja sekä käsiteltyjen mallien esitteitä. Lähteiden luotettavuutta on arvioitu Julkaisufoorumin (JUFO) määrittämän luokituksen avulla, mikäli sellainen on ollut saatavilla. Muita lähteitä, joille Julkaisufoorumin luokitusta ei ole, on pyritty arvioimaan lähdeorganisaation ja julkaisualustan perusteella.

Tutkielman ensimmäisessä osassa, sisältöluvuissa kaksi ja kolme, keskitytään määrittelemään tutkielmassa käytettyjä kyberuhan, riskienhallinnan sekä riskienhallintamallin käsitteitä, mitkä ovat tutkielman varsinaisen käsittelyosan kannalta oleellisia sisäistää. Lukija tulee ymmärtämään mitä tarkoitetaan kyberuhista puhuttaessa, millaisia kyberuhkia voidaan kohdata, mitä riskienhallinta ja riskienhallintamallit ovat sekä millaisia riskienhallintamalleja (Cyber Kill Chain) tässä tutkielmassa pääasiassa käsitellään. Toisessa osassa, luvussa neljä, esitetään kaikki käsiteltävät viitekehykset sekä tämän jälkeen toteutetaan varsinainen viitekehysten ominaisuuksien vertailu lähdemateriaalin perusteella. Lukijalle vertailu esitetään sekä tekstimuotoisesti että taulukkomuotoisesti ja pääkohdat pyritään tiivistämään taulukoihin havainnollisuuden tehostamiseksi.

2 KYBERUHAT

Kyberturvallisuuden aihepiirissä puhuttaessa uhista voidaan nähdä, että ne yhdessä muiden tekijöiden, kuten haavoittuvuuksien ja riskien kanssa muodostavat toisiinsa liittyvän kokonaisuuden (Lehto, 2021). Tässä kokonaisuudessa lähtökohtana on omistettu asia, esimerkiksi fyysinen esine, tieto tai osaaminen. Tätä asiaa halutaan tyypillisesti suojella, turvata sen olemassaolo sekä omistussuhde kyseiseen asiaan. Kyberturvallisuuden kokonaisuudessa kyberuhka on suoraan sidoksissa edellä mainittuihin omistettuihin asioihin (engl. ”assets”), riskeihin, haavoittuvuuksiin ja uhkavakoojiin (Lehto, 2021). Kyberuhat ovat siis vain yksittäinen osa suurempaa kyberturvallisuuden kokonaisuutta, mutta tässä tutkielmassa keskitytään pääasiassa vain uhan kontekstiin.

Tämän sisältöluvun tarkoituksena on ensin määritellä ja esittää kyberuhan käsite. Tämän jälkeen esitellään erilaisia uhkatyyppejä Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarjan 30/2017 määrityksen mukaisesti ja luvun päättää uhkien luokittelu niiden taustalla vaikuttavan motiivin perusteella.

2.1 Kyberuhan määritelmä

Kyberuhalla tarkoitetaan sellaista haitallista tai tietyn toiminnon vaarantavaa, mahdollisesti toteutuvaa tapahtumaa jonka kohteena on kybertoimintaympäristö tai jokin sen osa-alue (Turvallisuuskomitea, 2018). Kyberuhkia voi aiheuttaa sekä jo toteutuneet tietoturvauhat että esimerkiksi yhteiskunnan turvallisuutta vaarantava viestintä sähköisissä palveluissa.

Kyberuhka voi olla peräisin yksittäisen valtion sisältä tai sen ulkopuolelta, mikä tekee jäljitystyöstä erityisen haastavaa. Kyberuhan ei tarvitse olla yksilöity laitteisto, hyökkäys tai haavoittuvuus vaan sen voidaan nähdä tarkoittavan myös uhkaavaa toimijaa, yksilöä tai ryhmää, kuten esimerkiksi aktivistiryhmittymää tai valtiollista toimijaa (Mateski, 2012). Usein kyberuhan lähde yhdistetään myös rikollisuuteen ja terrorismiin. Joulukuussa 2010 julkaistussa Yhteiskunnan turvallisuusstrategiassa todetaan, että valmius tietojärjestelmien häirintään,

hyväksikäyttöön sekä tuhoamiseen liittyy useimpien valtioiden sotilaalliseen varautumiseen (Puolustusministeriö, 2010). Kohteena kyberuhille voi olla yhteiskunnan elintärkeät toiminnot, kriittinen infrastruktuuri tai jopa suoraan yksittäiset kansalaiset, joko suoraan tai välillisesti (Turvallisuuskomitea, 2018).

Uhkaa voidaan mitata numeerisesti, jolloin sen saama arvo on uhan todennäköisyys (Lehto, 2021). Koska ihmiset tekevät ja tulevat aina tekemään inhimillisiä virheitä ja tietoturva-aukot sisältyvät aina informaatioteknologiaan, ei kyberuhkia pystytä koskaan täysin poistamaan (Clapper, Lettre & Rogers, 2017).

2.2 Tyypillisimpiä kyberuhkia

Uma ja Padmavathi (2013) esittävät eri maiden lakitekstien ja valtiollisten dokumenttien perusteella kyberuhkien eri muotojen olevan kyberrikollisuus, -vakoilu, -terrorismi ja -sodankäynti. Tähän luokitteluun esimerkiksi Turvallisuuskomitea (2018) lisää vielä kyberaktivismin.

Lehto ym. (2017) esittävät tyypillisimpien kyberuhkien olevan merkittävän määrällisen kasvun kokeneet kiristyshaittaohjelmat, haavoittuvuuksien hyödyntäminen hyökkäyksen toteuttamiseksi, laitteistoihin kohdistuvat suorat uhat, organisaation sisäpiirin hyödyntäminen hyökkäyksen kanavana, yrityksen liiketoiminnan tuhoamiseen pyrkivät hyökkäykset ja hyökkäykset, joiden tavoitteena on varastaa yksilöiden henkilötietoja. Näiden useimmin esiintyvien uhkien lisäksi esiintyy toki runsaasti myös muita uhkia, kuten erilaisia huijauksia, tietojenkalastelua ja tietojenkalasteluoperaatioita, palvelunestohyökkäyksiä sekä kohdistettuja ja jatkuvia hyökkäyksiä (Lehto ym., 2017).

Haavoittuvuuksien esiintyminen on merkittävä tekijä kyberuhkien esiintymisen kannalta, sillä ne mahdollistavat kyberrikollisten toiminnan ja hyökkäykset (Lehto ym., 2017). Haavoittuvuuden löytäminen ja hyökkäyksen toteuttaminen haavoittuvuutta hyväksikäyttäen kasvattaa hyökkäyksen onnistumisen todennäköisyyttä, sillä haavoittuvuuksia löydetään usein viiveellä. Tätä rikollisten tavoittelemaa haavoittuvuuksien paikkaamista edeltävää aikaikkunaa on kuitenkin mahdollista lyhentää ylläpitämällä tietoa ja ymmärrystä haavoittuvuuksista sekä ylläpitämällä säännöllistä korjaustiedostojen päivitysrutiinia (Lehto ym., 2017).

2.2.1 Uhkien esiintyminen

Seuraavassa taulukossa (taulukko 1) on koottu yhteen Lehdon ym. (2017) näkemyksiä Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarjasta 30/2017. Taulukossa esitellään hyvin tiivistetysti tyypillisimpien kyberuhkien esiintymistä ja niiden toteutustapoja sekä taustalla vaikuttavia motiiveja ja tavoitteita.

TAULUKKO 1 Kyberuhkien esiintyminen, toteutustavat sekä vaikuttavat motiivit koottuna taulukkomuotoon, mukaillen Lehtoa ym. (2017)

Uhka	Tyypillisin toteutustapa	Motiivit
Älypuhelimet ja IoT	- Yhä kehittyneemmät haittaohjelmat, tietojenkalastelu- ja kiristysohjelmat.	- Minkä tahansa saatavilla olevan tiedon käyttäminen rikollisiin tarkoituksiin
Web	- Lisäosiin tai mainoksiin naamioidut haittaohjelmat, kooditason haavoittuvuuksien hyödyntäminen, todentamismekanismien murtaminen	- Minkä tahansa saatavilla olevan tiedon käyttäminen rikollisiin tarkoituksiin
Sosiaalinen media	- Sos. median profiilien analysointi, haittaohjelmat sähköpostiliitteissä tai linkkien takana - Usein tavoitteena saada kohdehenkilö klikkaamaan linkkiä, jonka takana on haittaohjelman sisältävä tiedosto	- Henkilötietojen ja muiden henkilökohtaisten tietojen käyttäminen rikollisiin tarkoituksiin. - Yrityksen työntekijöiden ja liiketoimintakontaktien hyödyntäminen luottamuksen kerryttämisessä, jotta voidaan toteuttaa mm. petoksia
Kohdistetut hyökkäykset	- Kohdeorganisaation palvelujen haavoittuvuuksien kautta toteutetut ammattimaiset hyökkäykset - Pitkä aikaväli, kampanjat, useat erilaiset tekniikat	- Kohteena kansalliset salatut tiedot, henkilötiedot sekä aineettomat pääomat - Usein hyökkääjällä pitkän tähtäimen päämäärä
Tietovuodot ja yksityisyyden suoja	- Pitkälle aikavälille hajautettu hyökkäys organisaation sisäverkkoon, jolloin tietoa vuodetaan jopa useiden kuukausien ajan ennen vuodon havaitsemista	- Tunnistautuminen ja pääsynhallinnan ohittaminen - Vakoilun tukeminen
Pilvipalvelut	- Hajautetut palvelunestohyökkäykset ja bottiverkkohyökkäykset palvelun poistamiseksi verkkokäytöstä. - Lisäksi yhdistettynä edelliseen haittaohjelmat, sisäverkkoon tunkeutuminen ja hakkerointi sekä tietovuodot	- Pääsy yritysten liiketoiminnan kannalta kriittiseen dataan (talous-, asiakkuus-, innovaatio- sekä henkilötietoja).

2.2.2 Kyberuhkien luokittelu motiivin perusteella

Lehto (2021) jakaa kyberuhat niiden taustalla vaikuttavien motiivien perusteella kuudeksi eri alakategoriaksi, josta muodostuu kuusitasoinen kyberuhkien rakennemalli. Tämä on kuvattu taulukossa alla (taulukko 2). Tässä tutkielmassa käsiteltävät riskienhallintamallit ovat pääasiassa luotu mallintamaan ja lievittämään kohdistettuja haittaohjelmahyökkäyskampanjoita eli APT-hyökkäyksiä (Lehto, 2021), joten tämän taulukon kontekstissa käsiteltävät mallit kattavat taulukon alemmalle puolikkaalle sijoittuvat uhat pääasiallisen toimintaperiaatteensa perusteella.

TAULUKKO 2 Esimerkki kyberuhkien rakennemallista (Lehto, 2021)

Taso	Käsite
6.	Kybersodankäynti
5.	Kybersabotaasi
4.	Kyberterrorismi
3.	Kybertiedustelu
2.	Kyberrikollisuus
1.	Kybervandalismi

Lehdon (2021) mukaan ensimmäinen taso on kybervandalismi. Se pitää sisällään haktivismin, hakkeroinnin ja kyberparveilun. Haktivismi, jota voidaan pitää yläkäsitteenä, tarkoittaa Limnéllin ym. (2014) mukaan palvelunestohyökkäysten toteuttamista, virtuaalista sabotaasia, nettisivujen kaappaamista ja sotkemista sekä luottamuksellisen tiedon levittämistä. Täten pyritään toteuttamaan jonkin yksilön tai ryhmittymän poliittista, ideologista tai sosiaalista motiivia (Limnéll ym., 2014). Nämä toimet eivät ole vaikutuksiltaan kovinkaan pitkäkestoisia, saati vaarallisia, mutta saavat silti runsaasti julkista näkyvyyttä (Lehto, 2021). Ne ovat myös osin rangaistavia (Limnéll ym., 2014). Sen vuoksi tämänkaltaisen toiminnan seuraukset yksittäiselle yritykselle tai yksilölle voivat olla taloudellisesta näkökulmasta katsottuna merkittäviä, sillä tiedon leviäminen internetissä tapahtuu nykypäivänä todella nopeasti.

