Ville Vatanen

VENÄJÄN LÄHIALUEILLAAN TOTEUTTAMIEN KYBEROPERAATIOIDEN ANALYSOINTI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Vatanen, Ville
Venäjän lähialueillaan toteuttamien kyberoperaatioiden analysointi
Jyväskylä: Jyväskylän yliopisto, 2020, 120+1 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaajat: Lehto, Martti; Siukonen, Veikko

Vuonna 2007 Venäjä toteutti Viron valtiota vastaan useita viikkoja kestäneen kyberoperaation. Tämä oli ensimmäinen kerta, kun valtio toteutti järjestelmällisen, hyökkäyksellisen operaation tietoverkkojen kautta toista valtiota vastaan. Vaikka vahingot jäivät lopulta vähäisiksi, herätti se huomiota erityisesti länsimaissa. Viron jälkeen Venäjän kyberoperaatioiden kohteina ovat olleet erityisesti sen naapurimaat. Nämä valtiot ovat tyypillisesti olleet vanhoja neuvostotasavaltoja, jotka ovat pyrkineet irtautumaan Venäjän valtapiiristä ja lähentymään länsimaiden kanssa tai asettuneet vastustamaan Venäjän geopoliittisia tavoitteita. Tämä pro gradu -tutkielma tutki Venäjän lähialueillaan toteuttamia kyberoperaatioita, jotka toteutettiin vuosien 2007 ja 2017 välisenä aikana. Tutkimuksen tutkimusstrategiana käytettiin monitapaustutkimusta, joka soveltuu hyvin tutkimuksiin, joissa kiinnostuksen kohteena on useampi kuin yksi tapaus. Tutkimus on saanut vaikutteita postpositivistisen tieteenfilosofian suuntauksesta. Tutkimuksen kirjallisuuskatsauksessa määriteltiin attribuution ja kyberoperaation käsitteet, selvitettiin, mitä kyberoperaatioita Venäjä on toteuttanut lähialueillaan sekä millaisia kyberhyökkäyksen mallintamisen menetelmiä on kehitetty. Katsauksen perusteella tutkimukseen valikoitui yhteensä kuusi operaatiota, jotka on toteutettu Viroa, Liettuaa, Georgiaa ja Ukrainaa vastaan. Ukrainaa kohtaan toteutettiin kolme erillistä kyberoperaatiota. Lisäksi operaatioiden analysointiin valittiin sovellettu yhdistetty tappoketju, joka on muokattu yhdistetyn tappoketjun pohjalta. Tappoketjun analysoinnin pohjalta saadut tulokset tulkittiin strategisen kulttuurin teorian avulla. Tutkimustuloksista käy ilmi, että Venäjän kyberoperaatiot ovat muuttuneet sekä tavoitteiltaan että rakenteeltaan kymmenen vuoden aikana. Ensimmäiset kyberoperaatiot toteutettiin ideologisista syistä, eikä niillä saavutettu juuri lyhytaikaisia vaikutuksia suurempaa lopputulosta. Liettuaa vastaan suoritetun operaation jälkeen operaatiot ovat olleet monimutkaisempia, paremmin suunniteltuja, ne on toteutettu geopoliittisista syistä ja niillä on tavoiteltu pitempiaikaista hyötyä. Kirjallisuuskatsauksen perusteella löydetyt mallintamisen menetelmät eivät myöskään sovellu täysin kyberoperaatioiden analysointia varten, sillä nämä ovat suunniteltu kyberhyökkäyksien analysointia varten. Mallille, joka on kehitetty kyberoperaatioiden analysointia varten, on siis tarvetta.

Asiasanat: kyberoperaatio, kyberhyökkäys, Venäjä, strategisen kulttuurin teoria, yhdistetty tappoketju, kyberhyökkäyksen mallintamisen menetelmä

ABSTRACT

Vatanen, Ville
An analysis on Russian cyber operations conducted against its neighbouring countries
Jyväskylä: University of Jyväskylä, 2020, 120+1 pp.
Cyber Security, Master's Thesis
Supervisors: Lehto, Martti; Siukonen, Veikko

In 2007, Russia conducted a cyber operation against Estonia. This was the first time when a country was attacked by another country through cyber environment. Even though the operation caused only minimal losses, the Western democracies realised that this was only a precedent. Afterwards, Russia has conducted multiple cyber operations against its neighbouring countries. These countries have typically been post-Soviet republics, which have tried to distance themselves from Russia. Cyber operations have been conducted against these countries after they had moved closer to the Western sphere of influence, or after Russia had deemed that these countries threaten the geopolitical objectives of Russia. The focus of this thesis is on the cyber operations that Russia has carried out between 2007 and 2017. The research strategy used in the study was a multiple case study strategy, which is especially useful when the researcher is interested in multiple cases. This research is based on the postpositivist paradigm. The literature review focused on defining the concepts of attribution and cyber operation, explaining the different cyber operations Russia has carried out against neighbouring countries, and presenting different kinds of attacking modelling techniques. Based on the literature review, six different cyber operations were chosen for the analysis: cyber operations against Estonia, Lithuania, Georgia and three different operations against Ukraine. A modified unified kill chain attacking modelling technique was chosen as the analysis tool. Strategic culture theory was used to explain the results. The results show that the goals and the structure of the Russian cyber operations have changed over the course of a decade. The first operations were based on ideological reasons, and they did not achieve any long-term goals. After the operation against Lithuania, these cyber operations were better planned, more complex, based on geopolitical reasons and they strived for longer-term results. A need for the development for a separate cyber operation modelling technique was also recognized for most of the current techniques are developed for cyber-attack analysis.

Keywords: cyber operation, cyber-attack, Russia, strategic culture theory, unified kill chain, attack modelling technique

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

10. toukokuuta 2007 yli miljoona tietokonetta yritti yhtäaikaisesti päästä Viron hallituksen verkkosivuille. Kyseessä ei ollut sattumalta syntynyt yhtäkkinen kiinnostus Viroa kohtaan, vaan maailman ensimmäinen, valtion tukema, useita kyberhyökkäyksiä sisällään pitänyt kyberoperaatio. Pölyn laskeuduttua muutaman viikon kuluttua maailma ei ollut entisensä. Nyt valtioiden tiedettiin pystyvän ja haluavan toteuttaa kyberoperaatioita osana poliittista vaikuttamista. (Osawa, 2017, s. 114).

Kyberoperaatioita on tämän jälkeen toteutettu ympäri maailmaa. Vaikutukset ovat vaihdelleet pienestä kiusanteosta, kuten verkkosivujen hidastumisista aina suurempien vahinkojen aiheuttamiseen, kuten tiedostojen ja laitteiden tuhoamiseen (Pernik, 2018, s. 56; Greenberg, 2018, s. 5). Kiinnostus kyberhyökkäyksiä kohtaan on noussut erityisesti Viron patsaskiistan jälkeen. Aiheesta tehdyt tutkimukset ovat kuitenkin rajoittuneet pääosin yhden tapauksen tutkimiseen tai enintään kolmen tapauksen keskinäiseen vertailuun ilman kunnon analyyttisen työkalun, mallin tai teorian käyttöä. Tarvetta on siis tutkimukselle, jossa analysoidaan useampaa kyberoperaatiota samalla analysointimenetelmällä. Lisäksi tarvetta on tutkimukselle, jossa analyysin tuloksia pohdintaan teorian kautta.

Tämän tutkimuksen tarkoituksena on analysoida Venäjän lähialueillaan toteuttamia kyberoperaatioita, jotka ovat tapahtuneet vuosien 2007–2017 aikana monitapaustutkimuksellisen tutkimusstrategian avulla. Tutkimuksen kirjallisuuskatsauksessa tutkittiin eri kyberhyökkäyksen mallintamisen menetelmiä. Lisäksi kirjallisuuskatsauksessa käsiteltiin Venäjän valtion lähialueillaan toteuttamat tai tukemat kyberoperaatiot vuosien 2007 ja 2017 välisenä aikana. Näistä operaatioista on valittu soveltuvimmat tapaukset varsinaista analysointia varten. Tapausten analysoinnissa käytettiin sovellettua yhdistettyä tappoketjua (Unified Kill Chain). Tulosten analysoinnin apuna käytetään strategisen kulttuurin teoriaa. Tutkimus on ottanut vaikutteita postpositivistisesta tieteenfilosofian suuntauksesta.

Tutkimuksen tuloksena selvisi, että Venäjän kyberoperaatiot ovat muuttuneet vuosien kuluessa sekä toteutustavoiltaan että tavoitteiltaan. Ensimmäiset kyberoperaatiot (Viroa ja Liettuaa vastaan tehdyt kyberoperaatiot) toteutettiin pitkälti ideologisista syistä, eikä niillä tavoiteltu pitkäaikaisia vaikutuksia. Myöhemmin toteutetut kyberoperaatiot (Georgiaa ja Ukrainaa vastaan tehdyt kyberoperaatiot) ovat olleet pitkäkestoisempia, niitä on valmisteltu pidemmän aikaa, ne on toteutettu geopoliittisiin syihin nojaten ja niillä on tavoiteltu pitkäaikaisempia ja tuhoisampia vaikutuksia. Sekä kirjallisuuskatsauksessa käsitellyt mallit, että analysointiin käytetyn mallin havaittiin olevan puutteellisia tämänkaltaisten operaatioiden analysointiin.

1.1 Tutkimuskysymys

Tutkimuksen päätutkimuskysymys on seuraava:

- Miten Venäjän toteuttamat kyberoperaatiot ovat rakentuneet ja miksi ne ovat rakentuneet juuri kyseisellä tavalla

Tutkimusta tukevat seuraavat apukysymykset:

- Millaisia eri kyberhyökkäyksen mallintamisen menetelmiä on kehitetty
- Mitä kyberoperaatioita Venäjä on toteuttanut lähialueillaan 2000-luvulla

1.2 Aiempi tutkimus

Kiinnostus kyberhyökkäyksiä kohtaan on ollut ymmärrettävästi valtaisa Viron tapahtumien jälkeen. Ennen 2000-lukua ja Viron patsaskiistasta syntyneitä iskuja ei kyberhyökkäyksiä ollut käytetty näin laajasti yksittäistä valtiota vastaan, eivätkä valtiot olleet aiemmin vastanneet koordinoidusti sitä vastaan tehtyihin kyberhyökkäyksiin (Davis, 2007). Tutkimuksia yksittäisistä kyberoperaatioista (eli esimerkiksi tutkimus Viroon kohdistuneista tietoverkkohyökkäyksistä) löytyy useita. Ottis (2008) tutki Viron hyökkäyksiä yleisemmin informaatiosodankäynnin näkökulmasta ja antaa yleiskuvan hyökkäyksistä menemättä kovin syvälle teknisiin yksityiskohtiin. Shackleford (2009) käyttää Viroa esimerkkinä siitä, miten tulevaisuudessa kyberhyökkäyksiä vastaan voitaisiin puolustautua. Czosseck, Ottis & Talihärm (2011) esittelevät, mitä laki- ja organisaatiomuutoksia Viroa vastaan toteutettu kyberoperaatio sai aikaan eri valtioissa. Hollis (2011) tutki Georgiaa vastaan tehtyjä kyberhyökkäyksiä sekä Georgian ja Venäjän välistä maasotaa ja pohti kyberhyökkäyksiä strategisesta näkökulmasta käsin. Korns & Kastenberg (2009) pohtivat, miten Georgiaa kohtaan tehdyt kyberhyökkäykset vaikuttavat amerikkalaisiin ja näiden ajatuksiin kybertoimintaympäristöstä. Swanson (2010) käsittelee Georgian ja Venäjän kybersotaa lainopillisesta näkökulmasta. Mshvidobadze (2015) käsittelee lyhyesti Georgian kyberoperaatiota osana georgialaista kyberbarometriä. Rios, Czosseck & Geers (2009) kategorisoivat Georgian kyberoperaation perusteella kyberhyökkäyksen vaiheet suunnittelusta lopputulokseen. Tämä tutkimus lähinnä esitteli löydetyt havainnot sitomatta niitä mihinkään teoriaan tai viitekehykseen. Viron ja Georgian kyberoperaatioita on käsitelty lyhyemmin tai näistä kirjoitetaan enintään kappaleen verran useassa muussa tutkimuksessa tai kirjassa (katso esimerkiksi Goodman, 2010; Goel, 2011; Bonner III, 2014; Green, 2015).

Tapaustutkimus on ollut verrattain suosittu tutkimusstrategia kyberhyökkäyksiä tutkittaessa. Tutkijat ovat käyttäneet sekä yksittäis- että monitapaustutkimusstrategioita. Darczewskan (2014) tapaustutkimus tutkii Krimin valloitusta ja informaatiosotaa. Dehlawi & Abokhodair (2013) käyttivät tapaustutkimusta Saudi-Arabian öljy-yhtiötä vastaan tehdyn kyberhyökkäyksen tutkimisessa. Tutkimuksen validiteettia parannettiin haastattelemalla hyökkäyksen kohteeksi joutuneen yhtiön henkilökuntaa. Kozlowski (2014) vertaili samanaikaisesti Viroa, Georgiaa ja Kirgisiaa vastaan tehtyjä hyökkäyksiä etsien samankaltaisuuksia näistä hyökkäyksistä. Tässä vertailussa ei käytetty tarkkaa viitekehystä, löydettyjä havaintoja verrattiin yksinkertaisesti keskenään tehtyjen havaintojen perusteella. Havaintoina Kozlowskilla oli esimerkiksi se, että Viron ja Kirgisian hyökkäysten nähtiin olevan taustoiltaan samanlaisia. Kumpaankin operaatioon liittyi poliittista kädenvääntöä ennen hyökkäystä (Viron tapauksessa operaation nähtiin alkaneen patsaskiistasta, Kirgisian tapauksessa päätöksestä pitää amerikkalaisten lentotukikohta jatkossakin auki). Zoller (2010) tutki Viron ja Georgian hyökkäyksiä ja suositteli amerikkalaisten käyttämään kyberstrategiaan muutoksia näiden kahden tapauksen perusteella. Ainut kirjallisuuskatsauksen perusteella löydetty, yli kolmen tapauksen monitapaustutkimus on Tikkin, Kaskan & Vihulin (2010) tutkimus Viroa, Radio Libertyä, Liettuaa ja Georgiaa vastaan tehdyistä kyberhyökkäyksistä lainopillisesta näkökulmasta.

Lähimpänä tutkimuksen lähestymistapaa ja näkökulmaa ovat Bundan (2020) pro gradu -tutkielma "Tapaustutkimus Venäjään yhdistettyjen kyberoperaatioiden kehittymisestä vuosina 2007–2016" sekä Connellin & Voglerin (2017) monitapaustutkimus "Russia's Approach to Cyber Warfare". Bundan pro gradu keskittyy yhteen Venäjään liitetyn APT (engl. Advanced Persistent Threat) -ryhmän toimintaan ja sen suorittamiin kyberoperaatioiden tutkimiseen tapaustutkimuksellisin menetelmin (Bunda, 2020, s. 55). Bunda käytti aineistonaan muun muassa hyökkäyksessä käytettyjen haittaohjelmatyökalujen teknisiä tietoja ja uhrien verkko-osoitteita (Bunda, 2020, s. 73). Tutkimuksen näkökulma oli siis tarkasti rajattu yhteen ryhmään ja näiden työkaluihin. Connell & Vogler tutkivat Venäjän lähestymistapaa kybersotaan sekä teoreettisesta että käytännöllisestä näkökulmasta, ja he käyttävät tapauksissa esimerkkeinä Viroa, Georgiaa ja Ukrainaa vastaan toteutettuja kyberoperaatioita. Tutkimuksen lähtökohta on hyvä, mutta analyysia ei tehdä minkään mallin avulla, ja johtopäätösten esittely jää pelkästään omien havaintojen pohtimisen tasolle, eikä niitä analysoida minkään teorian avulla.

Varsinaisten kyberhyökkäysten analysointiin on kehitetty lukematon määrä erilaisia työkaluja ja malleja. Esimerkiksi Lallie, Debattista & Bal (2020, s. 1) vertailivat tutkimuksessaan 180 eri hyökkäysmallia ja hyökkäyspuuta. Erilaisia kyberhyökkäysten mallintamisen menetelmiä esitellään tarkemmin luvussa kolme. Kirjallisuuskatsauksen perusteella suurin osa kehitetyistä kyberhyökkäyksen mallintamisen menetelmistä käytetään erilaisiin tietojärjestelmiin kohdistuvien kyberhyökkäysten analysointiin (esimerkiksi Kundur ym., 2011; Valdes & Skinner, 2000; Varuttamaseni, Bari & Youngblood, 2017; Mehta, Bartzis,

Zhu, Clarke & Wing, 2006). Tapaustutkimuksissa ei kyberoperaatioiden analysoinnissa ole kirjallisuuskatsauksen perusteella (Bundan [2020] pro gradua lukuun ottamatta) juurikaan käytetty kyberhyökkäysten analysointityökaluja tai -malleja. Tutkimukset, jotka tutkivat tapaustutkimuksen avulla kyberoperaatioita, keskittyvät pitkälti teollisuuden ja energiateknologian alalle (Liu, Li, Shuai & Wen, 2016; Lee, Assante & Conway, 2014).

Strategisen kulttuurin teoriaa käytettiin ensimmäistä kertaa vuonna 1977, kun Jack Snyder käytti kyseistä termiä tutkiessaan Neuvostoliiton strategista ajattelutapaa ydinaseisiin liittyen. Snyderin (1977) tutkimuksen lisäksi strategisen kulttuurin teoriaa on käytetty useissa tutkimuksissa selittämään Neuvostoliiton ja myöhemmin Venäjän tekemiä strategisia valintoja. Cassidy (2003) vertaa kirjassaan Neuvostoliiton Afganistanin sodassa tekemiä strategisia valintoja Venäjän Tšetšenian sodassa tekemiin strategisiin valintoihin. Monaghan tutkii Venäjän 2000-luvulla tekemiä valintoja ja sitä, miten nämä valinnat palvelevat niin kutsuttua ”venäläisten suurta strategiaa” (Monaghan, 2013, s. 1222). Neuvostoliitosta ja Venäjästä tehtyjen tutkimusten lisäksi strategisen kulttuurin tutkimusta on kohdistettu esimerkiksi Kiinan ja Intian strategisen kulttuurin tutkimiseen (Johnston, 1998; Bajpai, 2002) ja Yhdysvaltain ja Kiinan välisen kanssakäymisen selittämiseen sekä palestiinalaisten ja israelilaisten välisten jännitteiden tutkimiseen (Lantis, 2002, s. 87). Berger tutki Japanin ja Saksan sodanvastaisuutta sekä näiden maiden armeijavastaista kulttuuria strategisen kulttuurin teorian avulla (Berger, 1998). Martti Karin väitöstutkimuksessa strategisen kulttuurin teoriaa käytetään selittämään Venäjän käyttäytymistä kybertoimintaympäristössä (Kari, 2019a). Lähdeaineistona Kari on käyttänyt venäläisten virallisia asiakirjoja liittyen informaatioturvallisuuteen ja sotilasdoktriineihin. Karin aihepiiri on siis sama kuin tämän tutkimuksen, mutta lähteiden takia Karin näkökulma on eri.

Yhteenvetona voidaan todeta, että yksittäis- ja monitapaustutkimuksia kyberhyökkäyksistä on tehty aiemminkin. Nämä tutkimukset jäävät kuitenkin pintapuolisiksi tarkasteluiksi eri kyberoperaatioista tai ne lähestyvät tapauksia vain yhden kyberoperaation näkökulmasta. Kirjallisuuskatsauksen perusteella löydetyistä tutkimuksista ainoastaan yhdessä tutkittiin neljää tapausta samassa tutkimuksessa (Tikk ym., 2010). Aiemmin mainituissa tutkimuksissa ei ole tapausten analysointiin käytetty myöskään mitään tiettyä analysointityökalua. Monitapaustutkimukselle, jossa tapauksia analysoidaan perusteellisemmin ja pohjautuen johonkin kyberhyökkäyksen mallintamisen menetelmään, on siis tarvetta.

1.3 Aiheen rajaus

Tässä tutkimuksessa tutkitaan vuosien 2007 ja 2017 välissä tapahtuneita kyberoperaatioita, joiden toteuttajana tai kyberoperaatioon jotenkin osallisena arvioidaan olleen Venäjän valtio. Operaatiot on lisäksi kohdistettu Venäjän lähialueilla sijaitseviin valtioihin. Osawan (2017, s. 116–117) tutkimuksesta löytyy vuosien

2007-2017 välillä tapahtuneet, eri valtioiden toteuttamat tai tukemat kyberoperaatiot yhdestä taulukosta (liite 1). Valtioiden tukemia kyberoperaatioita on toteutettu myös vuoden 2017 jälkeen, kuten Yhdysvaltojen verkkohyökkäykset Irania vastaan (Newman, 2019), mutta tämän vuoden jälkeen tehdyistä operaatioista ja hyökkäyksistä ei ole joko tutkittu tarpeeksi tai näistä ei ole julkaistu riittävästi tutkimuksia. Mitä lähemmäksi nykyhetkeä tullaan, sitä vähemmän hyökkäyksistä on saatu tutkittua ja varmistettua tietoa, mikä vähentää tapausten tutkimusarvoa. Tällöin riittämätön tutkimustieto ei myöskään mahdollista operaatioiden seikkaperäistä analysointia, vaan liikaa olennaisia osa-alueita jää tutkimuksen ulkopuolelle. Raporttien julkisuus voi myös olla haaste. Raportteja ei välttämättä haluta julkaista niiden arkaluontoisen sisällön, kuten liikesalaisuuksien, takia. Kirjallisuuskatsauksen perusteella vuoden 2017 jälkeen tapahtuneista kyberoperaatioista ei ole julkaistu riittävästi materiaalia tai kyseisiä operaatioita ei ole tutkittu riittävästi, jotta näitä operaatiota olisi voinut ottaa tarkastelun kohteeksi tähän tutkimukseen.

Kirjallisuuskatsauksessa tarkasteltaviksi kyberoperaatioiksi ovat valikoituneet kyberoperaatiot Viroon, Liettuaan, Georgiaan, Kirgisiaan ja Ukrainaan liittyen. Ensimmäinen perustelu on se, että kyseisissä tapauksissa hyökkääjän epäillään olleen Venäjän valtio. Toinen perustelu on se, että näistä tapauksista on riittävän pitkä aika, jotta operaatioihin liittyvät yksityiskohdat ovat tulleet esiin. Esimerkiksi Georgian kyberhyökkäyksiin liittyen paljastui kolme vuotta operaation jälkeen, että venäläiset olivat asentaneet ennen Georgian ja Venäjän sotaa Georgian hallituksen tietokoneille vakoiluohjelman (Pernik, 2018, s. 59). Yksityiskohdat lähiaikoina tapahtuneista kyberoperaatioista ovat vielä epäselviä, ja tarkemmat tiedot voivat paljastua vasta vuosien kuluttua operaation päättymisen jälkeen. Kolmas perustelu on se, että edellä luetellut valtiot ovat suhteellisesti samassa tilanteessa. Niillä on Venäjä rajanaapurina, maiden asevoimat ovat suunnattu idästä tulevaa uhkaa vastaan ja kyseiset valtiot myös kokevat Venäjän uhkana.

1.4 Tutkimuksen rakenne

Kappaleessa yksi kerrottiin yleisesti tutkimuksen taustasta ja tästä tutkimuksesta. Lisäksi kappaleessa esiteltiin tutkimuksen rajaus ja aihealueesta aiemmin tehtyä tutkimusta. Kappaleessa kaksi esitellään tutkimuksen tieteenfilosofinen tausta ja tutkimuksessa käytetty tutkimusstrategia. Näiden lisäksi kappaleessa esitellään analysoinnin tuloksien pohdintaan käytetty strategisen kulttuurin teoria. Kappaleessa kolme esitellään eri kyberoperaatioita ja perustellaan, mitkä kyberoperaatiot otetaan mukaan tutkimuksen analyysivaiheeseen. Kappaleessa määritellään myös kyberoperaation ja attribuution käsitteet. Kappaleessa neljä esitellään Lallien ym. (2020) tutkimukseen kootut kyberhyökkäyksen mallintamisen menetelmät. Samassa kappaleessa perustellaan myös tutkimuksessa käytettävän mallintamisen menetelmän valinta. Kappaleessa viisi valitut kyberoperaatiot analysoidaan yhdistetyn tappoketjun avulla. Kappaleessa kuusi esitellään tutkimuksen

johtopäätökset, pohditaan tutkimuksen luotettavuutta sekä puutteita ja esitellään ajatuksia mahdollista jatkotutkimusta ajatellen.

2 MENETELMÄ

Tässä kappaleessa esitellään tutkimuksen tieteenfilosofinen suuntaus (postpositivismi), tutkimuksessa käytetty tutkimusstrategia (monitapaustutkimus) sekä tulosten analysoinnissa käytetty teoria (strategisen kulttuurin teoria).

2.1 Tutkimuksen tieteenfilosofinen suuntaus

Tämä tutkimus toteutetaan tapaustutkimuksena, ja tarkemmin monitapaustutkimuksena. Tapaustutkimuksen vahvuus on siinä, että sitä voidaan lähestyä useasta eri tieteenfilosofisesta näkökulmasta (Luck, Jackson & Usher, 2006). Postpositivistisen tapaustutkimuksen (Yin, 2014, s. 16) lisäksi tapaustutkimuksia on tehty ainakin positivistisesta, interpretivistisestä ja konstruktivistisesta näkökulmasta (Cavaye, 1996; Baxter & Jack, 2008). Tietojärjestelmätieteellisiä tutkimuksia on tehty sekä positivistisesta että interpretivistisestä näkökulmasta (DeVries, 2005, s. 163). Tämä tutkimus on ottanut vaikutteita postpositivistisesta näkökulmasta.

Jotta voidaan ymmärtää, mitä postpositivismilla tarkoitetaan, tulee ensiksi määritellä positivismin käsite. Positivismi tarkoittaa yksinkertaisimmillaan sitä, että minkä voi konkreettisesti tavoittaa ja mikä näkyy havainnoijalle, on totta. Tutkija on positivistisessa näkemyksessä objektiivinen tarkkailija, ja tarkkailun tuloksena saatavat tulokset ovat tutkijalle totuus. Tällainen karkea lähestymistapa on kuitenkin saanut kritiikkiä osakseen, mikä on synnyttänyt postpositivistisen tieteenfilosofian. Postpositivistin mukaan konkreettisesti tavoitettavat asiat ovat totta, mutta ymmärryksemme ulkopuolelle voi silti jäädä jotain, mitä ei jostain syystä tavoiteta tai havaita. Tätä käsitystä todellisuudesta voidaan kuvata ”kriittisen realistiseksi”. Postpositivisti myös yrittää tutkia kohdetta mahdollisimman objektiivisesti. (Metsämuuronen, 2011, s. 217.) Postpositivisti kuitenkin hyväksyy sen, että tutkija ei voi olla täysin objektiivinen. Pienetkin asiat ja ennakkoluulot voivat vaikuttaa tutkimukseen. Tutkijan näkemys vaikuttaa esimerkiksi siihen, millaisia tutkimusmetodeja tutkimuksessa käytetään. (Harrison, Birks, Franklin & Mills, 2017, s. 9.) Vaikuttaminen ja kanssakäyminen tutkimuskohteen kanssa tuleekin rajata minimiin, jotta tutkija vaikuttaisi saatuihin tuloksiin mahdollisimman vähän (Lincoln, Lynham, Guba, 2011, s. 168).

Postpositivismissa on myös tärkeää varmistaa kerätyn datan aitous, jotta lopputulokseen tulee vaikutettua mahdollisimman vähän. Tähän päästään käyttämällä mahdollisimman monia eri lähteitä ja datankeräystapoja. Mitä useampi lähde tutkijalla on käytettävissään, sitä pienemmäksi jää tutkijan mahdollisuus vaikuttaa lopputulokseen. Esimerkiksi käsittelemällä vain yhtä tapausta kerrallaan ei saavuteta välttämättä riittävää yleistettävyyttä ja tutkija tekee pahimmassa tapauksessa johtopäätöksensä vaillinaisen tiedon pohjalta. (Petersen & Gencel, 2013, s. 86.) Tässä tutkimuksessa analysoitaviksi tapauksiksi tulee ottaa

operaatioita, joiden tekijä on kohtalaisella varmuudella selvillä. Kyberoperaatioiden attribuutio-ongelman takia tekijän henkilöllisyyttä ei voida jokaisessa operaatiossa varmistaa täysin, mutta mitä useampaa lähdettä käyttää, sitä varmemman arvion tekijästä voidaan tehdä.

Kyberoperaatioiden suorittaja ei anna ymmärrettävistä syistä tarkkoja tietoja omista toimintatavoistaan. Tällöin havaintojen tekeminen hyökkääjästä jää joko hyökkäyksen kohteena olevan tahon tai jonkin kolmannen osapuolen tehtäväksi. Esimerkiksi Lookingglass Cyber Threat Intelligence Group (CTIG) –niminen ulkopuolinen tarkkailijaryhmä on analysoinut Ukrainaan kohdistunutta kybervakoilua (Lewis, 2015, s. 4).

2.2 Tapaustutkimus

2.2.1 Tapaustutkimuksen määrittelyä

Nimensä mukaisesti tapaustutkimuksessa käsitellään yhtä tai useampaa tapausta. Tapausten määrittely ja analysointi on tällaisen tutkimuksen keskeisin tavoite. Tapaustutkimuksiin kerätty aineisto voi olla kerätty eri tavoin, ja lähteet, joista aineisto on kerätty, voivat vaihdella paljonkin. Tyypillinen tapaustutkimus on laadullinen, mutta myös määrällistä aineistoa voidaan käyttää. Tapaustutkimuksissa voidaan myös käyttää monenlaisia aineiston analyysimenetelmiä. Tästä syystä tapaustutkimuksen voidaankin sanovan olevan koko tutkimusprosessia ohjaava strategia. (Eriksson & Koistinen, 2005, s. 4.)

Eriksson ja Koistinen (2005) jakavat tapaustutkimuksen kahteen erilaiseen ryhmään; intensiiviseen ja ekstensiiviseen tapaustutkimukseen. Intensiivinen tapaustutkimus keskittyy ainutlaatuiseen yhteen (tai useampaan) tapaukseen. Tapauksesta ei tehdä yleistyksiä, vaan tarkoitus on selvittää, miten ja miksi juuri kyseinen tapaus toimii. Tällaisessa tutkimuksessa kyseinen tapaus, tapaukseen liittyvä konteksti ja sen logiikka ovat tutkijan mielenkiinnon kohteina. Intensiivistä tapaustutkimusta on kritisoitu siitä, että aineiston analyysi on heikolla pohjalla ja johtopäätökset jäävät perustelematta. Haasteena onkin teoreettisten käsitteiden ja empiirisen analyysin yhdistäminen. Ekstensiivisessä tapaustutkimuksessa etsitään ilmiöistä ja prosesseista näitä yhdistäviä ominaisuuksia ja yleisiä malleja. Lisäksi tällaisessa tapaustutkimuksessa pyritään kehittämään uusia teoreettisia ideoita ja käsitteitä useamman tapauksen järjestelmällisen vertailun avulla. Päähuomio keskitetään teoriaan, eikä tosielämän tapausten ymmärtämiseen. Tavoite ekstensiivisessä tapaustutkimuksessa on "aiempien teoreettisten käsitteiden testaus ja täydentäminen uudessa ympäristössä, uusien teoreettisten ideoiden tai käsitteiden kehittäminen ja kokeilu tai uuden teoreettisen selitysmallin luominen" (Eriksson & Koistinen, 2005, s. 17.) Tapauksia vertaillaan jotenkin toisiinsa, ja oleellista on se, miten vertailu tehdään. Tutkimuksessa joudutaan päättämään, etsitäänkö tapauksista erilaisuuksia, näitä yhdistäviä ominaisuuksia tai näiden yhdistelmiä. Ekstensiivistä tapaustutkimusta on kritisoitu sen yksin-

kertaistavasta analyysista ja kontekstin puitteista. Tämä johtuu siitä, että tapauksia ei voida käsitellä niin monipuolisesti kuin intensiivisessä tutkimusstrategiassa. (Eriksson & Koistinen, 2005, s. 15–17.)

Stake (1995, s. 3) taas jakaa tapaustutkimukset kolmeen ryhmään. Nämä ovat itsessään arvokas (engl. intrinsic), välineellinen (engl. instrumental) ja kollektiivinen tapaustutkimus (engl. collective case study). Itsessään arvokasta tapaustutkimusta käytetään, kun halutaan keskittyä yhteen, tiettyyn tapaukseen, ja tutkija haluaa ymmärtää tätä kyseistä tapausta yksityiskohtaisesti. Välineellinen tapaustutkimus tarkoittaa taas sitä, että tutkimuksella yritetään ymmärtää jotain muuta kuin juuri sillä hetkellä tutkittavana olevaa tapausta. (Stake, 1995, s. 3.) Jos tutkimus lähestyy välineellistä tapaustutkimusta, on ideana etenkin teoreettisten ideoiden ja käsitteiden havainnollistaminen ja testaaminen valittujen tapausten avulla (Eriksson & Koistinen, 2005, 10). Välineellisessä tapaustutkimuksessa tapauksen tutkiminen auttaa laajempien, tapauksen taustalla vaikuttavien teemojen ymmärtämisessä. Kollektiivinen tapaustutkimus taas tutkii useampaa tapausta. Tärkeä osa tällaista tutkimusta on koordinoida näiden tapausten tutkimuksia keskenään, sillä idea on useampaa kohdetta tutkimalla muodostaa kokonaiskuvasta ymmärrystä tai muodostaa uutta teoriaa. (Stake, 1995, s. 3-4.)

Tapausta rajatessa oleellista on tehdä selkeä rajaus tutkittavan aihepiirin sisällä. Helpommin rajattavia tapauksia ovat esimerkiksi organisaatiossa toteuttavat projektit ja kehityshankkeet, vaikeammin rajattavia taas erilaiset muutosprosessit, tapahtumaketjut ja erilaiset ilmiöt (kuten johtaminen ja laatu). Tapauksen rajaaminen on kriittinen vaihe tutkimusta, ja tehty rajaus pitää myös pystyä perustelemaan. (Eriksson & Koistinen, 2005, s. 5-6.)

Tapaustutkimukselle ominaista on se, että se ei ole välttämättä kovin suoraviivainen prosessi. Tutkija voi käydä useita vaiheita läpi, palata aikaisempiin vaiheisiin ja tarkentaa aiempia vaiheita. Seuraavat vaiheet kuuluvat tapaustutkimuksen tekoon riippumatta tapaustutkimuksen tyypistä:

1. tutkimuskysymysten muotoilu
2. tutkimusasetelman jäsentäminen
3. mitä tapauksia tarvitaan ja käytetään
4. käytettävien teoreettisten näkökulmien ja käsitteiden määrittely
5. aineiston ja tutkimuskysymysten välisen vuoropuhelun logiikan selvittäminen
6. mitä analyysitapoja ja tulkintasääntöjä käytetään
7. mitä raportointitapaa käytetään. (Eriksson & Koistinen, 2005, s. 19.)

Edellä mainitut eivät välttämättä tapahdu numerojärjestyksessä, ja aiempiin kohtiin voi joutua palaamaan tutkimuksen edetessä. Teoriaa kehittävän tutkimuksen lähtökohtana ei ole valmis teoria tai hypoteesi. Tutkimuskysymyksen ei tarvitse olla täsmällisesti muotoiltu heti tutkimuksen alussa - on tavallista, että se jäsentyy tutkimuksen aikana. Tutkimuskysymys on kuitenkin tutkimuksen arvokkain

resurssi, ja sen puute hidastaa tutkimuksen etenemistä. (Eriksson & Koistinen, 2005, s. 19.)

Tutkimuskysymyksiä on kahdentyyppisiä: informaatio- ja asiakysymyksiä. Informaatiokysymykset ovat käytännönläheisempiä. Niiden on tarkoitus olla tutkimusta avustavia, ja ne ovat hyödyllisiä tutkittavan tapauksen kuvailun kannalta. Informaatiokysymysten ei ole tarkoitus olla varsinaisia tutkimuskysymyksiä. Tämän tehtävä on asiakysymyksillä. Niistä näkyy tutkimusta ohjaava teoria. (Eriksson & Koistinen, 2005, s. 20.)

Tapaustutkimuksia voidaan luokitella myös tutkimusasetelman näkökulmasta. Näitä ovat poikkileikkaustutkimus, pitkittäinen tapaustutkimus, ennen-jälkeen-tutkimus, tilkkutäkkitutkimus ja vertaileva tutkimus. Poikkileikkaustutkimusta pidetään vähiten merkityksellisimpänä, sillä sen tarkoitus on kuvata tiettyä organisaatiota (tai muuta kohdetta) tietyllä ajanhetkellä. Tämän ei nähdä antavan kovin yleistävää tai teoreettisesti vahvaa kuvaa. Pitkittäisissä tapaustutkimuksissa keskitytään pitempään ajankohtaan. Tällainen tutkimus voi esimerkiksi keskittyä muutokseen, joka tapahtuu tietyssä kohteessa. Ennen-jälkeen-tutkimuksen tarkoituksena on tutkia muutosta, mitä tietyssä kohteessa on tapahtunut tietyn ajankohdan jälkeen. Se on luonteeltaan pitkittäinen, mutta menee astetta syvemmälle, sillä tällöin voidaan vetää johtopäätöksiä syy-seuraussuhteista. Edellä mainittuja tutkimusasetelmia on kritisoitu siitä, että tällaisia tapaustutkimuksia voi olla vaikea yhdistää, koska ne voivat käyttää eri lähestymistapoja ja kattaa eri aikajaksoja. Tilkkutäkkitutkimusten tavoitteena on yhdistää edellä esitettyjä tutkimusasetelmia, jotta kohteesta saadaan mahdollisimman kokonaisvaltainen kuva. Vertailevat tutkimukset lähtevät samasta ideasta kuin tilkkutäkkitutkimukset, mutta niiden tavoitteena on laajentaa perspektiiviä entisestään. (Jensen & Rodgers, 2001, s. 237–239.)

Miten tapaus tai tapaukset tulisi valita? Eriksson & Koistinen (2005) painottavat, että tutkijan kannalta tärkeintä on valita aihe, joka kiinnostaa eniten. Tapaukset voidaan valita ennen tai jälkeen aineiston keruun ja ennen tutkimuskysymyksen muodostamista. Kiinnostus on esimerkiksi tässä tutkimuksessa tutkia kyberoperaatioita. Tutkija voi kerätä aineistoa esimerkiksi eri maissa tehdyistä hyökkäyksistä, ennen kuin tämä päättää, mitkä tapaukset otetaan tutkimukseen mukaan. Tapaukset voidaan valita joko teoriaan pohjautuen, tai havainnoimaan tutkimuskohteelle ominaisia piirteitä. Tapaukset tässä tutkimuksessa määritellään tutkimuksen kuluessa, joten kyseessä on aineistolähtöinen tapaustutkimus (Eriksson & Koistinen, 2005, s. 23–24). Tapauksia myös valitaan tutkimukseen enemmän kuin yksi. Eisenhardtin (1989, s. 537) mukaan useampi tapaus mahdollistaa havaintojen mahdollisen toiston. Tällöin teorian rakentaminen on vahvempaa, kun havainnot voivat nousta useasta eri tapauksesta ja vahvistaa toisiaan. Tapauksia saisi olla mieluiten 4 ja enintään 10. Alle neljän tapauksen kanssa on vaikeampi kehittää yksityiskohtaisempaa teoriaa. Yli kymmenen tapauksen yhtäaikainen yksityiskohtainen käsittely voi taas olla liian haastavaa juuri suuren datamäärän vuoksi. (Eisenhardt, 1989, s. 545.)

2.2.2 Monitapaustutkimus ja tutkimusstrategian valinta

Monitapaustutkimuksissa ollaan edelleen kiinnostuneita yksittäisistä tapauksista, sillä näiden kautta ymmärretään suurempaa kokonaisuutta. Edellä mainitussa kappaleessa olevat tapaustutkimukseen liittyvät kokonaisuudet pätevät myös monitapaustutkimuksen kohdalla. Se mikä erottaa monitapaustutkimuksen yksittäistapaustutkimuksesta on se, että tutkimuksen kohteena olevia tapauksia oletetaan yhdistävän jokin asia, jonka tutkijan tulee löytää. Tämän yhdistävän tekijän löytäminen on tapaustutkimuksen päätavoite. Kysymys siirtyykin yksittäistapaustutkimuksen ”Mikä auttaa minua ymmärtämään tapausta” kysymyksestä kysymykseen ”Mikä auttaa minua ymmärtämään kokonaisuutta”. Monitapaustutkimuksen alussa tutkijan tulee kuitenkin syventyä yksittäisiin tapauksiin. Tämän avulla ymmärretään paremmin sitä kokonaisuutta, johon yksittäiset tapaukset liittyvät. (Stake, 2006, s. 5–6.) Monitapaustutkimuksilla pyritään yleensä katsomaan yksittäistä tapausta laajempaa kuvaa. Tästä syystä monitapaustutkimukset ovat yleensä välineellisiä (Stake, 2006, s. 8).

Monitapaustutkimuksen tutkimuskysymyksen tavoitteena on selvittää, mikä on tapauksia yhdistävä kokonaisuus tai tekijä. Yleensä monitapaustutkimuksessa tutkimuskysymyksiä on enemmän kuin yksi. Tutkittaessa yksittäisiä tapauksia mielessä tulee pitää myös Stakesin (2006) nimittämä ”ongelma” (issue). Tämän ongelman selvittäminen ei vastaa tutkimuskysymykseen, vaan auttaa syventämään tietoutta yksittäiseen tapaukseen liittyen. Tutkimuskysymys on jatkojalostettu kysymys tästä ongelmasta. (Stakes, 2006, s. 9–10.) Tutkijan tulee kuitenkin varoa, että tämä ei kiinnitä liikaa huomiota tutkimuskysymykseen, jotta havaintoja voi tehdä myös tutkimuksen aikana nousevista uusista osa-alueista. Keskittymällä taas liian vähän tutkimuskysymykseen tutkijan huomio saattaa levitä liian laajalle, mikä voi estää tätä huomaamasta hienovaraisempia merkkejä tapauksia yhdistävistä tekijöistä. Tästä syystä tapausten kontekstin ymmärtäminen on tärkeää. Määrittämällä itselleen selkeät, mutta joustavat rajat, tutkija pitää narut käsissään olemalla kuitenkin avoin mahdollisia uusia havaintoja kohtaan. (Stakes, 2006, s. 13.)

Tätä tutkimusta toteutetaan ekstensiivisenä, vertailevana monitapaustutkimuksena. Ekstensiivinen lähtökohta soveltuu tämän tutkimuksen kyberoperaatioiden analysoimiseen hyvin, sillä tavoitteena on löytää ja analysoida operaatioiden taustalla vaikuttavia tekijöitä. Tapauksen rajaus tehdään tutkimuskysymyksen sekä määritelmien avulla. Soveltuvalla tutkimuskysymyksellä tutkimuksen päämäärä säilyy, ja määritelmillä voidaan sekä perustella kyberoperaatioiden soveltuvuus tutkimuskohteina, että valikoida soveltuvimmat operaatiot tutkimukseen. Esimerkiksi attribuution ja kyberoperaation käsitteiden määrittelyn avulla kyberoperaatioiden tekijän henkilöllisyys pyritään selvittämään mahdollisimman hyvin. Tekijää ei voida kuitenkaan täydellä varmuudella selvittää. Postpositivismin ajattelutavan mukaisesti kyberoperaatioihin liittyen hyväksytään se tosiasia, että kaikkia operaation yksityiskohtia ei pystytä saamaan selville. Lähteitä pyritään tästä syystä käyttämään mahdollisimman paljon varmistamaan, että tapauksesta löydetyt väitteet ovat mahdollisimman lähellä totuutta, eivätkä

nämä pohjaudu pelkästään yhden tutkijan tai lähteen ennakko-oletuksiin. Kyberoperaatioita analysoitaessa joudutaan näin ollen tekemään joitain oletuksia johtuen havaintojen puutteesta. Havaintojen puute on normaalia kybertoimintaympäristössä, sillä havainnot tietoverkossa tapahtuvasta toiminnasta on niin paikkaansa pitävää, mitä verkkoa analysoivat työkalut ja ihmiset kykenevät tuottamaan. Esimerkiksi ukrainalaisten sähköyhtiöiden tietoverkoissa ei ollut ollenkaan valvontatyökaluja, mikä helpotti sekä hyökkääjän toimia, että vaikeutti analysoijien työtä (Lee ym., 2016, s. 9). Tällöin johtopäätöksiä tehdään yleistyksiin pohjautuen. Tutkimuksessa tehdään esimerkiksi sellainen yleistys, että vaikka kaikissa tilanteissa ei tietoa ole asiaan liittyen saatu, on tutkittavia kyberoperaatioita edeltänyt tiedusteluvaihe, kuten yleensä perinteisiä sotilasoperaatioita edeltää (NATO, 2013, s. 79).

2.3 Strategisen kulttuurin teoria

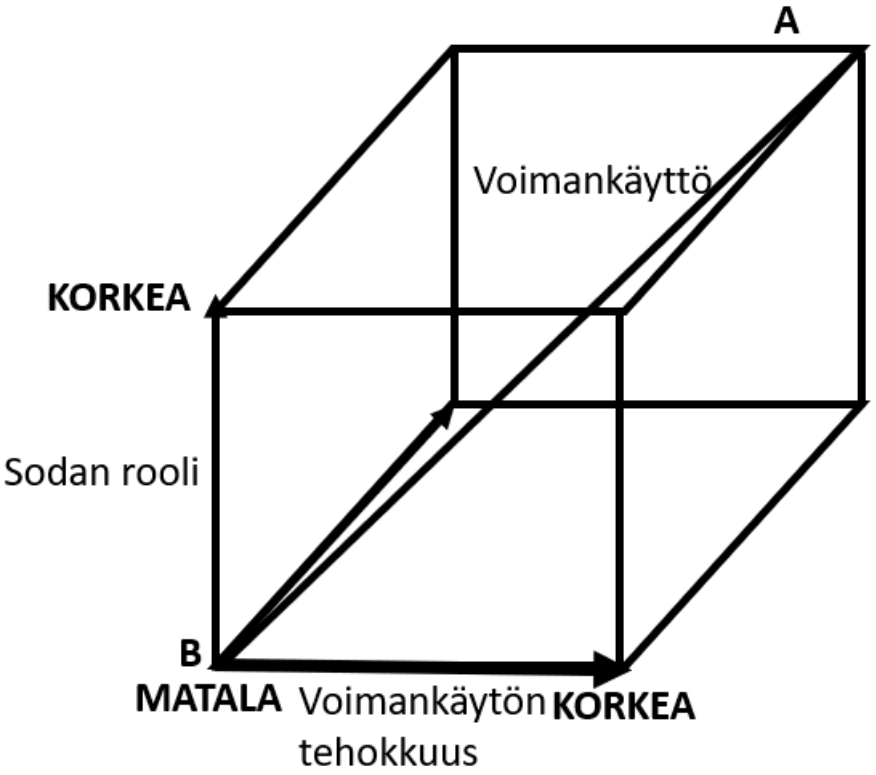
Valtioiden käyttäytymistä on pyritty selittämään valtion kulttuuriin vaikuttavien tekijöiden, kuten historiallisten ja poliittisten tekijöiden kautta. Jack Snyder käytti poliittisen kulttuurin viitekehystä tutkimuksessaan ”The Soviet Strategic Culture”. Tässä tutkimuksessa Snyder esitti, että Neuvostoliitossa esiintyy erilainen strategisen kulttuurin ilmapiiri, jonka avulla voidaan selittää neuvostoliittolaisten strategista ajattelutapaa ja käytöstä. Neuvostoliittolaisten tekemät päätökset eivät ole siis suoraa reagointia muuttuneeseen ympäristöön, vaan päätökset johtuvat taustalla vaikuttaneesta kulttuurisidonnaisesta ajattelumallista. (Snyder, 1977, s. 38.) Tämä teoria haastaa erityisesti neorealistisen teorian, jossa valtioiden tekemiä strategisia valintoja perustellaan hyötynäkökulmasta. Neorealistinen paradigma on se, että valtiot eivät eroa ajattelutavoiltaan juurikaan, vaan valtiot tekevät valintoja sen mukaan, kuinka paljon valtion oletetaan saavan hyötyä toteutuvan vaihtoehdon perusteella. Hyöty voi olla esimerkiksi alueluovutus tai jonkinlainen myönnytys toisen valtion suunnasta. (Vasquez, 1986, s. 321.) Tätä ajattelutapaa kohtaan on esitetty kritiikkiä johtuen sen heikosta selitysvoimasta. Neorealistinen paradigma ei esimerkiksi kykene selittämään hyvin tilanteita, jolloin valtioiden rakenteelliset lähtökohdat ovat samat, mutta kyseiset valtiot tekevät silti erilaisia strategisia ratkaisuja (Johnston, 1995, s. 35).

Snyderin jälkeen strategisen kulttuurin tutkimusta on jatkettu kolmeen eri sukupolveen jakautuvan jakson aikana. Ensimmäinen sukupolvi keskittyi selittämään amerikkalaisten ja neuvostoliittolaisten ajattelutavan eroavaisuuksia ydinaseiden käyttöön liittyen. Toisen sukupolven tutkijat lähtivät siitä ajattelutavasta, että johtoasemassa olevat henkilöt ajattelevat ja kertovat mahdollisista teoistaan hyvin eri tavalla, mitä he todella aikovat tehdä. Näissä kahdessa sukupolvessa oli Johnstonin (1995) mukaan paljon metodologisia puutteita, mikä vähensi strategisen kulttuurin vakuuttavuutta valtioiden käyttäytymisen selittämisessä. Ensimmäisen sukupolven alle menevä tutkimus ei esimerkiksi Johnstonin mukaan selittänyt strategian ja strategisen kulttuurin välistä suhdetta riittävän

selvästi, ja toisen sukupolven tutkimus jätti strategisen kulttuurin ja käyttäytymisen välisen suhteen merkityksen avoimeksi. Kolmannen sukupolven tutkimus, jota alettiin toteuttamaan 1990-luvulla, ei ottanut niin jyrkkää kantaa termistöihin kuin esimerkiksi ensimmäinen sukupolvi. Tämä mahdollistaa useamman eri lähestymistavan ja näkökulman käytön strategisen kulttuurin tutkimuksessa. Jotkut tutkijat voivat esimeriksi käyttää muuttujana asevoimien kulttuuria, ja toiset taas organisaatiokulttuuria. Kolmannen sukupolven tutkimukselle on myös ominaista erilaisten teorioiden vertailu ja testaaminen. (Johnston, 1995, s. 36–42.)

Strategisen kulttuurin lähtökohta on se, että jokaisella valtiolla on oma, toisistaan jollain tavalla eroava strateginen kulttuurinsa. Strateginen kulttuuri tarkoittaa ”yhteen liittyviä symboleita, kuten kieltä ja kielikuvia, jotka pyrkivät vakiinnuttamaan pitkäjänteisempiä strategisia valintoja täsmentämällä asevoimien käytön roolia ja tehokkuutta valtioiden välisessä kanssakäymisessä, ja projisoimalla tätä voimaa sellaisella varmuudella, että strategiset valinnat tuntuvat ehdottoman realistisilta ja tehokkailta.” (Johnston, 1995, s. 46.) Tämä kulttuuri koostuu erilaisista tekijöistä, kuten esimerkiksi yhteneväisistä ideoista ja arvoista. Nämä yhtenevät tekijät ohjaavat valtioiden turvallisuusajattelun suunnittelua ja toteutusta.

Strategiselle kulttuurille on yleensä ominaista sen hidas muuttuminen. Tekijät, jotka voivat kuitenkin vaikuttaa kulttuurin nopeampaan muutokseen, ovat ulkopuolelta tullut heräte, strategisen ajattelun kulmakivien ristiriitaisuus sekä valtion johdon vaikuttaminen strategiseen ajattelutapaan (Lantis, 2006). Esimerkki ulkoa tulleen herätteen vaikutuksesta on Saksan ulkopoliittisen ajattelutavan muuttuminen Bosnian humanitäärisen kriisin takia. Saksassa oli ollut toisen maailmansodan jälkeen vaikuttavana strategiana se, että maan asevoimia ei lähetetä valtion rajojen ulkopuolelle. Bosnian tilanne sai kuitenkin Saksan muuttamaan politiikkaansa, ja maa lähetti lopulta sotilashenkilöstöä tukemaan Yhdistyneiden kansakuntien operaatiota. Japanin strateginen kulttuuri taas joutui muutokseen, kun valtio joutui pohtimaan asevoimien käyttämistä rauhanturvaoperaatiossa 2000-luvun taitteessa. Kuten Saksa, myös Japani oli sitoutunut olemaan käyttämättä asevoimiaan maan rajojen ulkopuolella. Japani päätyi kuitenkin lähettämään joukkojaan rauhanturvaoperaatioon, mikä taas vaikutti maan strategiseen kulttuuriin asevoimien käytön suhteen. Yhdysvaltojen johto taas vaikutti suoraan maan strategiseen kulttuuriin ja asevoimien käyttötapaan, kun presidentti George Bush julisti sodan terrorismille New Yorkin terrori-iskujen jälkeen. Tällöin Yhdysvaltojen asevoimia aloitettiin käyttämään aktiivisemmin maan rajojen ulkopuolella terrorismin torjunnassa. (Kari, 2019a, s. 71.) Seuraavassa kuviossa (kuvio 1) on kuvattu strategisen kulttuurin viitekehys Johnstonin mukaan.



KUVIO 1 Strategisen kulttuurin teorian viitekehys (mukaillen Johnston, 1995, s. 47)

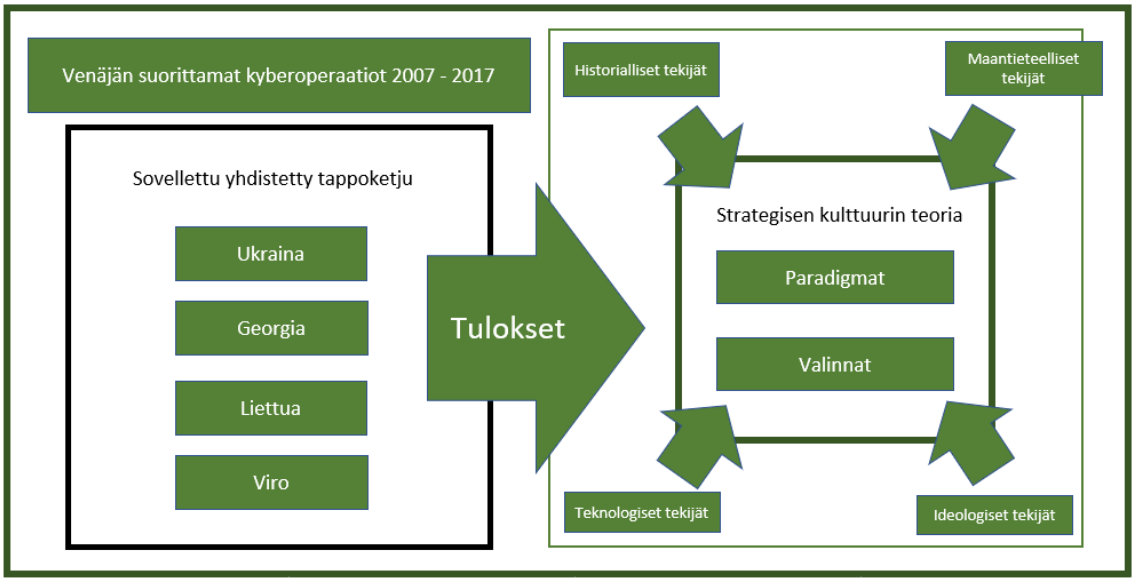
Strateginen kulttuuri rakentuu Johnstonin (1995) mukaan kahdesta osasta. Ensimmäinen osa koostuu teorian keskiössä olevasta yhdestä tai useammasta paradigmasta. Toinen osa koostuu paradigmaan liittyvistä valinnoista. Ensimmäisessä osassa olevaan paradigmaan liittyvät ajatukset sodan roolista maan sisäisessä sekä kansainvälisessä toiminnassa (frequency of conflict in human affairs), vastustajan rooli ja tämän muodostama potentiaalinen uhka (zero-sum nature of conflict) sekä voimankäytön tehokkuus ja miten voimalla kyetään muokkaamaan ympäröivää toimintaympäristöä haluamakseen (efficacy of violence). Kohdemaa pyrkii vähentämään strategisessa toimintaympäristössä olevaa epävarmuutta vaikuttamalla näihin paradigman kohtiin. Valtion käyttäytymistä pyritään ennustamaan valtion aiemmin tekemillä valinnoilla. Nämä valinnat heijastavat vallalla olevaa paradigmaa ja sitä, miten valtio todennäköisesti reagoi eteen tulleeseen tilanteeseen. Mitä hyökkäävämpi valtion valinta tilanteen ratkaisemiseksi on, sitä korkeammalle se sijoittuu edellä olevassa viitekehyksessä (eli lähemmäs kirjainta A). Mitä puolustuksellisemmasta vastauksesta on kyse, sitä matalammalle se viitekehyksessä sijoittuu (eli lähemmäs kirjainta B). Jokaiselle maalle ominainen strateginen kulttuuri alkaa vaikuttaa tässä vaiheessa valintojen hyökkäyksellisyyteen ja puolustuksellisuuteen. (Johnston, 1995, s. 47–48.) Tähän strategiseen kulttuuriin voivat vaikuttaa useat tekijät. Nämä tekijät voivat olla historiallisia, teknologisia, poliittisia tai hallinnollisia. Näiden neljän tekijän avulla on mahdollista selittää valtioiden tekemiä päätöksiä (Booth, 1990, s. 121; Kari, 2019b, s. 534), ja näin ollen myös valtioille ominaisia paradigmoja.

Strategisen kulttuurin teoriaa kohtaan on esitetty jonkin verran kritiikkiä. Gray (1988) esimerkiksi esitti väitteen, että sosiaalitieteet eivät ole kehittäneet tarkkaa metodia, jolla voitaisiin eritellä sellaisia strategisen kulttuurin osa-alueita, joilla voitaisiin selittää valtioiden toisistaan eroavat kulttuurit (Gray, 1988, s. 42). Strategisen kulttuurin määritelmä ei myöskään ole yleisesti hyväksytty (Eitelhuber, 2009, s. 4). Tämä näkyy tutkimuskirjallisuudessa, jossa eri tutkimuksissa on löydettävissä samoja Venäjään liitettyjä yleistyksiä, mutta yhtä tiettyä määritelmää venäläiselle strategiselle kulttuurille ei ole määritelty. Venäjään liitettyjä useammasta tutkimuksesta löytyviä yleistyksiä ovat esimerkiksi vastakkainasettelu Venäjän ja lännen välillä, etupiiriajattelu ja asevoimien rooli politiikassa (Ermarth, 2006; Eitelhuber, 2009; Sinovets, 2016; Covington, 2016).

Kybersodankäynti ja kyberoperaatiot nähdään lännessä usein osana hybridisodankäyntiä, ja näin ollen erillisenä toimialueena tavanomaisesta sodankäynnistä. Venäläisen näkemyksen mukaan tavanomainen sodankäynti (pitäen siis sisällään konventionaaliset joukot ja ydinaseet) ja länsimaisen näkemyksen mukainen hybridisodankäynti toimivat yhteisen päämäärän ja strategian mukaan. Venäjän strategisen kulttuurin mukaiset paradigmat ja valinnat heijastavat tämän takia valintoja myös kybertoimintaympäristöissä tehtäviin päätöksiin liittyen, joten strategisen kulttuurin teoriaa voidaan käyttää tarkastelemaan Venäjän reagointia ja päätöksiä kybertoimintaympäristössä. (Covington, 2016, s. 9; Kari, 2019a, s. 75.) Koska kyberoperaatiot ovat seurausta Venäjän strategisen kulttuurin pohjalta tekemistä päätöksistä, voidaan strategisen kulttuurin teoriaa käyttää kyberoperaatioiden analysoinnin tulosten pohdinnassa.

2.4 Tutkimuksen viitekehys

Alla olevassa kuviossa (kuvio 2) on esitetty tutkimuksen viitekehys.



KUVIO 2 Tutkimuksen viitekehys

Viitekehyksen vasemmalla puolella ovat Venäjän vuosien 2007 ja 2017 välillä suorittamat kyberoperaatiot, jotka on otettu tähän tutkimukseen mukaan. Ukraina-laatikko pitää sisällään NotPetyan lisäksi operaatio Armageddonin ja joulukuun 2015 sekä kesäkuun 2017 kyberoperaatiot. Nämä operaatiot analysoidaan kyberhyökkäyksen mallintamisen menetelmän, sovelletun yhdistetyn tappoketjun avulla. Perustelu tämän mallintamisen menetelmän valintaan esitellään kappaleessa 4. Operaatioista saaduista tuloksista on vedetty nuoli oikealle. Viitekehyksen oikealla puolella on kuvattu strategisen kulttuurin teorian kaksi keskeistä osaa: paradigmat sekä näistä johdetut valinnat. Näihin vaikuttavat ideologiset, teknologiset, historialliset ja maantieteelliset. Kyseiset tekijät ovat samat, mistä Booth (1990) esittää strategisen kulttuuriin vaikuttavien tekijöiden koostuvan. Tappoketjulla analyysin avulla saadut tulokset selitetään strategisen kulttuurin teorian avulla. Lopullisena tavoitteena on nostaa esiin operaatiokohtaisesti vaikuttaneet paradigmat ja näistä johtuneet valinnat, joita operaatioissa on tehty.

3 VENÄJÄÄN LIITETYT KYBEROPERAATIOT

Tämän luvun tarkoituksena on esitellä kirjallisuuskatsauksen perusteella löydetyt Venäjään liitetyt kyberoperaatiot. Ennen kyberoperaatioiden esittelyä määritellään kyberoperaation ja attribuution käsitteet. Kappaleen lopuksi tehdään yhteenveto ja määritellään, mitkä kyberoperaatiot otetaan lopulliseen analyysiin mukaan.

3.1 Kyberoperaatio

Kyberoperaation käsitteen määrittelemisen avulla voidaan rajata, millaisia tapauksia tutkimuksessa käsitellään. Käsitteen määrittelyllä tehdään myös ero kyberhyökkäyksen ja kyberoperaation käsitteiden välillä. Kyberoperaation määritelmä vaihtelee lähteen mukaan. Maanpuolustuskorkeakoulun Kyberkäsikirja määrittelee kyberoperaation suunnitelmalliseksi toimintojen kokonaisuudeksi, joka tapahtuu joko kybertoimintaympäristössä tai kybertoimintaympäristön avulla ja jolla pyritään vaikuttamaan kohteen toimintaan. Kyberoperaatiot nähdään osana laajempaa kokonaisuutta maa-, meri- ja ilmavoimien operaatioiden rinnalla. Niillä voidaan joko tukea muita operaatioita tai vaihtoehtoisesti muilla operaatioilla voidaan tukea kyberoperaatioita. (Laari, Flyktman, Härmä & Timonen, 2019, s. 49.) Kyberoperaatiot voidaan jakaa puolustuksellisiin ja hyökkäyksellisiin operaatioihin sekä johtamisjärjestelmäoperaatioihin (JOJÄ-operaatio). JOJÄ-operaatiolla tarkoitetaan kokonaisuutta, jossa on jatkuvasti käynnissä useita prosesseja, joilla ylläpidetään kohteen kyberturvallisuutta. Esimerkiksi Yhdysvalloilla on jatkuva ”DODIN OPS” -niminen JOJÄ-operaatio, jolla se pyrkii turvaamaan Yhdysvaltojen puolustusministeriön verkkojen operaatiovarmuuden. Lobelin (2011, s. 622) määritelmä kyberoperaatiosta on teknisempi ja se lähestyy operaation määritelmää hyökkääjän näkökulmasta. Hänen mukaansa hyökkäykselliset kyberoperaatiot voidaan jakaa kahteen eri kategoriaan: järjestelmiä vastaan tehtyihin hyökkäyksiin tai järjestelmien hyväksikäyttöön. Samaa jakoa käyttää myös Lin (2010, s. 63). Järjestelmiä vastaan tehtyjen hyökkäysten tarkoituksena on joko tiedon, tietoverkkojen tai laitteiston tuhoaminen (Owens, Dam & Lin, 2009, s. 73). Järjestelmien hyväksikäyttö taas ei välttämättä aiheuta mitään tuhoa fyysistä tuhoa kohteessa, vaan hyökkääjän tarkoituksena on saada tietoa kohteestaan (Clark & Landau, 2011, s. 6). Turvallisuuskomitean Kyberturvallisuuden sanaston määritelmän (Olin ym., 2018) voidaan nähdä olevan sekä Kyberkäsikirjan että Lobelin (2011) määritelmän yhdistelmä. Sen mukaan kyberoperaatio on ”suunnitelmallinen ja johdettu sarja pääosin kybertoimintaympäristössä” tapahtuvia toimintoja, joilla pyritään hankkimaan tietoa kohteesta tai vaikuttamaan sen toimintaan”. (Olin ym., 2018, s. 27.) Varsinaisten kyberoperaatioiden kesto voi vaihdella suurestikin. Ne voivat olla ohi sekunneissa (kuten aikautetuissa hyökkäyksissä), tai ne voivat olla pitkäkestoisia, useita vuosiakin

kestäviä operaatioita (Owens, Dam & Lin, 2009, s. 313; Laari ym., 2019, s. 38). Kyberoperaation toteuttaja voi olla yksittäinen henkilö, jokin rikollisryhmittymä tai valtiollinen toimija (Laari ym., 2019, s. 61; Olin ym., 2018, s. 27).

Kyberoperaatio eroaa kyberhyökkäyksestä siten, että kyberhyökkäyksen voi nähdä tarkoittavan yksittäistä ja pienempimuotoisempaa tapahtumaa kuin kyberoperaatio. Kyberhyökkäys voi tarkoittaa esimerkiksi palvelunestohyökkäystä tai haittaohjelman avulla tehtyä hyökkäystä. Kyberhyökkäys voi tarkoittaa myös muuta kuin tietoverkkojen kautta tehtyä hyökkäystä (Olin ym., 2018, s. 30). Kyberhyökkäys tehdään siis osana kyberoperaatiota, ja kyberoperaatio voi pitää sisällään useita kyberhyökkäyksiä (Laari ym., 2019, s. 37; Lin, 2010, s. 64).