Seuraavan tason muodostaa kyberrikollisuus (Lehto, 2021). Kyberrikollisuus voidaan määritellä tarkoittamaan sellaisia rikoksia, jotka joko toteutetaan sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyksi käyttäen tai joiden kohteena edellä mainitut verkot tai järjestelmät ovat (EU-komissio, 2017). Tietoverkkorikollisuudeksi luetaan kaikki sähköisiä viestintäverkkoja tai tietojärjestelmiä hyväksi käyttäen tehdyt perinteisen rikollisuuden muodon täyttävät rikokset, kuten esimerkiksi häirintä, petokset ja uhkailu (EU-komissio, 2017). Lisäksi tietoverkkorikollisuutta on kaiken sellaisen sisällön julkaiseminen sähköisissä viestintäpalveluissa mikä on määritetty olevan laitonta, kuten esimerkiksi rasistinen sisältö (EU-komissio 2017). Myös tietoverkkoa vastaan toteutetut hyökkäykset, palvelunestohyökkäykset sekä hakkerointi ja muut vastaavat rikokset, joita toteutetaan vain sähköisissä verkoissa, on EU-komission pohdinta asiakirjan (2017)

mukaan tietoverkkorikollisuutta. Edellä kuvatun perusteella tietoverkkorikollisuus voidaan eritellä kolmeen erilaiseen alaryhmään, komissio toteaa.

Kolmas sekä neljäs taso muodostuvat kybervakoilusta ja kyberterrorismista (Lehto 2021). Kybervakoilu on Liaropouloksen (2010) mukaan määriteltävissä toimiksi, jotka ovat laittomia, tapahtuvat sähköisissä verkoissa, ohjelmistoissa tai internetissä sekä niiden tavoitteena on saada toimijan haltuun salattuja tietoja tietyiltä toimijoilta tai yksilöiltä joko poliittisen, taloudellisen tai sotilaallisen edun kerryttämiseksi. Yksinkertaisesti tämä voi siis tarkoittaa kilpailevan yrityksen tai armeijan tietojärjestelmään murtautumista ja sieltä salatun tiedon keräämistä. Limnéll ym. (2014) lisäävät määritelmään myös kriisitilannetta ennakoivan tai valmistavan tiedustelutoiminnan, joka kohdistuu kriittiseen infrastruktuuriin. Kyberterrorismi puolestaan tarkoittaa vahinkojen tuottamista, pelon lietsontaa ihmisten keskuudessa sekä poliittisen johdon painostamista tietoverkkojen kautta toteutettujen hyökkäysten avulla. Näiden hyökkäysten kohteena on usein kriittiset informaatiojärjestelmät ja hyökkäysten tavoitteena on niiden kontrollointi (Beggs, 2006).

Viides taso muodostuu kybersabotaasista. Lehto (2021) määrittelee sen olevan toimintaa, jossa valtiollinen tai jokin valtion tukema toimija aiheuttaa esimerkiksi poliittista tai yhteiskunnallista epävakautta kohdevaltiossa, testaa omia kyberhyökkäyskyvykkyyksiään tai jopa valmistelee hybridioperaatiota tai sotaa. Tällainen toiminta ei kuitenkaan täysin täytä sodan tunnusmerkkejä, joten se on mallissa kuvattu omalla sotaa alemmalla tasollaan.

Kuudes ja korkein taso on kybersodankäynti. Sen käsitettä käytetään varsin laajalti nyky-yhteiskunnassa kuvaamaan eri valtiollisten toimijoiden kybermaailmassa toteuttamia operaatioita, eikä sille siksi ole yksittäistä yleisesti hyväksyttyä määritelmää (Lehto, 2021). Suomessa Turvallisuuskomitea (2018) on määritellyt termillä tarkoitettavan valtioiden välistä vihamielistä toimintaa, joka pyrkii hyödyntämään tietoverkkoja ja erityisesti niiden haavoittuvuuksia. Vastaavasti voidaan puhua myös tietoverkkosodankäynnistä. Lisäksi Uman ja Padmavathin (2013) mukaan kybersotaa käyvät valtiolliset toimijat joko sodankäynnin yhteydessä tai vaihtoehtoisesti suoritetut toimet ovat muutoin verrannallisia aseelliseen hyökkäykseen. Käsitteen määrittely on haasteellista, sillä sotaa ei voida rajata vain yhteen toimintaympäristöön (Turvallisuuskomitea, 2018), vaan valtioiden välisen kybersodankäynnin edellytyksenä on sotatilan julistaminen, jolloin kyberoperaatiot ovat toteutettavien sotilaallisten operaatioiden yksi osa-alue (Lehto, 2021)

3 RISKIENHALLINTAMALLIT

Parhaimmillaan riskienhallintamallit ja riskienhallinta tukevat organisaation päätöksentekoa ja kehittymistä. Tärkeintä on riskien tunnistaminen ja niihin oikealla tavalla reagoiminen. Usein riskienhallinnan kompastuskiviksi organisaation sisällä nousevat prosessin epäjohdonmukaisuus tai systemaattisuuden puute. Tähän ongelmaan tässä tutkielmassa käsiteltävät riskienhallintamallit ovat oiva kehityskeino. Tässä sisältöluvussa analysoidaan useita riskienhallinnan määritelmiä, kuten myös riskienhallintamallin määritelmä sekä määritetään tiivistetysti kill chain-mallin käsite.

3.1 Riskienhallinnan ja riskienhallintamallin määritelmä

Valtionvarainministeriö (2017) määrittää riskienhallinnan olevan tavoitteellista ja järjestelmällistä toimintaa, joka tukee organisaation kehittymistä ja johtamisen päätöksentekoa ohjaamalla ja hallinnoimalla organisaation riskejä. Sen tavoitteena on mahdollistaa organisaation toiminnan jatkuvuus ja tavoitteiden saavuttaminen löytämällä niihin vaikuttavat riskitekijät sekä tunnistaa ja ehkäistä ne mahdollisimman aikaisessa vaiheessa. Riskienhallinta on keskeinen osa organisaation johtamisen ja operatiivisen toiminnan prosessien toteutusta, suunnittelua sekä seurantaa (Valtionvarainministeriö, 2017). Täten riskienhallintaa ei voida käsittää vain organisaation johdon työkaluna, vaan se koskettaa myös jokaista yksittäistä organisaation jäsentä (Valtionvarainministeriö, 2017), esimerkiksi velvoittamalla kaikesta normaalista poikkeavien havaintojen ilmoittamiseen omalle esimiehelle.

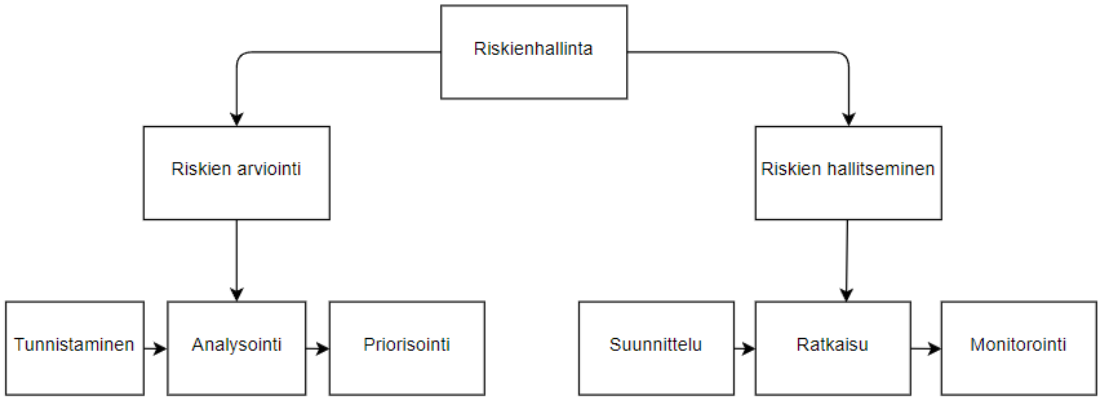
Valtionvarainministeriön (2017) mukaan riskienhallinnan avulla voidaan tietyissä tilanteissa myös tunnistaa riskeihin sisältyviä mahdollisuuksia ja täten jopa säilyttää valittuja riskejä organisaatiossa. Riskienhallinnan avulla organisaatiolle voidaan määrittää tietty riskinottokyvyn taso, jota voidaan hyödyntää riskienoton määrää pohdittaessa.

Bannermanin (2008) mukaan riskienhallinta on kokoelma toimintamalleja ja käytänteitä riskitekijöiden tunnistamiseksi, analysoimiseksi ja käsittelemiseksi. Riskienhallinnan perimmäisenä tarkoituksena on edistää yksittäisen (tietojärjestelmä)projektin onnistumismahdollisuuksia ja vastavuoroisesti pyrkiä estämään sen epäonnistuminen.

Riskienhallinta voidaan jakaa kahteen osaan, kuten Boehm (1989) mallissaan. Osat ovat seuraavat:

1. Riskien arviointi
2. Riskien hallitseminen

Nämä edellä mainitut riskienhallinnan osat voidaan jakaa vielä useampiin alakategorioihin, joiden avulla voidaan johtaa riskien tunnistus-, arviointi- ja hallintaprosessit. Aslam (2017) esittää edellä mainitut prosessit visuaalisesti kuten alla kuviossa on esitetty (kuvio 1).



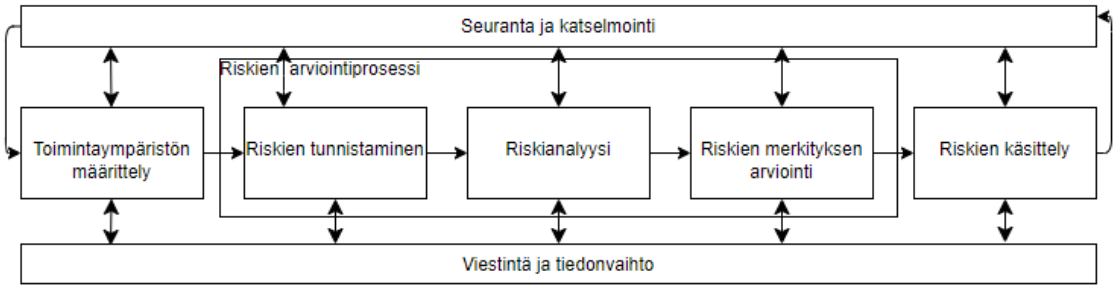
KUVIO 1 Riskien hallinta ja arviointi prosessina (Aslam, 2017)

Kuviosta nähdään, että sekä riskien arviointi että riskien hallitseminen koostuvat kumpikin kolmesta eri prosessista. Riskien arvioinnin kohdalla nämä ovat tunnistaminen, analysointi ja priorisointi. Riskien tunnistamisprosessi pyrkii identifioimaan ja jollain tapaa listaamaan mahdollisia riskejä. Analysointiprosessi tuottaa tunnistetuista riskeistä analyysin, jonka avulla riskit voidaan järjestää vaikutus- ja todennäköisyysperusteisesti kolmannessa prosessivaiheessa (Aslam, 2017).

Suunnittelu-, ratkaisu- ja monitorointiprosessi muodostavat puolestaan riskien hallitsemisen kokonaisuuden. Suunnitteluprosessin tavoitteena on pyrkiä löytämään keinoja riskien ratkaisuprosessin toteuttamiseksi. Näiden keinojen avulla päästään ratkaisuun, joka voi riskienhallinnassa tarkoittaa esimerkiksi riskien välttämistä, sietämistä, vaikutuksen pienentämistä tai hyväksyntää. Monitorointiprosessin tarkoitus on erilaisia valvontatyökaluja hyödyntäen seurata mahdollisten riskien realisoitumista ja kerätä niistä dataa organisaatiolle seuraavien projektien riskienhallinnan suunnittelun tueksi (Aslam, 2017).

Valtiovarainministeriö (2017) esittää riskienhallintaprosessin malliksi viisiosaisen prosessimallin, joka pohjaa ISO 31000-standardiin. Prosessimalli on

esitetty seuraavassa kuviossa (kuvio 2). ISO 3100-standardi on esitelty myöhemmin lyhyesti luvussa 4.6.2.



KUVIO 2 Esimerkki riskienhallintaprosessista (Valtiovarainministeriö, 2017; SFS-ISO 31000)

Kuviosta nähdään, että mallissa on yhteneväisyyttä Aslamin malliin. Esimerkiksi koko riskien arviointiprosessi on lähes identtinen. Eroavaa on suoran kahtiajaon puuttuminen riskien arvioinnin ja hallinnan väliltä. Lisäksi kyseinen ISO 31000-standardin mukainen malli on luotu enemmän prosessimallin näkökulmasta kuin Aslamin malli. Valtiovarainministeriön mallissa varsinainen riskienhallintaprosessi alkaa toimintaympäristön määrittelystä. Siinä tarkennetaan riskien arvioinnin kohde, eli tehdään keskeinen rajaus siitä, mitä riskien arviointiin aiotaan sisällyttää ja mitä jätetään sen ulkopuolelle (Valtiovarainministeriö, 2017). Riskien arvioinnin osalta mallit ovat hyvin samankaltaisia, mutta suurin eroavaisuus esiintyy riskien hallitsemiseen. Valtiovarainministeriön mallissa on omana kokonaisuutenaan riskien käsittelyprosessi, jossa määritetään riskikohtaiset toimenpiteet ja niistä vastuussa olevat toimijat. Prosessin sisältö on kuitenkin lähes sama kuin Aslamin mallin 'riskien hallitseminen' -prosessissa.

Lisäksi Valtiovarainministeriön esittelemään ISO 31000-standardin mukaiseen malliin liittyy keskeisinä osina niin seuranta ja katselmointi, joka on osana mallin varsinaista prosessikiertoa, kuin viestintä ja tiedonvaihto, joka puolestaan liittyy jokaiseen yksittäiseen prosessin toimintavaiheeseen kaksisuuntaisin suhtein.

Riskienhallinnalla tarkoitetaan siis koko prosessia, jonka päämääränä on toimintaa uhkaavien riskien tunnistaminen sekä niiden toimenpiteiden määrittäminen, joiden avulla havaitut riskit saadaan minimoitua tai eliminoitua kokonaan (Nippala, 2019).

Riskienhallintamallit ovat täten edellä esiteltyä prosessia kuvaavia malleja tai viitekehyksiä, joiden avulla riskienhallintatyötä voidaan toteuttaa.

4 RISKIENHALLINTAMALLIT KYBERUHKIIN VARAUTUMISEN VÄLINEINÄ

Tähän sisältölukuun sisältyy tiivis yhteenveto kaikista tässä tutkielmassa käytetyistä riskienhallintamalleista. Jokaisen mallin kohdalla on kuvattu kunkin sisältämät ominaisuudet ja niiden käyttötarkoitukset. Vertailussa käytetyt mallit on valittu niiden saavuttaman suosion ja ilmaantuvuuden perusteella, sekä pääosin kill chain-mallien kohdalla saatavilla olevan lähdemateriaalin perusteella.

Tämän kappaleen tarkoituksena on esitellä tutkielmassa vertailtavat riskienhallintamallit kontekstin vuoksi, myöhemmän vertailuvaiheen ymmärtämiseksi. Jo tässä vaiheessa on syytä huomata, että osaa näistä malleista voidaan käyttää myös samanaikaisesti entistä kattavamman puolustuksen kehittämiseksi.

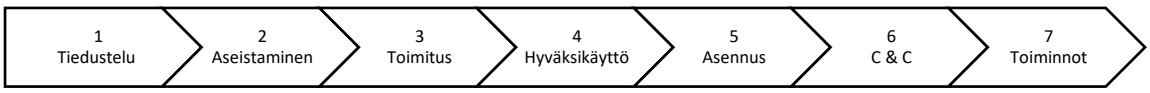
4.1 Cyber Kill Chain-mallit

Tässä tutkimuksessa keskitytään riskienhallintamalleissa pääasiassa kill chain-malleihin, jotka ovat kyberuhkien tunnistamiseen ja ehkäisemiseen kehitettyjä malleja (Lockheed Martin, 2015). Ne perustuvat Yhdysvaltain asevoimien kehittämään kill chain-taktiikkaan, mistä kollektiivinen mallien nimitys kill chain-malleiksi myös juontuu (Kiwia ym., 2017).
Kyberhyökkäyksen uhrin näkökulmasta on erittäin hyödyllistä ymmärtää, miten organisaation sisäisiin tietokoneisiin ja käyttäjätileihin pääsyn avanneet kyberhyökkäykset ja tietomurrot on todellisuudessa toteutettu. Tämän ymmärryksen ja tiedon avulla organisaatiot kykenevät vastaisuudessa havaitsemaan ja estämään mahdollisia hyökkäyksiä toteutumasta, sillä jokainen yksittäinen vaihe on mahdollisuus puolustautumiseen (Donaldson ym., 2015). Tämä ymmärrettiin Lockheed Martinilla, jonka tutkijat julkaisivat vuonna 2011 APT-hyökkäyksiä käsittelevän tutkimuksen. Tutkimuksessa havaittiin, että jokaisessa hyökkäyksessä toistuu sama tapahtumien järjestys ja että tutkimalla tätä tapahtumien ketjua ja sen eri askeleita voidaan hyökkäyksen eteneminen koittaa estää (Donaldson ym., 2015)

4.2 Cyber Kill Chain

Lockheed Martinin Cyber Kill Chain -malli julkaistiin vuonna 2011, kun useat yhtiön tutkijat toteuttivat tutkimuksen kohdistetuista haittaohjelmahyökkäyskampanjoista (APT-hyökkäyskampanjat) ja havaitsivat jokaisen hyökkäyksen noudattavan tiettyä järjestystä (Hutchins ym. 2011). Lockheed Martinin malli oli myös ensimmäinen julkaistu Cyber Kill Chain-malli, ja se tuli tunnetuksi viitekehykseksi, kun DNC:n (Democratic National Committee) tietoverkot hakkeroitiin (Hutchins ym. 2011). Cyber Kill Chain -viitekehys on kyberuhkien tunnistamiseen ja ehkäisyyn tarkoitettu malli (Lockheed Martin, 2015). Se perustuu Yhdysvaltain asevoimien kehittämään kill chain-taktiikkaan (engl. find, fix, track, engage & assess) (Kiwia ym., 2017).

Cyber Kill Chain -mallissa on seitsemän vaihetta, joista jokaisessa hyökkäys voidaan pysäyttää (Lockheed Martin, 2015). Lisäksi jokainen vaihe on osaltaan kriittinen hyökkäyksen pysäyttämisessä, sillä jokaista vaihetta varten voidaan suunnitella suojautumiskeinoja (Yadav & Rao, 2015). Mallissa on edellä mainittujen seitsemän varsinaisen vaiheen lisäksi myös kolme seurantatoimenpidettä paremman kyberturvallisuuden rakentamiseksi, jotka ovat analyysi, rekonstruktio ja joustavuus (Lockheed Martin, 2015).
Kuviossa alla (kuvio 3) on esitelty Cyber Kill Chain-mallin eri vaiheet, jotka jäljentävät kohdistetun haittaohjelmahyökkäyksen (APT) vaiheita.



KUVIO 3 Lockheed Martinin Cyber Kill Chain (Lockheed Martin, 2015)

Mallin vaiheet ja niiden kuvaukset ovat Lockheed Martinin (2015) ja Donaldsonin ym. (2015) mukaan seuraavat:

1. **Tiedustelu**. Tässä vaiheessa hyökkääjä pyrkii löytämään pääsyn kohdetietoverkkon tekemällä yksityiskohtaista tutkimusta. Tutkimus voi olla myös verkkosivujen, sähköpostitilien tai sosiaalisen median profiilien hyödyntämistä, hyökkäystavasta riippuen. Tehtyä tutkimusta hyödyntäen hyökkääjä tunnistaa sekä valitsee hyökkäyksen kohteen tai kohteet (Donaldson ym., 2015). Vastavuoroisesti tietoverkkoa hallinnoiva 'puolustaja' pyrkii havaitsemaan hyökkääjän toimet.
2. **Aseistaminen**. Tämän vaiheen aikana hyökkääjä valmistelee hyökkäyksen. Puolustajan on mahdotonta havaita itse aseistamista, mutta esimerkiksi haittaohjelma voidaan analysoida, jos sellainen havaitaan puolustajan järjestelmässä. Tyypillisesti aseistaminen tapahtuu haittaohjelman yhdistämisellä johonkin kohteeseen lähetettävään tiedostoon, useimmiten

Adobe Portable Document Format (PDF) -tiedostoon tai Microsoft Office -tiedostoon (Donaldson ym., 2015).

3. **Toimitus**. Toimitusvaiheessa vihollinen sananmukaisesti toimittaa haittaohjelman kohdeympäristöön ja täten käynnistää hyökkäysoperaation. Puolustajalle tämä on koko kill chain-mallin kriittisin vaihe hyökkäyksen estämisen näkökulmasta. Donaldsonin ym., (2015) mukaan tyypillisimpiä toimitustaktiikoita ovat liitetiedostot sähköposteissa, verkkosivut sekä USB-laitteet.
4. **Hyväksikäyttö**. Hyväksikäyttövaihetta estääkseen tai viivyttääkseen puolustaja voi esimerkiksi nostaa käyttäjien tietoisuustasoa tai muin keinoin pyrkiä edistämään turvallisemman IT-ympäristön kehitystä, mutta tässä Cyber Kill Chain-mallin vaiheessa hyökkääjä saavuttaa lopulta pääsyn kohteeseen. Kun haittaohjelma on saatu toimitettua onnistuneesti, alkaa se hyväksikäyttää jotain kohdejärjestelmän haavoittuvuutta tai sovellusta pystyäkseen ajamaan hyökkääjän koodia uhrin järjestelmäympäristössä (Donaldson ym., 2015).
5. **Asennus**. Tässä vaiheessa hyökkääjän haittaohjelma asentaa etähallittavan Troijalaisen tai niin kutsutun 'takaoven' kohdejärjestelmään, jonka tarkoituksena on ylläpitää hyökkääjän pysyvä pääsy järjestelmään (Donaldson ym., 2015). Asennusvaiheen aikana puolustaja voi pyrkiä havaitsemaan haittaohjelman asennuksen järjestelmässään ja estämään hyökkäyksen etenemisen.
6. **Komento & Kontrolli**. Tästä vaiheesta käytetään myös nimityksiä C&C ja C^2. Tämän vaiheen aikana hyökkääjän haittaohjelma pyrkii mahdollistamaan toimivan etäyhteyden, jotta hyökkääjä voi kontrolloida ja käskyttää saastuneita laitteita. Tyypillisesti etäyhteys haittaohjelmaan luodaan hyökkääjän omien Internet-palvelimien kautta (Donaldson ym., 2015).
7. **Toiminnot**. Mallin viimeisessä vaiheessa hyökkääjä saavuttaa tavoitteensa (Lockheed Martin, 2015). Tyypillinen tavoite on usein tietojen suodattaminen, tiedon kerääminen, salaus ja poimiminen kohdeympäristöstä. Lisäksi loukkaukset tiedon eheyteen ja saatavuuteen voivat olla mahdollisia tavoitteita (Donaldson ym., 2015). Lisäksi hyökkääjä voi käyttää alkuperäistä kohdetta välietappina muiden järjestelmien saastuttamisessa ja liikkuakseen poikittain tietoverkon sisällä (Donaldson ym., 2015). Tässä vaiheessa puolustajan tärkeimpänä tehtävänä on analysoida tarkasti tapahtumien kulku ja siihen johtaneet syyt, sekä pyrkiä palauttamaan järjestelmänsä toimintakyky (Lockheed Martin, 2015).

4.3 ATT&CK viitekehys

ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) viitekehys on MITRE:n kyberturvallisuuden ammattilaisille kehittämä avoimen lähdekoodin rakenne. Se on luotu, jotta alalla olisi yleisesti hyväksytty, yhtenäinen

toimintamalli kuvaamaan kyberhyökkäyksien elinkaaren vaiheita eri teknologia-alueilla (Legoy, 2019). Teknologia-alueilla tarkoitetaan seuraavaa:

1. ”Yritys (engl. ”enterprise)”, joka kuvaa käyttäytymistä Linux, macOS ja Windows käyttöjärjestelmiä hyödynnettäessä.
2. ”Mobiili”, joka keskittyy puolestaan Android ja iOS käyttöjärjestelmiin.

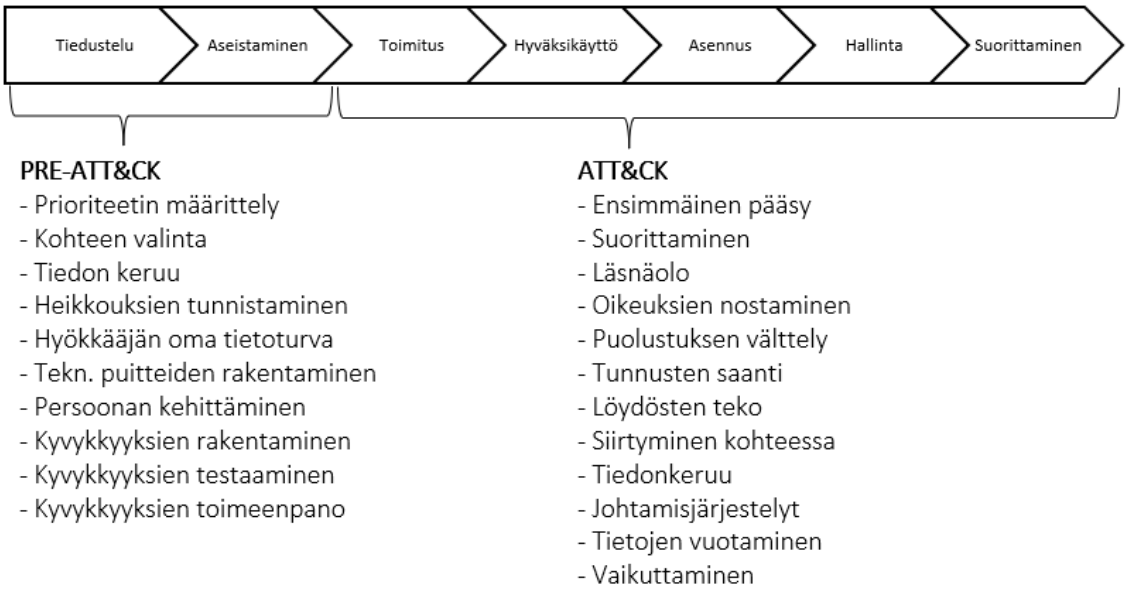
Näiden alueiden lisäksi mallia pystytään hyödyntämään myös kyberhyökkäystä edeltävässä niin kutsutussa tiedustelu- ja aseistautumisvaiheessa, jota varten viitekehykseen on luotu lisäksi PRE-ATT&CK-nimike (Legoy, 2019).