Tässä tutkimuksessa kyberoperaatiolla tarkoitetaan kybertoimintaympäristössä tai kybertoimintaympäristön avulla tapahtunutta operaatiota, jonka toteuttajana tai tukijana on ollut valtio tai valtiollinen toimija. Operaation osana on voitu toteuttaa yksi tai useampi kyberhyökkäys vaihtelevalla aikavälillä kybertoimintaympäristössä samaa kohdetta vastaan. Kybertiedustelun nähdään tässä yhteydessä kuuluvan osaksi kyberoperaatiota, sillä sen nähdään olevan erottamaton osa hyökkäysketjua (Sanghvi & Dahiya, 2013, s. 36; Yadav & Mallari, 2015, s. 438). Kyberoperaatio toteutetaan osana muuta vaikuttamista, joka voi olla esimerkiksi kineettistä (kuten maaoperaatio) tai poliittista vaikuttamista. Kyberoperaatiolla hyökkääjä pyrkii saavuttamaan jonkin tavoitteen, joka on osa strategisen tasan tavoitetta. Tämä määrittely ohjaa analysoitavien tapausten valitsemista. Täytyy ottaa kuitenkin huomioon, että kyseisen määritelmän tekoa ovat ohjanneet länsimaiset lähteet. Venäjä ei esimerkiksi käytä omissa doktriineissaan termiä kyberympäristö. Tämän sijasta venäläiset käyttävät termiä informaatioympäristö (engl. information space). Tähän ympäristöön lukeutuu länsimaisen ajattelutavan mukainen informaatiosodankäynti (kuten harhauttavan materiaalin jakaminen verkossa) (Giles, 2016, s. 9). Syy, miksi kyberoperaation määritelmä on tehty länsimaisesta näkökulmasta, on se, että operaatioiden lähteinä käytettävät tutkimukset ovat myös länsimaalaisia.

3.2 Attribuutio

Tämän tutkimuksen tarkoituksena on analysoida Venäjän toteuttamia kyberoperaatioita. Toisin kuin konventionaalisten hyökkäysten tapauksessa, kyberhyökkäysten (ja tätä kautta kyberoperaatioiden) liittäminen yhteen tiettyyn tekijään on haastavaa (McDermott, 2010, s. 229). Digitaalisessa toimintaympäristössä hyökkääjän nimeäminen voi olla jopa mahdoton tehtävä (Kallberg, 2016, s. 103). Tämä luo niin sanotun attribuutio-ongelman. Attribuutio tarkoittaa ”hyökkäyksellisen kyberoperaation toteuttajan tunnistamista, paikantamista ja tarvittaessa oikeudellista vastuuseen saattamista”. Hyökkäykselliseen kyberoperaatioon liittyen hyökkääjä saattaa käyttää kaapattuja palvelimia, tietokoneita tai muita verkkolaitteita. Tämän takia pelkkä IP-osoitteen perusteella tehtävä paikannus ei ole luotettava, sillä osoite ohjaa ainoastaan kaapatun laitteen luokse. Ongelmaksi tu-

lee myös se, että valtioiden erilaiset oikeuskäytännöt tai yksinkertaisesti haluttomuus edesauttaa omien kansalaistensa edesvastuuseen saattamista voivat estää hyökkäyksen toteuttajan tuomitsemisen, vaikka hyökkääjä olisikin saatu tunnistettua. (Olin ym., 2018, s. 27.)

Attribuutio-ongelman ratkaisua voidaan lähestyä kolmelta eri tasalta: taktistekniseltä, operatiiviselta ja strategiselta tasalta. Taktisteknisen tasan tarkoituksena on selvittää, miten hyökkäys on tapahtunut. Tämä tarkoittaa esimerkiksi niiden keinojen selvittämistä, joilla hyökkääjä on päässyt sisälle järjestelmiin. Operatiivisen tasan analyysillä pyritään selvittämään hyökkäyksen arkkitehtuurin rakennetta, kuten mitä kautta hyökkääjä on tunkeutunut järjestelmään sisälle. Lisäksi tavoitteena on selvittää, millainen hyökkääjän profiili on (tähän profiiliin kuuluvat esimerkiksi hyökkääjän käyttämän laitteiston yksityiskohdat sekä IP-osoite). Strategisen tasan tarkastelulla pyritään selvittämään hyökkääjän henkilöllisyys ja syy, miksi kyseinen hyökkäys on tehty. Analyysin vaatima tarkkuus pienenee, lähemmäs strategista tasaa siirrytään. Teknisen analyysin pohjalta voidaan vastata hyvinkin tarkasti esitettyihin kysymyksiin, esimerkiksi siihen, mistä IP-osoitteesta hyökkäykset tulivat. Strategiseen analyysiin taas voi liittyä paljon olettamuksia ja johtopäätöksiä. (Rid & Buchanan, 2015, s. 10–11.)

Triangulaation avulla hyökkääjän henkilöllisyys voidaan saada todennäköisemmin selville. Tämä tarkoittaa sitä, että mitä enemmän analyysiä tekevällä henkilöllä on lähteitä käytössään, sitä lähemmäs oikeaa tekijää analyysissä päästään. (Rid & Buchanan, 2015, s. 10–11.) Lähteet voi jakaa esimerkiksi tiedusteluorganisaatioiden lähteisiin, poliittisiin lähteisiin, tekniseen tietoon sekä hyökkäykseen yhdistettäviin tekijöihin. Tiedusteluorganisaatioilla voi olla sisäpiirin tietoa tai heillä voi olla seurannassaan henkilöitä, joiden kautta raskauttavaa tietoa hyökkääjän henkilöllisyydestä saadaan selville. Poliittinen lähde voi tarkoittaa valtion tai organisaation lausuntoa hyökkäyksen vastuunottamisesta. Teknisiin tietoihin voidaan laskea laitteen sijaintitiedot, mutta myös hyökkäyksen laajuus. Esimerkiksi suuren mittakaavan palvelinestohyökkäys rajaa pienempiä rikollisryhmiä ja yksittäisiä kansalaisia pois epäiltyjen listalta. Yhdistettäviin tietoihin lasketaan ne yksityiskohdat, jotka voidaan yhdistää varmasti hyökkääjään. Esimerkiksi Georgian ja Venäjän sodassa sodan osapuolien henkilöllisyyksistä ei ollut epäilystä. Tällöin Georgiaa vastaan tehdyn kyberoperaation hyökkääjän henkilöllisyys oli helpompi yhdistää venäläisiin hakkereihin. (Owens, Dam & Lin, 2009, s. 19.)

Muita tapoja henkilöllisyyden varmistamiseksi on esimerkiksi se, että useampi tutkija päätyy samaan lopputulokseen. Tällöin selville saatua henkilöllisyyttä voidaan pitää kohtuullisen luotettavana. Hyökkääjä voi myös käyttäytyä selvästi erottautuvalla tavalla (McDermott, 2010, s. 235). Esimerkiksi Red October-niminen APT-ryhmä kohdisti iskunsa pääasiassa Itä-Eurooppaan, entisiin Neuvostoliiton jäsenmaihin sekä Keski-Aasian valtioita kohtaan (Mwiki, Dargahi, Dehghantanha & Choo, 2019, s. 224). Tämän tyyppiset selkeästi erottuvat ominaisuudet helpottavat hyökkääjän henkilöllisyyden selvittämistä.

Attribuution lopullisena tavoitteena on siis selvittää hyökkäyksen toteuttanut organisaatio tai valtio. Päätavoite ei siis ole yksilöiden henkilöllisyyden selvittäminen. Henkilöllisyyksien selvittämisellä voidaan kuitenkin edesauttaa taustalla vaikuttavan organisaation selvittämistä. Esimerkiksi vuonna 2014 ”cpyy”-nimisen pseudonyymin takana toimiva henkilö saatiin yhdistettyä videoblogeista ja valokuva-albumeista saadun tiedon kautta Chen Ping-nimiseen henkilöön. Pingin valokuvien kautta löydettiin katuosoite, joka saatiin yhdistettyä Kiinan armeijan tiedusteluyksikköön. Valtiollisen toimijan selvittämiseen tarvittiin siis hyvinkin yksityiskohtaista, henkilötasolle menevä analyysia. Analysoijan tulee kuitenkin varoa, että ennakkoluulot eivät ohjaa analyysin tekemistä liikaa. (Rid & Buchanan, 2015, s. 13.) Esimerkiksi venäläisiä voi olla helppo syyttää uusista kyberhyökkäyksistä ilman tarkempaa todistusaineistoa. Tällaiseen syytökseen voi johtaa esimerkiksi venäläisten aiempi käytös rajanaapureitaan kohtaan sekä venäläisten käyttämä retoriikka. Jos kiinalaiset ovat tehneet yhden hyökkäyksen amerikkalaisten tietoverkkoja kohtaan, on kiinalaisia helppo syyttää seuraavistakin hyökkäyksistä, vaikka tietoa hyökkääjien identiteetistä ei olisikaan ehditty kerätä riittävästi (McDermott, 2010, s. 232).

Yleinen attribuutioon liittyvä ongelma on rajallinen aika. Hyökkääjän henkilöllisyys halutaan saada mahdollisimman pian selville, jotta vastatoimenpiteet voidaan käynnistää. Kiirehtiminen hyökkääjän henkilöllisyyden selvittämisessä voi johtaa kuitenkin virheisiin ja pahimmassa tapauksessa väärän analyysin tekemiseen. (Owens, Dam & Lin, 2009, s. 19.) Tämän tutkimuksen tapauksessa aikaresurssi ei ole ongelma. Se on ainoastaan tutkimuksen operaatioiden valintaa rajaava tekijä. Jos operaatiosta ei ole kulunut riittävän pitkää aikaa, ei kyberoperaation tehneen hyökkääjän henkilöllisyyttä ole välttämättä voitu varmistaa.

Tässä tutkimuksessa attribuutio-ongelma pyritään ratkaisemaan käyttämällä mahdollisimman laajasti eri lähteitä, jotta operaatiokohtaiset tiedot pystytään varmistamaan. Lähteiden tulee myös olla samaa mieltä siitä, kuka hyökkäyksen on toteuttanut. Jos johonkin operaatioon liittyen ei löydetä riittävästi tietoa, ei kyseistä operaatiota oteta mukaan lopulliseen analyysiin.

3.3 Viro

Viron tasavalta on yksi niistä Baltian maista, joka itsenäistyi uudelleen Neuvostoliitosta vuonna 1991. Itsenäistymisensä jälkeen Viro suuntasi katseensa länteen, ja liittyi heti tilaisuuden tullen sekä Euroopan Unioniin, että Natoon. Samalla maa alkoi kehittää yhteiskuntaansa voimakkaasti teknologiasta riippuvaisemmaksi. Tämän seurauksena 2000-luvulle tultaessa moni virolainen peruspalvelu oli siirtynyt verkkoon. Esimerkiksi vuonna 2007 yli 95 prosenttia pankkisiirroista tehtiin verkon kautta, ja monet muut palvelut, kuten opetus ja vaaleissa äänestäminen, tehtiin ainakin joiltain osin verkon välityksellä. (Ashmore, 2009, s. 4.) Riippuvuus teknologiasta ja teknologian läsnäolo lähes jokaisella yhteiskunnan osa-alueella olivat osasyitä siihen, että Viroa vastaan toteutettiin ensimmäinen valtiotason kyberoperaatio (Ashmore, 2009, s. 7).

Huhtikuussa 2007 Viron hallitus päätti siirtää venäläisen toisen maailmansodan aikaisen muistomerkin Tallinnan keskustasta läheiselle sotilashautausmaalle. Kyseisellä patsaalla on ollut kaksijakoinen merkitys tallinnalaisten ja virolaisten silmissä. Viron venäläistaustaiselle väestölle patsas symbolisoi Venäjän roolia maan ja Euroopan vapauttajana toisessa maailmansodassa, kun taas virolaisille patsas muistuttaa vuosikymmenten neuvostovallan ja sorron alla olemisesta. (Ottis, 2008, s. 3.) Patsaan siirto aiheutti voimakkaan vastareaktion juuri Viron venäjänkielisessä väestössä, ja vironvenäläiset alkoivat osoittaa mieltään siirtoa vastaan (Libicki, 2009, s. 1). Siirtosuunnitelmat aiheuttivat Venäjän ja Viron hallitusten välien kiristymisen. Painostuskeinona Viroa kohtaan Venäjä keskeytti raideliikenteen Tallinnan ja Pietarin välillä ja uhkasi patsaan poistamisen olevan Virolle kohtalokasta (Ashmore, 2009, s. 7; Davis, 2007). Mielenosoitukset yltyivät 27.4. väkivaltaisiksi, jolloin mielenosoittajat hyökkäsivät mellakkapoliisia vastaan ja aiheuttivat vahinkoa läheisille liiketiloille. Samoihin aikoihin Viroa kohtaan tehtiin useita kyberhyökkäyksiä. Nämä hyökkäykset kuuluivat kyberoperaatioon, jossa valtio pyrki vaikuttamaan ensimmäistä kertaa laajamittaisesti kyberkykyjen avulla toisen valtion toimintaan. (Davis, 2007.) Kyberhyökkäykset Viroa kohtaan alkoivat 26.4.2007, ja ne kestivät aina kesäkuun alkuun saakka. Hyökkäysten intensiteetti ja määrä vaihtelivat tällä ajanjaksolla, mutta suurin osa kyberhyökkäyksistä yhdistettiin patsaan siirtämisestä aiheutuneeseen diplomaattiseen kiistaan. (Ottis, 2008, s. 2–3.) Hyökkäykset alkoivat laantua 19. päivä toukokuuta diplomaattisen tilanteen helpottuessa. Joitain hyökkäyksiä toteutettiin vielä toukokuun lopulla. (Tikk ym., 2010, s. 16).

Pääosa hyökkäyksistä koostui palvelunestohyökkäyksistä, eli niin kutsutuista DDoS (engl. Distributed Denial of Service) -hyökkäyksistä. Hyökkääjät toteuttivat esimerkiksi suuren määrän ping-kyselyitä, vääristyneitä verkkokyselyitä ja roskapostihyökkäyksiä. Vähäisissä määrin havaittiin myös SQL-injektiohyökkäyksiä. Verkkokyselyissä havaittiin vihamielisiä viestejä, kuten "ANSIP_PIDOR=FASCIST" (Ansip oli Viron pääministeri vuonna 2007). (Ottis, 2008, s. 3.) Palvelinestohyökkäysten lisäksi käytettiin puhelinestohyökkäyksiä ainakin Viron parlamentin jäseniä ja hätänumeropalvelua kohtaan (Green, 2015, s. 17; Tikk ym., 2010, s. 21). Muissa hyökkäyksissä hakkerit käyttivät hyväkseen tunnettuja haavoittuvuuksia, kuten Apache-palvelinohjelmiin ja PHP-kieleen liittyviä haavoittuvuuksia (Aslanoğlu & Tekir, 2012, s. 3.) Hyökkäysten apuna käytettiin laajamittaisesti bottiverkkoja (Ashmore, 2009, s. 7). Bottiverkkojen ohella hyökkäyksiä varten rekrytoitiin Venäjän kansalaisia ja venäjää puhuvia rekrytointiin perustettujen verkkosivujen avulla. Näillä sivustoilla oli tarkat ohjeet siitä, miten ja milloin hyökkäys tulisi toteuttaa, mikä helpotti asiaan vihkiytymättömän henkilön hyökkäyksiin osallistumista. (Ottis, 2008, s. 2.) Hakkerit onnistuivat myös murtautumaan virolaisen reformipuolueen nettisivuille, jonne hyökkääjät laittoivat väärennetyn anteeksipyynnön patsaan siirrosta. Anteeksipyyntöön oli väärennetty Viron pääministerin allekirjoitus. (Tikk ym., 2010, s. 21.)

Hyökkäykset kohdistuivat verkkotasolla verkko-, sähköposti- ja DNS-palvelimia sekä reitittimiä kohtaan. Hyökkäyksen kohteina olivat Viron ministeriöt, parlamentti, poliisin toimipisteet, pankkisektori, internetin palveluntarjoajat,

verkkomedia sekä useat pienet yritykset ja paikallishallinnot. (Ottis, 2008, s. 3.) Hyökkäysten havaittiin tulevan ulkomailta ja erityisesti venäläisistä osoitteista (Kozlowski, 2013, s. 238). Viro vastasi hyökkäyksiin estämällä pääsyn hyökkäyksen kohteena oleviin verkkosivuihin, ja sulkemalla kaiken verkkoliikenteen, joka tuli Viron rajojen ulkopuolelta. (Aslanoğlu & Tekir, 2012, s. 3). Hyökkäysten vaikutuksesta maksujen tekeminen korteilla ei hetkellisesti onnistunut ja matkapuhelinliikenteessä oli ajoittaisia häiriöitä. Hyökkäykset eivät kuitenkaan onnistuneet vaikuttamaan tavalliseen kansalaisen elämään, sillä häiriöt olivat lyhytaikaisia (Pernik, 2018, s. 56).

Vaikka hyökkääjän henkilöllisyyttä ei virallisesti ole kyetty todistamaan, epävirallisesti syyllisenä pidetään Venäjää. Todistusaineiston puuttumisen löytymistä on haitannut erityisesti se, että Venäjä ei ole ollut halukas auttamaan tutkinnan etenemisessä ja niiden syyllisten löytämisessä, jotka toimivat Venäjän maaperältä käsin (Ottis, 2007, s. 3).

On kuitenkin perusteltua epäillä, että Venäjän hallituksella on ollut jonkinlainen osa Viroa vastaan tehdyissä kyberhyökkäyksissä. Osa hyökkääjistä on todennäköisesti ollut venäläisiä patriootteja, jotka Venäjän hallituksen retoriikan innoittamana saivat syyn hyökätä Viroa vastaan. Tätä väitettä tukevat verkkosivut, joiden kautta tavallinen kansalainen pystyi helposti ottamaan osaa hyökkäyksiin. Kyberhyökkäykset myös tapahtuivat samaan aikaan, kun Venäjän ja Viron välit olivat tulehtuneet patsaskiistan takia. Iskujen jälkeen venäläinen, Kremlin-myönteinen nuorisoryhmä otti vastuun iskujen toteuttamisesta. Tämän on nähty yhtenä todisteena siitä, että Venäjän hallituksella olisi ollut jotain tekemistä kyberhyökkäysten kanssa. Hyökkäykset eivät myöskään kohdistuneet tiettyyn yritykseen tai organisaatioon, vaan ne kohdistuivat koko Viron valtiota kohtaan. (Ashmore, 2009, s. 6.) Osassa operaation myöhäisemmässä vaiheessa toteutetuista hyökkäyksistä oli keskitetyn johtamisen piirteitä ja viitteitä siitä, että hyökkääjillä oli käytössään suurempi määrä resursseja mitä tavallisilla hakkereilla normaalisti on käytössään. Hyökkäykset myös tehtiin aalloissa, jotka oli aikautettu täsmällisesti. (Tikk ym., 2010, s. 23.)

Yksi oletettu syy kyberhyökkäysten tekemiseen oli pakottaa Viro luopumaan patsaan siirrosta, mikä olisi samalla voitu nähdä Venäjän näkökulmasta poliittisena saavutuksena. Toinen syy on mahdollisesti ollut testata Venäjän kybertoimintakykyjä ja seurata erityisesti Naton reaktiota, kun yhtä sen jäsenmaata kohtaan toteutetaan perinteisestä ajattelutavasta (eli konventionaalisesta hyökkäyksestä) poikkeava hyökkäys. Kolmas syy on voinut olla halu näyttää EU:lle ja Natolle, että tämäntyyppistä hyökkäystä vastaan on vaikea puolustautua. Ashmoren (2009, s. 7) mukaan hyökkääjän tavoitteena oli myös internetin sulkeminen Viron laajuisesti. Hyökkäysten voidaan todeta kuitenkin epäonnistuneen tavoitteissaan. Patsas siirrettiin pois alkuperäisestä paikasta, ja Viro sai syyn kehittää kyberpuolustuskykyjä entisestään. (Kozlowski, 2013, s. 238.) Hyökkäys oli myös Natolle tietynlainen herätys, ja Nato onkin lisännyt jäsenmaidensa välistä yhteistyötä kyberpuolustuskykyjen kehittämisessä, kyberharjoitusten järjestämisessä ja ottanut kybertoimintaympäristön paremmin huomioon puolustuspolitiikoissaan ja tavoitteissaan (Joubert, 2012, s. 6).

3.4 Liettua

Liettua itsenäistyi uudelleen vuonna 1991 Neuvostoliiton hajoamisen jälkeen (Osawa, 2017, s. 118). Itsenäistymisensä jälkeen Liettua aloitti Viron tavoin lähentymisen länsimaita kohti. Valtio liittyikin heti tilaisuuden tullen Natoon ja Euroopan Unioniin, ja on pyrkinyt pitämään välit erityisesti Yhdysvaltoihin hyvinä (Šešelgytė, 2010, s. 28). Liettuaa vastaan tehtiin 28. kesäkuuta – 2. heinäkuuta 2008 useita kyberhyökkäyksiä. Hyökkäykset tapahtuivat sen jälkeen, kun Liettua kielsi lakimuutoksella neuvostoliittolaisten ja kommunististen symbolien käytön. Venäjä sekä Valko-Venäjä protestoivat Liettuan päätöstä vastaan, kun taas Liettuassa asunut venäläisväestö suhtautui asiaan rauhallisemmin kuin Virossa asunut venäläisväestö Viron patsaskiistan aikaan. (Tikk ym., 2010, s. 63.)

Hyökkäyksiä toteutettiin lopulta noin 300 liettualaista verkkosivua kohtaan, ja ne kohdistuivat pääosin yhtä internetin palveluntarjoajaa vastaan (Alexander, 2014, s. 9). Toisin kuin Viro, Liettuan valtio oli saanut hyökkäyksistä tiedon etukäteen, ja vastatoimiin pystyttiin ryhtymään ennen hyökkäyksiä. Tämä tieto ei kuitenkaan kantautunut yksityiselle sektorille asti, joiden verkkosivut ja järjestelmät joutuivat kärsimään hyökkäyksistä eniten. (Tikk ym., 2010, s. 55; Rhodin, 2008.)

Verkkosivuja vastaan tehdyt hyökkäykset koostuivat pääosin verkkosivujen häpäisyistä sekä roskapostien lähettämisestä. Verkkosivuille lisättiin Neuvostoliittoon liittyviä symboleita sekä Venäjämyönteistä tekstiä. Hyökkääjät käyttivät verkkosivujen muuttamiseen PHP-nimistä ohjelmaa. Sivuille päästiin esimerkiksi Ranskassa ja Ruotsissa sijainneiden palvelimien kautta. (Tikk ym., 2010, s. 54.) Epäselväksi jäi, oliko sivustoilla tai palvelimissa jokin haavoittuvuus, jota kautta hakkerit pääsivät kohteisiinsa. Roskapostiviestien avulla hyökkääjät levittivät poliittista manifestia, jossa tuomittiin länsimaiden ja Naton toiminta Venäjää kohtaan (Tikk ym., 2010, s. 54). Puolustajien hämäämiseksi hyökkääjät olivat piilottaneet henkilöllisyytensä eri tavoilla. Tikkin ym. (2010, s. 55) tutkimuksessa mainitaan nimeltä ainoastaan Tor-verkon käyttö, vaikka kyseisessä tutkimuksessa annetaan myös ymmärtää, että jälkiä oli peitelty muillakin tavoilla.

Operaatioon osallistuneet hakkerit olivat pääosin venäläisiä tai venäjää puhuvia, sillä rekrytointi tapahtui suurimmaksi osaksi venäjänkielisen hackwars.ru -nimisen verkkosivuston kautta. Tällä ja muilla vastaavilla sivustoilla hyökkäyksiin yllyttämisessä käytettiin retoriikkaa, joka sitoi hyökkäyksiin osallistumisen uskollisuuden näyttämiseksi Venäjää kohtaan. Verkkosivustot siis antoivat ymmärtää, että jos et osallistunut hyökkäyksiin, et ollut uskollinen Venäjän valtiolle. (Tikk ym., 2010, s. 55.) Osa hyökkäyksiä tehneistä tahoista yhdistettiin myös venäläisiin rikollisorganisaatioihin, jotka saivat mahdollisesti tukea venäläisten tiedustelupalvelulta (Daricili, 2014, s. 9).

Hyökkäyksiä ei kohdistettu mitään tiettyä verkkosivustoa tai tietyn organisaation sivustoja kohtaan (Tikk ym., 2010, s. 54). Hyökkäyksistä ei siis saatu esimerkiksi rahallista hyötyä. Tämä sulkee sen mahdollisuuden pois, että operaation suorittajina olivat pelkästään rikollisia tai rikollisryhmittymiä. Rikollisten

tulisi jollain tavalla saada hyötyä operaation suorittamisesta. Rahoitusta on tällöin saatu joltain muulta taholta, kuten esimerkiksi valtiolta (Shakarian, 2011, s. 67). Ihmisiä yllytettiinkin hyökkäyksiin lähinnä kansallistunteeseen vetoamalla. Nämä seikat tukevat teoriaa siitä, että kyberoperaatiolla oli ideologinen tavoite. Kyberoperaation poliittisen tason tavoitteita ja tekijää ei tiedetä, koska operaation taustavaikuttajat ovat jääneet hämärän peittoon. Epäilyt kuitenkin kohdistuvat Valko-Venäjää ja Venäjää kohtaan (McLaughlin, 2008). Erityisesti Venäjän osuutta puoltaa venäläistaustaisten hakkereiden osuus hyökkäysten toteuttajina. Oletettavasti tavoitteena oli jollain tavalla vaikuttaa Liettuan valtioon, sillä operaatiolla voidaan nähdä olevan samankaltaisuuksia Viron patsaskiistaan liittyneessä kyberoperaatiossa, vaikkakin pienemmässä mittakaavassa. Operaation voidaan todeta epäonnistuneen oletetuissa tavoitteissaan, sillä pysyvää vahinkoa tai haittaa ei juurikaan päässyt syntymään. Suurin vahinko syntyi yksityiselle sektorille, jolle varoitus tulevista kyberhyökkäyksistä ei välittynyt. Yritysten kärsimät vahingot eivät muodostuneet kuitenkaan suuriksi. (Tikk ym., 2010, s. 63.)

3.5 Georgia

Georgia on vanha neuvostoliittolainen satelliittivaltio, joka Viron tavoin itsenäistyi uudestaan Neuvostoliiton hajottua. Myös Georgia alkoi itsenäistymisensä jälkeen lähentyä länsimaita. Tämä trendi kasvoi erityisesti vuoden 2003 jälkeen, kun Mikheil Saakashvili valittiin Georgian presidentiksi. (Kozlowski, 2013, s. 238.) Hänen tavoitteenaan oli integroida Etelä-Ossetian ja Abkhazian maa-alueet takaisin Georgiaan. Kyseiset alueet olivat historiallisesti olleet aina lähellä Venäjää, ja joiden kanssa Georgia oli aiempina vuosikymmeninä käynyt pienimuotoisempia aseellisia yhteenottoja (Cornell & Starr, 2009, s. 17). Yritykset integroida nämä alueet takaisin Georgiaan johtivat lopulta vuoden 2008 elokuussa käytyyn sotaan Venäjää vastaan (Kozlowski, 2013, s. 238).

Heinäkuun 19. päivänä palvelinestohyökkäys Saakashvilin verkkosivuja kohtaan sulki kyseisen sivuston yhdeksi vuorokaudeksi. Tämä oli alkusoitto suuremmalle kyberoperaatiolle, joka alkoi muutamaa viikkoa myöhemmin, 7. elokuuta 2008. Tällöin koordinoidut hyökkäykset georgialaisia verkkosivuja vastaan aloitettiin päivää ennen venäläisjoukkojen vastahyökkäystä georgialaisten maajoukkoja vastaan. (Ashmore, 2009, s. 10.) Kyseessä oli ensimmäinen laajamittainen kyberoperaatio, joka tuki samanaikaisesti toteutettua konventionaalista maahyökkäystä (Shakarian, 2011, s. 68). Hyökkäysten takia suurimpaan osaan Georgian hallituksen verkkosivuista ei ollut pääsyä. Tämän takia Georgian hallinnon kyky toimia ja viestiä kansalaisilleen verkon kautta oli hyvin rajoitettu, mikä ajoikin hallituksen siirtämään kriittisimmät palvelunsa Yhdysvalloissa, Virossa ja Puolassa sijainneille palvelimille. (Korns & Kastenberg, 2009, s. 60.) Toisin kuin vuotta aikaisemmin Viron tapauksessa, Georgia joutui siis turvautumaan ulkopuoliseen ja myös yksityisyritysten tarjoamaan apuun, jotta hallitus pystyi jälleen toimimaan verkossa (Korns & Kastenberg, 2009, s. 66–67).

Venäläisten toteuttama kyberoperaatio georgialaisia vastaan jaetaan Shakarianin mukaan (2011) kahteen osaan. Ensimmäisessä vaiheessa, joka alkoi elokuun 8. päivä, palvelinestohyökkäykset kohdistettiin hallituksen ja valtion verkkosivuja vastaan. Nämä hyökkäykset toteutettiin bottiverkkojen avulla, ja ne olivat pääosin raakaa voimaa käyttäviä hyökkäyksiä (engl. brute force DDoS attack, nämä hyökkäykset suuntaavat verkkosivustolle enemmän liikennettä, mitä ne pystyvät käsittelemään, ja saavat sivuston kaatumaan). (Shakarian, 2011, s. 64.)

Toisessa vaiheessa hyökkäykset hallituksen ja median verkkosivuja vastaan kiihtyivät. Tässä vaiheessa kyberhyökkäykset laajenivat pankkisektoria, yksityisiä yrityksiä, koulutuslaitoksia ja länsimaisia verkkosivuja vastaan. Nämä hyökkäykset koostuivat palvelinestohyökkäyksistä, verkkosivujen häpäisystä (kuten georgialaisvastaisten kuvien ja tekstien lisäämisestä sivustoille) sekä roskapostihyökkäyksistä poliitikkojen sähköpostitilejä vastaan. (Shakarian, 2011, s. 64.) Myös ping flood -hyökkäyksiä (ping flood tarkoittaa lukuisten yhteyskyselyiden toteuttamista) käytettiin verkkosivuja vastaan (Nazario, 2009, s. 168). Edellä mainittujen hyökkäysten lisäksi verkkosivuja kohtaan tehtiin myös SQL-injektiohyökkäyksiä (Shakarian, 2011, s. 64).

Hyökkäyksiin osallistuivat ainakin Russian Business Network (joka on venäläinen kyberrikollisorganisaatio) sekä niin kutsutut patrioottiset hakkerit. Hakkereita rekrytoitiin verkossa tähän tarkoitukseen perustettujen sivustojen avulla. Osa näistä sivuista perustettiin venäläisten maaoperaation alkaessa, esimerkiksi StopGeorgia.ru perustettiin 9. elokuuta. Sivustoilla tarjottiin yksinkertaiset ohjeet hyökkäysten tekemiseksi, joten asiaan vihkiytymätönkin käyttäjä pystyi halutessaan ottamaan osaa hyökkäyksiin. Nämä ohjeet sisälsivät tiedot siitä, mitä kautta verkkosivuihin pääsi (palvelimet olivat joko Venäjällä tai Liettuassa), ja lista siitä, mitä haavoittuvuuksia sivustoilla oli. Nämä rekrytointisivustot myös estivät ulkopuoliset porttiskannaukset, vaikeuttaen näin puolustajien toimintaa. Georgialaiset hakkerit perustivat vastatoimena huijausrekrytointisivuston. Tällä sivustolla yritettiin huijata venäläisiä käyttäjiä hyökkäämään georgialaisia palvelimia vastaan, jotka todellisuudessa olivatkin venäläisten hallinnoimia sivustoja. Vastatoimia toteuttivat myös venäläiset, jotka olivat ottaneet oppia Viroa vastaan toteutetusta kyberoperaatiosta. Kun georgialaiset estivät venäläisistä osoitteista tulevan liikenteen, muuttivat hyökkääjät osoiteavaruutensa muista osoitteista tulevaksi. Tämän ansiosta hyökkäykset jatkuivat normaalisti. (Shakarian, 2011, s. 64–65.) Hyökkäysten vaikutuksesta suurinta osaa Georgian hallinnon verkkosivuja ei voinut käyttää 10. elokuuta saakka. Myös maksuliikenne ja puhelinverkko saatiin kaadettua täysin (Kozlowski, 2013, s. 239).

Hyökkäyksen tavoitteeksi on veikattu halua eristää Georgian verkkoympäristö ulkomaailmasta (Corbin, 2009) ja tukea samaan aikaan tehtyä maahyökkäystä (Aslanoğlu & Tekir, 2012, s. 7). Shakarian (2011, s. 66) olettaa, että venäläisillä olisi ollut myös kyky hyökätä SCADA-järjestelmiä (eli esimerkiksi sähkön- ja energianjakelusta vastaavia tietojärjestelmiä) vastaan, mutta hakkerit pidättäytyivät tekemästä pysyvää vahinkoa. Myöskään fyysisiä yhteyksiä ulkomaailmaan ei katkennut (esimerkiksi Georgian ja sen naapurimaiden väliset tiedonsiirtokaapelit pysyivät koskemattomina).