ATT&CK viitekehyksen tavoitteena on Stromin (2018) mukaan parantaa yritysten kyberhyökkäysten havaitsemiskykyä mallintamalla niitä askelia, mitä pitkin hyökkääjä on mahdollisesti edennyt toimissaan.

ATT&CK-mallin kuvaama hyökkäys jaetaan seuraaviin kahteen osaan: hyökkääjän päämäärät hyökkäyksen aikana eli *taktiikat* sekä *tekniikat* ja *toimenpiteet*, joiden avulla hyökkääjä pyrkii saavuttamaan päämääränsä (Pols, 2017). ATT&CK noudattaa seitsemänvaiheista toimintamallia, joka on hyvin samankaltainen muiden vastaavien viitekehysten rungon kanssa (Straub, 2020). Se koostuu vaiheista, jotka ovat:

- Tiedustele
- Aseista
- Toimita
- Hyväksikäytä
- Hallitse
- Suorita
- Ylläpidä

Taktiikat puolestaan nähdään hyökkäyksen perustuksina ja ne voivat ilmentyä eri vaiheissa hyökkäystä – niillä ei siis ole tiettyä määrättyä esiintymisjärjestystä (Pols, 2017). Alla esitetystä kuviosta (kuvio 4) nähdään, että mallissa on kaksi päävaihetta. Vertailun vuoksi vaiheet on kuvattu suhteessa Lockheed Martinin Cyber Kill Chain-mallin mukaiseen hyökkäyksen elinkaareen. Esivaihe (engl. ”pre-phase”) PRE-ATT&CK kattaa valmistelutekniikat eli tiedustelun ja aseistamisen. Hyökkääjä pyrkii toteuttamaan hyökkäyksen valmisteluvaiheet kohdeorganisaation näkökentän ulottumattomissa, joka vaikeuttaa niiden havaitsemista. Toinen päävaiheista, ATT&CK-vaihe kuvaa itse hyökkäyksen, joka koostuu 11 erilaisesta taktiikasta ja yhdestä tavoitteesta (Strom, 2018). Tässä työssä keskitytään käsittelemään varsinaista ATT&CK-päävaihetta.



KUVIO 4 PRE-ATT&CK ja ATT&CK-mallien taktiikat kuvattuna vertailun vuoksi suhteessa Cyber Kill Chain-mallin mukaiseen hyökkäyksen elinkaareen (Strom, 2018)

Yhteensä ATT&CK-mallissa on 14 eri taktiikkaa ja niiden sisällä lukuisia eri tekniikoita. Seuraavien 12 taktiikan voidaan nähdä olevan mallin keskeisimmät. Hallinta, suoritus sekä ylläpitovaiheen aikana viitekehys käyttää taktiikoita saavuttaakseen asetetut tavoitteet (Straub, 2020). Nämä taktiikat ja niiden selitykset ovat Lehdon (2022) mukaan seuraavat:

1) **Ensimmäinen sisäänpääsy**. Hyökkääjä pyrkii pääsemään sisään tietoverkkoon.
2) **Suorittaminen**. Hyökkääjä pyrkii ajamaan haitallisen koodin kohdeympäristössä.
3) **Läsnäolo**. Hyökkääjä pyrkii säilyttämään ja ylläpitämään saavuttamaansa sisäänpääsyä, eli ns. pitämään jalkaa oven välissä.
4) **Oikeuksien nostaminen**. Hyökkääjä pyrkii saavuttamaan korkeamman tason käyttöoikeuksia.
5) **Puolustuksen välttely**. Hyökkääjä pyrkii välttelemään havaituksi tulemista.
6) **Tunnuksien saanti**. Hyökkääjä pyrkii varastamaan käyttäjätunnuksia ja salasanoja.
7) **Löydösten teko**. Hyökkääjä pyrkii tutustumaan kohdeympäristöön.
8) **Siirtyminen kohteessa**. Hyökkääjä pyrkii liikkumaan kohdeympäristön sisällä.
9) **Tiedonkeruu**. Hyökkääjä pyrkii keräämään tavoitteitansa tukevaa tietoa kohdeympäristöstä.
10) **Komento & Kontrolli**. Hyökkääjä yrittää kommunikoida vaarantuneiden järjestelmien kanssa saadakseen ne hallintaansa.
11) **Tietojen vuotaminen**. Hyökkääjä yrittää varastaa dataa.

12) **Vaikuttaminen**. Hyökkääjä yrittää manipuloida, keskeyttää tai tuhota kohdejärjestelmän tai sen datan.

Tämän listauksen perusteella ATT&CK muistuttaa suuresti muita vastaavia hyökkäyksen elinkaarta jäljitteleviä viitekehyksiä. ATT&CK-malli eroaa kuitenkin vertaisistaan siinä, kuinka laajalti se ottaa huomioon hyökkäyksen ja hyökkääjän mahdollisen liikkeen järjestelmän sisällä. Useilla vastaavilla malleilla kyvykkyys toteuttaa hyökkäystä lieventäviä toimia rajoittuu liian kapeaan tarkastelualueeseen (Strom, 2018).

4.4 Microsoft STRIDE

STRIDE (engl. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) on Microsoftin kehittämä riskienhallintamalli ja uhkien havaitsemisen keskittyvä menetelmä. Sen toiminta perustuu muistitekniseen metodiin, jonka mukaan uhat ovat järjestelmän tai laitteen ominaisuuksien (negatiivisia) vastakohtia. STRIDE on varsin hyödyllinen muistisääntö kaikenlaiseen teknologiaan kohdistuvien uhkien tunnistamisessa. Malli luokittelee uhat kuuden eri periaatteen mukaan, joiden perusteella uhkia voi syntyä. Nämä ovat esitetty myöhemmin taulukossa 3 (taulukko 3) (Shostack, 2014). Tämän lisäksi STRIDE-mallissa on viisi vaihetta uhka-analyysin suorittamiseksi (Khan, ym. 2018). Khanin ym. (2018) mukaan nämä vaiheet ovat seuraavat:

- Purkaminen
- Tietovuokaavioiden luominen
- Tietovuokaavioiden analysointi uhkien varalta
- Haavoittuvuuksien tunnistaminen uhkien perusteella
- Lieventävien lähestymistapojen kehittäminen

STRIDE suunniteltiin auttamaan turvallisempien ohjelmistojen kehittämisessä, tavallisesti kohdattavien hyökkäystyyppien tunnistamisen avulla. Mallin uhat ovat kuten edellä mainittua, täysin vastakohtia ominaisuuksille, joita järjestelmässä voitaisiin toivoa olevan: aitoutta, eheyttä, kiistattomuutta, luottamuksellisuutta, saatavuutta sekä tunnistautumista. Mallia käytetäänkin uhkien etsimisessä pääasiassa vain niiden asioiden tunnistamiseen, jotka voivat epäonnistua. Epäonnistumisen takaista mekaniikkaa voidaan arvioida paremmin myöhemmässä vaiheessa, kun mallin toimintaa ymmärretään täydellisemmin (Shostack, 2014).

STRIDEN tarkoituksena ei ole toimia varsinaisena kyberhyökkäysten kategoriointiin tarkoitettuna työkaluna, vaan yksinkertaisesti sen tehtävä on vain tunnistaa hyökkäyksiä. Shostack (2014) toteaa, että on tärkeämpää sijoittaa resursseja hyökkäyksen torjumiseen, kuin sen sijoittamiseen oikeaan kategoriaan, jos hyökkäys on jo tunnistettu.

Taulukko alla (taulukko 3) esittää aiemmin tekstissä mainitut STRIDE-mallissa käsiteltävät uhat, niiden selityksen sekä kohteena olleen ominaisuuden (Shostack, 2014).

TAULUKKO 3 STRIDE-mallin uhat ja selitykset (Shostack, 2014)

Uhka	Selite	Kohdeominaisuus	Hyökkääjän toimet
Huijaaminen, väärentäminen (engl. ”Spoofing”)	Hyökkääjä pyrkii esittämään olevansa joku tai jokin muu kuin oikeasti on	**Tunnistautuminen**	Tiedostojen uudelleennimeäminen, Tiedostojen luominen, IP-vakoilu ja uudelleenohjaaminen, Identiteettivarkaus, käyttäjätilin hakkerointi
Peukalointi (engl. ”Tampering”)	Jonkin levyllä, tietoverkossa tai muistissa olevan muokkaamista	**Eheys**	Tiedoston muokkaaminen, linkkien muokkaaminen, koodin muokkaaminen, datavirran uudelleenohjaus
Kieltäminen (engl. ”Repudiation”)	Jonkin tehdyn tai vastuun kieltämistä. Kieltäminen voi olla rehellistä tai valheellista, olennaista ovat todisteet	**Kiistattomuus (engl. ”Non-repudiation”)**	Viestin vastaanottamisen kiistäminen, Petoksen uhriksi joutumisen väittäminen, toisen henkilön käyttäjätilin käyttäminen, toisen maksuvälineen käyttäminen
Tietojen vuotaminen	Tiedon tai datan toimittaminen sellaiselle taholle, jolla ei ole kyseiseen materiaaliin oikeutta	**Luotettavuus**	Salaisuuksien poimiminen virheilmoituksista, heikkojen tietokantojen käyttöoikeuksien hyväksikäyttö, datan lukeminen tietovirrasta tai -varastoista, opiskelee toimintaa tietoliikennettä analysoimalla, kirjautumistietojen hyväksikäyttö, tiedostonimien analysointi
Palvelunesto	Palvelun tuottamiseen tarkoitettujen resurssien tarkoituksellinen omaksuminen	**Saatavuus**	Muistin (RAM tai levy) tai laskentatehon (CPU) tukahduttaminen, tietovaraston täyttäminen, järjestelmän hidastaminen kyselyillä, verkkoresurssien kuluttaminen
Oikeuksien väärentäminen	Sallitaan jonkun tehdä jokin toimi, johon kyseisellä toimijalla ei ole todellista oikeutta	**Valtuuttaminen**	Virheellisten kirjautumistietojen syöttäminen ohjelmistovirhettä tavoitellen, pääsy lukemaan tai kirjoittamaan muistiin, levylle talletettujen asioiden muokkaaminen tekemään toista kuin valtuutettu käyttäjä toivoo

Microsoft (2022) määrittää verkkoartikkelissaan STRIDE-mallissa käsiteltävät uhat ja niiden selitykset, joihin Shostack (2014) tietonsa pohjaa. Microsoftin oma mallin esittely on hyvin pelkistetty ja kuuluu seuraavasti:

Huijaaminen sisältää toisen käyttäjän todennustietojen, kuten käyttäjätunnuksen ja salasanan, laittoman hankkimisen ja käyttämisen.

Peukalointi sisältää tietojen haitallisen muuttamisen. Esimerkiksi luvattomasti tehdyt muutokset tietokannassa oleviin pysyviin tietoihin sekä avoimessa verkossa (esim. Internet) kahden tietokoneen välillä virtaavien tietojen muuttaminen.

Kieltäminen liittyy käyttäjiin, jotka kieltävät toiminnon suorittamisen ilman, että muut osapuolet pystyvät todistamaan toisin – esimerkiksi käyttäjä suorittaa laittoman toiminnon järjestelmässä, jolla ei ole kykyä jäljittää kiellettyjä toimintoja. Kiistattomuudella vastavuoroisesti tarkoitetaan järjestelmän kykyä torjua kieltäytymisuhkia.