Bumgarnerin ja Borgin (2009, s. 7) mukaan kyberhyökkäyksiä oli valmisteltu etukäteen, sillä bottiverkot otettiin ensimmäisessä vaiheessa todella nopeasti käyttöön, rekrytointiverkkosivuilla jaettiin valmistellun oloiset ja yksityiskohtaiset ohjeet hyökkäysten tekemiseksi ja SQL-haavoittuvuudet olivat etukäteen tiedossa. Valmistelusta kielii myös se, että heinäkuun 20. päivä, noin kolme viikkoa ennen Georgian ja Venäjän välisen sodan alkamista, georgialaisille verkkosivustoille ohjattiin datapaketteja, jotka sisälsivät esimerkiksi tekstinpätkän "win+love+in+Rusia." Tämän ja presidentin sivustoja vastaan kohdistuneiden palvelinestohyökkäysten oletetaan olleen harjoitushyökkäyksiä elokuun varsinaista hyökkäystä varten. (Thomas, 2009). Kyseiset kyberhyökkäykset pystyttiin yhdistämään Machbot Network -nimiseen bottiverkkoon, jota ovat käyttäneet pääosin venäläiset hakkerit (Korns & Kastenberg, 2009, s. 65). Venäläisillä keskustelukanavilla ja chattipalstoilla käytiin myös keskustelua ennen maahyökkäyksen alkua, pitäisikö Georgiaa vastaan tehdä palvelinestohyökkäyksiä (Hollis, 2011, s. 10).

Hyökkääjille oli eduksi myös se, millaiseksi georgialainen verkkoinfrastruktuuri oli muodostunut. Georgia sai yhteyden internetiin käytännössä kahden valtion, Venäjän ja Turkin, kautta. Tämä mahdollisti osaltaan sen, että venäläishakkerit saivat käyttöönsä suuren kaistanleveyden hyökkäyksiä varten (Nazario, 2009, s. 168).

Shakarian (2011, s. 67) toteaa, että vaikka Venäjän hallinto ei olisikaan ollut suoraan vastuussa kyberiskuista, hyökkäykset olivat silti venäläisille hyödyksi. Lazarin (2008, s. 503) mukaan kyberhyökkäykset georgialaista Gorin kaupunkia vastaan tukevat väitettä siitä, että kyseessä oli ylempää ohjattu kyberoperaatio. Gorin kaupungin verkkosivuja vastaan tehtiin kyberhyökkäyksiä juuri ennen kaupunkia vastaan tehtyjä ilmaiskuja. Jos kyseessä olisivat olleet ainoastaan kyberaktivistit, ei aktivisteilla olisi ollut yhtä hyviä mahdollisuuksia tiedustella ja sovittaa hyökkäyksiä etukäteen konventionaalisten joukkojen hyökkäysten kanssa. (Lazar, 2012, s. 503.) Myöskään pelkästään rikollisryhmittymien vastuulle kyberhyökkäyksiä ei voi siirtää, sillä rikollisten tulisi jollain tavalla hyötyä operaatiosta, ja täten saada rahoitusta joltain taholta, kuten valtiolta (Shakarian, 2011, s. 67). Yhteys kyberhyökkäyksen ja maahyökkäyksen välillä on Levinen mukaan ilmeinen, sillä kyberhyökkäyksiä ei näennäisesti edeltänyt tiedustelu, vaan hyökkäykset soveltuivat saman tien kohteiden tiedettyjä haavoittuvuuksia vastaan (Levine, 2009). Georgian hallinnon viranomaiset myös löysivät vakoiluohjelmiston koneiltaan, joka keräsi tietoa hallituksen, teollisuuden ja kolmannen sektorin toimijoista. Tämä vakoiluohjelmisto löydettiin maaliskuussa 2011. Georgialaisten mukaan vakoiluohjelma oli venäläistä alkuperää. (Pernik, 2018, s. 59.)

3.6 Kirgisia

Kuten aiemmat tässä kappaleessa mainitut valtiot, myös Kirgisia on entinen neuvostoliittolaissatelliittivaltio, joka itsenäistyi 1990-luvun alussa. Valtio oli pitkään

läheinen Venäjän kanssa, mutta tämä muuttui, kun Kirgisiassa tapahtui niin sanottu tulppaanivallankumous. Silloinen presidentti syöstiin vallasta, ja uusi presidentti alkoi lähentää välejään länteen ja Yhdysvaltoihin. Yhdysvallat saivat esimerkiksi jatkaa Kirgisian alueella olevan lentotukikohdan käyttöä. Vuoden 2009 aikana Venäjän ja Kirgisian välillä neuvoteltiin kauppasopimuksesta, jonka yhtenä ehtona Venäjän puolelta oli kyseisen lentotukikohdan sulkeminen. Kirgisian oppositio vastusti kyseistä sulkemista voimakkaasti. Tähän tilanteeseen liittyen Kirgisian neljää internetyhteyden tarjoajaa vastaan tehtiin laajamittaisia palvelunestohyökkäyksiä. Näiden hyökkäysten seurauksena kolmen palveluntarjoajan järjestelmät kaatuivat ja yli 80 prosenttia maan verkkoliikenteestä pysähtyi. Sähköpostin lähettäminen, tietyille verkkosivuille pääsy ja matkapuhelinten käyttö estyi. Tämä ei vaikuttanut samalla tavalla kirgisialaisten elämään kuin Georgian ja Viron kyberhyökkäysten tapauksessa, sillä isolla osalla kirgisialaisista ei ollut pääsyä verkkoon tai he eivät omistaneet matkapuhelinta. (Kozlowski, 2014, s. 240.)

Rhoads (2009) yhdistää hyökkäykset venäläisiin, sillä hänen mukaansa hyökkäyksiin käytetyt palvelimet näyttivät olevan samoja, joita käytettiin Georgiaa ja Viroa vastaan tehdyissä hyökkäyksissä. Russian Business Networkin epäiltiin olevan yksi hyökkäyksen toteuttaneista rikollisryhmittymistä, kuten aiemmissakin Venäjään yhdistetyissä kyberoperaatioissa. Kyseisten hyökkäysten tavoitteen oletetaan olleen poliittinen, eli saada Kirgisia taipumaan Venäjän painostukseen ja sulkemaan amerikkalaisten lentotukikohta. (Kozlowski, 2014, s. 240.) Joidenkin lähteiden mukaan Kirgisian hallitus suuntasi itse palvelinestohyökkäykset maan oppositiota kohtaan (Mackey, 2009; Lemos, 2009; Nazario, 2009, s. 172).

Kyberhyökkäyksissä Viroa, Georgiaa ja Kirgisiaa vastaan on Ashmoren (2009, s. 11) mukaan kaksi yhteistä tekijää. Ensimmäinen on se, että kyberhyökkäykset käynnistettiin tilanteessa, jossa Venäjän hallitus kohtasi poliittista vastustusta. Toinen yhteinen tekijä on se, että todisteita Venäjän hallituksen yhteydestä kyberhyökkäyksiin ei ole löydetty, vaikkakin venäläiset on pystytty yhdistämään jossain määrin jokaiseen hyökkäykseen. Ashmore toteaakin, että Venäjän hallinnon vastustaminen voi olla yksi tekijä kyberhyökkäyksen käynnistämisessä uhria kohtaan.

3.7 Ukraina

Ukrainalla ja Venäjällä on pitkä historia takanaan. Vaikka Ukraina on sekä maantieteellisesti että väestöllisesti suuri valtio, on se historiansa aikana ollut aina Venäjän varjossa, ja ukrainalaisia on pidetty toisen luokan kansalaisina sekä tsaarin Venäjällä että Neuvostoliitossa. Neuvostoliiton hajoaminen muutti tilanteen täysin. Samalla, kun Ukraina julistautui itsenäiseksi, sen täytyi ryhtyä rakentamaan omaa kansallista ja kansainvälistä identiteettiään. Nyt myös länsimailla oli ensimmäistä kertaa mahdollisuus vuorovaikuttaa poliittisella tasolla itsenäisen Uk-

rainan kanssa. Vaikka 1990-luvulla Ukrainassa olikin länsivastaista mielialaa johtuen Euroopan yhteisön viileästä suhtautumisesta Ukrainaa kohtaan, oli kansalaisten mieliala muuttunut positiivisemmaksi Eurooppaa kohtaan 2010-luvulle tultaessa. Kansalaiset eivät olleet samaa mieltä poliittisten päättäjien kanssa, jotka pyrkivät lähentymään poliittisesti ja taloudellisesti Venäjän kanssa. Vuonna 2014 väkivaltaisiksi äityneet mielenosoitukset venäläismielistä hallintoa vastaan saivat hallituksen irtisanoutumaan, ja uuden hallituksen aloittamaan lähentymisen länttä kohti. Ukrainalaiset ovat olleet epäluuloisia Venäjän antamia turvallisuustakuita vastaan, mikä on ajanut maan tekemään yhteistyötä ja solmimaan sopimuksia länsimaisten demokratioiden kanssa. (Morrison, 1993; Freire, 2017.)

EU:n ja Ukrainan välien lähentymisen jälkeen Ukrainaa vastaan on 2010-luvulla tehty sekä yksittäisiä kyberhyökkäyksiä että laajamittaisempia kyberoperaatioita, jotka ovat vaikeuttaneet sekä hallituksen toimintaa että tavallisten kansalaisten elämää. Nämä hyökkäykset ovat koskettaneet Ukrainan lisäksi myös länsimaita. Esimerkiksi Naton verkkosivut kaatuivat hetkellisesti Euromaidan-protestien aikana loppuvuodesta 2013, kun liittouman sivuja vastaan tehtiin palvelinestohyökkäyksiä (Geers, 2015, s. 11). Tässä alakappaleessa esitellään kolme Ukrainaa kohtaan suunnattua kyberoperaatiota. Nämä esimerkit on valittu sillä perusteella, että kyberhyökkäykset ovat vaikuttaneet merkittävällä tavalla joko Ukrainan valtioon tai ukrainalaisten normaaliin arkeen, ja niissä on nähtävissä selkeä suunnitelmallisuus ja strategisemman tasan tavoitteet. Esimerkiksi yksittäistä ukrainalaista pankkia kohtaan tehtyä tietomurtoa ei ole otettu tutkimuksen kohteeksi, sillä kyseisentyyppinen hyökkäys on liian pienimuotoinen vaikuttaakseen laajemmalti ihmisten elämään tai edistääkseen Venäjän valtion tavoitteita (Blank, 2017, s. 91).

3.7.1 Operaatio Armageddon (vuodet 2013–2015)

Ukrainan ja Venäjän sota eroaa Georgian ja Venäjän välillä vuonna 2008 käydystä sodasta siten, että Krimin konfliktissa kyberkykyjä ei ole nähty laajamittaisessa käytössä (Lewis, 2015, s. 41). Poikkeuksen tekee operaatio Armageddon. Kyseisen kyberoperaation tarkoituksena oli kybervakoilun avulla saada arkaluontoista tietoa Ukrainan hallituksesta, viranomaisista ja armeijasta ja käyttää tätä tietoa parantamaan Venäjän poliittista ja sotilaallista asemaa Euroopan Unioniin ja Ukrainaan nähden. Ukrainan tiedustelupalvelu on yhdistänyt tämän operaation Venäjän tiedustelupalveluun, ja sen on havaittu olleen aktiivisena ainakin vuoden 2013 kesästä lähtien. (Lewis, 2015, s. 3.) Tämä alakappale pohjautuu Lewisin (2015) raporttiin kyseisestä kybervakoiluoperaatiosta. Raportti on julkaistu vuonna 2015, ja se käsittelee aikaväliä 2013–2015. On mahdollista, että operaatio on jatkunut myös vuoden 2015 jälkeen. Kirjallisuuskatsauksen perusteella ei kuitenkaan löytynyt todisteita muista tähän operaatioon yhdistetyistä kybervakoilutapauksista. Tämän takia tutkimuksessa käsitellään operaatioon liittyen vuosia 2013–2015.

Operaatio sai nimensä aikaleimasta ”Armagedon”, joka löydettiin uhreille lähetettyjen Word-tiedostojen metatiedoista. Operaation epäillään saaneen alkunsa, kun Ukraina päätti hyväksyä AA-sopimuksen (Ukraine-European Union

Association Agreement). Sopimuksella tavoiteltiin Ukrainan ja Euroopan Unionin välisen yhteistyön syventämistä. Ensimmäinen kerta, kun ”Armagedon” -aikaleimaa havaittiin, oli 26. kesäkuuta 2013. Kybervakoilutapaukset olivat jatkuneet vuoteen 2015 saakka (johon raportti päättyy), ja niiden oletettiin jatkuvan niin kauan, kuin konflikti Krimin alueella jatkuu. (Lewis, 2015, s. 4–5.)

Vakoiluyritykset kohdistettiin ajallisesti kahta eri ryhmää kohtaan. Ensimmäinen ryhmä koostui Ukrainan hallituksen virkamiehistä, opposition jäsenistä ja oppositiomyönteisistä journalisteista. Vakoilua kohdistettiin näihin henkilöihin erityisesti ennen Euromaidan-protesteja ja Ukrainassa tapahtunutta vallankumousta. Vallankumouksen jälkeen vakoilua toteutettiin pääosin toisen ryhmän henkilöstöä kohtaan. Tähän ryhmään kuului erityisesti Ukrainan hallituksen ja virkavallan henkilöstöä. (Lewis, 2015, s. 7–8.)

Vakoilu aloitettiin tietojenkalasteluhyökkäyksillä, joiden tavoitteena oli saada uhri avaamaan saastutettu sähköpostin liitetiedosto tai linkki, joka ohjasi käyttäjän hyökkääjän suunnittelemalle sivustolle tai hyökkääjän kaappaamalle palvelimelle. Tiedoston avaamisen tai sivustolle päätymisen jälkeen uhrin tietokoneelle ladattiin etäkäyttöohjelma, jota kautta hyökkääjät pääsivät uhrin koneeseen käsiksi. Etäkäyttöohjelman avulla hyökkääjät kykenivät lataamaan tiedostoja uhrin koneelta omaan verkkoonsa. Tiedostoja käytettiin oletettavasti sekä tiedonhankintaan että tulevien hyökkäysten suunnittelun apuna. Hämäyksen vuoksi käyttäjän koneelle ladattiin saastuneen tiedoston lisäksi aidolta vaikuttava ohjelma tai päivitys, jonka yhteydessä etäkäyttöohjelma asentui. Tiedosto saattoi olla esimerkiksi päivitys Google Chromeen. (Lewis, 2015, s. 8.) Hyökkääjät latasivat tällaisten etäkäyttöohjelmien avulla lisää haittaohjelmia uhrin tietokoneelle. Kaapattuja tiedostoja käytettiin myöhemmin vähentämään uhrien epäilyksiä. Lähettämällä aitoja tiedostoja (kuten presidentin tiedoksiantoja) sähköpostitse, uhrit avasivat todennäköisemmin nämä tiedostot. Aidon tiedoston yhteyteen oli tällöin lisätty haittaohjelma, joka samalla asentui uhrin koneelle. Tätä taktiikkaa ei käytetty operaation alusta alkaen, vaan ensimmäiset tällaiset sähköpostit, joissa aidon tiedoston mukana tuli haittaohjelma, havaittiin vuoden 2014 loppupuolella. (Lewis, 2015, s. 10–13.)

Vaikka tietojenkalasteluhyökkäyksiä tehtiin koko tarkastelukauden (vuodet 2013–2015) aikana, vakoilua toteutettiin pääasiassa samanaikaisesti erilaisten tapahtumien kanssa, joita oli joko Ukrainan maaperällä tai jotka liittyivät Ukrainaan. Esimerkiksi ensimmäiset tietojenkalasteluhyökkäykset aloitettiin samaan aikaan, kun EU:n ja Ukrainan väliset neuvottelut AA-sopimukseen liittyen olivat käynnissä. Näiden kalasteluhyökkäysten tavoitteena oletetaan olleen tarve saada tietoa tapaamisessa tehdyistä poliittista päätöksistä. Hyökkäyksissä pyrittiin Adobe Flash Player -ohjelman asennustiedoston avulla saamaan etäkäyttöohjelma uhrien koneille. Asennustiedostoa jaettiin ukrainalaisen kosmetiikkayritykseltä kaapatun palvelimen kautta. (Lewis, 2015, s. 19.)

Venäjän vallattua Krimin alueen huhtikuun 2014 aikana Ukrainan presidentti antoi julkilausuman terrorismin vastaisten operaatioiden aloittamisesta. Samanaikaisesti kybervakoilu siirtyi poliittisten tietojen keräämisestä sotilaallis-

ten tietojen keräämiseen. Samaan aikaan havaittiin myös ensimmäiset sähköpostit, joilla yritettiin saada kohdehenkilö avaamaan sähköpostin liitetiedosto ja siinä ollut saastunut tiedosto. Samanlaisia kalastelusähköposteja lähetettiin sotilashenkilöille sen jälkeen, kun ukrainalainen sotilaskone ammuttiin alas kesäkuussa 2014. Kalastelun tarkoituksena oli oletettavasti saada selville, miten Ukrainan armeija reagoisi koneen alasampumiseen. Ainakin osa kalasteluhyökkäyksistä oli yhdistettävissä Krimillä käytyihin sotilasoperaatioihin. Esimerkiksi Debaltseven kaupungissa käytyjen taistelujen aikana tehtiin kalasteluhyökkäyksiä kaapattujen palvelimien kautta. Hyökkäykset loppuivat, kun ukrainalaisjoukot vetäytyivät kaupungista. (Lewis, 2015, s. 20–23.)

3.7.2 Joulukuu 2015

Jouluaatonaattona 2015 Länsi-Ukrainassa sijainnutta, Prykarpattyaoblenergo-nimistä energiayhtiötä sekä kahta muuta alueella sijainnutta energiayhtiötä vastaan toteutettiin kyberoperaatio. Operaatioon liittyneiden kyberhyökkäysten ansiosta useampi muuntaja saatiin suljettua, ja noin 225 000 ukrainalaista ei saanut sähköä. Hyökkäykset toteutettiin koordinoidusti noin puolen tunnin sisällä toisistaan. Sähkökatkos ei kestänyt kovin kauaa (sähköt saatiin palautettua asiakkaille muutamassa tunnissa), mutta tämä hyökkäys oli silti ensimmäinen laatuaan, jossa kyberhyökkäyksen seurauksena oli sähkökatkos. (Lee, Assante & Conway, 2016, s. 5.) Hyökkääjät saivat haltuunsa voimanjakokeskusten operaattoreiden työasemat, ja sulkivat ja avasivat kyseisten järjestelmien piirejä saaden järjestelmät sammumaan. Hyökkääjät vaikuttivat noin 50 muuntajan toimintaan, mikä aiheutti noin 130 megawatin häviön sähkönjakelussa. Hyökkääjät pääsivät läpi kuuden yhtiön sähkönjakokeskuksiin, mutta jostain syystä vain kolmen yhtiön järjestelmiin vaikutettiin sähkökatkoksen aikaansaamiseksi. (Whitehead, 2017, s. 1.)

Hyökkääjät käyttivät useampaa eri tekniikkaa operaation aikana. Kohdennettua verkkourkintaa käytettiin yhtiöiden sisäverkkoon pääsemiseksi, josta tarvittavat käyttöoikeudet hankittiin järjestelmässä ja verkoissa liikkumisen mahdollistamiseksi (Lee ym., 2016, s. 8). Kohdehenkilöille lähetettiin esimerkiksi Excel- ja Word-tiedostoja, joihin oli liitetty BlackEnergy 3-niminen haittaohjelma. Avattuaan sähköpostin liitetiedoston, ohjelma suositteli makrojen käyttöönottamista. Käyttöönoton jälkeen haittaohjelma asentui koneelle. (Lee ym., 2016, s. 13.) Virtuaaliset erillisverkot (engl. Virtual Private Network, jäljempänä VPN) mahdollistivat sisäverkosta yhteyden sähköverkon hallintajärjestelmiin. VPN:t eivät vaatineet kaksivaiheista tunnistautumista, mikä helpotti järjestelmiin tunkeutumista. Koska järjestelmiä suojasi ainoastaan yksinkertainen salasana, oli sen murtaminen helppoa. Hyökkääjät pääsivät hallintajärjestelmään sisään päästyään käsiksi etätyökaluihin, joilla he saivat suljettua haluamansa järjestelmät. Jälkiensä peittämiseksi hyökkääjät käyttivät KillDisk -nimistä ohjelmaa lokitietojen poistamiseen. (Lee ym., 2016, s. 8–9). Hyökkäysten aikana yhtiöiden asiakaspalvelupisteitä kohtaan toteutettiin puhelinestohyökkäyksiä. Tuhannet aiheettomat puhelut saivat asiakaspalvelulinjat tukkoon, mistä syystä asiakkaat eivät kyenneet

hetkellisesti ottamaan puhelimitse yhteyttä ja selvittämään, mistä katkos johtui (Lee ym., 2016, s. 15).

Hyökkääjät olivat valmistelleet hyökkäyksiä pitkään. Kohdejärjestelmissä ei ollut tietoturvan valvontajärjestelmää, joka olisi ilmoittanut luvattomista pääsy-yrityksistä ja sisäänkirjautumisista. Tämä mahdollisti sen, että hyökkääjät toimivat jopa kuusi kuukautta yhtiöiden järjestelmissä ilman, että luvatonta käyttöä havaittiin. (Lee ym., 2016, s. 9.)

BlackEnergy-haittaohjelma on yhdistetty Sandworm-nimiseen ryhmään, joka toimii Venäjältä käsin. Ryhmä on toteuttanut aiemmin kybervakoilua ja kyberhyökkäyksiä Natoa, Ukrainan ja Puolan hallintoa sekä eurooppalaisia yrityksiä kohtaan (Lemos, 2014; Dragos, 2017, s. 10). Siitä ei ole varmuutta, onko kyseisellä ryhmällä yhteyksiä Venäjän hallitukseen. Ukrainan turvallisuuspalvelu kuitenkin syytti suoraan Venäjää iskujen tekemisestä (Volz & Finkle, 2016). Venäjän osallisuus on todennäköistä, sillä Ukrainan ja Venäjän välit olivat kireällä Venäjän otettua Krimin alueen haltuunsa vuonna 2014. Joulukuussa 2015, ennen venäläisten toteuttamaa kyberoperaatiota, ukrainalaisaktivistit hyökkäsivät Krimillä olleita muuntajia vastaan aiheuttaen laajoja sähkökatkoja, jotka vaikuttivat noin kahteen miljoonaan ihmiseen. Tämän on veikattu olevan osasyy Ukrainassa tapahtuneiden sähkökatkosten aiheuttamiseen. Valmistelut hyökkäystä varten alkoivat tosin jo puolta vuotta ennen Krimin sähkökatkoja, joten ainoa syy tämä ei voinut olla. Lee ym. (2016) spekuloivat, että Ukrainan hallituksen suunnitelmat kansallistaa yksityiset energiayhtiöt Ukrainan maaperällä ovat saattanut johtaa Venäjän ryhtymään toimenpiteisiin kansallistamisen ehkäisemiseksi. Osa kyseisistä yrityksistä on nimittäin venäläisten oligarkkien hallussa (Zetter, 2016). Park ym. (2017) pohtivat, että Ukrainasta on tullut jonkinlainen testialusta venäläisille uusien kyberkykyjen testaamisessa samalla, kun nämä käyttävät kyberhyökkäyksiä Ukrainan painostamiseen poliittisesti. Norvannon ym. (2019, s. 84–85) haastateltaessa ukrainalaisia tutkimustaan varten ei osa haastatelluista edes tiennyt, että kyseinen hyökkäys oli tapahtunut. Ukrainassa sähkökatkot ovat yleisiä, mikä osaltaan selittää haastateltavien tietämättömyyden. Tämä tukee väitettä siitä, että hyökkäyksillä tavoiteltiin todennäköisemmin uuden teknologian ja järjestelmien kestävyyden testaamista, eikä hyökkäyksillä tavoiteltu poliittisten tavoitteiden täyttämistä

3.7.3 Kesäkuu 2017

Keväällä 2017 Sandworm iski jälleen. Ryhmän jäsenet pääsivät murtautumaan Ukrainassa sijaitsevan Linkos Group -nimisen ohjelmistoyrityksen palvelimille, mikä avasi takaportin tietokoneille, joihin oli asennettu yhtiön M.E.Doc -niminen ohjelmisto (Greenberg, 2018, s. 3). Murtautumisen apuna käytettiin kohdennettuja sähköposteja, joiden Word-liitetiedostoissa oli haittaohjelmia. Kun käyttäjät avasivat liitetiedoston, haittaohjelma asentui uhrin tietokoneelle ja samalla hyökkääjille aukesi pääsy yrityksen sisäverkkoon (Watson, 2017). Sisäverkkoon päästyään hyökkääjät ottivat haltuunsa yhtiön palvelimet (joille M.E.Doc- tilinhallintaohjelmiston päivitys oli keskitetty) ja latasivat NotPetya-haittaohjelmiston ky-

seisille palvelimille. Kun Linkos Groupin asiakkaat hakivat ohjelmistoihinsa päivityksiä yrityksen palvelimilta, levisi NotPetya näiden asiakkaiden koneille. NotPetya levisi tätä kautta myös muualle maailmaan aina Yhdysvaltoja ja Australiaa myöten. (Greenberg, 2018, s. 3–4.) Haittaohjelma levisi yritysten koneissa sekä haavoittuvuuksia että varastettuja käyttäjätietoja käyttämällä (Simos, 2018). Käyttäjien koneet menivät tämän jälkeen lukkoon näyttäen joko loputtomasti lataavaa asennuskuvaketta tai kiristysviestiä, missä annettiin ohjeet tiedostojen palauttamiseksi (BBC, 2018). NotPetya levisi Ukrainassa neljään pääkaupungissa olleeseen sairaalaan, kuuteen energiayhtiöön, kahteen lentokenttään, yli 22 pankkiin ja tätä kautta näiden pankkiautomaatteihin sekä käytännössä koko Ukrainan hallintoon. Erään arvion mukaan noin 10 prosenttia Ukrainassa olleista tietokoneista ja näissä olleista tiedoista pyyhkiytyi tyhjäksi. (Greenberg, 2018, s. 7.)

Kuten aiemmissakin kyberhyökkäyksissä, Sandworm-ryhmän yhteyttä Venäjän hallintoon ei ole pystytty aukottomasti todistamaan. Valkoinen talo ja Iso-Britannian hallitus antoivat kuitenkin vuoden 2018 aikana lausunnot, joissa valtiot syyttivät iskusta suoraan Venäjän hallitusta (Ahmad, 2018; Press Secretary, 2018). Näiden maiden hallitukset yhdistävät hyökkäyksen Venäjän tavoitteisiin heikentää Ukrainan hallintoa ja talouselämää. Yritykset, joilla oli kontakteja tai toimipisteitä Ukrainassa, kärsivät eniten haittaohjelmasta, sillä nämä olivat ensimmäisiä kohteita, joihin NotPetya levisi. Tämä tukee väitettä, että haittaohjelman tarkoituksena oli myös toimia pelotteena yrityksiä vastaan, jotka toimivat Ukrainan maaperällä (Greenberg, 2018, s. 14).

NotPetya erosi tavallisesta kiristyshaittaohjelmasta siten, että NotPetyan tarkoitus ei ollut alun perinkään palauttaa tiedostoja uhreille, vaan se tyhjensi koneiden kovalevyt (ja niiden sisältämät tiedostot) lopullisesti. Tämä tukee väitteitä siitä, että NotPetyan takana oli jokin muu taho kuin tavallinen rikollisryhmä (Greenberg, 2018, s. 5; Nakashima, 2018; National Cyber Security Centre, 2018). Toinen erikoisuus hyökkäyksessä oli se, että haittaohjelma levisi (oletetun) kohdealueen ulkopuolelle (Carrazana, 2018, s. 5). Hyökkäys myös vaikutti enemmän tavallisten ihmisten arkeen kuin aiemmissa operaatioissa. Maksuliikenne pysähtyi täysin, ja ihmiset eivät kyenneet esimerkiksi nostamaan rahaa pankkitileiltään tai käyttämään luottokorttejaan. (Norvanto, Ruotsalainen & Schroderus, 2019, s. 85.)

3.8 Yhteenveto kyberoperaatioista

Edellä esitellyissä kyberoperaatioissa yhdistyy sekä epäilys että varmuus Venäjän hallinnon osuudesta kyberoperaatioihin. Kyberoperaatioiden tekijöiksi on todettu Venäjällä toimineet aktivistit tai hakkerit, mutta näiden yhteys Venäjän hallintoon on epäselvempi. Tämä menee yksiin Venäjän strategian kanssa erityisesti Ukrainan tapauksessa. Venäjän tavoitteena on ollut salata se tosiasia, että venäläisjoukkoja on ollut Ukrainassa sekä Venäjän hallinnon tavoitteet konfliktiin liittyen. (Snegovaya, 2015, s. 7.) Todistusaineistoa on kuitenkin riittävästi, jotta kyberoperaatioiden voidaan todeta olleen Venäjän toteuttamia tai edesauttamia.

Edellä esitetyistä tapauksista ainoastaan Kirgisian kyberoperaatiota ei voida ottaa analyysiin mukaan. Tähän operaatioon liittyen ei kirjallisuuskatsauksen perusteella löytynyt riittävästi eri lähteitä, jotta operaatioon liittyvät tiedot olisi voinut todeta luotettaviksi. Lisäksi kyberoperaation tekijä jäi epäselväksi. Joidenkin lähteiden mukaan kyberoperaation toteuttajana olisi voinut olla Kirgisian hallinto. Tästä syystä Kirgisian kyberoperaatio jätetään käsittelemättä. Muista operaatioista on riittävästi kirjallisuutta, jotta niitä voidaan käsitellä analyysivaiheessa. Analyysivaiheeseen otetaan siis mukaan Viron, Liettuan ja Georgian kyberoperaatiot sekä Ukrainaa kohtaan tehdyt kolme kyberoperaatiota.

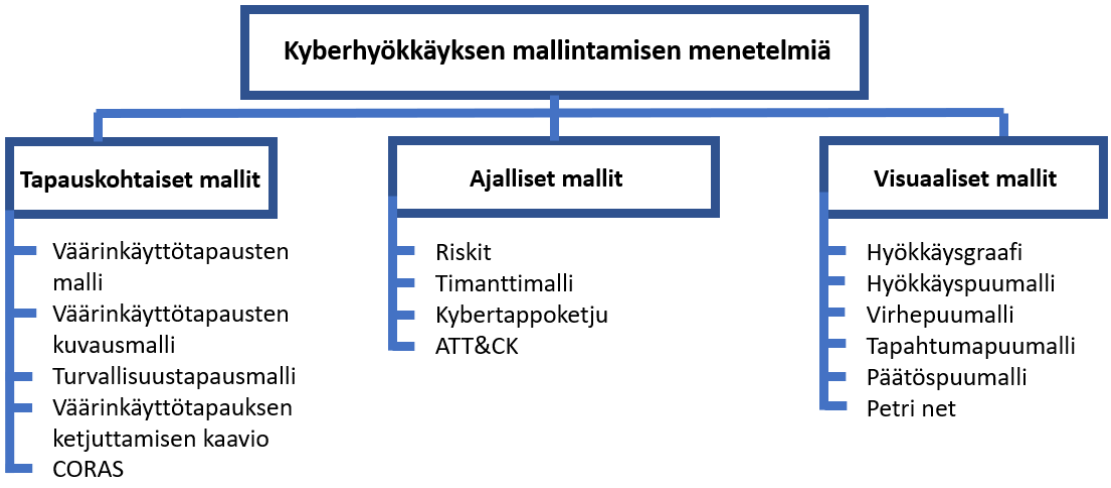
4 MALLINTAMISEN MENETELMIÄ

Kyberoperaatioiden sekä kyberhyökkäysten mallintamisen menetelmien tavoitteena on auttaa analysoijia hahmottamaan uhkaympäristöä ja suunnittelemaan puolustusmekanismeja uhkia vastaan (Lallie, 2020, s. 1; Staheli ym., 2014, s. 49). Kirjallisuuskatsauksen perusteella havaittiin, että kyberoperaatioiden analyysiin tarkoitettuja menetelmiä on kehitetty ja käytetty verrattain vähän tutkimuskirjallisuudessa. Sen sijaan kyberhyökkäysten mallintamiseen tarkoitettuja menetelmiä taas löytyy useita erilaisia vaihtoehtoja. Yksi syy tähän epäsuhtaan on se, että kirjallisuudessa kybersodankäynnin, kyberoperaatioiden ja kyberhyökkäysten termejä käytetään hieman ristiin (katso esimerkiksi Grant, Burke & van Heerden, 2012; Maybaum, 2013; Andress & Winterfeld, 2013). Tästä syystä tässä kappaleessa käsitellään sekä kyberoperaation analyysiin tarkoitettuja menetelmiä että kyberhyökkäyksen mallintamisen menetelmiä.

Kyberhyökkäyksen mallintamisen menetelmistä käytetään yhteisnimitystä AMT (engl. Attacking Modelling Techniques) (Lallie ym., 2020, s. 1). Lallie ym. (2020, s. 3) jakavat nämä hyökkäysmallit kolmeen kategoriaan. Nämä ovat:

1) tapauskohtaiset mallit (engl. use case based ATMs),
2) ajalliset mallit (engl. temporal methods)
3) visuaaliset mallit (engl. graph-based methods).

Alla olevassa kuviossa (kuvio 3) näkyy havainnollistettuna mallien jako näihin kolmeen kategoriaan.



KUVIO 3 Hyökkäysmallit (mukaillen Lallie ym. 2020, s. 3)

Edellä olevaan kuvioon liittyen kirjallisuuskatsauksen perusteella tutkittavaksi malliksi otetaan myös yhdistetty tappoketju (engl. Unified Kill Chain), sillä se on kehitetty kybertappoketjun pohjalta. Seuraavissa alakappaleissa esitellään edellä

mainitut kyberoperaatioiden ja kyberhyökkäysten analyysimenetelmät. Kappaleen lopuksi esitellyistä malleista valitaan soveltuvin analyysimenetelmä tutkimuksessa käsiteltävien operaatioiden analyysiä varten.

4.1 Kyberoperaatioiden analyysimenetelmiä

4.1.1 Siviilivahinkojen välttämiseen suunnattu operaatiotyökalu

Fanellin ja Contin (2012) tutkimus tunnistaa lainopillisen haasteen kybertoimintaympäristössä. Heidän mukaansa tutkimuskirjallisuus ei keskity siihen, miten kansainvälisten lakien ja asetusten mukaisesti kyberoperaatioita olisi laillista toteuttaa. Tutkimus tarjoaa suunnittelijoiden käyttöön mallin, jolla kyetään kategorisoimaan kyberoperaation vaikutuksia, kohteen ominaisuuksia ja keinoja rajoittaa kyberoperaation vaikutuksia. (Fanelli & Conti, 2012, s. 319.)

Fanellin ja Contin (2012) suunnittelemassa viitekehyksessä on siis kolme osaa: kyberoperaation vaikutusten määrittely (engl. Cyber Operations Effects), kohteen ominaisuuksien määrittely (engl. Target Attributes and Control Features) sekä analysointi- ja arviointivaihe (engl. Methodology for Enumeration and Analysis). Kyberoperaation vaikutusosa on jaettu kahteen alakategoriaan: vaikutukseen (engl. Effect) ja kestoon (engl. Persistence of Effect). Nämä alakategoriat on jaettu edelleen kolmeen osaan. Vaikutus voi olla joko suoraa (engl. Primary), toissijaista (engl. Secondary) tai epäsuoraa (engl. Indirect) Suora vaikutus tarkoittaa esimerkiksi haittaohjelman aiheuttamia konerikkoja tai ihmishengen menetyksiä. Toissijaiset vaikutukset eivät välttämättä näy saman tien. Näihin vaikutuksiin lukeutuu esimerkiksi tiedostojen korruptoituminen, joka havaitaan vasta operaation jälkeen. Epäsuoralla vaikutuksella tarkoitetaan esimerkiksi siviiliväestöön kohdistetun propagandan toimittamista kybertoimintaympäristön välityksellä. Kesto jaetaan niin ikään kolmeen osaan: pysyvään (engl. Permanent), väliaikaiseen (engl. Temporary) ja hetkelliseen (engl. Transient). Pysyvä vaikutus voi olla esimerkiksi haittaohjelman aiheuttama konerikko. Hetkellinen vahinko voi aiheuttaa toiminnan pysähtymistä, mutta sen vaikutuksista selvitään yleensä esimerkiksi käynnistämällä laite uudestaan. Hetkellinen haitta voi mennä jopa itsestään ohi, kuten esimerkiksi palvelinestohyökkäysten tapauksessa. (Fanelli & Conti, 2012, s. 322–323.)

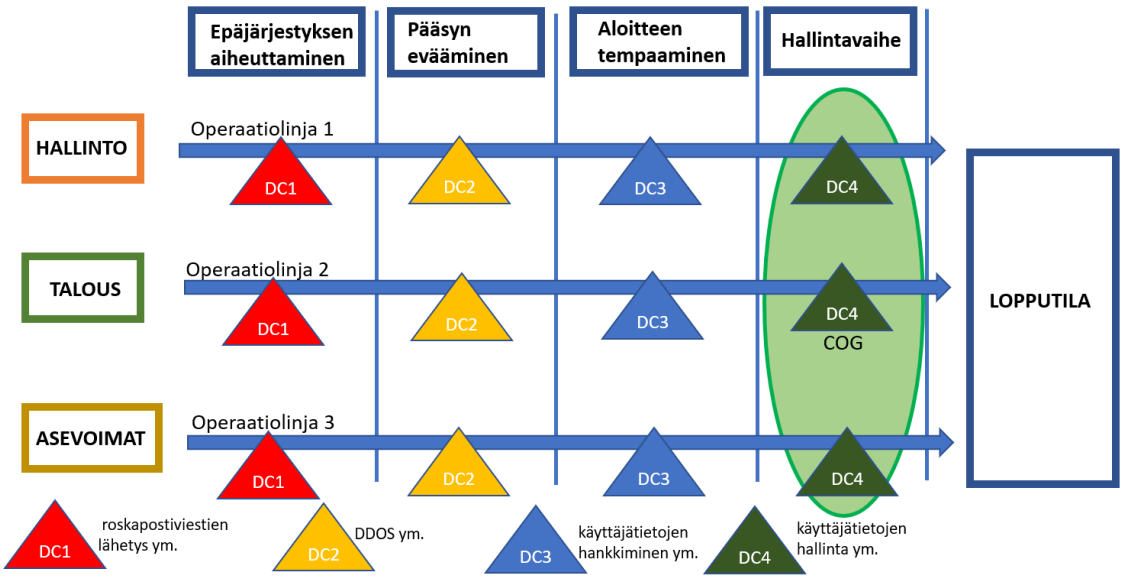
Kohteen ominaisuuksien määrittelyn avulla tavoitellaan tilannetta, jossa tavoite voidaan saavuttaa aiheuttamatta vahinkoa siviiliuhreille. Näitä mallissa olevia ominaisuuksia ovat maantieteelliset ominaisuudet (engl. Geography), kohteen toiminto (engl. Function), kohteen henkilöllisyys (Persona), laitteen tiedot fyysiset tiedot, kuten sarjanumero ja malli (engl. Physical Plane), laitteen loogisen tason tiedot, kuten IP-osoite (engl. Logical plane) ja kohteen kyberpersoonallisuus (engl. Cyber Persona Plane). Kohteen kyberpersoonallisuudella tarkoitetaan sen selvittämistä, koostuuko kohde yhdestä henkilöstä vai mahdollisesti useammasta tekijästä. Esimerkiksi Anonymous-nimisessä ryhmässä toimii use-

ampi hakkeri, mutta he käyttävät samaa pseydonyymiä. Analysointi- ja arviointivaiheessa käytetään kahden edellä esitellyn osa-alueen tietoja hyödyksi määriteltäessä operaation lainopillista lähtökohtaa ja operaation mahdollisia lopputuloksia. (Fanelli & Conti, 2012, s. 325–326.)

Edellä esitelty malli ei sovellu tämän tutkimuksen kyberoperaatioiden analysointiin, sillä mallin lähtökohta on lainopillinen. Mallilla pyritään selvittämään lähinnä se, pystytäänkö kohteeseen vaikuttamaan ilman, että siviilit kärsivät vahinkoja. Venäjä on suunnannut kyberhyökkäyksiään myös siviili-infrastruktuuria vastaan (Jensen, 2019, s. 229), joten tätä mallia ei voida käyttää tämän tutkimuksen operaatioiden analyysissä.

4.1.2 Kyberoperaatioiden suunnittelumalli

Moni kyberoperaatiota käsittelevä malli on tarkoitettu sotilasoperaatioiden suunnittelijoita varten tai mallit ovat ottaneet vaikutteita operaatiosuunnitteluun tarkoitetusta työkaluista. Yhtenä esimerkkinä mallista, joka on ottanut vaikutteita tällaisista työkaluista, on kyberoperaatioiden suunnittelumallin (engl. Cyber Operational Design, jäljempänä COD). Sen lähtökohtana on ollut auttaa operaatiosuunnittelijoita ymmärtämään paremmin kyberoperaatioiden monimutkaisuutta, painopisteen (engl. Center of Gravity, myöhemmin COG) merkitystä ja operaatiosuunnittelua (Karaman, Catalkaya, Gerehan & Goztepe, 2016, s. 21). Seuraavassa kuviossa (kuvio 4) esitellään mallin keskeisimmät osa-alueet.



KUVIO 4 Kyberoperaatioiden suunnittelumalli (mukaillen Karaman ym., 2016, s. 27)

Mallin tärkeimmät osat ovat operaatiolinjat (engl. Line of Operations), tärkeät tapahtumat (engl. Decisive Points, DC) sekä painopiste (COG). Malli on jaettu neljään pystysuuntaiseen osaan: epäjärjestyksen aiheuttamiseen (engl. Confusion Initiation), pääsyn eväämiseen (engl. Blocking Accessibility), aloitteen tempaamiseen (engl. Seize Initiative) sekä hallintaan (engl. Dominate). Operaatiosuunnat tähtäävät lopputilaan (engl. End State), mihin operaatiolla pyritään. Operaatiosuunnat tarkoittavat osa-alueita (hallinto, yhteiskunta ja asevoimat),

joihin kyberoperaatiot kohdistuvat. Näitä voi olla useampia samassa operaatiossa. Tärkeät tapahtumat ovat esimerkiksi roskapostin lähettämistä, DDoS-hyökkäyksiä, tietojen keräämistä ja tilanteen ylläpitämistä. (Karaman ym., 2016, s. 26–27.)

COD soveltuu paremmin operaatioiden suunnitteluun (ja tämä onkin ollut mallin suunnittelun lähtökohtana) kuin kyberoperaatioiden analyysiin. Myöskään sitä, miten mallia varsinaisesti käytetään, ei tutkimuksessa esitellä. Verrattuna esimerkiksi yhdistettyyn tappoketjuun (engl. Unified Kill Chain), COD ei anna riittävästi esimerkkejä erilaisista tilanteista, jotka mallin eri vaiheissa voisivat tapahtua. Jos esimerkkejä annetaan liikaa, ne voivat ohjata ja rajata suunnittelijan toimintaa liikaa. Hyvät esimerkit pystyvät kuitenkin auttamaan suunnittelijaa alkuun. Mallista myös puuttuu olennaisia osa-alueita. Yksi näistä on jonkinlainen suunnittelu/tiedusteluvaihe, joka edeltää yleensä aina operaatioiden toteutusvaihetta (NATO, 2013, s. 61). Toinen osa, joka mallista puuttuu, on operaatioon johtaneet syyt. Valtiotasolla tehdyt operaatiot pohjautuvat strategisen kulttuurin teorian perusteella valtion taustalla vaikuttavaan strategiseen kulttuuriin, jonka mukaan voidaan selittää myös se, miksi operaatioon alun perin ryhdyttiin (Johnston, 1995, s. 46).

4.1.3 Ohje strategisen kyberympäristön operaatioista

Yhdysvaltojen asevoimien ohje strategisen kyberympäristön operaatioista (2018) keskittyy operaatioiden suunnittelutyökalujen esittelyyn ja kyberoperaatioiden käyttöön eri puolustushaarojen operaatioiden yhteydessä. Ohjeessa käytetään esimerkkinä vuoden Georgian ja Venäjän välistä sotaa. Siinä kyberoperaatio on jaettu kolmeen vaiheeseen: estovaiheeseen (engl. Deter), aloitteen tempaisuun (engl. Seize the Initiative) ja hallintavaiheeseen (engl. Dominate). Näiden vaiheiden sisällä on esimerkkjä eri toiminnoista. Esimerkiksi estovaiheeseen lukeutuu kohteisiin tunkeutuminen, aloitteen tempaisuun palvelinestohyökkäysten tekeminen ja hallintavaiheeseen georgialaisten hakkereiden porttiskannausten estäminen. (United States Army War College, 2018, s. 62). Malli on selkeästi kehitetty ainoastaan olemaan esimerkinomainen havainnollistamaan kyberoperaation vaiheita paremmin, eikä sitä ole tarkoitettu analysointityökaluksi.

4.1.4 CyCOP

CyCOP (Cyber Comon Operational Picture) on havainnollistava työkalu, joka ottaa huomioon sekä sodankäynnin tavanomaisen toimintaympäristön että kybertoimintaympäristön. Sen tarkoituksena on mallintaa kohdeorganisaation kykyjä (niin konventionaalisia kuin kyberkykyjäkin), havainnollistaa eri toimintaympäristöjen aiheuttamia uhkia ja tarjota eri vaihtoehtoja, millä uhkiin voidaan resurssien puitteissa vastata. Se pyrkii tarjoamaan erityyppisiä visuaalisia näkymiä riippuen siitä, halutaanko toimia taktisella, operatiivisella tai strategisella tasalla. (Esteve, Peréz, Palau, Carvajal & Hingant, 2016).

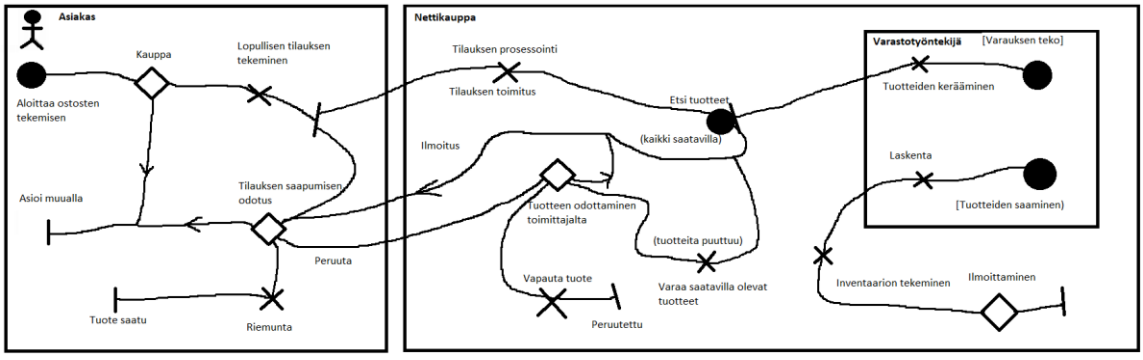
CyCOP on visuaalisiin ratkaisuihin keskittynyt työkalu, jonka käyttöön tarvittaisiin lisäksi erillinen tietokoneohjelma. Tästä syystä menetelmä ei sovellu tämän tutkimuksen kyberoperaatioiden analyysiin.

4.1.5 Yhteenveto kyberoperaatioiden mallintamisen työkaluista

Varsinaisia kyberoperaatioiden mallintamisen menetelmiä löytyi yllättävän vähän. Löydetyt ohjeet ja tutkimukset keskittyivät pitkälti asevoimien suunnittelunäkökulmaan tai visuaalisten työkalujen esittelyyn. Fanellin ja Contin (2012) esittelemä malli on hyvä, mutta se ei rajatun aihepiirinsä takia sovellu tämän tutkimuksen operaatioiden analysoimiseen. Karamanin ym. (2016) esittelemä malli on lähempänä sitä, mitä tämän tutkimuksen mallilta haetaan. Se on kuitenkin liian puutteellinen ominaisuuksiltaan soveltuakseen käytettäväksi sellaisenaan tämän tutkimuksen operaatioiden analyysia varten.

4.2 Tapauskohtaiset mallit

Seuraavista neljästä mallista kolme (väärinkäyttötapausmalli, väärinkäyttötapausten kuvausmalli ja turvallisuustapausmalli) pohjautuvat käyttäjätapausmalliin (engl. user case maps, jäljempänä UCM). UCM kuvaa järjestelmäarkkitehtuuria ja järjestelmässä tapahtuvaa käyttäytymistä. Se kuvaa mahdollisia käyttäjien toteuttamia skenaarioita ja sitä, miten nämä skenaariot käytännössä. (Karpati, Sindre & Opdahl, 2010, s. 264.) Alla olevassa kuviossa (kuvio 5) on esimerkki käyttäjätapausmallista.

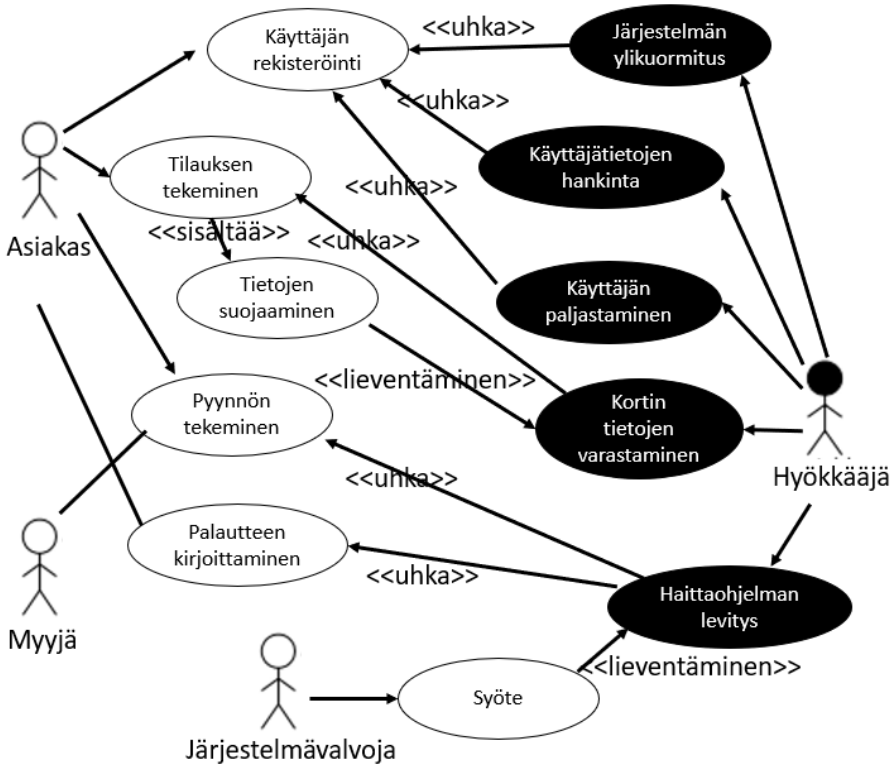


KUVIO 5 Käyttäjätapausmalli (mukaillen Kealey & Amyot, 2007, s. 3)

UCM:ää on kritisoitu siitä, että se kuvaa järjestelmiä liian yleisellä tasolla. Tällöin esimerkiksi turvallisuuteen liittyvät yksityiskohdat eivät välttämättä nouse esiin, eikä niitä tällöin osata ottaa huomioon järjestelmiä suunniteltaessa (Arlow, 1998, s. 151–152; Sindre & Opdahl, 2004, s. 35). Seuraavaksi esiteltävistä neljästä mallista kolme ensimmäistä ovatkin pyrkineet korjaamaan UCM:stä puuttuneen turvallisuusnäkökulman. Neljännen mallin (CORAS) avulla tehdään riskianalyysia kriittisten systeemien turvallisuuteen liittyen.

4.2.1 Väärinkäyttötapausten malli

Väärinkäyttötapausmallia (engl. misuse cases, jäljempämä MUC) on lähetetty kehittämään käyttäjätapausmallin (engl. user case maps, jäljempänä UCM) pohjalta (Sindre & Opdahl, 2004, s. 35). Sindre & Opdahl (2004) tuovat malliin mukaan negatiiviset käyttötapaukset, kuten järjestelmän väärinkäytöt. Tämä on päinvastainen ajattelutapa käyttäjätapausmalliin nähden, joka pyrkii kuvaamaan järjestelmään suunnitellut tapaukset ja niiden vaikutukset. Alla olevassa kuviossa (kuvio 6) havainnollistetaan MUC-mallia.



KUVIO 6 Väärinkäyttötapausmalli (mukaillen Sindre & Opdahl, 2004, s. 35)

Väärinkäyttötapaus tarkoittaa tässä kontekstissa tiettyjä ketjutettuja toimenpiteitä, joita esimerkiksi tietojärjestelmässä voi toteuttaa, ja joka aiheuttaa haittaa muille käyttäjille, jos nämä toimenpiteet suoritetaan loppuun asti. Mallin yhteyteen tehdään kirjallinen selitys väärinkäyttötapauksesta, kuten väärillä tiedoilla järjestelmään rekisteröitymisestä, ja vaihtoehtoisista skenaarioista, mitä uhkia tapaukseen liittyy. Esimerkiksi käyttäjä saattaa rekisteröityä täysin väärillä tiedoilla järjestelmään, tai vaihtoehtoisesti käyttää jonkun toisen henkilön tietoja rekisteröitymisessä. Malliin kuuluu myös viiden kohdan ohjeistus, jonka avulla järjestelmän turvallisuutta voidaan parantaa. Nämä viisi kohtaa ovat:

- järjestelmän kriittisten osa-alueiden tunnistaminen
- turvallisuustavoitteiden määrittäminen
- uhkien tunnistaminen

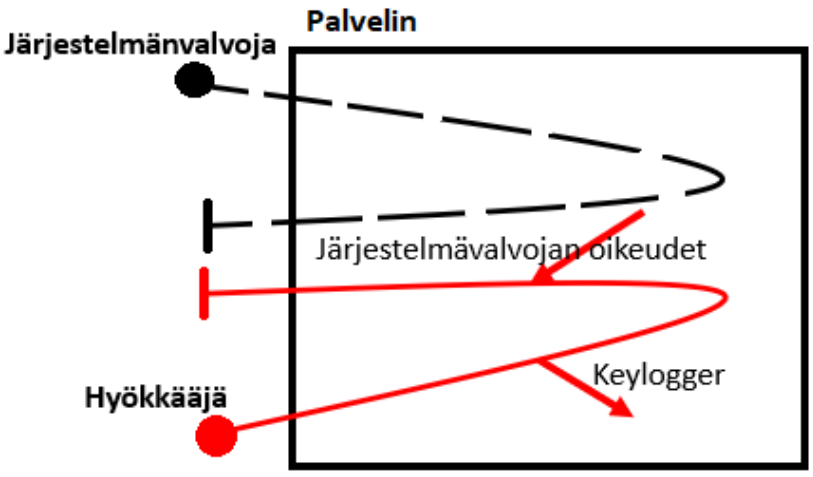
- riskien tunnistaminen ja analysointi
- turvallisuusvaatimusten määrittäminen

Näitä viittä kohtaa tulee pohtia järjestelmien kehitysvaiheessa samanaikaisesti väärinkäyttötapausten analysoinnin kanssa. Tällä tavalla järjestelmiä voidaan kehittää estämään mahdollisia väärinkäyttötapauksia. (Sindre & Opdahl, 2004, s. 35–38.)

Mallin avulla voidaan keskittyä sovelluskehityksessä etukäteen järjestelmää tai palvelua kohtaan kohdistuviin uhkiin ja näiden torjumiseen menemättä teknisiin yksityiskohtiin. Riskinä on, että alkuvaiheessa mahdollisuuksia eri väärinkäyttötapauksille syntyy liikaa, jolloin mahdolliset kriittiset tapaukset jäävät triviaalimpien tapausten varjoon. Väärinkäyttötapauksia ei pystytä myöskään aina kohdentamaan tiettyyn käyttäjään. Esimerkiksi haittaohjelmien leviäminen ei ole enää hyökkääjän kontrollissa. (Sindre & Opdahl, 2004, s. 41.) Malli soveltuu sovelluskehityksen alkuvaiheeseen ja yksittäisten, jo käytössä olevien, järjestelmien ja näitä kohtaan mahdollisesti kohdistuvien käyttäjälähtöisten uhkien analysointiin. Malli ei katso juurikaan ulospäin - se keskittyy järjestelmän analysointiin ja siinä olevien haavoittuvuuksien havaitsemiseen. Malli ei esimerkiksi ota huomioon ulkoisia tekijöitä, kuten inhimillistä virhettä tai palvelinestohyökkäystä (palvelinestohyökkäyksen onnistuminen ei ole varsinaisesti kiinni järjestelmässä olevasta yksittäisestä haavoittuvuudesta, vaan käytettävissä olevasta palvelinkapasiteetista).

4.2.2 Väärinkäyttötapausten kuvausmalli

Väärinkäyttötapausten kuvausmalli (engl. misuse case maps, jäljempänä MUCM) yhdistää hyökkääjän käyttäytymisen mallintamisen ja palvelinarkkitehtuuriajattelun. Se pohjautuu käyttäjätapausmalliin (engl. user case maps, jäljempänä UCM). Käyttäjätapausmalli esiteltiin edellisessä alakappaleessa "Väärinkäyttötapausten malli". MUCM laajentaa UCM:n turvallisuusaluetta lisäämällä malliin väärinkäyttöreitit. Alla olevassa kuviossa (kuvio 7) on esimerkki yksinkertaisesta MUCM:stä.



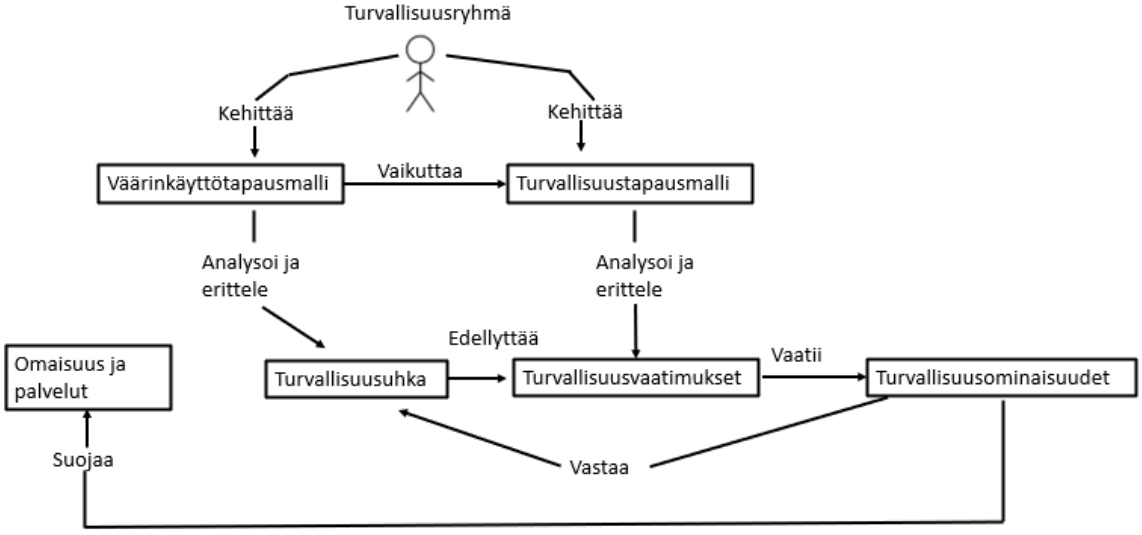
KUVIO 7 Väärinkäyttötapausten kuvausmalli (mukaillen Karpati ym., 2010, s. 267)

MUCM:ssä väärinkäyttöreitit (kuvassa punaisella) on piirretty laatikoiden päälle, jotka kuvaavat järjestelmän eri komponentteja, tässä tapauksessa palvelinta. Normaali käyttäjätoimenpide, tässä tapauksessa ylläpitäjän kirjautuminen sisään palveluun, on kuvattu katkoviivalla. Normaalin käyttöreitin ja väärinkäyttöreitin risteyskohdassa on haavoittuvuus, mikä mahdollistaa komponentin (tässä tapauksessa palvelimen) haavoittuvuuden hyväksikäytön. Kuvaamalla haavoittuvuuksia tällä tasolla, mallin avulla pyritään saamaan useita eri taustan omaavia henkilöitä järjestelmäkehittelyyn mukaan (kuten verkkopalveluasiantuntijoita ja järjestelmäkehittäjiä). Tällä tavalla myös haavoittuvuuksia pystyy tarkastelemaan eri näkökulmista ja mahdollisimman aikaisessa vaiheessa palvelukehitystä. (Karpati ym., 2010, s. 273.)

Malli vaikuttaa hyvältä sovelluskehityksen näkökulmasta. Tällä mallilla pystyy todennäköisesti tarkastelemaan järjestelmiä laajemmasta näkökulmasta, kun mukaan otetaan eri taustan omaavia asiantuntijoita. Malli soveltuu tosin myös ainoastaan sovellusten kehitysvaiheeseen tai yksittäisten, valmiiden järjestelmien analysointiin. Sitä ei ole tarkoitettu hyökkäysten analysointiin. Kuten väärinkäyttötapausmalli, myöskään tämä malli ei ota huomioon ulkoisia tekijöitä tai järjestelmän toiminnasta riippumattomia uhkia, kuten palvelinestohyökkäyksiä.

4.2.3 Turvallisuustapausmalli

Turvallisuustapausmalli (engl. security use cases, jäljempänä SUC) pohjautuu väärinkäyttötapausmalliin (engl. misuse cases, jäljempänä MUC). Firesmith (2003, s. 53) toteaa, että väärinkäyttötapausmalli soveltuu hyvin turvallisuusuhkien analysointiin, mutta huonosti turvallisuusvaatimusten määrittämiseen. SUC käyttääkin MUC:n analyysiä hyväksi kehittämään turvallisuusvaatimuksia. Alla oleva kuvio (kuvio 8) havainnollistaa SUCin ja MUCin suhdetta.



KUVIO 8 Turvallisuustapausmalli (mukaillen Firesmith, 2003, s. 54)

Edellä olevasta kuviosta näkee, miten MUC:n analyysin perusteella saadut tapaukset otetaan SUC:in analyysiketjuun mukaan. Esimerkkitapauksena Firesmithin (2003) artikkelissa käytetään tilannetta, jossa käyttäjä nostaa käteistä pankkiautomaatilta. MUC:n analyysin perusteella on havaittu kolme mahdollista tapausta, jotka vaarantavat käyttäjän käteisnostotapahtuman. Nämä tapaukset voivat olla esimerkiksi käyttäjän PIN-koodin varastaminen tarkkailemalla käyttäjää kauempaa, käyttäjätunnusten haltuun saaminen lähettämällä kalasteluviesti käyttäjälle tai järjestelmien haavoittuvuuksien hyväksikäyttö rahojen siirtämiseksi käyttäjien tililtä rikollisen tilille. Näitä hyväksikäyttötapauksia analysoidaan SUCin avulla, jotta järjestelmille saadaan järjestelmäkehitystä varten turvallisuusvaatimukset, jotka järjestelmän tulee täyttää. (Firesmith, 2003, s. 55.)

Malli soveltuu turvallisuusvaatimusten määrittelyyn kehitteillä olevien ja jo valmiiden tietojärjestelmien vaatimusten määrittelyyn. Se vaatii kuitenkin valmiiksi tehdyn uhka-analyysin toisesta mallista (tässä tapauksessa MUCista). Se ei siis sovellu uhka-arvioiden tekemiseen, eikä mallia olekaan tähän alun perin tarkoitettu.

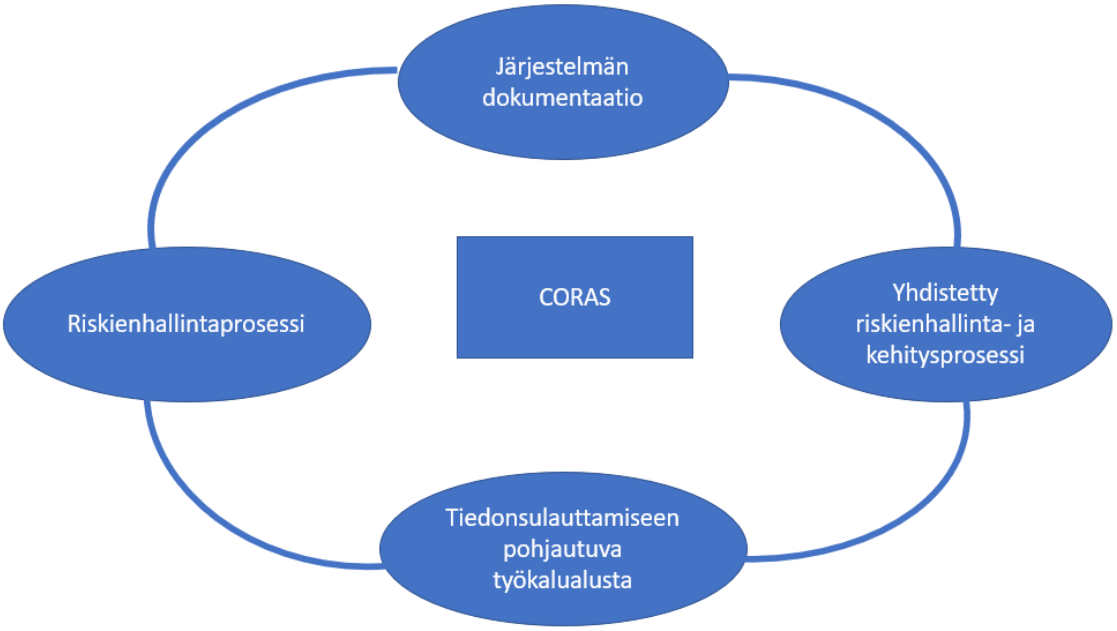
4.2.4 Väärinkäyttötapausten ketjuttamisen kaavio

Väärinkäyttötapausten ketjuttamisen kaavio (engl. misuse sequence diagrams, jäljempänä MUSD) yhdistää väärinkäyttötapausmallin (engl. misuse case, jäljempänä MUC) ja ketjugraafin (engl. sequence diagram, jäljempänä SD). MUSD ei juurikaan eroa MUC-mallista. Se ainoastaan lisää erilaisia UML-kaavion osia, jotta mallilla voidaan vielä laajemmin esittää järjestelmässä olevia kohteita, niiden haavoittuvuuksia ja sitä, miten näitä haavoittuvuuksia voidaan käyttää hyväksi. (Katta ym., 2010, 4–5.) MUSDiin liittyvät hyvät ja huonot puolet ovat tähän perustuen samat, kuin mitä MUC:tä käsittelevässä kappaleessa on esitelty.