Tietojen vuotaminen käsittää tietojen paljastamisen henkilöille, joilla ei pitäisi olla pääsyä niihin – tällä tarkoitetaan esimerkiksi käyttäjien kykyä lukea tiedostoa, johon heillä ei ole annettu käyttöoikeutta tai tunkeilijan mahdollisuutta lukea dataa sen siirtyessä kahden tietokoneen välillä.

Palvelunesto - Palvelunestohyökkäykset (DoS) estävät palvelun todellisilta käyttäjiltä esimerkiksi saamalla Web-palvelimen tilapäisesti pois käytöstä tai saatavilta. DoS-uhilta on suojauduttava järjestelmän saatavuutta ja luotettavuutta parantaakseen.

Oikeuksien väärentämisellä tarkoitetaan sitä, että valtuuttamattomat käyttäjät saavat valtuudet käyttöoikeuksiin ja sisäänpääsyyn ja siten riittävät oikeudet vaarantamaan tai tuhoamaan koko järjestelmän. Valtuutusuhkia ovat tilanteet, joissa hyökkääjä on tunkeutunut kaikkiin järjestelmän suojauksiin ja tullut osaksi luotettua järjestelmää.

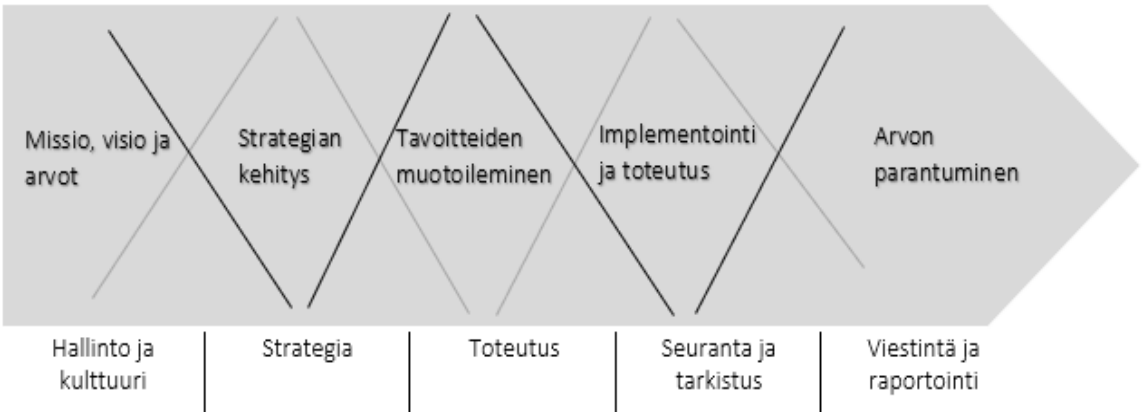
4.5 COSO-ERM

Committee of Sponsoring Organizations of the Treadway Commission eli tunnetummin COSO, on yksityinen ja riippumaton, paremman ja eettisemmän kansainvälisen elinkeinoelämän edellytysten puolestapuhuja ja merkittävä toimija. COSO on perustettu vuonna 1985 ja vuosina 1992 ja 2004 se julkaisi sisäisen valvonnan mallinsa, josta moni strategiamalli ja yritysten toimintatapamalli on saanut perusteensa. COSO-malli on maailmanlaajuisesti käyttöönotettu malli, joka vaikuttaa vankasti eri standardien taustalla. (COSO, 2021; Ilmonen ym., 2010). Mallia on kutsuttu jopa sisäisen kontrollin johtavaksi malliksi (Moeller, 2007).

COSO-ERM-malli, jota tässä työssä tarkastellaan, on julkaistu varsinaisesti ensimmäistä kertaa vuonna 2004 ja sittemmin sitä on päivitetty vuonna 2017 (COSO, 2017). Se on kokonaisvaltaisen organisaatioiden riskienhallinnan (Enterprise Risk Management, ERM) malli (Leino ym., 2005). COSO-ERM-mallin (2004) mukaan riskienhallinnan päämääränä on:

- Strategian ja riskinottohalun yhdenmukaistaminen
- Riskienhallinnallisten ratkaisujen tehostaminen
- Minimoida toiminnalliset yllätykset sekä tappiot
- Toistuvien sekä koko organisaation laajuisten riskien havaitseminen ja hallinta
- Oikeiden tilaisuuksien tunnistaminen ja hyödyntäminen
- Pääoman käytön tehokkuus

COSO-ERM-2017-malli on kuvattu vaihejanana alla olevassa kuvassa (kuvio 5) (COSO, 2017). Uudistettu versio antaa organisaatioille paremman tuen etenkin kyberriskeihin varautumiseen (Rubino, 2018).



KUVIO 5 COSO-ERM-2017-viitekehys riskienhallintaprosessille vaihejanana esitettynä (COSO, 2017)

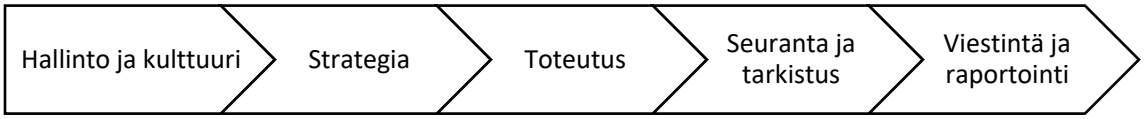
Vuonna 2017 uudistetussa COSO-ERM-mallissa riskienhallinnan käsite koostuu joukosta periaatteita, jotka on jaettu viiteen toisiinsa liittyvään komponenttiin. Näitä edellä mainittuja periaatteita viitekehyksessä on yhteensä 20, ja ne on havainnollistettu prosessin vaiheiden ohella taulukossa alla (taulukko 4). Periaatteiden joukko kattaa kaiken prosessin sisällön aina hallinnasta valvontaan (COSO, 2017).

TAULUKKO 4 COSO-ERM-2017 viitekehyksen periaatteet (COSO, 2017).

Hallinto ja kulttuuri	Strategia	Toteutus	Seuranta ja tarkistus	Viestintä ja raportointi
1.Hallituksen riskinhallinta 2. Toimintamallien luominen	6.Toimintaympäristön analysointi 7. Riskinottohalun määrittely 8. Vaihtoehtoisten strategioiden arviointi	10. Riskien tunnistaminen 11. Vakavuuden arviointi 12. Riskien priorisointi	15. Muutosten arviointi 16. Riskien ja suorituskyvyn arviointi 17. Pyrkimys kokonaisvaltaisen	18. Tiedon ja teknologian hyödyntäminen 19. Riskitiedon viestintä 20. Kulttuurin, riskin ja

3. Halutun kulttuurin määrittely 4. Sitoutuminen ydinarvoihin 5. Yksilöiden kehittämisen ja osaamisen tukeminen, ylläpito ja motivointi	9. Toiminnan tavoitteiden asettaminen	13. Vastuiden määrittäminen 14. Riskiportfolion luominen ja ylläpito	riskienhallinnan kehitykseen	suorituskyvyn raportointi

Seuraavassa kuviossa (kuvio 6) COSO-ERM-2017-mallin vaiheet on esitetty perinteisessä prosessimallin muodossa. Tämän jälkeen mallin vaiheet ja niiden vastuut sekä ominaisuudet on esitelty COSO Enterprise Risk Management: Integrating with Strategy and Performance -tiivistelmän mukaisesti.



KUVIO 6 COSO-ERM-2017-viitekehyksen vaiheet esitettynä perinteisenä prosessimallina (COSO, 2017)

Ensimmäinen mallin komponenteista on **hallinto ja kulttuuri**, jonka tehtävänä on varmistaa valvontavastuun vakiintuminen sekä vahvistaa organisaation riskienhallinnan merkitystä. Kulttuurisesta näkökulmasta komponentin osana on organisaation sisäiset eettiset arvot, toivottu käyttäytyminen sekä riskin ymmärtäminen. Tämän periaatteen tarkoituksena on auttaa laadukkaan pohjan luomisessa organisaation riskienhallinnalle sekä edistää sen sisäistämistä organisaatiossa (COSO, 2017).

Seuraava komponentti on **strategia ja tavoitteiden asettaminen**. Organisaation riskienhallinta, strategia sekä tavoitteiden asettaminen toimivat yhdessä strategian suunnitteluprosessissa. Tässä vaiheessa kartoitetaan organisaation riskienottokyky ja asetetaan se samaan linjaan organisaation strategian kanssa. Osa riskienottokyvyn määritystä on myös valmistella strategiat riskien tunnistamiseksi, riskien arvioimiseksi sekä riskeihin vastaamiseksi. Strategia ja suunnittelu ovat suuressa roolissa organisaation riskienhallinnan toteutuksen ja onnistumisen kannalta (COSO, 2017).

Suorittaminen on mallin kolmas komponentti. Se käsittää organisaation strategian ja liiketoiminnan tavoitteiden saavuttamiseen liittyvien riskien tunnistamisen, arvioimisen sekä riskien vakavuuden arvioinnin. Tunnistamisen ja arvioinnin jälkeen organisaatio valitsee toimet reagoidakseen riskiin, sekä tiedostaa kuinka suuren osan riski on kuluttanut riskienottokyvystä. Viimeisenä toimena riskistä tulee raportoida avainasemassa oleville sidosryhmille (COSO, 2017).

Läpikäynti ja tarkistus on mallin neljäs komponentti ja sen avulla organisaatio voi arvioida riskienhallinnan komponenttien toimintaa ajan ja muutosten

saatossa sekä riskienhallinalle asetettujen tavoitteiden täyttymistä. Tämän perusteella saadaan luotua kuva siitä, mitä mahdollisia tarkennuksia tai korjauksia on syytä riskienhallintaprosessiin tehdä (COSO, 2017).

Informaation ja raportoinnin komponentti on viides ja viimeinen mallin komponenteista. Siinä tunnistetaan organisaation riskienhallinnan olevan jatkuva, koko organisaation laajuinen oleellisen tiedon hankkimisen ja jakamisen prosessi (COSO, 2017).

COSO-ERM-viitekehyksen keskeisin toimintaperiaate on jokaisen yksittäisen osatekijän huomioiminen riskienhallinnassa. Täten pyritään varmistamaan laajalti, että organisaatio ja sen johto pystyy tunnistamaan ja hallitsemaan organisaation strategiaan ja sen toiminnan tavoitteisiin vaikuttavia riskejä (COSO, 2017). Mallia voidaan soveltaa niin eri tavoin toimiville kuin eri kokoisille organisaatioille.

4.5.1 COSO-ERM:n vertailukelpoisuus kyberuhkiin valmistautumisen kontekstissa

COSO-ERM-2017-mallin osalta vertailun toteuttaminen osoittautui oletettua haastavammaksi. Lähdemateriaalia löytyi pääasiassa vain mallin yleiseen vertailuun soveltuvien aineistojen muodossa, eikä tapaustutkimusta mallin käytöstä kyberuhkien vastaiseen reagointiin löytynyt, vaikka COSO ERM-viitekehys on laajalti käytetty riskienhallinnan viitekehys. Seuraavaksi analysoidaan kuitenkin lyhyesti COSO-ERM-2017 ja aikaisemman COSO-ERM mallin havaittuja yleisiä heikkouksia ja vahvuuksia.

COSO ERM-2017-mallin suurimpia heikkouksia ovat Diasin (2017) mukaan itse riskin käsittely pelkästään negatiivisesta näkökulmasta ja mallin keskittyminen vahvasti vain riskin lieventämiseen sekä lähes pelkästään sisäisiin tekijöihin ulkoisten tekijöiden näkökulman sijaan. Myös useat eri tavat riskin määrittelemiseksi ovat jo sellaisenaan omiaan aiheuttamaan ristiriitaa riskienhallintaprosessissa (Elms, 2019).

Dias (2017) esittelee myös muutamia teknisiä haasteita, mitä COSO-ERM-2017-mallista voidaan tunnistaa. Näitä ovat mm. riskikriteerien asettamisessa sidosryhmien ja heidän tavoitteidensa huomiotta jättäminen, riskien näkeminen tapahtumina, jotka eivät ole liitoksissa tavoitteisiin sekä riskin esiintymisen väärä arviointi todennäköisyyden ja seurausten suhteen sekä tästä seuraavat ”haamuriskit”.

Lisäksi mallissa epäselvyyttä voi aiheuttaa myös käsitteiden määrittely. Diasin (2017) mukaan riskinsietokyky ja riskinottohalu käsitteinä sekoittuvat viitekehyksessä usein keskenään, mikä aiheuttaa haasteita.