4.2.5 CORAS

CORAS on kehitetty sähköisten järjestelmien riskianalyysiä varten (Raptis, Dimitrakos, Gran & Stølen, 2002, s. 169). Sen keskiössä on riskinmallintamisen viitekehys, jota tuetaan erilaisilla työkaluilla. Mallintamisen avulla pystytään kuvaamaan kohdetta riittävällä yleisellä tasolla. Tämä mahdollistaa tilanteen, jossa järjestelmän parissa toimivat eri alan asiantuntijat pystyvät paremmin keskustelemaan järjestelmän kehittämisestä. Myös riskien arvioinnin tulokset pystytään paremmin dokumentoimaan.

CORAS-mallin viitekehyksessä on neljä osa-aluetta: järjestelmän dokumentaatio, riskinhallintaprosessi, tiedonsulauttamiseen pohjautuva työkalualusta sekä yhdistetty riskienhallinta- ja kehitysprosessi (kuvio 9).



KUVIO 9 CORAS (mukaillen Raptis ym., 2002, s. 172)

Järjestelmän dokumentoinnin viitekehys sekä riskienhallintaprosessi pohjautuvat ISO-standardeihin (ISO10746 sekä ISO17799). CORAS-viitekehyksen työkalut pohjautuvat XML-ohjelmointikieleen. Yhdistetty riskienhallinta- ja kehitysprosessi pohjautuu AS/NZS 4360 riskienhallintastandardiin. (Raptis ym., 2002, s. 172.)

Viitekehyksen avulla on tarkoitus edetä viiden prosessin kautta analysoitaessa kohteena olevan järjestelmän riskejä. Ensimmäisessä vaiheessa tunnistetaan konteksti, jossa järjestelmä on, ja siihen liittyvät erityispiirteet esimerkiksi UML-kaavioiden avulla. Toisessa vaiheessa tunnistetaan järjestelmään liittyvät riskit. Kolmannessa vaiheessa riskit analysoidaan. Neljännessä vaiheessa riskit arvioidaan tärkeysjärjestykseen riippuen järjestelmän ominaisuuksista ja siitä, mitkä osat todetaan toiminnan kannalta kriittisiksi. Viidennessä ja viimeisessä vaiheessa tunnistetuille riskeille kehitetään keinot, joilla riskiä saadaan pienennettyä. (Stamatiou ym., 2003, s. 208–209.)

CORAS soveltuu parhaiten sovelluskehittämisen alkutaipaleelle, mutta kehittäjien mukaan se soveltuu myös jo käytössä olevan järjestelmän kehittämisen analysointiin (Raptis ym., 2002, s. 174). Mallin vahvuutena on se, että se pohjautuu olemassa oleville ja hyväksytyille standardeille sekä riskianalyysimalleille. Mallin heikkoutena vaikuttaa olevan sen monimutkaisuus, joka todennäköisesti johtuu useamman riskianalyysimallin ja työkalun mukana olosta. Dahl ym. (2007, s. 32) myöntävätkin, että ulkopuolisten, jotka eivät ole olleet prosessissa mukana, voi olla haastavaa ymmärtää prosessin perusteella syntynyttä analyysiä.

4.2.6 Tapauskohtaisten mallien yhteenveto

Käyttäjätapausmallikategoriaan kuuluvat hyökkäysanalyysimallit eivät ole niinkään hyökkäysten analysointiin vaan riskien ja väärinkäyttötapausten analysointia varten tarkoitettuja malleja. Näiden mallien suurin anti on todennäköisesti järjestelmien ja palveluiden kehittäjille, joiden täytyy pohtia turvallisuusnäkökulmaa järjestelmien kehitysvaiheessa. Malleilla pystyykin kuvaamaan tarkemmin teknisiä ominaisuuksia ja niihin liittyviä riskejä ja haavoittuvuuksia. Mallit soveltuvat huonommin laajemmassa mittakaavassa tapahtuvaan analysointiin. Ne eivät ota huomioon järjestelmään teknisiin ominaisuuksiin liittymättömiä osa-alueita. Näitä ovat esimerkiksi onnettomuudet ja järjestelmien sabotointi esimerkiksi fyysisin keinoin, kuten katkaisemalla fyysisiä tiedonsiirtokaapeleita tai sähköjohtoja. Mallit myös jättävät analysoinnin ulkopuolelle hyökkäyksiin johtuvien syiden analysoinnin. Niiden lähtökohta on järjestelmien koventaminen, eikä mahdollisten hyökkäysten syihin paneutuminen ja hyökkäysten estäminen. Tästä syystä tähän kategoriaan kuuluvat mallit eivät sovellu kyberoperaatioiden analysoimiseen.

4.3 Ajalliset mallit

Ajallisiin malleihin (engl. Temporal models) kuuluvat Lallien ym. (2020, s. 3) mukaan Riskit, kybertappoketju (engl. Cyber Kill Chain) sekä timanttimalli (engl. Diamond Model). Näiden kolmen mallin lisäksi esitellään ATT&CK-malli sekä yhdistetty tappoketju (engl. Unified Kill Chain). ATT&CK ja yhdistetty tappoketju on otettu tarkasteluun mukaan, koska yhdistetty tappoketju on kehitetty kybertappoketjun pohjalta, ja kyseinen malli on ottanut vaikutteita ATT&CK-mallista (Pols, 2017, s. 1).

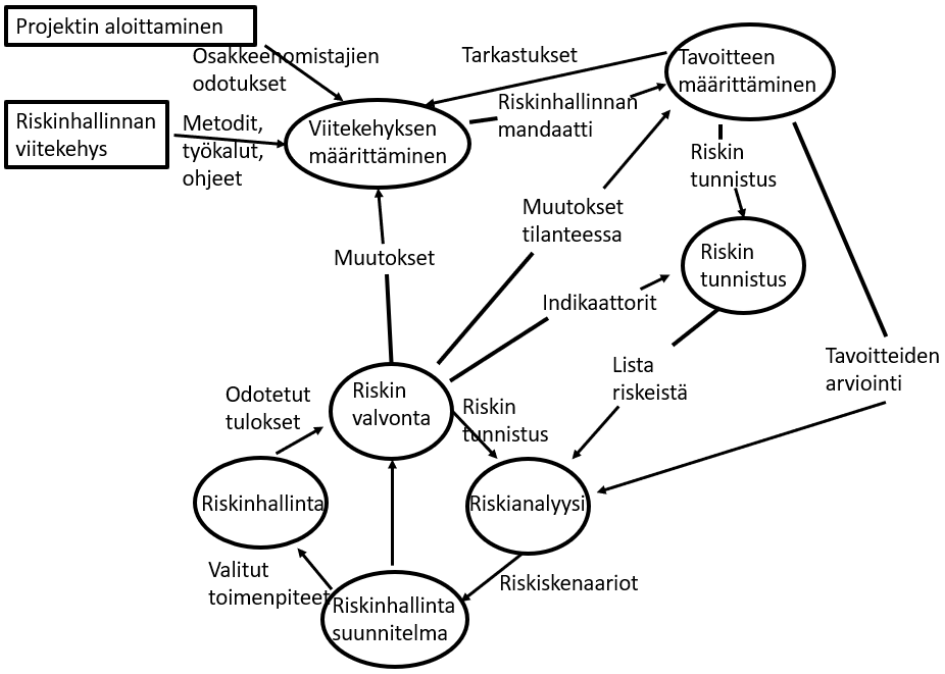
4.3.1 Riskit

Riskit on ohjelmistotuotannon riskienhallintaan kehitetty malli (Kontio, 1997, s. 4). Kontio (1997) kritisoi, että artikkelin ilmestymisvuoteen mennessä ilmestyneissä riskienhallintamalleissa on viisi heikkoutta:

1. Riski jää käsitteenä liian abstraktille tasolle, ja käyttäjillä ei ole työkaluja määritellä riskiä tarkempaa analyysia varten.
2. Riskienhallintamallit arvioivat riskiä määrällisesti, eivät laadullisesti. Tämän takia riskistä tehty analyysi jää vaillinaiseksi.
3. Riski voi käsitteenä tarkoittaa eri henkilöille eri asioita. Kontion mukaan harvat mallit tarjoavat tukea eri näkemyksille.
4. Riskit saattavat vaikuttaa projektiin useammalla kuin yhdellä tavalla (silloiset mallit eivät ilmeisesti ole tarkastelleet riskiä riittävän monesta näkökulmasta).

5. Silloiset riskienhallintamallit ovat joko liian vaikeita oppia tai liian kalliita ottaa käyttöön.

Riskitin luvataan vastaavan edellä oleviin kohtiin. (Kontio, 1997, s. 6.) Seuraavassa kuviossa (kuvio 10) on esitelty Riskitin riskinhallintaprosessi.



KUVIO 10 Riskit-mallin mukainen riskinhallintaprosessi (Kontio, 1997, s. 16)

Viitekehyksen määrittäminen (engl. risk management mandate definition) tarkoittaa riskinhallinnan laajuuden ja vastuiden määrittämistä. Tällöin määritetään esimerkiksi se, mitkä projektin osa-alueet ovat tärkeitä ja joihin riskien analysoinnissa tulee kiinnittää erityistä huomiota (Kontio, 1997, s. 17–18). Tavoitteen (engl. goal review) määrittäminen varmistetaan, että mahdollisimman moni projektiin liittyvä riski pystyttäisiin ottamaan huomioon. Jos tavoite ei ole selkeä, voi jokin riski jäädä huomioimatta (Kontio, 1997, s. 19). Riskin tunnistamisessa (engl. risk identification) yritetään löytää mahdollisimman moni projektia kohtaava uhka ja tästä muodostuva riski. Tämä on myös olennainen osa ennen riskien analysointia (engl. risk analysis) (Kontio, 1997, s. 22). Kun projektiin vaikuttava riskit on analysoitu, tehdään riskienhallintasuunnitelma (engl. risk control planning). Tämän osaprosessin tarkoituksena on määrittää, mihin riskeihin otetaan kantaa ja miten näihin riskeihin suhtaudutaan. Hallintamenetelmä voi olla esimerkiksi se, että riskiä ei aiheuta toimenpiteitä, vaan riskin olemassaolo hyväksytään. Muita keinoja ovat esimerkiksi riskin välttäminen työskentelymenetelmiä muuttamalla tai riskin todennäköisyyden pienentäminen esimerkiksi prosessin säännöllisellä seurannalla. (Kontio, 1997, s. 35.) Kun riskienhallintamenetelmät on suunniteltu, riskinhallinnasta (engl. risk control) tulee osa projektia. Malli ei tarjoa yksityiskohtaisia ohjeita tämän osa-alueen suorittamisesta, vaan viittaa siihen, että nämä hallintakeinot ovat projekti- ja organisaatiokohtaisia (Kontio, 1997, s. 39–40). Ris-

kien seuranta (engl. risk monitoring) on jatkuva prosessi, ja riskejä seurataan prosessin aikana määriteltyjen mittareiden avulla. Tarkasteluväliksi Kontio ehdottaa viikon tai kahden välein tehtävää tarkastelua (Kontio, 1997, s. 40).

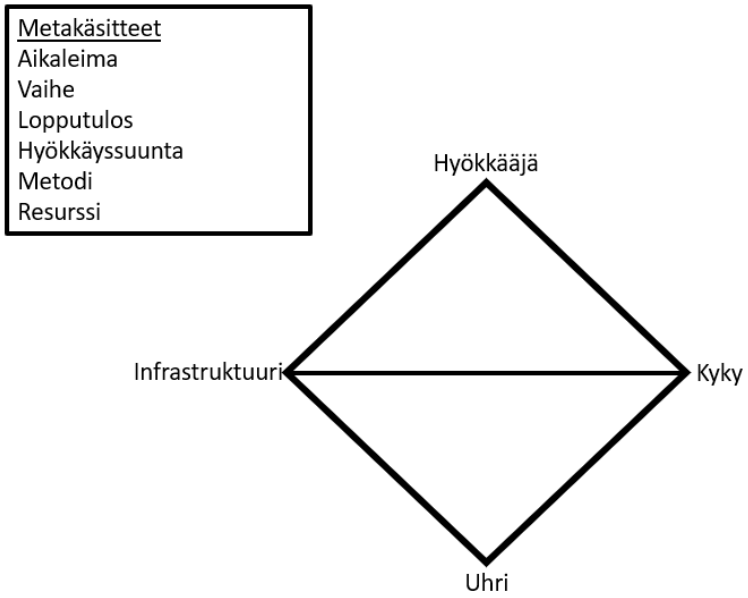
Riskit soveltuu parhaiten erilaisten ohjelmistoprojektien riskienhallintaan erityisesti isommissa organisaatioissa. Nokia käytti ainakin jossain vaiheessa tätä mallia oman organisaationsa riskienanalysoinnissa (Arias & Stern, 2011, s. 63). Mallin vahvuutena pidetään sen tarkempaa riskinmäärittelyä sekä joustavuutta käyttää mallia käytännössä missä tahansa organisaation osa-alueen riskienhallintamallina. Heikkoutena mallissa on se, että numeraalista arviota riskistä on vaikea yhdistää tämän mallin analysointiin, mikä vaikeuttaa myös riskin tarkempaa arviointia. (Arias & Stern, 2011, s. 65.)

Tämän tutkimuksen analysoitavissa tapauksissa käsitellään osittain tietoverkkoja ja ohjelmistoja, mutta tutkimuksen kohteena ei ole tapausten tietoverkkojen tai ohjelmistoympäristöjen riskienhallinta. Tästä syystä Riskit ei sovellu tämän tutkimuksen tapausten analysointiin.

4.3.2 Timanttimalli

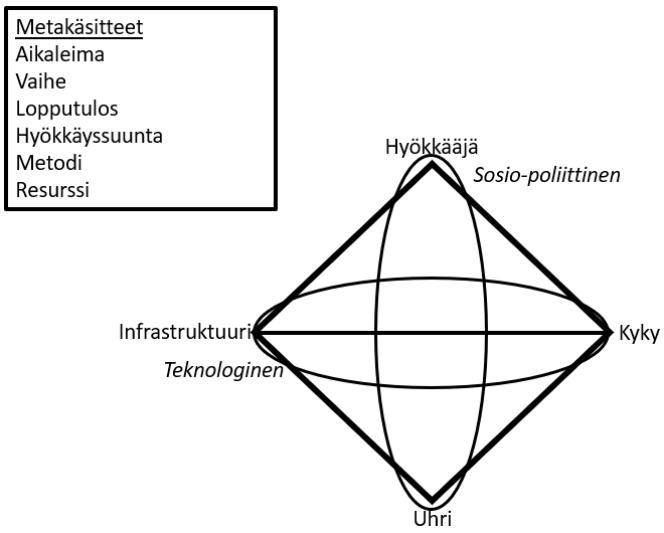
Timanttimalli (engl. Diamond Model) on yksi yksinkertaisimmista kyberhyökkäysmalleista. Mallissa on neljä perusominaisuutta: hyökkääjä (engl. adversary), joka käyttää jotain kykyä (engl. capability) uhrin (engl. victim) infrastruktuuria (engl. infrastructure) vastaan. Perusominaisuuksille voidaan määrittää alaominaisuuksia, kuten esimerkiksi uhrin järjestelmissä olevat haavoittuvuudet. Näiden perusominaisuuksien lisäksi malliin kuuluu kuusi metatason ominaisuutta: aikaleima (engl. timestamp) sekä operaation alussa että lopussa, vaihe (engl. phase), lopputulos (engl. result), hyökkäyssuunta (engl. direction), metodi (engl. methodology) ja resurssit (engl. resources). Näitä metaominaisuuksia käytetään tapahtumien analysointiin, ryhmittelyyn ja suunnitteluun. Malli antaa tekijöidensä mukaan hyvän listan siitä, mitä jokaisesta tapahtumasta pitäisi tietää. Jos jokin kohta jää avoimeksi, osoittavat nämä niitä osa-alueita, joista täytyy

saada lisää informaatiota. (Caltagirone, Pendergast & Betz, 2013, s. 7–10.) Timanttimalli on kuvattu seuraavassa kuviossa (kuvio 11).



KUVIO 11 Timanttimalli (mukaillen Caltagirone ym., 2013, s. 9)

Laajennetussa mallissa otetaan huomioon myös hyökkääjän ja puolustajan välinen suhde sekä hyökkäyksissä käytetty teknologia. Erityisesti sosiopoliittiseen aspektiin kiinnitetään huomiota. Hyökkääjän ja puolustajan välinen suhde voi olla muodollinen (eli tällöin hyökkääjällä ja puolustajalla ei ole varsinaista suhdetta, vaan hyökkääjä toteuttaa persoonattomamman hyökkäyksen, kuten esimerkiksi laajamittaisen kalastelukampanjan), tai henkilökohtainen. Henkilökohtaisella suhteella tarkoitetaan esimerkiksi tilannetta, jossa sosiaalista manipulointia kohdistetaan tiettyyn henkilöön, tai jokin valtio (kuten Venäjä) toteuttaa hyökkäyksen toista valtiota (kuten Yhdysvaltoja) vastaan. (Caltagirone ym., 2013, s. 21–24.) Laajennettu malli on kuvattu seuraavassa kuviossa (kuvio 12).



KUVIO 12 Laajennettu timanttimalli (mukaillen Caltagirone ym., 2013, s. 19)

Timanttimallin keskeisimpänä ominaisuutena pidetään analyyttistä käännöstä (engl. analytic pivoting). Tämä tarkoittaa sitä, että hyökkäystapahtumista saa vähitellen lisää tietoa, joka muuttaa analysoijan hypoteesia eri suuntaan. Ensimmäinen käänne voi tapahtua esimerkiksi silloin, kun uhri löytää haittaohjelman verkosta, toinen käänne tapahtuu analysoitaessa haittaohjelmaa ja sen ympäristöä, kolmas käänne löydettäessä hyökkääjän IP-osoite haittaohjelma-analyysin avulla, neljäs käänne tapahtuu analysoitaessa verkon palomuurilokeja, joista IP-osoitteen avulla löydetään muita mahdollisia saastuneita koneita ja viides käänne silloin, kun hyökkääjästä saadaan IP-osoitteen avulla tietoja, jolla hyökkäys voidaan pysäyttää ja jopa kääntää tätä vastaan. (Caltagirone ym., 2013, s. 26.)

4.3.2.1 Timanttimallin käsitteitä

Hyökkääjällä timanttimallissa tarkoitetaan yksilöä tai organisaatiota, joka käyttää kykyä uhria vastaan saavuttaakseen tavoitteensa. Yleensä hyökkääjästä ei tiedetä juuri mitään, ainakaan hyökkäyksen alussa. Hyökkääjä jaetaan mallissa kahteen osaan: operaattoriin (engl. adversary operator) ja asiakkaaseen (engl. adversary customer). Operaattori on se taho, joka varsinaisesti toteuttaa toimet uhria kohtaan. Asiakas on taas se osapuoli, joka hyötyy hyökkäyksestä. (Caltagirone ym., 2013, s. 12.)

Kyvyllä (engl. capacity) tarkoitetaan niitä työkaluja tai tekniikoita, joita hyökkääjä käyttää hyökkäyksessä. Työkaluilla voidaan tarkoittaa esimerkiksi manuaalista salasanan arvausta tai automatisoituja salasananmurtamistyökaluja. Kykykapasiteetilla (engl. capability capacity) tarkoitetaan niitä kaikkia haavoittuvuuksia, joita hyökkääjä pystyy käyttämään kohteesta riippumatta. Hyökkääjän kyvyillä (engl. adversary arsenal) tarkoitetaan hyökkääjän käytössä olevia suorituskykyjä. Nämä kyvyt ovat tärkeässä osassa analyysia, jonka avulla pyritään ennustamaan hyökkääjän käyttämiä hyökkäystapoja ja -reittejä. (Caltagirone ym., 2013, s. 12–13.)

Infrastruktuurilla tarkoitetaan niitä fyysisen tai loogisen tason rakenteita, joita hyökkääjä käyttää hyökkäyksen toteuttamiseen ja ylläpitoon. Verkkorakenteisiin kuuluvat esimerkiksi IP-osoitteet, sähköpostin käyttäjätunnukset ja USB-tikku, jolla haittaohjelma viedään uhrin koneelle. Caltagirone ym. (2013) jakavat infrastruktuurin kolmeen eri tyyppiin. Tyypin 1 infrastruktuuri on hyökkääjän täydessä kontrollissa tai välittömässä läheisyydessä. Tyypin 2 infrastruktuuriin taas lukeutuu niin kutsuttu välittäjä (tahtomattaan tai tarkoituksellisesti tähän rooliin päätynyt henkilö), jonka uhri näkee hyökkääjänä. Tämä voi olla esimerkiksi toisen käyttäjän roskapostia lähettävä tietokone, johon hyökkääjä on asentanut haittaohjelman. Tyyppiin kolme kuuluvat palveluntarjoajat, jotka mahdollistavat hyökkääjälle kyvyn toimia esimerkiksi sähköpostipalvelimen kautta. (Caltagirone ym., 2013, s. 13–14.)

Uhri on hyökkääjän kohde. Kohde voi olla esimerkiksi henkilö, IP-osoite tai organisaatio, jota vastaan hyökätään. Kohde jaetaan kahteen eri kategoriaan: henkilöihin ja alustoihin. Henkilöihin lukeutuvat ihmiset ja organisaatiot, alustoihin taas hyökkäyspinnat, kuten tietojärjestelmät, sähköpostit ja käyttäjäprofiilit. Caltagirone ym. (2013, s. 14) muistuttavat, että alustavan hyökkäyksen kohde ei ole välttämättä hyökkääjien lopullinen tavoite, vaan ainoastaan välitavoite, jota hyökkääjät käyttävät lopulliseen kohteeseen päästäkseen.

4.3.2.2 Timanttimallin metakäsitteet

Metakäsitteet ovat ei-kriittisiä, mutta tärkeitä elementtejä timanttimallissa. Ne eivät myöskään ole kiveen hakattuja, vaan Caltagironen mukaan mallia käyttävät voivat laajentaa mallia kokemustensa perusteella. Caltagirone ym. (2013) ovat esitelleet malliin liittyen seuraavat metakäsitteet: aikaleima, vaihe, lopputulos, hyökkäyssuunta, metodi ja resurssi. Aikaleima kertoo ajanhetken tapahtumasta. Yhdistämällä aikaleimat muihin havaittuihin tapahtumiin voidaan saada selville esimerkiksi se, onko hyökkäyksessä jaksollisuutta. (Caltagirone ym., 2013, s. 15.) Vaihe koostuu useammasta tapahtumasta. Vaiheiden erottelu on tärkeää, sillä hyökkäykset sisältävät yleensä useampia, ketjutettuja tapahtumia (Hutchins, Cloppert & Amin, 2011, s. 116). Lopputuloksen selvittämisellä voidaan saada tietoa hyökkääjän kyvyistä ja tavoitteista. Lopputuloksen dokumentointiin tarjotaan useampia vaihtoehtoja, kuten "3-tuple"-metodia (Success, Failure, Unknown -vaiheiden dokumentointi) tai CIA-triadin osa-alueiden pohjalta tehtyä analyysiä. Hyökkäyssuunnan määrittäminen on myös tärkeää, sillä tällöin voidaan selvittää, missä osassa järjestelmää on mahdollisia haavoittuvuuksia. Hyökkääjä voi esimerkiksi yrittää murtautua palomuurien läpi, tai hyökkääjä voi olla jo päässyt järjestelmiin sisälle esimerkiksi varastettujen käyttäjätunnusten avulla. Metodi voi tarkoittaa esimerkiksi porttiskannausta, tietojenkalastelusähköpostia tai muuta vastaavaa tapaa toteuttaa hyökkäys tai hyökkäyksen osa. Metodin selvittäminen auttaa suunnittelemaan kohdennettua puolustusta. Esimerkiksi tietojenkalastelusähköposteista voidaan tiedottaa organisaation laajuisesti ja tietyt portit voidaan sulkea ennaltaehkäisevästi. Resursseihin lukeutuvat hyökkääjän käyttämät työkalut, kuten haittaohjelmat, jotka yritetään ujuttaa sähköpostin välityksellä tietojärjestelmiin. (Caltagirone ym., 2013, s. 16–18.)

4.3.2.3 Timanttimallin käyttö

Timanttimallin käyttöön on kehitetty useampi erilainen lähestymistapa. Caltagirone ym. (2013) esittävät kuusi tällaista tapaa: uhrikeskeinen (engl. Victim-Centered Approach), kykykeskeinen (engl. Capability-Centered), infrastruktuurikeskeinen (engl. Infrastructure-Centered), hyökkääjäkeskeinen (engl. Adversary-Centered), sosiopoliittinen (engl. Social-Political-Centered) ja teknologiakeskeinen lähestymistapa. Uhrikeskeisessä lähestymistavassa tietoverkkoa seurataan eri monitorointityökaluilla, ja huomion voi keskittää tiettyihin verkon osiin tai käyttäjiin. Hyökkääjän voi johdatella haluttuihin paikkoihin niin kutsutuilla hunajapurkeilla, jotka houkuttelevat hyökkääjät paljastamaan suorituskykyjään. Suorituskeskeisessä lähestymistavassa tutkitaan nimensä mukaisesti hyökkääjän suorituskykyjä ja näistä johdettavaa tietoa (kuten uhria, jota vastaan suorituskykyä käytetään tai infrastruktuuria, jolla suorituskykyä ylläpidetään). Esimerkiksi Duqu-niminen haittaohjelmakokoelma yhdistettiin Stuxnet-haittaohjelmaan näiden suorituskykyjen samankaltaisuuksien kautta. Tätä kautta Duqua vastaan pystyttiin suunnittelemaan vastatoimenpiteitä Stuxnetistä saatujen oppien avulla. (Caltagirone ym., 2013, s. 28).

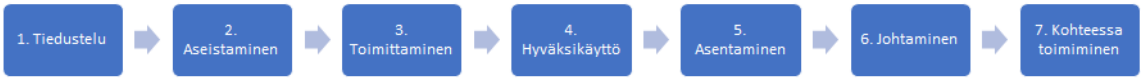
Infrastruktuurikeskeisessä lähestymistavassa tutkitaan laitteistoa ja laitteiston ominaisuuksia. Tällä lähestymistavalla voidaan esimerkiksi löytää lisää laitteistoja, joita ei ole käytetty hyökkäyksessä, mutta voivat olla silti hyökkääjän hallussa. Hyökkääjäkeskeinen lähestymistapa on yksi vaikeimmista tavoista. Tämä johtuu siitä, että hyökkääjän henkilöllisyyden tai tämän suorituskykyjen selvittäminen voi olla joissain tilanteissa mahdotonta. (Caltagirone ym., 2013, s. 29). Jos tietoa kuitenkin saadaan hyökkääjästä selville, pystytään tällä tavalla parhaiten ehkäisemään hyökkäyksiä tai jopa suunnittelemaan ja toteuttamaan vastahyökkäyksiä (Duffy, 2018).

Sosiopoliittisen lähestymistavan avulla voidaan selvittää hyökkääjän ja uhrin suhdetta, ja tätä kautta voidaan saada selville hyökkääjän henkilöllisyys (Caltagirone ym., 2013, s. 29). Jos esimerkiksi Iran on käyttänyt voimakasta retoriikkaa Yhdysvaltoja vastaan ja uhannut tätä kyberhyökkäyksillä, ja yhdysvaltalaisia pankkeja kohtaan tapahtuu jonkin ajan kuluttua palvelunestohyökkäyksiä, voidaan hyökkääjästä tehdä alustavia hypoteeseja. Teknologiakeskeisellä lähestymistavalla tarkoitetaan esimerkiksi tilannetta, jolloin analysoija tutkii havaittua uutta tai epänormaalia teknologiaa. Tätä kautta voidaan löytää uusia suorituskykyjä, joita hyökkääjät käyttävät. (Caltagirone ym., 2013, s. 30).

Timanttimallia käytetään Caltagironen ym. (2013) artikkelissa rinnakkain tappoketjun kanssa. Timanttimallin avulla tehdään tappoketjun eri vaiheista analyysi timanttimallin neljästä eri ominaisuudesta. (Caltagirone ym., 2013, s. 31). Tällä tavalla syy-seuraussuhteet voidaan saada selville, ja ymmärtää, miten esimerkiksi tietty käyttäjätunnus on saatu haltuun, tai miten hyökkääjä on päässyt tunkeutumaan verkkoon. Tästä syystä pelkän timanttimallin käyttö kyberoperaatioiden analysoinnissa ei onnistu.

4.3.3 Kybertappoketju

Kybertappoketju (engl. Cyber Kill Chain) perustuu Yhdysvaltain puolustusministeriön tappoketjumalliin, jonka osa-alueet ovat kohteen löytäminen, paikantaminen, seuraaminen, aseistuksen valinta, hyökkääminen ja vaikutusten arviointi (engl. find, fix, track, target, engage, assess) (Lo & Au, 2010, s. 95). Tätä mallia on sovellettu kybertappoketjuun, jonka osa-alueet ovat: tiedustelu (engl. reconnaissance), aseistaminen (engl. weaponization), toimittaminen (engl. delivery), hyväksikäyttö (engl. exploitation), asentaminen (engl. installation), johtaminen engl. (command & control tai C2) ja kohteessa toimiminen (engl. actions on objectives). Ideana on analysoida jokaisessa vaiheessa eri indikaattoreita, jotka kasvattavat puolustajan tietämystä hyökkääjästä. Indikaattoreista saadun tiedon avulla voidaan kehittää jatkon varalle vastatoimenpiteitä ja pysäyttää tulevat hyökkäykset aikaisemmassa vaiheessa ketjua. (Hutchins ym., 2011, s. 115–117). Kybertappoketju on esitelty seuraavassa kuviossa (kuvio 13).



KUVIO 13 Kybertappoketju (mukaillen Hutchins ym., 2011, s. 117)

Tiedusteluvaiheessa hyökkääjä hankkii puolustajasta mahdollisimman paljon tietoa, esimerkiksi sosiaalisella manipuloinnilla tai yleisistä lähteistä tietoja keräämällä (Hutchins ym., 2011, s. 116). Tiedustelu voidaan jakaa vielä tiedustelun aloittamiseen, kohteen valintaan ja profilointiin. Tiedot saadaan yleensä internetin kautta, kuten blogeja, yritysten verkkosivuja ja muuta avointa materiaalia lukemalla. Tiedustelua voidaan tehdä passiivisena ja aktiivisena, riippuen siitä kerätäänkö tietoja yleisistä lähteistä vai pyritäänkö suorittamaan aggressiivisempaa tiedustelua. Aggressiivista tiedustelua voi olla esimerkiksi porttiskannausten tekeminen. (Yadav & Mallardi, 2015, s. 439.) Lopputuloksena löydetään sopiva kohde, jota vastaan hyökkäys lopulta toteutetaan.

Aseistamisella tarkoitetaan esimerkiksi tilannetta, jossa Word- tai PowerPoint-tiedostoon on lisätty haittaohjelma (Hutchins ym., 2011, s. 116). Yleensä nämä haittaohjelmat ovat etäkäyttötyökaluja (engl. Remote Access Tool, jäljempänä RAT), jotka antavat pääsyn hyökkääjälle uhrin järjestelmiin. Tämä haittaohjelma on kyberaseen niin kutsuttu hyötykuorma. RATissa on kaksi osaa; käyttäjä (engl. client) ja palvelin (engl. server). Käyttäjäosa on se osa koodia, joka varsinaisesti käynnistää koodin kohteessa. Palvelin on taas kyberaseen "osa", joka mahdollistaa hyötykuorman viemisen kohteeseen. On olemassa tapoja viedä hyötykuorma kohteeseen ilman palvelinta, kuten sulauttamalla RAT osaksi aitoa ohjelmistokoodia. (Yadav & Mallardi, 2015, s. 440.)

Toimittamisella tarkoitetaan halutun haittaohjelman siirtämistä kohteeseen. Tämä voi tapahtua esimerkiksi sähköpostin, valesivuston tai fyysisen siirtovälineen, kuten USB-tikun avulla (Hutchins ym., 2011, s. 116). Toimitusvaiheessa

hyökkääjällä on suuri riski jäädä kiinni, mistä syystä esimerkiksi sähköpostilla lähetetyt haittaohjelmat tulevat yleensä hyökkäystä varten luoduista sähköpostiosoitteista. Hyökkääjät saattavat kokeilla useampaa eri lähestymistapaa, sillä mikään kuljetustapa ei takaa täysin varmaa kohteeseen pääsyä. (Yadav & Mallardi, 2015, s. 440.)

Hyväksikäyttö tarkoittaa vaihetta, jolloin haittaohjelma aktivoituu. Tämä tarkoittaa esimerkiksi tilannetta, jolloin uhri avaa haitallisen tiedoston (Hutchins ym., 2011, s. 116). Tämä vaihe vaatii sen, että kuljetusvaihe on onnistunut. Myös seuraavien ehtojen tulee täyttyä:

1. Uhrin tulee käyttää ohjelman tai käyttöjärjestelmän versiota, johon RAT on suunniteltu
2. Uhrin käyttöjärjestelmä tai ohjelmistot eivät saa päivittyä versioon, joka estää haavoittuvuuden käytön
3. Uhrin tietoturvamekanismit (kuten virustorjuntaohjelmat) eivät saa havaita koodin käynnistystä.

Jos kaikki edellä mainitut ehdot täyttyvät, haittaohjelma saadaan asennettua uhrin järjestelmään. (Yadav & Mallardi, 2015, s. 440.)