COSO-ERM-viitekehyksen etuna on selvästi se, että mallin avulla voidaan tunnistaa ja valita osuvin riskeihin reagoinnin tapa: riskien välttäminen, vähentäminen, jakaminen tai hyväksyminen (Almgren, 2014). Sen on lisäksi esitetty olevan kattavin organisaation riskienhallintamalli verrattuna muihin viitekehyksiin (Rubino, 2018). COSO-ERM-viitekehyksellä pystytään myös virtaviivaistamaan helpommin riskiä, kasvua sekä tulosta mikä puolestaan johtaa mahdolliseen liiketoiminnan kehitykseen (Almgren, 2014).

Rubinon (2018) mukaan vuoden 2017 päivitys COSO-ERM-malliin parantaa kuitenkin sen kyberriskien hallintakykyä sekä keskittyy varsinaisesti henkilöstöä tukevaan tehokkaaseen raportointiin, jotta riskin, kulttuurin ja suorituskyvyn suhteita ymmärretään paremmin. Myös päätöksenteko strategian ja tavoitteiden asettamisesta, hallinnosta ja päivittäisistä toiminnoista on parantunut.
Vuonna 2017 päivitetty malli ottaa kuitenkin etenkin edellä mainittuja heikkouksia paremmin huomioon, erityisesti kulttuuria ja strategiaa painottamalla. Kuitenkin useat yritykset käyttävät riskienhallinnassa vaihtoehtoista ratkaisua: ISO31000-standardin mukaista mallia, yksinkertaisesti vain siksi, että se on helppokäyttöisempi (Dias, 2017).

Koska lähdekirjallisuutta COSO-ERM-2017-mallin käytöstä kyberuhkien torjuntaan tai kyberuhilta varautumiseen ei löytynyt, ei sitä voida sisällyttää tutkielman vertailuosioon. Mallin yleisen kyvykkyyden esittelyn ohessa herääkin kysymys, miksei COSO-ERM-2017-mallista löydy tutkimusta kyberuhkiin reagoimisen välineenä, sillä mallin suosio on maalimanlaajuista organisaatioiden riskienhallinnan parissa? Yksi syy voidaan nähdä olevan se, että malli on korkeamman tason riskienhallintamalli, joka keskittyy painotettuna kokonaisvaltaiseen yritysjohtamiseen ja organisaation hallintaan itse riskienhallinnan korostamisen sijaan. COSO-ERM-2017-mallin käyttäminen kyberuhkiin reagoimisen välineenä on mahdollista, muttei kovin tarkoituksenmukaista, sillä tarjolla on laaja skaala erilaisia nimenomaisesti kyberuhkien torjuntaan ja lievitykseen räätälöityjä riskienhallintamalleja.

4.6 Muita malleja

Tässä kappaleessa kuvataan varsin lyhyesti kaksi muuta riskienhallinnan työkalua. Mandiantin Attack Lifecycle-malli on hyvin samankaltainen kuin muut kill chain-mallit, mutta tutkielman tarkoituksen kannalta sen sisällyttäminen osaksi vertailua ei ollut mielekästä. Sen lisäksi on olemassa myös useita hyvin samankaltaisia malleja, joita ei vertailuun sisällytetty samoista syistä. ISO 31000-standardi puolestaan on maailmanlaajuinen riskienhallintaprosessin malli, jonka mukaista prosessimallia sivuttiin jo tutkielman luvussa 3.1.

4.6.1 Mandiant's Attack Lifecycle

Mandiantin Attack Lifecycle-malli kuvaa APT-hyökkäykset syklimallisena. Malli koostuu kahdeksasta tasosta, jotka ovat esitiedustelu, ensimmäinen murtautuminen, jalansijan saaminen, oikeuksien korottaminen, sisäinen tiedustelu, siirtyminen kohteen sisällä, läsnäolon ylläpito ja tehtävän valmiiksi saattaminen. Mallin vaiheiden 3–6 ei tarvitse ilmentyä tietyssä järjestyksessä joka kerta ja sama sykli toistuu APT-ryhmien päästyä tietoverkon sisään niin kauan, kunnes ne poistetaan tietoverkosta (Lehto, 2022).

4.6.2 ISO 31000-standardi

ISO 31000-standardi on ISO:n (International Organization for Standardization) eli kansainvälisen standardisoimisjärjestöjen liiton riskienhallintaprosessin standardi. ISO 31000-standardi on tarkoitettu käyttäjille, jotka riskejä hallitsemalla, päätöksiä tekemällä, suorituskykyä parantamalla sekä tavoitteita asettamalla ja saavuttamalla kasvattavat organisaation arvoa sekä säilyttävät sitä. Standardi on yleinen toimintamalli, jota voidaan soveltaa toimialasta ja riskienhallintatyypistä riippumatta. Standardia on mahdollista käyttää kaikissa organisaation elinkaaren vaiheissa ja sitä voidaan soveltaa organisaation kaikkiin toimintoihin (SFS ISO 31000, 2018).

4.7 Mallien vertailu

Tässä kappaleessa vertaillaan aikaisemmissa kappaleissa esiteltyjen kill chain-pohjaisten mallien toimintaa ja ominaisuuksia toisiinsa. Tavoitteena on arvioida näiden mallien kyvykkyyttä toimia kyberuhkien ehkäisyn välineinä niiden ominaisuuksien, hyötyjen, puutteellisuuksien sekä käyttötapojen avulla, sekä määrittää se malli, jota käyttämällä riskien torjunnalle tai tässä kontekstissa kyberuhilta puolustautumiselle asetetut tavoitteet voidaan parhaiten saada täyttymään. Lisäksi vertailussa keskitytään mallien ominaisuuksien eroavaisuuksiin ja niiden vaikutuksiin mallien käyttötavoissa. Vertailun havainnollisuuden tehostamiseksi pääkohdat on pyritty esittämään taulukkomallisesti, kuten seuraavassa taulukossa (taulukko 5), jossa mallien avainominaisuudet on esitetty.

TAULUKKO 5 Mallien avainominaisuudet mukaillen Straubin (2020) taulukkoa

Viitekehys	**Erityisominaisuudet**
Cyber Kill Chain	- Asennustoimien erittely hyväksikäyttö- ja valvontatoimista
ATT&CK	- Ylläpitovaiheen tunnistaminen - Kymmenen taktiikkakategorian tunnistaminen käytettäväksi ohjaamis-, suorittamis- ja ylläpitovaiheen ajaksi
STRIDE	- Tietovirtaperusteinen menetelmä
COSO-ERM-2017	- Hallinnon ja kulttuurin korostaminen strategian ja tavoitteiden asettamisessa, keskittyminen kokonaisvaltaiseen organisaation riskienhallintaan

Vaikka esitellyillä viitekehyksillä (Cyber Kill Chain, ATT&CK, STRIDE & COSO-ERM-2017) onkin jonkin verran käsitteellistä samankaltaisuutta, sekä Cyber Kill

Chain- ja ATT&CK-viitekehyksissä on varsin huomattavaa päällekkäisyyttä, on jokaisella mallilla kuitenkin itselleen ainutlaatuisia ominaisuuksia (Straub, 2020).

4.7.1 Cyber Kill Chain- ja ATT&CK-mallin vertailu

Cyber Kill Chain- ja ATT&CK-viitekehyksistä voidaan tunnistaa keskenään eniten samankaltaisuuksia, sillä malleissa on varsin yhdenmukaiset vaiheet (Straub, 2020). Näiden viitekehysten vaiheiden vertaileva havainnollistus on toteutettu taulukossa 6 (taulukko 6).

TAULUKKO 6 ATT&CK ja Cyber Kill Chain-mallien samankaltaisuudet (Straub, 2020)

Cyber Kill Chain	**ATT&CK**
Tiedustelu	Tiedustele
Aseistaminen	Aseista
Toimitus	Toimita
Hyväksikäyttö	Hyväksikäytä
Asennus	-
Komento & Kontrolli	Hallitse
Toiminnot	Suorita
-	Ylläpidä

Eroavaisuutta näissä malleissa esiintyy siinä, että Cyber Kill Chain-malli tunnistaa erityisesti tarpeen asennustoimille hyväksikäytön jälkeen, ennen kuin kontrollitoimet pystytään aloittamaan. ATT&CK-malli puolestaan tunnistaa selkeästi tarpeen jälkitoimille eli ylläpitovaiheelle. Suorita- ja ylläpidä-vaiheiden voidaan nähdä toimivan toisiaan täydentävästi ja tarpeen vaatiessa, tietyissä sykleissä (Straub, 2020).

Puolestaan yksi tärkeimmistä ATT&CK:n muista malleista erottavista ominaisuuksista on sen abstraktiotaso hyökkääjän taktiikoita ja tekniikoita kuvattaessa. Mallin ominaisuus heijastaa tehokkaasti muun muassa hyökkääjän toimia, toimien relaatioita sekä toimien seurauksia hyökkääjän tavoitteisiin nähden. Nämä seikat tekevät siitä erittäin sopivan työkalun kokonaisvaltaiseen ja loogiseen riskienhallintaan (Strom, ym. 2018).

Lockheed Martinin Cyber Kill Chain-viitekehys on Pajalan (2020) mukaan käytetyin malli kyberuhkien vastatoimia suoritettaessa. Cyber Kill Chain-viitekehys on kehitetty kill chain-malleista ensimmäisenä, ja suurin osa kaikista malleista pohjautuu lopulta siihen. Pajalan (2020) mukaan hänen tutkielmansa osoitti, että mikäli hyökkääjä on jo saanut pääsyn sisään järjestelmään, se havaitaan usein vasta seitsemännessä eli viimeisessä vaiheessa, vaikka uhka periaatteessa olisikin mahdollista havaita missä tahansa mallin vaiheessa. Samalla viimeisessä vaiheessa aloitetaan myös toimet uhkaa vastaan.

Hutchins ym. (2011) esittävät Lockheed Martinin Computer Incident Response Teamin vuonna 2009 toteuttaman tapaustutkimuksen perusteella aineistoa Cyber Kill Chain mallin kyvykkyydestä lievittää hyökkäystä jo aikaisemmassa vaiheessa ja sen pysäyttämisestä viimeistään viimeisessä vaiheessa.

Tutkimuksessa havainnoitiin kolmea hyökkäysyritystä, joissa sähköpostiviestin liitetiedostossa toimitettiin haitallisia sovelluksia. Hutchinsin ym. (2011) mukaan viitekehyksen vankan toimintamallin ansiosta puolustajat pystyivät aloittamaan hyökkäystä lieventävät toimet jo toimitusvaiheessa, joka on järjestykseltään kolmas vaihe. Tätä lieventävää toimintaa jatkamalla läpi jäljellä olevien vaiheiden, puolustaja onnistui pakottamaan hyökkääjän luopumaan aikeistaan toteuttaa varsinaiset hyökkäystoimet kohteeseensa viimeisessä, eli seitsemännessä vaiheessa. Myös Pajala (2020) toteaa, että hyökkäystä voidaan mahdollisesti viivyttää jo aikaisemmassa, jopa neljännessä vaiheessa.

4.7.2 STRIDE-mallin vertailu Cyber Kill Chain- ja ATT&CK-malleihin

Microsoftin STRIDE-viitekehyksellä on tiettyjä samankaltaisuuksia ATT&CK- ja Cyber Kill Chain-viitekehyksiin. Straubin (2020) mukaan kaikki näistä viitekehyksistä pyrkivät analysoimaan järjestelmiä havaitakseen mahdollisesti hyväksikäytettävissä olevia heikkouksia. Khan ym. (2018) esittävät tutkimuksessaan havaitsemansa perusteella, että STRIDE-viitekehys auttoi tunnistamaan sen, että hyökkääjä voi saavuttaa tietyn haitallisen tavoitteen monin eri keinoin, eikä pelkästään tietyllä, yhdellä tavalla.

Tämän lisäksi Straub (2020) kuitenkin toteaa, että STRIDE eroaa ATT&CK- ja Cyber Kill Chain-malleista merkittävällä tavalla, joka tulee esiin sen puolustusnäkökulmasta – Straubin (2020) mukaan STRIDE keskittyy selvästi muita edellä mainittuja malleja enemmän pelkästään uhilta puolustautumiseen. Niin ATT&CK kuin Cyber Kill Chain-viitekehyksiä voidaan käyttää suoraan sekä hyökkääviin että puolustuksellisiin ja puolustusta testaaviin toimiin, kun taas STRIDE-malli ei sisällä varsinaisesti työkaluja muuhun kuin puolustavaan käyttöön. Straub (2020) toteaa lisäksi, että hyökkäyskehityksen tukemiseksi STRIDE-viitekehystä käytettäessä voidaan siihen yhdistää jonkin muun viitekehyksen osia.

Seuraava taulukko (taulukko 7) näyttää ATT&CK, Cyber Kill Chain sekä STRIDE-mallit ja niiden hyökkäystä kuvaavat vaiheet suhteessa yleiseen kyberhyökkäyksen elinkaareen. Taulukosta huomataan yksinkertaistettuna myös vertailtavien mallien eroavaisuudet hyökkäyksen vaiheiden mallinnuksessa.

TAULUKKO 7 Vertailumallit suhteessa hyökkäyksen yleiseen elinkaareen (Lehto, 2021)

Hyökkäyksen elinkaari	**MITRE ATT&CK**	**LM Cyber Kill Chain**	**Microsoft STRIDE**
Tiedustelu: kohteen tunnistaminen, sijainti sekä tuntomerkit	1. Tiedustelu	1. Tiedustelu	1. Purkaminen 2. Tietovuokaavioiden luominen
Aseistus: operaation valmistelu ja haittaohjelmat	2. Aseistus	2. Aseistaminen	3. Tietovuokaavioiden analysointi uhkien varalta 4. haavoittuvuuksien tunnistaminen

Sisäänpääsy: pääsy kohdejärjestelmään, läpäisy, sitkeys, hyväksikäyttö, asennus, välttely	3. Sisäänpääsy 4. Suorittaminen 5. Kärsivällisyys 6. Oikeuksien nostaminen 7. Puolustuksen välttteleminen 8. Tunnusten saaminen 9. Löydösten teko	3. Toimitus 4. Hyväksikäyttö 5. Asennus	5. Lieventävien lähestymistapojen kehittäminen
Sivusuuntainen liike: tiedustelu, ympäristön laajentaminen	10. Sivusuuntainen liike		-
Komento & Kontrolli: hyökkäyksen hallinta, läsnäolon ylläpitäminen	11. Komento & Kontrolli	6. Komento & Kontrolli	-
Suorittaminen: datan keruu, manipulointi ja suodatus	12. Tiedonkeruu 13. Tietojen vuotaminen 14. Vaikuttaminen	7. Toiminnot	-
Lopputila: hyökkäyksen päättäminen	-	-	-

Straub (2020) jatkaa eroavaisuudesta puolustautumisnäkökulmassa huomauttamalla, että STRIDE-viitekehyksessä on myös vaiheiden osalta merkittävä sisällöllinen eroavaisuus ATT&CK ja Cyber Kill Chain-viitekehyksiin. Se sisältää ainoana varsinaisen nimetyn puolustuksellisen askeleen mallissa, lieventämisen (engl. mitigation). Muitakin malleja voidaan mahdollisesti käyttää puolustuskäytössä, mutta niissä puolustus ei ole nimetty osa prosessin etenemistä, kuten se on STRIDE-viitekehyksessä. Tämä on esitetty taulukossa (taulukko 8), josta nähdään myös STRIDE-viitekehyksen neljän ensimmäisen vaiheen olevan käytännössä laajennuksia kahdesta ensimmäisestä ATT&CK- ja Cyber Kill Chain-viitekehysten vaiheesta.

TAULUKKO 8 ATT&CK, Cyber Kill Chain sekä STRIDE-mallien vertailu (Straub, 2020)

ATT&CK	Cyber Kill Chain	STRIDE
Tiedustele	Tiedustelu	- Järjestelmän purkaminen komponentteihin - Tietovuokaavioiden luominen
Aseista	Aseistaminen	- Tietovuokaavioiden analysointi uhkien varalta

		- Haavoittuvuuksien tunnistaminen
-	-	- Lievennysstrategian suunnittelu

Khan ym. (2018) toteavat tutkimuksensa havaintojen perusteella, että STRIDE-viitekehyksessä tunnistetut uhat ovat tiettyjen turvallisuusominaisuuksien osalta vajavaisia, ja tulisikin aina varmistaa kuuden olennaisen turvallisuusominaisuuden (valtuutus, todennus, luottamuksellisuus, eheys, saatavuus ja kiistattomuus) olevan varmistetut jokaisen komponentin osalta, kun suunnitellaan uhkien lievennysstrategiaa.

Khan ym. (2018) toteavat STRIDE-viitekehyksen olevan tehokas malli edistämään järjestelmän turvallisuutta komponenttien tasolla. STRIDE-viitekehyksen avulla pystytään toimimaan niin haavoittuvuuksien kuin niiden fyysisten seurauksienkin ehkäisemiseksi. STRIDE-viitekehystä käytettäessä saavutetut tulokset ovat mielekkäämpiä, helposti ymmärrettäviä sekä riittävän kattavia asianmukaisten turvallisuusratkaisujen kehittämistä varten. Tuloksia voidaan myös käyttää kaikkein kriittisimpien uhkien osoittamiseksi sekä tehokkaimpien lieventämistoimien kehittämiseksi.

4.8 Vertailun tulokset

Yhteenvetona STRIDE-mallin osalta voitaneen todeta, että Microsoftin viitekehyksen suurin eroavaisuus MITRE ATT&CK sekä Lockheed Martinin Cyber Kill Chain-viitekehyksiin on sen puolustusorientoitunut lähestymistapa. STRIDE-viitekehyksen koko prosessin viimeinen vaihe on uhkien lievennysvaihe, joka on täysin puolustava vaihe. STRIDE-viitekehys ei siis perusta toimintaansa uhkien täydelliseen torjumiseen tai hyökkäyksen pysäyttämiseen, vaan se perustuu läpikotaisen analyysin ja uhkien tunnistamisen avulla luomaan parhaan mahdollisen uhan lievittämiseen soveltuvan strategian.

Kun siis STRIDE-viitekehyksen prosessi tähtää suoraan uhkien lievittämiseen ja vahingon minimointiin, voidaan ATT&CK-sekä Cyber Kill Chain-viitekehysten avulla pyrkiä puolustautumisen ohella jopa hyökkäävämpiin toimiin uhan tai hyökkäyksen pysäyttämiseksi. Tästä syystä STRIDE-viitekehys ei voi parhaiten vastata kyberuhkien torjunnalle asetettuihin tavoitteisiin, eikä yllä niin laajaan prosessityöskentelyyn kuin ATT&CK- Cyber Kill Chain-viitekehykset.

Lockheed Martinin kehittämän Cyber Kill Chain-mallin osalta on välttämätöntä todeta, että se on kill chain-mallien edelläkävijä, joka on perustana kaikille myöhemmin kehitetyille malleille. Malli on pätevä työkalu kyberuhkien ja hyökkäysten havaitsemiseksi ja pysäyttämiseksi, kuten Hutchinsin ym. (2011) tutkimuksessa havaitaan. Cyber Kill Chain-mallilla on todella laaja käyttöaste maailman mittakaavassa ja sen tehokkuuden puolesta puhuu mallin yksinkertaiset sekä yksiselitteiset prosessin vaiheet.

ATT&CK-viitekehyksen etuna puolestaan voidaan todeta olevan ehdottomasti sen kattava taktiikoiden kirjo sekä lukuisat eri tekniikat niihin sidottuna. Tämän ansiosta prosessityöskentelyn räätälöiminen yksittäistä uhkatapausta varten on mahdollista. Tämä on omiaan nostamaan mallin tehokkuutta. Malli tuottaa kyberuhilta suojautuvalle tai niitä ehkäisevälle taholle eniten tietoa muihin malleihin verrattuna juuri kattavan taktiikka- ja tekniikkakirjon ansiosta. Tiedon tuottaminen tulee esiin siinä, miten tarkka kuva hyökkäyksestä saadaan puolustajalle etenkin hyökkääjän näkökulmasta.

ATT&CK-viitekehys vastaa todella kattavasti kysymykseen hyökkääjän askelista ja toimista hyökkäyksen kohteena olevan tietojärjestelmän sisällä. Malli on omiaan kuvaamaan hyökkäyksen läpikotaisesti, ja ero Cyber Kill Chain-viitekehykseen on juuri mallien kattavuuden välillä. Tämän lisäksi lähdekirjallisuuden perusteella ei voida yksiselitteisesti määrittää, kumpaa mallia käyttämällä kyberhyökkäys saadaan torjuttua aikaisemmassa vaiheessa. Näistä syistä ATT&CK-viitekehystä voidaan puoltaa kyberuhkien torjunnan tavoitteisiin parhaiten vastaavana riskienhallintamallina. Cyber Kill Chain-viitekehys ei kuitenkaan missään tapauksessa ole heikompi viitekehys, vaikka sen prosessin työkalupakki ei ole yhtä kattava.

5 YHTEENVETO

Riskienhallinta koostuu pääasiassa riskien tunnistamisesta, analysoinnista sekä niihin reagoinnista, oli se sitten torjuvaa tai lievittävää toimintaa. Tätä perusperiaatetta myös kill chain-pohjaiset viitekehykset hyödyntävät kyberuhkien havaitsemisessa ja torjunnassa. Kyberuhkien havaitsemisen kannalta mallien järjestelmällinen eteneminen riskienhallinnan prosessissa on tehokas keino havaita mahdollisimman moni uhkaava toimi.

Tutkimuskysymys, johon tutkielman avulla pyrittiin vastaamaan, oli:
"*Mitkä ovat vertailtavien riskienhallintamallien tai kill chain-mallien ominaisuudet ja eroavaisuudet sekä mitä mallia hyödyntämällä kyberuhkien torjunnalle asetetut tavoitteet todennäköisimmin täyttyvät?*".

Tutkielma toteutettiin kuvailevana kirjallisuuskatsauksena käyttäen tietokantahakuja tiedonhankintamenetelmänä. Tutkielman toisessa ja kolmannessa sisältöluvussa keskityttiin määrittelemään kyberuhan käsite sekä luokittelemaan eri uhkia, määrittelemään riskienhallinnan ja riskienhallintamallin käsite sekä esittelemään vertailtavat riskienhallintamallit ja niiden ominaisuudet. Neljännessä sisältöluvussa lähdekirjallisuuden perusteella voitiin todeta, että mallien joukossa mukana olleen COSO:n kokonaisvaltaisen organisaatioiden riskienhallinnan (COSO-ERM-2017) mallia hyödyntävää tapaustutkimusta kyberuhkien torjunnasta tai uhkiin varautumisesta ei löytynyt. Aineistoa oli mahdollista löytää vain mallin yleisistä kyvykkyyksistä. Täten mallia ei voitu arvioida sen kyberuhkien torjunnan kyvykkyyden osalta.

Tutkielmassa käy ilmi, että Microsoftin STRIDE-viitekehys eroaa MITRE ATT&CK ja Lockheed Martinin Cyber Kill Chain-viitekehyksistä sen puolustusorientoituneen lähestymistavan myötä. Koska mallin tavoitteena ei voi aktiivisesti olla hyökkäyksen pysäyttäminen, tutkielmassa todetaan, että malli ei voi vastata parhaiten kyberuhkien torjunnalle asetettuihin vaatimuksiin. Vertailussa kandidaateiksi jäivät siis ATT&CK- sekä Cyber Kill Chain-mallit.

Tässä vaiheessa tutkielmaa heräsi kysymys, ovatko MITRE:n ATT&CK ja Lockheed Martinin Cyber Kill Chain-viitekehykset parhaita valintoja kyberuhkien torjumisen viitekehyksiksi? Tutkielmassa esitetyn pohjalta voitaneen todeta, että ovat. Cyber Kill Chain on kyseisten mallien edelläkävijä, johon kaikki

myöhemmin kehitetyt mallit osaltaan pohjaavat. Malli on edelleen todella pätevä työkalu kyberuhkien ja hyökkäysten havaitsemiseksi ja pysäyttämiseksi, kuten esimerkiksi Hutchins ym. (2011) esittävät oman tutkimuksensa havaintojen perusteella. Tämän lisäksi mallin tehokkuutta puoltaa sen edelleen nauttima laajakäyttöaste ja yksinkertaiset sekä yksiselitteiset prosessin vaiheet. Lähdekirjallisuuden perusteella ei ollut mahdollista selvittää yksiselitteisesti sitä, kumpaa mallia käyttämällä kyberhyökkäys tai uhka saadaan lievitettyä tai torjuttua aikaisemmassa vaiheessa.

Tutkielmassa todetaan, että ATT&CK-viitekehyksen puolesta puhuvat sen kattavat taktiikat ja lukuisat eri tekniikat niiden alla. Prosessityöskentely on mahdollista räätälöidä viitekehyksen avulla juuri tietyn tapauksen tarpeita vastaavaksi, ja kattavan taktiikka- ja tekniikkakirjon ansiosta viitekehys tuottaa malleista eniten tietoa puolustajalle. ATT&CK-viitekehyksen avulla tuotetaan parempi kuva siitä, miltä hyökkäys näyttää sekä puolustajan, mutta etenkin hyökkääjän näkökulmasta.