Asennusvaiheessa haittaohjelma asentuu uhrin järjestelmään (Hutchins ym., 2011, s. 116). Nykyään uhrin koneelle asentuvat haittaohjelmat alkavat olla todella hienovaraisia, ja niissä on useampi vaihe, jotka vähentävät haittaohjelmien paljastumistodennäköisyyttä. Haittaohjelmassa on yleensä kaksi osaa. Dropper on ohjelman osa, joka asentaa ja käynnistää haittaohjelman kohteessa. Nämä yrittävät samalla sammuttaa uhrin puolustusmekanismit. Downloader toteuttaa samaa tehtävää kuin dropper, mutta ne ovat yleensä kooltaan pienempiä. Tämä johtuu siitä, että hyötykuorman kantamisen sijaan niiden tehtävä on ottaa yhteys hyökkääjän palvelimeen. (Yadav & Mallardi, 2015, s. 441.)

Johtamisvaiheessa yhteys muodostetaan uhrin järjestelmän ja hyökkääjän järjestelmän välille (Hutchins ym., 2011, s. 116). Tämän järjestelyn avulla haittaohjelma mahdollistaa etäkäytön uhrin järjestelmiin. Nämä yhteydet perustuvat kolmelle eri tyylille; perinteiselle keskitetylle järjestelmälle, hajautetulle järjestelmälle ja järjestelmiin, jotka pohjautuvat sosiaalisiin verkkoihin. Keskitetyssä järjestelmässä yksi keskuspalvelin hallitsee kaikkia saastuneita koneita. Haittoina hyökkääjän näkökulmasta tällaisen järjestelmän käytölle on se, että keskuspalvelimen mennessä nurin menetetään yhteys myös uhrien järjestelmiin. Hajautettu järjestelmä käyttää P2P (peer-to-peer) -arkkitehtuuria, eli järjestelmä koostuu bottiverkosta. Jokainen saastunut on vastuussa pienestä osasta verkon ylläpitoa. Tämä mahdollistaa paremman vikasietokyvyn. Sosiaalinen media taas mahdollistaa suurten verkkojen saastuttamisen. Monet sosiaalista mediaa käyttävät työkalut ja alustat ovat ilmaisia, ja niitä käyttävät myös monet yritykset. Tämä mahdollistaa laajan hyökkäyspinta-alan käytön. (Yadav & Mallardi, 2015, s. 442.)

Hyökkääjät pyrkivät nykyään piilottamaan uhrin ja hyökkääjän järjestelmien välisen keskustelun, sillä tämä on perinteinen järjestelmänvalvojien tapa valvoa järjestelmiensä verkkoliikennettä ja pyrkiä havaitsemaan saastuneiden

koneiden lähettämää liikennettä. IRC-keskustelukanavien, TCP, HTTP ja FTP-protokollien ja TOR-verkon käyttö ovat esimerkkejä tavoista, joilla hyökkääjät yrittävät piilottaa liikennettään. (Yadav & Mallardi, 2015, s. 442.)

Tavoitteen vaatimat toimenpiteet tarkoittavat sitä vaihetta, kun hyökkääjä on saavuttanut jalansijan uhrin järjestelmässä ja hyökkääjä toteuttaa haluamiaan toimenpiteitä kohteessa. Toimenpiteitä voivat olla esimerkiksi tietojen lataaminen kohdejärjestelmästä, järjestelmien sammuttaminen tai toisten käyttäjätietojen hankkiminen. (Hutchins ym., 2011, s. 116.)

4.3.3.1 Kybertappoketjun käyttö

Strategisella tasolla kybertappoketjun käyttö hyödyttää pitempiaikaisia puolustuksia suunniteltaessa. Analysoitaessa useaa eri ketjua voidaan hyökkääjästä saada tietoja, joiden avulla hyökkääjä voidaan tulevissa hyökkäysyrityksissä havaita. Hyökkääjä saattaa käyttää eri hyökkäyksissä samaa IP-osoitetta, jolloin kyseisestä osoitteesta tuleva liikenne voidaan estää kokonaan. Näin kävi Hutchinsin ym. (2011) tutkimuksen esimerkeissä. Kyseisessä esimerkissä Lockheed Martinin CIRT-ryhmä (Cyber Incident Response Team) analysoi kolmea eri organisaation järjestelmiin kohdistunutta hyökkäystä. Ryhmä pystyi joka kerran jälkeen parantamaan järjestelmiensä suojauskykyä, koska he löysivät hyökkääjästä tietoja, jotka yhdistivät eri aikaan tehdyt hyökkäykset toisiinsa. (Hutchins ym., 2011, s. 119.)

Ensimmäinen hyökkäysyritys toteutettiin kohdennetulla sähköpostilla ja sähköpostin liitteenä olleella haittaohjelmalla. Analysoimalla hyökkäysketjun eri vaiheita hyökkäyksestä saatiin seuraavassa kuviossa (kuvio 14) olevat tiedot selville. Tiedusteluvaiheeseen sijoitettiin sähköpostin saaneiden henkilöiden osoitteet. Asevaiheeseen sijoitettiin haittaohjelman sisältänyt liitetiedosto. Kuljetusvaihe toteutettiin sähköpostilla, ja tähän kohtaan sijoitettiin lähettäjän sähköposti. Käynnistysvaiheeseen sijoitettiin PDF-tiedostoon liittyvä haavoittuvuus, joka oli tiedossa (mutta jota ei ollut vielä viestin lähetyshetkellä korjattu). Asennusvaiheeseen sijoitettiin haittaohjelman käynnistystiedosto (fssm32.exe). Johtamisvaiheeseen sijoitettiin analyysin perusteella löydetty IP-osoite, jonne haittaohjelma olisi lähettänyt HTTP-pyynnön kautta järjestelmistä saamaansa tietoa. Viimeiseen kohtaan eli toimenpiteisiin ei laitettu mitään, koska hyökkäys pystyttiin estämään kuljetusvaiheessa. (Hutchins ym., 2011, s. 121).

Vaihe	Indikaattori
Tiedustelu	[Recipient List] Benign File: tcnom.pdf
Aseistaminen	Trivial encryption algorithm: Key 1
Kuljetus	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]
Hyväksikäyttö	CVE-2009-0658 [shellcode]
Asentaminen	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\EXPLORE.hlp
Johtaminen	202.abc.xyz.7 [HTTP request]
Kohteessa toimiminen	-

KUVIO 14 Case-esimerkin ensimmäisen hyökkäyksen ketjun analysointi (mukaillen Hutchins ym., 2011, s. 121)

Toinen hyökkäys, joka tapahtui heti seuraavana päivänä, pystyttiin yhdistämään edelliseen hyökkäykseen samojen indikaattoreiden avulla. Seuraavassa kuviossa (kuvio 15) näkee, miten hyökkäyksessä käytettiin eri elementtejä (esimerkiksi lähetetty tiedosto oli eri), mutta lähettäjä sekä haittaohjelma olivat samoja. (Hutchins ym., 2011, s. 122.)

Vaihe	Hyökkäys 1	Hyökkäys 2
Tiedustelu	[Recipient List] Benign File: tcnom.pdf	[Recipient List] Benign File: MDA_Prelim.09.pdf
Aseistaminen	Trivial encryption algorithm: Key 1	
Kuljetus	Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]	Downstream IP: 216.avc.xyz.76 Subject: 7th Annual U.S. Missile Defense Conference [Email body]
	dn…etto@yahoo.com	
Hyväksikäyttö	CVE-2009-0658 [shellcode]	
Asentaminen	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\EXPLORE.hlp	
Johtaminen	202.abc.xyz.7 [HTTP request]	
Kohteessa toimiminen	-	-

KUVIO 15 Case-esimerkin ensimmäisen ja toisen hyökkäyksen analysointi (mukaillen Hutchins ym., 2011, s. 122)

Kolmas hyökkäys tapahtui kaksi viikkoa toisen hyökkäyksen jälkeen. Tämä hyökkäys erosi edellisestä hyökkäyksestä siten, että se yritti hyödyntää nollapäivähaavoittuvuutta (engl. zero-day exploit). Tämä haavoittuvuus ei ollut järjestelmänvalvojien tiedossa. Se, mikä paljasti hyökkääjän olleen sama kuin aiemmin, oli saman IP-osoitteen käyttö kuin aiemmissakin hyökkäyksissä. Seuraavassa kuviossa (kuvio 16) näkyvät kaikkien hyökkäysten analysointiketjut. (Hutchins ym., 2011, s. 123.)

Vaihe	Hyökkäys 1	Hyökkäys 2	Hyökkäys 3
Tiedustelu	[Recipient List] Benign File: tcnom.pdf	[Recipient List] Benign File: MDA_Prelim.09.pdf	[Recipient List] Benign File: MDA_Prelim.09.pdf
Aseistaminen	Trivial encryption algorithm: Key 1		Trivial encryption algorithm: Key 2
Kuljetus	[Email subject] [Email body]	[Email subject] [Email body]	[Email subject] [Email body]
	dn…etto@yahoo.com		ginette.c…@yahoo.com
Hyväksikäyttö	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Asentaminen	C:\...\fssm32.exe		
Johtaminen	202.abc.xyz.7		
Kohteessa toimiminen	-	-	-

KUVIO 16 Kaikkien hyökkäysten eri ketjujen analysointi (mukaillen Hutchins ym., 2011, s. 123)

Pols (2017, s. 10–11) kritisoi kybertappoketjua sen harhaanjohtavuudesta. Polsin mukaan ketju tekee liikaa oletuksia hyökkääjän mahdollisista toimista. Jos nämä toimet eivät toteudukaan, johtaa ketjun perusteella tehty malli puolustajia harhaan. Kritiikkiä on myös esitetty siitä, että malli ei huomioi sisältä päin tulevia uhkia, vaan keskittyy ainoastaan ulkoapäin tuleviin hyökkäyksiin (Reidy & Randal, 2013; Laliberte, 2016).

4.3.4 Variaatioita kybertappoketjusta

Kybertappoketjuun on esitetty erilaisia parannuksia ketjua kohtaan syntyneen kritiikin pohjalta. Laliberten mallissa ketjusta otetaan aseistusvaihe pois, ja tilalle tulee poikittaisliike järjestelmän sisällä. Laliberten mukaan hyökkääjät eivät pyri murtautumaan lopulliseen kohdejärjestelmään, vaan etsivät helpompaa reittiä päästäkseen verkkoon sisälle ja tätä kautta kohdejärjestelmään käsiksi. Hänen mukaansa aseistus on myös vaihe, jota vastaan puolustaja ei voi varsinaisesti varautua. Poikittaisliikkeen sen sijaan voi havaita ja estää. (Laliberte, 2016.)

Nachreiner on samoilla linjoilla Laliberten kanssa, sillä myös hänen ehdottamasta mallistaan (Kill Chain 3.0) puuttuu aseistusvaihe. Nachreiner perustelee tätä sillä, että puolustajan tulisi vaikuttaa ketjun jokaiseen vaiheeseen jollain tavalla. Nachreinerin mukaan aseistusvaiheeseen puolustaja ei kykene vaikuttamaan. (Nachreiner, 2015.) Kuten Laliberte & Nachreiner, myös Bryant & Saiedian esittävät kybertappoketjusta aseistamisvaiheen poistamista. Heidän esittämäänsä ketjuun lisätään poikittaisliike järjestelmän sisällä, ja ketjun loppuun vaihe tiedon siirtämisestä järjestelmästä ulos. Mallia käytetään yhdessä erilaisten tietojenkeruujärjestelmien kanssa vähentämään turhien hälytysten määrää ja helpottamaan järjestelmävalvojien työtä tunkeutujien löytämisessä. (Bryant & Saiedian, 2017, s. 198.) Malone laajentaa kybertappoketjua kaikkein eniten. Hän jättää alkuperäisen ketjun ennalleen, mutta lisää kaksi ylimääräistä ketjua malliin mukaan. Nämä lisätyt ketjut kuvaavat hyökkääjän toimia järjestelmässä sen jälkeen, kun hyökkääjä on päässyt tietoverkkoihin sisälle. (Malone, 2016.)

Edellä esitetyistä muokatuista kybertappoketjuista ainoastaan Bryantin & Saiedianin (2017) ketju on esitelty alan julkaisussa, muut mallit esiintyvät ainoastaan kirjoittajien verkkosivuilla tai esitysmateriaalissa. Kyseisiin malleihin tulisi kohdistaa tarkempaa tutkimusta, jotta ne olisivat luotettavampia analyysityökaluja. Bryantin & Saiedianin (2017) malli on määrällinen, ja sen käyttö edellyttää pääsyä kohdejärjestelmän tietokantaan, jotta mallin mukainen analyysi onnistuisi.

4.3.5 ATT&CK

ATT&CK on sekä malli että viitekehys, jonka tarkoitus on auttaa järjestelmänvalvojia kuvaamaan ja havaitsemaan hyökkääjän liikkeet järjestelmän sisällä. Malli lähtee siis siitä näkökulmasta liikkeelle, että hyökkääjät ovat jo päässeet järjestelmään sisälle (Strom ym, 2017, s. 2). ATT&CK-malli perustuu viidelle periaatteelle:

1. Järjestelmän sisäinen tarkkailu. Tätä perustellaan sillä, että jossain vaiheessa hyökkääjä voi päästä puolustusmekanismeista läpi, ja järjestelmää tulee tarkkailla myös sisäpuolelta käsin.
2. Käyttäytymismallien havainnoinnin kehittäminen. Järjestelmän puolustusmekanismien tulisi kehittyä havainnoimaan hyökkääjän aiheuttamia signaaleja myös järjestelmän sisäpuolella. Staattiset, oppimattomat puolustusmekanismit eivät kykene tunnistamaan hyökkääjää, joka muuttaa käyttäytymismallejaan päästyään järjestelmään sisälle.
3. Uhkamallin käyttö. Puolustusmekanismien tulisi pohjautua ajantasaisimmalle uhkamallille.
4. Jatkuva kehittäminen. Hyökkääjät ja näiden menetelmät kehittyvät jatkuvasti, sama periaate pitäisi olla myös puolustajalla mielessä.
5. Kehitys ja testaus realistisessa ympäristössä. Vain tällä tavalla saadaan palautetta, joka auttaa tositilanteeseen valmistautumiseen. (Strom ym., 2017, s. 5.)

Malli jakautuu taktiselle ja tekniselle tasalle. Taktisella tasalla kuvataan kymmenen eri tavoitetta, joihin hyökkääjä pyrkii järjestelmään tunkeutuessaan. (Strom ym, 2017, s. 9–10.) Taktisen tasan tavoitteet ovat seuraavat:

1. Sitkeys. Hyökkääjän täytyy tehdä toimenpiteitä pysyäkseen järjestelmässä sisällä, kuten yrittää saada laajempia käyttöoikeuksia haltuunsa.
2. Käyttöoikeuksien laajentaminen. Hyökkääjä voi pyrkiä syvemmälle järjestelmään saadakseen arkaluontoisempia tietoja käsiinsä.
3. Välttely. Hyökkääjä yrittää pitää tekemänsä toimenpiteet piilossa mahdollisimman pitkään.
4. Käyttöoikeuksien saaminen ja laajentaminen.
5. Järjestelmätietojen löytäminen.
6. Liikkuminen eri järjestelmien välillä.
7. Koodin käynnistäminen järjestelmässä.
8. Tietojen kerääminen ja lataaminen järjestelmästä.
9. Tietojen siirtäminen järjestelmän ulkopuolelle.
10. C&C. Tämä tarkoittaa tekniikoita, joilla hyökkääjä kommunikoi niiden järjestelmien kanssa, joihin tämä on päässyt sisälle. (Strom ym., 2018, s. 10.)

Tekniikat ovat yksityiskohtaisempia kuvailuita siitä, miten hyökkääjä saavuttaa edellä mainitut tavoitteet. Esimerkkinä annetaan etäkäytön saaminen schtasks.exe-prosessin avulla (Strom ym., 2018, s. 13).

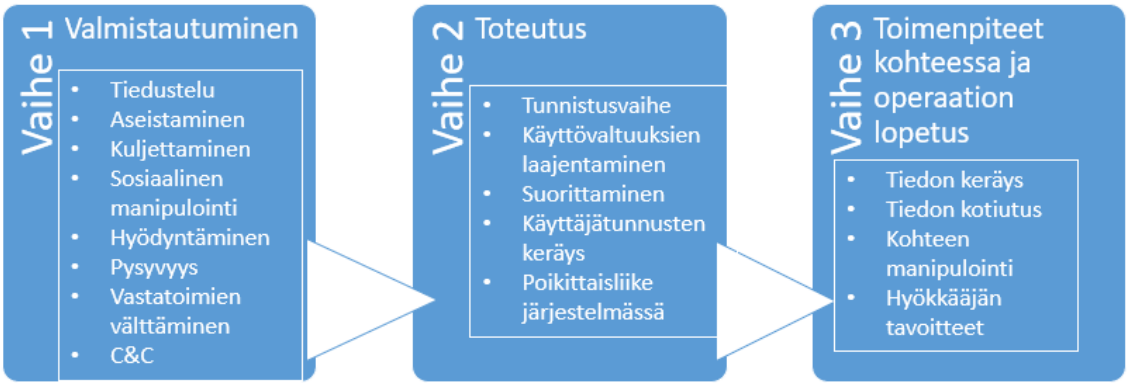
Vaikka ATT&CK-malli puuttuukin kybertappoketjua (CKC) kohtaan osoitettuun kritiikkiin siitä, että CKC ei huomioi sisältä päin tulevia uhkia, ATT&CK ei sovellu tämän tutkimuksen tapausten tutkimiseen. Sen laajuus on liian kapea kyberoperaation tapausten tutkimiseen. Malli menee myös liian yksityiskohtaiseen analyysiin, sillä tapauksista ei ole tarvetta saada tarkkoja hyökkäysmalleja

selville. Tällä tarkoitetaan esimerkiksi tarkkojen prosessien tai hyökkääjän käyttämien ohjelmien selvittämistä. Tutkimuksessa on tavoitteena myös ottaa huomioon hyökkääjän tavoitteet ennen operaatiota ja järjestelmiin pääsemistä sekä toimet operaation jälkeen. Näihin osa-alueisiin ATTK&CK-malli ei ota kantaa.

4.3.6 Yhdistetty tappoketju

Yhdistetty tappoketju (engl. Unified Kill Chain, jäljempänä UKC) on Paul Polsin lopputyössään luoma malli. Se pohjautuu kybertappoketjuun (CKC) ja se on myös ottanut vaikutteita ATT&CK-mallista yhdistäen näin sekä CKC:n että ATT&CK-mallin ominaisuuksia. Tähän malliin on yhdistetty myös CKC:n erilaisten variaatioiden ominaisuuksia. UKC:ta on myös kehitetty huomioiden tapaustutkimusstrategian vaatimukset (Pols, 2017, s. 27). Lopputuloksena on viitekehys, jolla voi analysoida ja verrata hyökkäysketjuja alusta loppuun ja suunnitella puolustusmekanismeja hyökkäyksiä vastaan. Erityisesti tavoitteena on ollut luoda malli, joka kuvaisi realistisesti APT-ryhmien toimintaa, jonka organisaatioiden Red Team –ryhmät voivat toistaa (Pols, 2017, s. 12.)

Pols loi alustavan mallin kirjallisuuskatsauksen perusteella. Katsaus keskittyi CKC:iin ja tämän eri kehitysmuotoihin. Kirjallisuuskatsauksen ja alustavan mallin kehittämisen jälkeen Pols analysoi yhden Red Team –ryhmän ja APT28 –ryhmän toimintaa (APT28 on yhdistetty Venäjän tiedustelupalveluun). Analyysi kohdistui näiden ryhmien suorittamaan tunkeutumiseen kolmea eri järjestelmää vastaan. Kun malli oli riittämätön selittämään ryhmän toimintaa, sitä muutettiin paremmin toimintaa vastaavaksi (Pols, 2017, s. 47.) Tapausten analysoinnin jälkeen Pols toteutti haastatteluja, joilla mallin luotettavuutta paranneltiin (Pols, 2017, s. 51). Alla olevassa kuviossa (kuvio 17) näkyy UKC:n rakenne ja vaiheet.



KUVIO 17 Yhdistetty tappoketju (mukaillen Pols, 2017, s. 78)

Operaation ensimmäisessä vaiheessa (valmistautumisvaiheessa) hyökkääjä toteuttaa joko aktiivista tai passiivista tiedustelua. Tiedustelun tavoitteena on kohteen löytäminen ja valitseminen. APT28-ryhmä on esimerkiksi tiedustellut avoimista lähteistä sopivia kohdehenkilöitä, joille kohdennettuja sähköposteja on lähetetty. Aseistamisella tarkoitetaan hyötykuormalla varustetun ohjelman valmistelua. Tämä voi olla esimerkiksi troijalainen, joka on ujutettu PowerPoint-tie-

dostoon. APT28-ryhmä on käyttänyt sekä nollapäivähaavoittuvuuksia että julkisuuteen tulleita haavoittuvuuksia hyväkseen. Kuljettamisella tarkoitetaan niitä välineitä, joilla haittaohjelmalla varustettu ohjelma saadaan ladattua kohdeympäristöön. Aiemmin mainittu kohdennettu sähköposti on osoittautunut toimivaksi tavaksi päästä kohdeorganisaation tietoverkkoihin käsiksi. Sosiaalinen manipulointi on yksi esimerkki vaiheesta, jolla kohdeorganisaation henkilöstöön kuuluva voidaan huijata lataamaan haittaohjelma koneelleen. Kun ohjelma on saatu koneelle, hyökkääjä alkaa käyttämään järjestelmän haavoittuvuuksia hyväkseen edistääkseen tavoitteitaan. Tämä tarkoittaa myös niiden toimenpiteiden tekemistä, joilla hyökkääjä saa pidettyä jalansijan järjestelmässä, ja välttämään puolustajan vastatoimenpiteitä (kuten järjestelmäskannauksia). APT28 on esimerkiksi modifioinut järjestelmien lokitietoja välttyäkseen kiinnijäämiseltä. Komentovaihe (C&C) on koko operaation ajan jatkuvaa, jolla hyökkääjä kommunikoi etätyökaluilla hallussaan olevien järjestelmien kanssa. (Pols, 2017, s. 55.)

Operaation toisessa vaiheessa (toteutusvaihe) hyökkääjä toteuttaa toimenpiteitä, joilla se vahvistaa asemiaan kohteena olevassa järjestelmässä. Tämä voi tarkoittaa esimerkiksi toimenpiteitä, joilla hyökkääjä saa lisää tietoa järjestelmän ominaisuuksista, laajentaa käyttöoikeuksiaan sekä liikkumaan sivusuunnassa myös muissa kohdeverkon järjestelmissä. Järjestelmissä olevilla haittaohjelmilla voidaan ladata lisää työkaluja, joilla hyökkääjät toteuttavat esimerkiksi järjestelmäskannauksia ja tiedostojen lataamista. Erityisen mielenkiinnon kohteena APT-ryhmillä ovat olleet käyttäjätunnusten hankkiminen ja käyttöoikeuksien laajentaminen. Käyttäjätunnusten avulla ryhmät ovat järjestelmiin tunkeutumisen jälkeen kyenneet siirtymään myös järjestelmän paremmin suojattuihin osiin. (Pols, 2017, s. 56.)

Operaation kolmannessa vaiheessa (toimenpiteet kohteessa ja operaation lopetus) hyökkääjä toteuttaa tavoitteidensa mukaiset toimenpiteet kohteessa. Tavoitteisiin voi kuulua esimerkiksi tiedon keräämistä ja siirtämistä järjestelmän ulkopuolelle tai kohteen manipulointia. Manipuloinnilla voidaan tarkoittaa myös tietojen tuhoamista. Esimerkiksi APT28 on hyökännyt ranskalaista TV5-televisiokanavaa vastaan ja poistanut ohjelmistoja yhtiön palvelimilta. Kerätty tieto on koostunut esimerkiksi sähköpostiosoitteista ja järjestelmästä otetuista ruutukaappauksista. Järjestelmästä ulos siirrettävät tiedot on tallennettu niin, että järjestelmän uudelleenkäynnistyskään ei poista tallennettuja tietoja. (Pols, 2017, s. 56.)

UKC:n vahvuutena on sen laajempi hyökkäyksien mallinnus kuin mitä CKC mallintaa. UKC esimerkiksi ottaa huomioon tavalliset käyttäjät sosiaalisen manipuloinnin kautta. Myös tiedon käsittelyn määritelmää on laajennettu. Hyökkääjä ei välttämättä halua saada tietoa ulos järjestelmästä, vaan tälle riittää tietojen tuhoaminen. Malli myös lähestyy hyökkäysten analysointia laadullisemmasta näkökulmasta. (Pols, 2017, s. 77.) Malli myös haastaa CKC:n näkemyksen siitä, että onnistuneen hyökkäyksen täytyy koostua ketjusta, joissa jokaisen osa-alueen täytyy onnistua, jotta lopulliseen tavoitteeseen päästään (Pols, 2017, s. 14).

Pols myöntää, että hänen kehittämässään mallissa on puutteita. Yksi suuri haaste on puumallisten hyökkäysten analysointi. Tällaisissa hyökkäyksissä on

useampi hyökkäysreitti. Analysoijan tulee siis huomioida useamman mahdollisen reitin olemassaolo eikä tyytyä vain yhteen analysoitavaan reittiin. Sama tilanne tulee vastaan hyökkäyksissä, joissa hyökkääjä saattaa toistaa jotain vaihetta useamman kerran tavoitteensa saavuttamiseksi. Pols on myös käyttänyt hyvin kapeaa aineistoa. Kohderyhminä hän käyttää ainoastaan yhtä Red Teamia ja yhtä APT-ryhmää. Pols sivusi kuitenkin lyhyesti myös APT29-ryhmää, ja toteaa, että alustavalla tarkastelulla mallia voidaan käyttää myös tämän ryhmän toimenpiteiden analysointiin. (Pols, 2017, s. 77–78). APT29, toiselta nimeltään Cozy Bear, on vuodesta 2010 lähtien toiminnassa ollut hakkeriryhmä, joka on toteuttanut kyberhyökkäyksiä pääasiassa länsimaisia hallituksia ja yrityksiä vastaan (Modderkolk, 2018, s. 3). Hypoteesina Polsilla on siis se, että mallia pystyy käyttämään yleisemmin APT-tyyppisten ryhmien toiminnan analysoinnissa.

UKC ottaa laajimmin huomioon kyberoperaatioon liittyvät eri vaiheet. Mielestäni varsinkin lisäys tiedon tuhoamisesta yhdeksi mahdolliseksi hyökkääjän toimeksi kohteessa on hyvä huomio. Kyberoperaatioiden tavoitteena ei välttämättä ole aina pelkästään tiedon saaminen ulos järjestelmästä, vaan tietojen tuhoaminen riittää.

4.3.7 Yhteenveto ajallisista malleista

Ajalliset mallit kuvaavat tutkimuksen näkökulmasta parhaiten kyberoperaatioiden eri vaiheita (lukuun ottamatta Riskitiä, joka on riskinhallintaan suunniteltu viitekehys). Timanttimallin avulla ei pystytä kuvaamaan operaation ajallista etenemistä. Tässä mallissa hyvänä puolena on kuitenkin se, että malli huomioi uhrin ja hyökkääjän välisen suhteen. Kybertappoketjulla pystyy kuvaamaan ja vertailemaan huomattavasti paremmin operaation eri vaiheita, kuten Hutchinsin ym. (2011) tapaustutkimuksessa todettiin. Mallissa on kuitenkin puutteita, jotka yhdistetty tappoketju paikkaa parhaiten tämän tutkimuksen näkökulmasta. Jokainen malli keskittyy pitkälti tietoverkkojen analysointiin, mutta UKC:ssa otetaan huomioon samat operaation osa-alueet kuin mitä tavallisiin kineettisiin operaatioihin sisältyy. Nämä ovat suunnittelu, toteutus ja siirtymävaihe (johon operaatio päättyy) (NATO, 2013, s. 61).

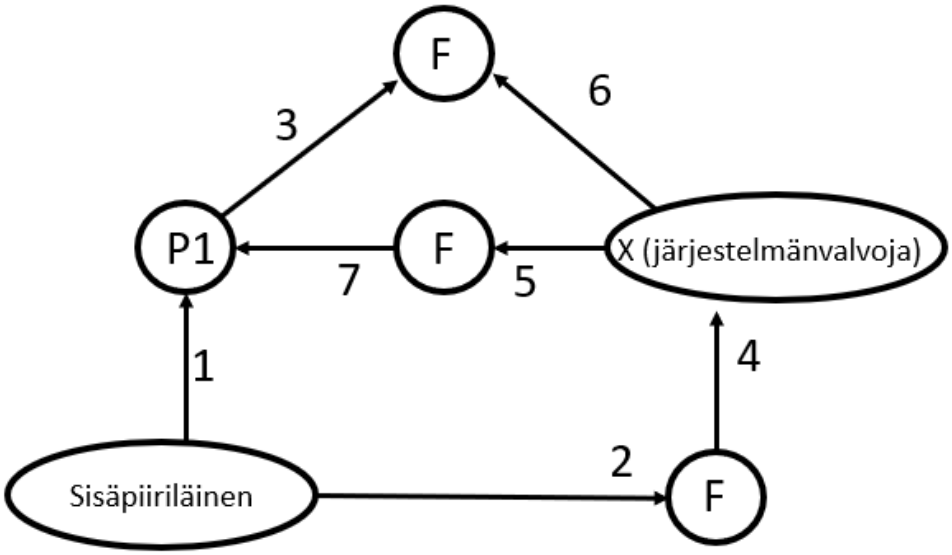
4.4 Kuvaajamallit

Kuvaajapohjaiset kyberhyökkäysmallit (engl. Graph Based Methods) koostuvat solmuista (engl. vertice) ja suhteista (engl. edge) (Lallie ym., 2020, s. 7). Solmut voivat esittää joko haavoittuvuutta (Noel & Jajodia, 2004, s. 111), edellytystä tai jälkiehtoa (engl. postcondition) tai edellisten yhdistelmiä. Suhteet tarkoittavat siirtymisiä yhdestä solmusta toiseen. Esimerkiksi haavoittuvuuden syymallissa (engl. vulnerability cause graphs) on solmu, johon on kuvattu tapaus, jossa virheellisen syötteen kirjoittamista ei ole huomioitu palvelun turvallisuusvaatimuksissa. Tämä johtaa siirtymiseen toiseen solmuun, jossa kuvataan, että palveluun ei kehitetä mahdollisuutta estää virheellistä syötettä (ja tätä kautta järjestelmään

muodostuu haavoittuvuus). (Chaufette & Haag, 2007, s. 3.) Sekä solmuille että suhteille voidaan asettaa painoarvoja, jotka voivat kuvata esimerkiksi hintaa, todennäköisyyttä ja riskiä. Todennäköisyysarvo voi kuvata esimerkiksi sitä, mitä hyökkäysreittiä hyökkääjä todennäköisimmin käyttää (Xie, Cai, Tang, Ju & Chen, 2009, s. 133). Kuvaajapohjaiset mallit voivat olla joko syklisiä (engl. cyclic) tai asyklisiä (engl. asyclic). Syklisissä malleissa reitit saattavat palata edellisiin solmuihin, kun taas asyklisissä malleissa kuljetaan ainoastaan yhteen suuntaan. Kuvaajamalleista suosituimpia ovat hyökkäysgraafit ja hyökkäyspuumallit (Lallie ym., 2020, s. 7). Seuraavissa alakappaleissa esitellään eri kuvaajamalleja, jotka pohjautuvat Lallien ym. (2020, s. 3) tutkimuksen kuvioon.

4.4.1 Hyökkäysgraafi

Hyökkäysgraafia (engl. Attack Graph) käytetään analysoimaan hyökkäyksen kohdetta ja sitä, miten hyökkäyksen voi toteuttaa (Lallie ym., 2020, s. 7). Seuraavassa kuviossa (kuvio 18) on esimerkki käyttöoikeusgraafista, jossa kuvataan hyökkääjän (sisäpiiriläinen) reittiä kohteeseen A käyttäjän P1 kautta. (Ortalo ym., 1999, s. 634–635.)



KUVIO 18 Käyttöoikeusgraafi (mukaillen Ortalo ym., 1999, s. 635)

Hyökkäysgraafilla pyritään laskemaan ja näyttämään kaikki mahdolliset vaihtoehdot, jotka johtavat hyökkääjän tavoitteiden täyttymiseen (Kotenko & Chechulin, 2013, s. 2). Hyökkäysgraafi on yläkäsite, eikä yhtä tiettyä mallia kuvaava termi. Tällaisia graafeja on kehitetty lukuisia eri vaihtoehtoja. Esimerkiksi Lallien ym. (2020, s. 7) tutkimuksessa käsiteltiin yhteensä 118 erilaista hyökkäysgraafia. Koska hyökkäysgraafeja on kehitetty näin valtava määrä, ei niiden yksityiskohtainen käsittely ole tämän tutkimuksen laajuudessa mahdollista. Tästä syystä kirjallisuuskatsauksen perusteella tehdään omasta mielestäni tarpeellisimmat nostot.

Zhun (1990) kehittämä tartuntagraafi laskee haavoittuvimman reitin, jota virus saattaa käyttää kohdeympäristöönsä päästäkseen. Ortalon, Deswarten & Kaânichen (1999) käyttöoikeusgraafi mallintaa haavoittuvuuksia Linux-ympäristössä ja pyrkii laskemaan hyökkääjän todennäköisimmät hyökkäysreitit näiden haavoittuvuuksien perusteella. Mallissa kuvataan, miten hyökkääjä pääsee kohteeseensa solmujen kautta (jotka ovat yksittäisiä käyttäjiä ja näiden käyttäjäoikeuksia). Käyttäjillä saattaa olla haavoittuvuuksia, mitä hyökkääjä käyttää hyväkseen. Näitä haavoittuvuuksia ovat esimerkiksi arvattavat salasanat tai oikeuden saaminen .rhosts-tiedostoon (jota voi käyttää etäyhteyden ottamiseen ilman salasanaa).