Organisaation johdossa voidaan esimerkiksi pohtia seuraavaa: ”Mitkä ovat ne asiat mitä kyberhyökkääjät pyrkivät tekemään ja saavuttamaan verkossamme, jotta osaamme varautua asianmukaisin toimin?” Tutkielmassa todetaan, että tähän kysymykseen ATT&CK-viitekehys vastaa käytännössä parhaiten läpikotaisen hyökkäyksen kuvantamisen tuloksena. Juuri tämän vuoksi ATT&CK-viitekehys voidaan nähdä sinä viitekehyksenä, jota hyödyntämällä kyberuhkien torjunnalle asetetut tavoitteet todennäköisimmin täyttyvät. Cyber Kill Chain-viitekehystä ei ole kuitenkaan syytä rajata millään tapaa heikommaksi työkaluksi. Ero näiden mallien välillä on hiuksenhieno, mutta syntyy niiden kattavuudesta.

Lähdemateriaalin haussa ilmeni, että tutkimusta mallien käytöstä kyberuhkien torjumisessa tai lievittämisessä ei ole juurikaan saatavilla. Kaikki löydetyt aineistot olivat kuitenkin samassa linjassa keskenään esittämiensä väitteiden kanssa. Tämän johdosta korkeamman tasoluokituksen aineistoja vertailemalla matalamman tason julkaisuihin voitiin tuottaa luotettavaa tietoa. Lisäksi tutkielmassa määritelmien osalta pohjattiin vahvasti valtiollisiin asetuksiin.

Syy aihepiirin tutkimusten puutteeseen voi olla tiedon turvaluokittelu. Valtiollista ja puolustushallintojen toteuttamaa tutkimusta kyberturvallisuuden aihepiiristä ei aseteta julkiseksi tiedoksi. Tämän vuoksi on todennäköistä, että tutkimusta aiheesta ja etenkin mallien vaiheittaisesta käytöstä ja analysoinnista kyberuhkien torjunnassa ei ole yksinkertaisesti saatavilla juuri lainkaan.

Tutkielman tulokset ovat omiaan selkeyttämään organisaatioiden riskienhallintamallin valintaa kyberuhkien lievittämisen tai torjumisen työkaluksi. Suosituimpien riskienhallintamallien ja useiden samankaltaisten Cyber Kill Chain-viitekehykseen pohjautuvien mallien joukosta valittujen mallien vertailulla on tunnistettu se malli, jonka prosessin mukaisesti työskentelemällä uhkien lievitykselle ja torjunnalle asetetut tavoitteet todennäköisimmin saavutetaan. Lisäksi on tunnistettu parhaiten asetettuja tavoitteita vastaava vaihtoehto, mikä tutkielman tulosten perusteella on ATT&CK-malli. Tämän lisäksi tutkielma selventää eroavaisuuksia ja soveltuvuuksia eri riskienhallintamallien välillä.

Aikaisempaa riskienhallinta- tai kill chain-malleja vertailevaa ja etenkin luokittelevaa tutkimusta ei aineistonhakuvaiheessa löytynyt, joten tutkielma tuottaa ensimmäisten joukossa kontribuutiota mallien kyvykkyyksiin ja tehokkuuteen perustuvan luokittelun muodossa. Tulevaisuudessa tätä luokittelua mallien välillä olisi suotavaa tutkia lisää, etenkin sellaisten tutkimusten pohjalta, jossa mallien käyttöä kyberhyökkäysten ilmentyessä on analysoitu perinpohjaisesti. Täten voitaisiin saada entistä tarkempaa tietoa mallien kyvykkyyksistä ja tehokkuuksista, olkoonkin että kyberturvallisuuden kentällä uhat ja niihin reagoinnin työkalut kehittyvät jatkuvasti.

Sisäministeriö (2017) monen muun tapaan pitää tulevaisuuden suurimpana uhkakuvana hyökkäyksiä yhteiskunnan kriittistä infrastruktuuria kohtaan. Kyberrikolliset kehittävät hyökkäysmenetelmiään jatkuvasti, ja vaikka puolustustekniikat ja -järjestelmät kehittyvät yhtä lailla, on arvaamattomien hyökkääjien toiminnan ennakointi ja siihen vastaaminen verrattain haasteellista. Kyberuhilta puolustautumisesta puhuttaessa voitaisiinkin puhua loputtomasta kamppailusta uusia haavoittuvuuksia hyödyntäviä tahoja vastaan. Tämän vuoksi olisi erittäin suotavaa, että riskienhallintamallien kyvykkyyttä tutkittaisiin enemmän. Relevantteja aiheita olisivat nimenomaan tapaustutkimukset Kill Chain-tyylisten riskienhallintamallien käytöstä, vaikka haasteena niissä onkin valtiolliset turvallisuussäädökset ja tiedon julkisuusluokitukset. Lisäksi olisi tärkeää keskittyä mahdollisen kyberhyökkäyksen elinkaaren kuvaamisen sijasta tunnistamaan niitä toimia, jolla hyökkäystä voidaan ennaltaehkäistä, lieventää tai sitä, millä toimin se voidaan kokonaan estää? Kuinka aikaisessa vaiheessa ja kuinka tehokkaasti se on mahdollista estää? Hyökkääjän toimintamallien tunnistaminen ennakkoon on toki tärkeää ja tutkimusta aiheesta on ylläpidettävä, mutta painopistettä tulisi kallistaa enemmän puolustajan näkökulmaan tulevaisuuden kehittyneempiä uhkakuvia ajatellen.

LÄHTEET

Almgren, K. (2014). Implementing COSO ERM Framework to Migitate Cloud Computing Business Challenges. *International Journal of Business and Social Science,* Vol.5, No.9, 71-76

Aslam, A. (2017). Decision Support System for Risk Assessment and Management Strategies in Distributed Software Development. *IEEE Access, 5*, 20349-20373.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software,* 81(12), 2118-2133.

Beggs, C. (2006). Proposed Risk Minimization Measures for Cyber-Terrorism and SCADA Networks in Australia, *Proceedings of the 5th European Conference on Information Warfare and Security*, National Defence College, Helsinki, Finland, 1-2 June 2006.

Boehm, B. W. (1989). *Software risk management*. Washington (D.C.): IEEE Computer Society Press.

Clapper, J., Lettre, M. & Rogers, M. (2017). Foreign Cyber Threats to the United States. Hampton Roads International Security Quarterly, 1. Haettu 24.4.2022 osoitteesta https://www-proquest-com.ezproxy.jyu.fi/docview/1865125438?pqorigsite=primo.

COSO. (2004). Enterprise Risk Management – Integrated Framework (Kokonaisvaltainen ajatusmalli organisaation riskienhallintaan)

COSO. (2017). Enterprise Risk Management. Integrating with strategy and performance. Committee of Sponsoring Organizations of the Treadway Commission, June, 2017. Haettu 17.4.2022 osoitteesta https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

COSO. (2021). COSO. Haettu 17.4.2022 osoitteesta https://www.coso.org/Pages/default.aspx

Dias, A. P. (2017). A more effective audit after COSO ERM 2017 or after ISO 31000:2009? *Perspectiva Empresarial, 4*(2), 73–82.

Donaldson, S., Siegel, S., Williams, C. & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build Successful Cyberdefence Program Against Advanced Threats*. 1. painos. New York: Apress Media, LLC.

Elms, D. (2019). Limitations of risk approaches. *Civil Engineering and Environmental Systems*, *36*(1), 2–16. https://doi.org/10.1080/10286608.2019.1615474

EU komissio. (2017). Tiedonanto Euroopan parlamentille, Eurooppaneuvostolle ja neuvostolle-Seitsemäs raportti edistymisestä kohti toimivaa ja todellista turvallisuus-unionia, COM(2017) 261 final, Strasbourg 16.5.2017.

Hutchins, E. M., Cloppert, M. J., Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Haettu 5.3.2022 osoitteesta https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Ilmonen, I., Kallio, J., Koskinen, J., & Rajamäki, M. (2010). *Johda riskejä: käytännön opas yrityksen riskienhallintaan*. Helsinki: Tammi.

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2018). STRIDE-based Threat Modeling for Cyber-Physical Systems. In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings IEEE . https://doi.org/10.1109/ISGTEurope.2017.8260283

Kiwia, D., Dehghantanha, A., Choo, K. K. R., & Slaughter, J. (2017). A cyber kill chain based taxonomy of banking trojans for evolutionary computational intelligence. *Journal of Computational Science*, 27, 394–409. https://doi.org/10.1016/j.jocs.2017.10.020

Legoy, V. (2019). Retrieving ATT&CK tactics and techniques in cyber threat reports. University of Twente. M.sc. Thesis.

Lehto, M. (2021). Digitaalisen kybermaailman ilmiöitä ja määrittelyä. *Kyber on kaikkialla – Jyväskylän yliopisto, tiedeblogi. 15,* 19-125. http://urn.fi/URN:NBN:fi:jyu-201703271763

Lehto, M. (2022). APT Cyber-attack Modelling : Building a General Model. In R. P. Griffin, U. Tatarand, & B. Yankson (Eds.), ICCWS 2022 *: Proceedings of the 17th International Conference on Cyber Warfare and Security* (17, pp. 121-129). Academic Conferences International Ltd. The proceedings of the 17th international conference on cyber warfare and security. https://doi.org/10.34190/iccws.17.1.36

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston kanslia. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja Nro 30/2017

Leino, M., Steiner, M.-L. & Wahlroos, J. (2005) *Corporate Governance ja riskienhallinta*. Teoksessa H. Kuusela & R. Ollikainen (toim.) Riskit ja riskienhallinta. Tampere: Tampere University Press.

Liaropoulos, A. (2010). War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory. *Proceedings of the 9th European Conference on Information Warfare and Security*. Department of Applied Informatics University of Macedonia Thessaloniki Greece 1-2 July 2010, 177-182.

Limnéll, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus*, 29, 113-150. Jyväskylä: Docendo.

Lockheed Martin. (2015). Gaining the Aavantage Applying Cyber Kill Chain® Methodology to Network Defense. Haettu 10.4.2022 osoitteesta https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Mateski, M. Cassandra M. Trevino, Cynthia, K. Veitch, Michalski, K. Harris, Maruoka, S & Frye, J. (2012) Cyber Threat Metrics. Sandia National Laboratories

Microsoft. (2022). Microsoft Threat Modeling Tool threats: STRIDE model. Haettu 2.3.2022 osoitteesta https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Moeller, R. R. (2007). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes*. New York: John Wiley & Sons.

Nippala, A. (2019). Riskienhallinta hajautetussa tietojärjestelmäprojektissa. Jyväskylän yliopisto. Informaatioteknologian laitos. Pro Gradu.

Pajala, E. (2020). Situation awareness and cyber kill chain when russia ncyber operations hacked the democratic national committee. Jyväskylän yliopisto. Informaatioteknologian laitos. Kandidaatintutkielma.

Pols, P. (2017). The Unified Kill Chain, Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks. Cyber Security Academy (CSA). The Hague.

Puolustusministeriö. (2010). Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 16.12.2010. Haettu 19.4.2022 osoitteesta https://www.defmin.fi/files/1705/yts_2010_fi_nettiin.pdf

Rubino, M. (2018). A Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance. *International Journal of Business and Management*, 13(12), 203. https://doi.org/10.5539/ijbm.v13n12p203

SFS-FI ISO 31000. (2018). Riskienhallinta. Ohjeet. Suomen standardoimisliitto SFS ry.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. New York: Wiley.

Simi, J. (2017). Tiedon luokittelu osana organisaation kokonaisarkkitehtuurin riskienhallintaprosessia. Jyväskylän yliopisto. Informaatioteknologian laitos. Pro Gradu.

Straub, J. (2020). Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks. *2020 IEEE International Conference on Smart Cloud* (SmartCloud), 2020, pp. 148-153, doi: 10.1109/SmartCloud49737.2020.00035.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., Thomas, C. B. (2018). MITRE ATT&CK: Design and Philosophy. Haettu

3.3.2022 osoitteesta https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Turvallisuuskomitea. (2018). Kyberturvallisuuden sanasto. Haettu 2.3.2022 osoitteesta https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Uma, M. & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security*, 15, 390-396.

Valtiovarainministeriö. (2017). Ohje riskienhallintaan: Valtiovarainministeriön julkaisuja 22/2017. Haettu 15.4.2022 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

Yadav, T., Rao, A.M. (2015). Technical Aspects of Cyber Kill Chain. Teoksessa Abawajy, J., Mukherjea, S., Thampi, S., Ruiz-Martínez, A. (toim.), Security in Computing and Communications. SSCC 2015. *Communications in Computer and Information Science,* 536. Springer, Cham. https://doi.org/10.1007/978-3-319-22915-7_40