Käyttöoikeusgraafissa käytetään kolmea eri vaihtoehtoa reitin laskemiseen: yhden reitin (engl. single path, jäljempänä SP), kokonaismuistin (engl. total memory, jäljempänä TM) ja muistittoman (engl. memoryless, jäljempänä ML) reitin vaihtoehtoa. Yhden reitin vaihtoehdossa oletetaan, että hyökkääjä valitsee lyhimmän reitin kohteeseensa. TM:n tapauksessa hyökkääjän oletetaan valitsevan helpoimman reitin kohteeseensa, tämä ei välttämättä ole kaikkein lyhin reitti. ML:ssä taas hyökkääjä pohtii reittivalintaansa pitempään. Vaikka seuraavassa solmussa olisikin helposti hyväksikäytettävä haavoittuvuus, ei reittivalinta auta juurikaan, jos tätä seuraavat solmut ovat paremmin suojattuja. (Ortalo ym., 1999, s. 636.) Mallia voi käyttää työkaluna eri hyökkäysreittivaihtoehtojen todennäköisyyksien laskemiseen, mutta itsenäiseen operaatioiden analysointiin malli on liian vajavainen.

Abraham ja Nair (2015) käyttävät tutkimuksessaan hyökkäysgraafia ja CVSS-pisteytystä laskemaan kohdejärjestelmän turvallisuutta (CVSS on pisteytysjärjestelmä, jolla mitataan järjestelmään kohdistuvien haavoittuvuuksien vakavuutta [Scarfone & Mell, 2009, s. 516]). CVSS-pisteytystä käytetään yhtenä syötettävän arvona myös Nicholsin, Hawrylakin, Halen & Papan (2017, s. 3) tutkimuksessa hybridihyökkäysgraafeista.

Aguessyn (2016) kehittämä hyökkäysgraafi on kehitetty tietojärjestelmää kohtaan kohdistuvien riskien analysointiin ja hallintaan. Aguessy kritisoi, että aiemmat hyökkäysgraafit skaalautuvat monimutkaisempia järjestelmiä kuvatessa liian vaikeasti luettaviksi. Eri graafien perusteella tehdyt mallit ovat myös hänen mukaansa liian staattisia; ne eivät reagoi käynnissä olevaan hyökkäykseen ja muokkaa hyökkäysreittien todennäköisyyttä hyökkäyksen aikana (Agueyssy, 2016, s. 3–4). Idea mallin dynaamisesta on hyvä. Aguessyn malli tarvitsee kuitenkin tarkemmat järjestelmäkohtaiset tiedot, jotta mallista on hyötyä.

Jotkin hyökkäysgraafit käyttävät tietopankkeja tai isoja määriä dataa luodakseen järjestelmiin kohdistuvista hyökkäyksistä valmiita malleja. Esimerkiksi Artzin (2002, s. 10–11) tutkimuksessa hyökkäysgraafi muodostettiin reaaliajassa NetSPA-nimisellä työkalulla, joka kerää datan esimerkiksi nmap- tai Nessus-nimisistä ohjelmista. Gaon, Hen & Lingin (2018) malli yhdistää järjestelmästä saadut tiedot haavoittuvuuksista, verkkokonfiguraatioista ja yhteyksistä MULVAL-nimiseen työkaluun, joka luo tiedon perusteella hyökkäysgraafin järjestelmästä.

Braynovin ja Jadliwalan (2003, s. 49) tutkimus keskittyi hyökkäysgraafien muodostamiseen tilanteissa, joissa järjestelmää kohtaan hyökätään samanaikaisesti useammasta eri suunnasta. Simuloiduista hyökkäyksistä saatu tieto syötettiin erilliseen ohjelmaan, jonka tulosteena ovat suositukset siitä, miten järjestelmää kannattaa koventaa.

Järjestelmästä saatu tiedon määrä voi olla joillekin järjestelmille ja ohjelmille liikaa. Tällöin ei saada luotua riittävän yksinkertaisia ja selkeitä malleja päätöksentekoa varten. Chengin, Wangin & Longin (2010, s. 1031) ehdottama mallinnuskeino vähentää järjestelmässä olevien samankaltaisten haavoittuvuuksien tuottamaa tietoa ja tekee hyökkäysgraafeista yksinkertaisempia kuvata. Saman ongelman nostivat esille Barik & Mazumdar (2011, s. 1), joiden lähtökohta on helpottaa ison tietomäärän käsittelyä isoissa organisaatioissa, jotka keräävät tietoa monesta eri lähteestä. Nanda & Deo (2007, s. 663) käyttävät hyökkäysgraafia ennustamaan hyökkääjän käyttämiä reittejä mallissaan, joka pyrkii vähentämään vääriä hälytyksiä, jotka johtuvat suuresta datamäärästä.

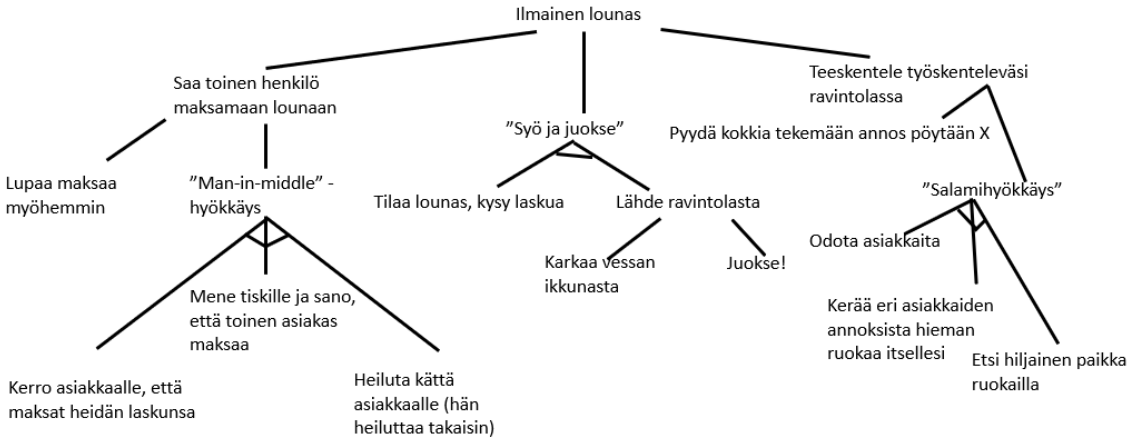
Feng & Jin-Shu (2008, s. 426) algoritmi auttaa järjestelmänvalvojia suojaamaan järjestelmiä tilanteissa, joissa dataa on vähemmän saatavilla. Lippmannin ym. (2005) tutkimuksessa pyritään vähentämään Red Teamien työtä automatisoimalla analysointia. Hyökkäysgraafeilla kuvataan järjestelmiä hyökkääjän näkökulmasta ja hyökkääjän reittiä palomuurien läpi (Lippmann ym., 2005, s. 2).

Peliteoriaa ja hyökkäysgraafeja on käytetty tutkimuksissa, joissa sekä hyökkääjän että puolustajan tekemät valinnat pyritään esittämään samanaikaisesti. Näin on tehty ainakin Nguyenin, Wrightin, Wellmanin & Bavejan (2017, s. 87) tutkimuksessa, jossa hyökkäysgraafien avulla ennustetaan hyökkääjän ja puolustajan samanaikaisesti tekemiä päätöksiä ja näistä seuraavia reitti- tai puolustusvalintoja. Peliteoriaa ja hyökkäysgraafia käytettiin myös Durkotan, Lisyn, Kiekintveldin & Bosanskyn (2015, s. 1773) tutkimuksessa, jossa puolustajalla on käytössään niin kutsuttu hunajapurkki, jolla yritetään hämätä hyökkääjää. Hyökkäysgraafilla kuvataan hyökkääjän oletettua suhtautumista näiden hunajapurkkien olemassaoloon.

Hyökkäysgraafeista tehdyn kirjallisuuskatsauksen perusteella kyseisiä graafeja käytetään pääasiassa kuvaamaan hyökkääjän käyttämiä reittejä erilaisissa tietojärjestelmissä. Hyökkäysgraafien laskemiseen tarvitaan yksityiskohtaista tietoa järjestelmistä, kuten reitittimien, laitteiden ja käyttäjien sijaintitiedot sekä järjestelmässä olevat haavoittuvuudet (ja joissakin tapauksissa näiden haavoittuvuuksien CVSS-pisteet). Tarvittavan tiedon tulee olla tarkkaa, jotta graafeista ja ennusteista olisi hyötyä. Ilman riittävää tarkkuutta graafeista ei ole järjestelmävalvojille riittävästi apua järjestelmiä kehittäessä. Tällaisella tarkkuudella olevia järjestelmäkuvauksia tai julkisia ominaisuuksia ei tutkimuksen kohteena olevista operaatioista ole saatavilla. Hyökkäysgraafien käsittelynäkökulma on myös liian yksityiskohtainen tämän tutkimuksen laajuuteen nähden. Operaatioista ei ole tarpeellista analysoida esimerkiksi IP-osoitteita tai hyökkääjän käyttämiä protokollia.

4.4.2 Hyökkäyspuumalli

Hyökkäyspuumallit (engl. Attack Tree) ovat hyökkäysgraafien ohella suosituin graafinen malli esittää kyberhyökkäyksiä. Kuten hyökkäysgraafit, hyökkäyspuumalli on yläkäsite joukolle erilaisia malleja (Lallie ym., 2020, s. 2). Hyökkäyspuumallit esitetään yleisesti asyklisinä. Tapahtumat etenevät alhaalta ylöspäin kohti tavoitetta, ja siirtyminen on ainoastaan yhteen suuntaan (Lallie ym., 2020, s. 9). Malleilla voidaan esittää systemaattisesti eri tapoja, joilla tietojärjestelmää kohtaan voidaan hyökätä. Mallissa olevat solmut (engl. node) kuvaavat hyökkääjän mahdollisia alatavoitteita, jotka edistävät päätavoitteen saavuttamismahdollisuutta. (Mauw & Oostdijk, 2005, s. 186.) Hyökkäyspuumalleja on käytetty tietojärjestelmiä kohtaan tehtävien hyökkäysten analysoinnin lisäksi ilmailualalla sekä energiasektorilla (Ingoldsby, 2010, s. 2). Seuraavassa kuviossa (kuvio 19) on esimerkki hyökkäyspuumallista.



KUVIO 19 Hyökkäyspuumalli (mukaillen Mauw & Oostdijk, 2005, s. 187)

Edellä olevassa esimerkissä hyökkääjän tavoite on saada ilmainen lounas. Tähän on laskettu kolme vaihtoehtoa. Osa vaihtoehdoista (kuten "salamihyökkäys" on kuvattu niin, että kaikkien alatavoitteiden tulee täyttyä, jotta vaihtoehto onnistuu. Tavoitteisiin voidaan myös sisällyttää lukuarvoja kuvaamaan tavoitteiden ominaisuuksia. Nämä ominaisuudet voivat olla esimerkiksi tavoitteen saavuttamisen todennäköisyys tai kustannus, joka aiheutuu puolustajalle haavoittuvuuden paikkaamiseksi. (Schneier, 1999, s. 22.)

Useimmat hyökkäyspuumallit ovat määrällisiä, ja useimmissa malleissa lasketaan numeraalista todennäköisyyttä tai arvoa eri hyökkäysreiteille. Esimerkiksi Royn, Kimin & Trivedin (2010, s. 1) mallissa algoritmiin syötetään hyökkäyspuumallin tapahtumat. Algoritmin avulla pyritään laskemaan eri hyökkäysreittien todennäköisyyksiä ja kustannuksia. Kumarin, Rujitersin & Stoelingan (2015, s. 6) mallin avulla pystytään laskemaan hyökkääjän käyttämä minimiaika, jolla tämä pääsee järjestelmään sisälle. Hyökkäyspuumallit pyrkivätkin usein vastaamaan esimerkiksi kysymyksiin "kuinka paljon tietty hyökkäys tulee aiheuttamaan kustannuksia" ja "mikä hyökkäys ei vaadi erityisosaamista" (Mauw & Oostdijk, 2005, s. 195).

Kuten kaikkien mallien tapauksissa, myös hyökkäyspuumallit ovat riippuvaisia analysoijan ammattitaidosta. Yhteen järjestelmään tehdystä hyökkäyspuumallista saatuja havaintoja voi olla myös vaikea soveltaa yleisesti muihin järjestelmiin. Vaikka järjestelmät olisivat identtisiä ominaisuuksiltaan, voi niihin kohdistuvat uhkat silti olla täysin erilaisia. Näistä uhkista johtuvat seuraukset voivat olla myös täysin erilaiset. (Ingoldsby, 2010, s. 1–2.)

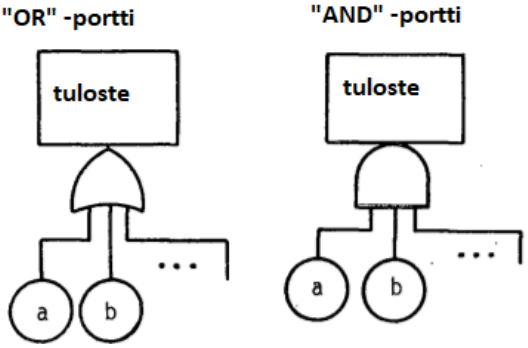
4.4.3 Virhepuumalli

Virhepuumallin (engl. Fault Tree) käytöllä on pitkät perinteet järjestelmäanalyysin osana. Malli esiteltiin ensimmäistä kertaa vuonna 1961 (Lee, Grosh, Tillman & Lie, 1985, s. 194), ja sitä on käytetty analysoitaessa erilaisten järjestelmien, kuten ydinreaktorien, luotettavuutta. Mallia käytetään myös arvioitaessa useammasta komponentista johtuvaa häiriötä ja erityisesti silloin, kun etsitään odottamattomia ja ei-toivottuja järjestelmähäiriöitä. Mallin on tarkoitus auttaa järjestelmän suunnittelussa, jotta ei-toivotun häiriön todennäköisyys saadaan laskettua riittävän pienelle tasolle. Schroderin (1969, s. 1–2) mukaan virhepuumalli on hyödyllinen kolmesta eri syystä:

1. Mallia voidaan käyttää analysoimaan onnettomuuksia, joita järjestelmän käytön seurauksena on tapahtunut. Oikeanlaisella käytöllä virhepuumalli johtaa juurisyihin, jotka ovat aiheuttaneet vikatilan järjestelmässä.
2. Virhepuumallin avulla pystytään paremmin esittämään häiriöstä johtuneen tapahtuman tulokset. Jos suunnittelussa on tehty virheitä, kyetään mallin avulla näyttämään ne osa-alueet, jotka ovat johtaneet häiriön syntymiseen. Jos taas suunnittelu on ollut riittävää, voidaan mallin avulla näyttää, että suunnittelussa on otettu huomioon riittävässä määrin eri mahdollisuudet.
3. Mallilla pystytään esittämään todennäköisyydet, jotka johtavat eri häiriötilanteisiin.

Mallin rakentaminen aloitetaan valitsemalla mielenkiinnon kohteena oleva järjestelmähäiriö (Schroder, 1969, s. 3; Lee ym., 1985, s. 195). Tämä häiriö asetetaan puun päällimmäiseksi osaksi. Tämän jälkeen häiriöön johtaneet (tai mahdollisesti jossain vaiheessa johtavat) syyt eritellään yksi toisensa jälkeen, kunnes kaikki mahdolliset syyt on yksilöity. Syyt on yksilöity riittävällä tarkkuudella, kun analyysissa päästään yksittäisten komponenttien aiheuttamiin häiriöihin. Syyt yhdistetään häiriöön niin kutsuttujen loogisten porttien avulla, jotka staattisessa häiriöpuumallissa voidaan kuvata kahdella eri tavalla: “OR”- tai AND” -

portilla. (Schroder, 1969, s. 3–4.) Seuraavassa kuviossa (kuvio 20) on esimerkit loogisista porteista.



KUVIO 20 "OR"- ja "AND"-portit, häiriöpuumalli (mukaillen Schroder, 1969, s. 4)

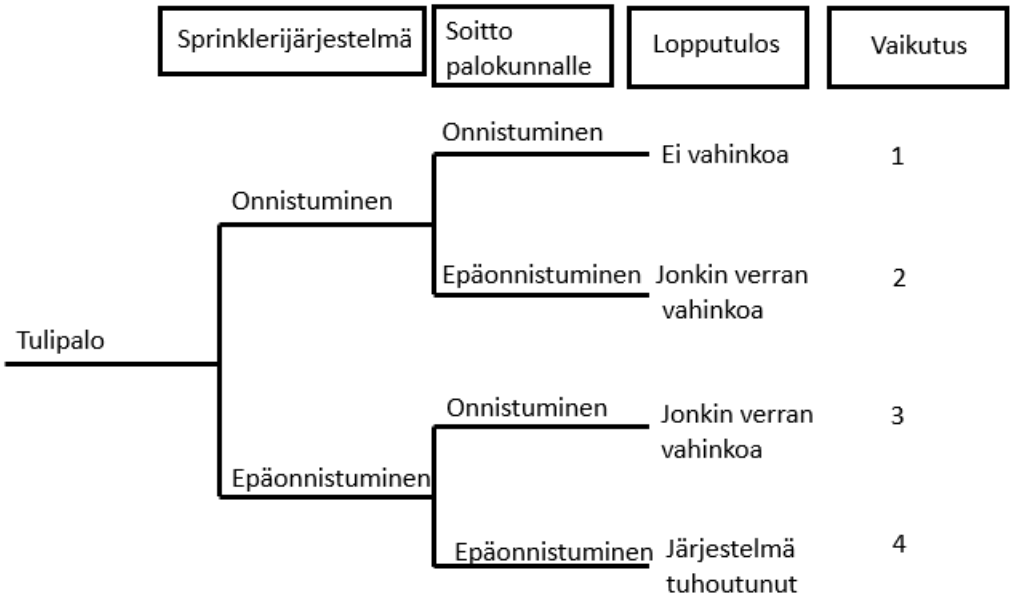
"OR"-portin tapahtumassa joko a:n tai b:n täytyy tapahtua, jotta portti aktivoituu. "AND" -portin tapahtumassa kummankin häiriön (a ja b) täytyy tapahtua, jotta portti aktivoituu, ja häiriöketju etenee seuraavalle tasolle. (Schroder, 1969, s. 4.)

Virhepuumalleja on kahta erilaista tyyppiä: staattista virhepuumallia sekä dynaamista virhepuumallia. Dynaaminen malli lisää kolme uutta porttia alkuperäiseen malliin verrattuna: PAND-, spare- sekä FDEP-portit. PAND-portilla kuvataan häiriötä, kun komponenttiin liittyvät osa-alueet pettävät tietyssä järjestyksessä. Spare-portti pettää, kun siihen liittyvä pääkomponentti pettää, ja varalle määritetyt komponentit pettävät myös (tämä tilanne voi tulla esimerkiksi järjestelmässä, jolle on määritelty sekä pää- että varavirtavoimalähteet). FDEP-portti (engl. functional dependency) tarkoittaa tilannetta, jossa ulkopuolinen tapahtuma vaikuttaa kyseisen järjestelmän komponentteihin, mikä johtaa häiriötilanteeseen. (Boudali, Crouzen & Stoelinga, 2007, s. 710.) Mallit voidaan myös jakaa laadullisiin ja määrällisiin malleihin. Laadullisissa malleissa pyritään selvittämään lyhimmät ja yleisimmät häiriöketjut. Määrällisissä malleissa lasketaan todennäköisyydet eri häiriöketjuille (Lee ym., 1985, s. 197–198).

Virhepuumallin heikkouksina pidetään sen tarkkuutta vaativaa analysointia, sekä kallista käyttöönottoa. Analysoijan täytyy olla ammattitaitoinen ja tuntea järjestelmä hyvin, jotta kaikki häiriöön johtavat syyt tulee otettua huomioon. Määrällisissä virhepuumalleissa haasteellisinta on saada riittävä määrä relevanttia tietoa, jotta todennäköisyydet saadaan laskettua. (Fussell, 1973, s. 3; Lee ym., 1985, s. 200.) Tässä tutkimuksessa virhepuumalli ei sovellu kyberoperaatioiden analysointityökaluksi. Mallilla voisi analysoida esimerkiksi voimalaitokseen kohdistuneen kyberhyökkäyksen seurauksesta tapahtuvia häiriöketjuja, jotka johtaisivat voimalaitoksen sulkeutumiseen. Tällainen tilanne kävi Ukrainan tapauksessa vuonna 2015 sekä 2016 (Sullivan & Kamensky, 2017; Greenberg, 2017). Malli on kuitenkin tarkoitettu tietojärjestelmissä tapahtuvien häiriöiden analysointiin ja järjestelmäsuunnittelun parantamiseen teknisestä näkökulmasta erityisesti ydinvoimaloissa (Čepin & Mavko, 2002, s. 83), eikä laajempien operaatioiden analysointiin, joihin liittyy muita kuin teknisiä osa-alueita (kuten poliittinen ilmapiiri tai kohdemaan tai organisaation kulttuuri).

4.4.4 Tapahtumapuumalli

Tapahtumapuumalli (engl. Event Tree) toimii samalla periaatteella kuin virhepuumalli. Mallin tarkoituksena on kuvata häiriöstä johtuneet mahdolliset seuraukset ja niiden tapahtumistodennäköisyydet, jolloin tapahtumiin voidaan varautua paremmin (Lacasse ym., 2008, s. 23). Mallia käytetään myös analysoimaan häiriöistä johtuneita tapahtumia (Kenarangui, 1991, s. 120). Kyseistä mallia on käytetty pääosin tekniikan alalla, kuten voimalaitosten tietojärjestelmien tapahtumien analysoinnissa (Alfonsi ym., 2013, s. 5), mutta mallia on käytetty myös alan ulkopuolella. Yksi esimerkki mallin sovelluskohteesta on tutkimus Norjassa sijaitsevan Aknes-nimiseen vuonoon kohdistuvan kivivyöryn seurausten analysoinnissa (Lacasse, Eldsvik, Nadim, Hoeg & Blikra, 2008). Alla olevassa kuviossa (kuvio 21) on esimerkki tapahtumapuumallista, jota on sovellettu kiinteistössä tapahtuvaan tulipaloon.



KUVIO 21 Tapahtumapuumalli (mukaillen Lacasse ym., 2008, s. 23)

Mallissa on esimerkkihäiriöksi otettu rakennuksessa syttynyt tulipalo. Rakennuksessa on sprinklerijärjestelmä, jonka pitäisi estää vahingon syntyminen tai laajeneminen. Jos järjestelmä toimii, ja palokunta saa palon sammutettua, vahingot pysyvät minimissä. Jos taas sprinklerijärjestelmä toimii, mutta palokunta ei saavu paikalle, jonkinasteista vahinkoa syntyy. Jos taas sammutusjärjestelmä ei toimi, mutta palokunta saapuu paikalle, vahinko saadaan jossain määrin rajattua. Sekä sammutusjärjestelmän toimimattomuus että palokunnan puuttuminen johtavat kiinteistön ja omaisuuden tuhoon. Yllä olevassa kuviossa tapahtumien perässä on numeraalinen arvio siitä, mitkä vaikutukset eri tapahtumilla ovat (numeron yksi ollessa vähiten vahinkoa aiheuttava, ja numeron neljä eniten vahinkoa aiheuttava). (Lacasse ym., 2008, s. 23.)

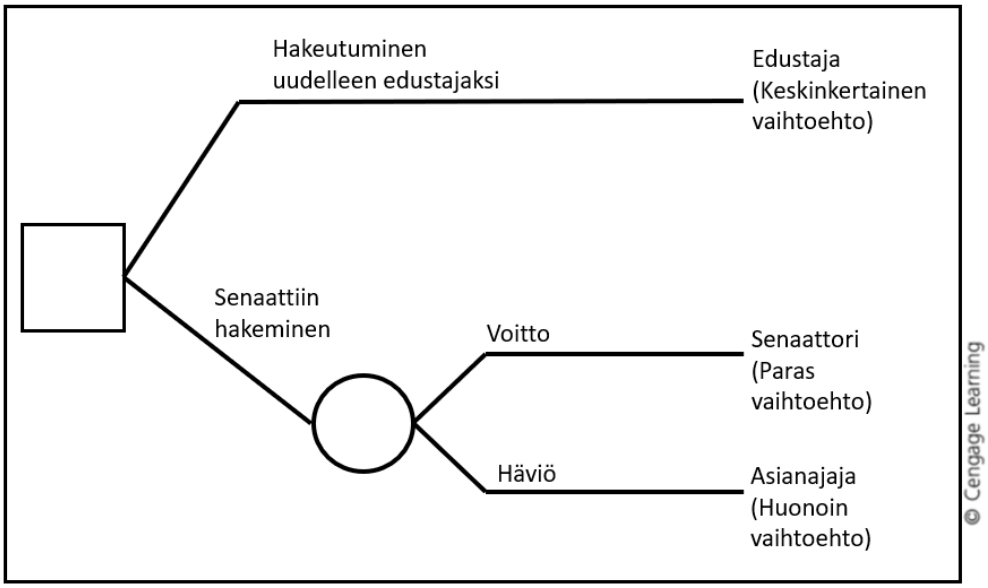
Tapahtumapuumallia on kritisoitu sen subjektiivisesta luonteesta. Subjektiivisuus voi johtaa siihen, että joitain tapahtumaketjuja ei osata ottaa huomioon.

Tämä voi johtua myös liian vähäisestä määrästä asiantuntijoita, tai asiantuntijoiden osaamattomuudesta, joka johtaa epätarkkojen arvioiden tekemiseen. (Ferdous, Khan, Sadiq, Amyotte & Veitch, 2009, s. 292.)

Tapahtumapuumallin avulla tehty tutkimus kivivyöryn seurausten analysoinnista on hyvä esimerkki siitä, miten kyberhyökkäysten mallintamisen menetelmiä voidaan käyttää hyvinkin erilaisiin käyttötarkoituksiin, kuin mihin malli on alun perin tarkoitettu. Tapahtumapuumalli soveltuu erityisesti ennaltaehkäisevään suunnitteluun tekniikan alalla, mikä on pääteltävissä myös monista eri mallia käsittelevistä tutkimuksista (esimerkiksi Andrews & Dunnett, 2000; Kenarangui, 1991; Bucci ym., 2008). Mallia käytetään tapahtumien ennustamisessa riskienhallinnan yhteydessä, eikä niinkään jo tapahtuneiden häiriöiden tai onnettomuuksien analysointityökaluna (tällaisia analysoivia tutkimuksia ei kirjallisuuskatsausta tehdessä löytynyt). Tehdyt tutkimukset myös keskittyivät pääosin yhden tapauksen tai tilanteen tutkimiseen (katso esimerkiksi Beim & Hobbs, 1997), eikä useampiin tapauksiin keskittyvää tutkimusta löytynyt. Edellä oleviin syihin perustuen tapahtumapuumalli ei sovellu useamman kyberoperaation analysointiin ja vertailuun.

4.4.5 Päätöspuumalli

Päätöspuumallia (engl. Decision Tree) on käytetty muun muassa kyberhyökkäysten analysoinnin sekä liiketoiminnan päätöksenteon apuna ja tehdessä lääketieteellisiä diagnooseja (Amor, Benferhat & Elouedi 2004; Quinlan, 1987; Kamiński, Jakubczyk & Szufel, 2018). Päätöspuumallia käytetään myös koneoppimisen kehittämisessä, ja tätä soveltamisalaa käytetään kyberhyökkäysten analysoinnissa (Amor ym., 2004, 420). Päätöspuumallilla pyritään helpottamaan päätöksentekoa kuvaamalla päätöksentekoprosessia graafisella mallilla (Kamiński ym., 2017, s. 135; Clemen & Reilly, 2013, s. 21). Alla olevassa kuviossa (kuvio 22) on esimerkki päätöspuumallista.



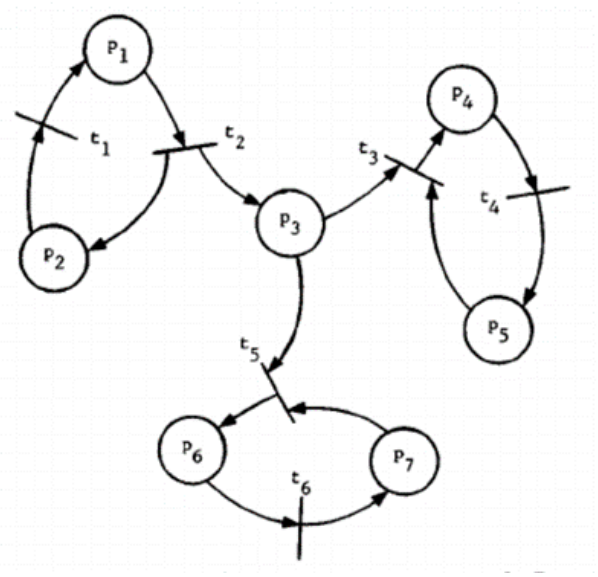
KUVIO 22 Päätöspuumalli (mukaillen Clemen & Reilly, 2013, s. 77)

Edellä olevassa esimerkissä on kuvattu poliitikon päätösketjun mahdolliset vaihtoehdot tilanteessa, jossa hänen täytyy tehdä päätös uransa edistämiseksi. Poliitikolla on mahdollisuus hakea uudelleen edustajaksi, jolloin hänen uransa ei etene, mutta nykytilanne pysyy samanlaisena (huomiona täytyy sanoa, että poliitikolla on myös mahdollisuus hävitä edustajistovaalit, vaikka sitä ei mallissa ole kuvattukaan). Henkilö voi hakea senaattoriksi, jolloin mahdollisuutena on joko voittaa tai hävitä vaalit. Häviäminen voi tarkoittaa pahimmillaan palaamista vanhaan työhön asianajajana. Malliin on kuvattu päätöksentekoa helpottamaan vaihtoehtojen arvot (mikä vaihtoehto on huonoin ja mikä on paras). Päätöksentekijän tehtävänä on pohtia, onko parhaan vaihtoehdon tavoittelu riskin arvoinen. (Clemen & Reilly, 2013, s. 76–77.) Päätöksenteon helpottamiseksi eri vaihtoehdoissa voidaan kuvata esimerkiksi vaihtoehdolle laskettua tapahtumistodennäköisyyttä tai vaihtoehdon arvoa (kuten menetettävää tai ansaittavaa rahamäärää) (Kamiński ym., 2018, s. 138).

Kirjallisuuskatsauksen perusteella päätöspuumallia käytetään apuna myös määrälliseen todennäköisyyslaskentaan. Tällöin eri vaihtoehdoille määritetään lukuarvo, mikä taas auttaa päätöksen tekemisessä. Esimerkiksi Friedlin ja Brodleyn (1997) tutkimuksessa käytetään päätöspuumalliin pohjautuvaa algoritmia auttamaan maa-alan määrittelyyn liittyvien ongelmien ratkaisussa. Mallia käytetään siis ennen jotain tapahtumaa, ei tapahtuman jälkeen. Kyberoperaatioiden vertailuun ja analysointiin malli ei siis sovellu, sillä tässä tapauksessa operaatiot ovat jo tapahtuneet. Mallia voisi käyttää esimerkiksi laskemaan todennäköisyyksiä kyberhyökkäyksille, ja auttamaan näin esimerkiksi järjestelmän koventamiseen liittyvässä päätöksenteossa.

4.4.6 Petri net

Petri net on malli, jota käytetään mallintamaan niitä järjestelmiä, joissa tapahtuu paljon samanaikaisia ja eriaikaisia tapahtumia. Petri netin graafisessa mallissa on kahden tyyppisiä solmuja: ympyröitä (engl. circles), joita kutsutaan paikoiksi (engl. places) ja palkkeja (engl. bars), joita kutsutaan siirtymiksi (transition). Näiden solmujen välit on yhdistetty kaarilla. Kaari yhdistää mallissa syötteen ja tulosteen nuolella. Merkillä "token" voidaan kuvata tapahtumaa, joka on syntynyt tilanteen käynnistymisen (engl. firing) jälkeen. Merkki kuvaa tilaa, jossa järjestelmä on (eli merkki siirtyy syötekohdasta tulostekohtaan). Seuraavassa kuviossa (kuvio 23) on esimerkki Petri netistä.



KUVIO 23 Petri net (Peterson, 1977, s. 225)

Kyberhyökkäyksiin liittyen Petri nettiä on käytetty esimerkiksi järjestelmänvalvonnan raportoinnin nopeuttamisessa sekä tietojärjestelmien valvonnassa (Jasiul, Szpyrka & Śliwa, 2014, s. 6618; Mixia, Qiuyu, Hong & Dongmei, 2008, s. 545). Kiinnostavin sovellus Petri netin käytöstä on Chenin, Sanchez-Aarnoutsen & Bufordin (2011) tutkimuksessa, jossa mallia käytettiin analysoimaan sähkökatkosta. Sähkökatkos aiheutui inhimillisistä syistä, mutta järjestelmän vikaantuminen olisi tutkijoiden mukaan voinut yhtä hyvin johtua järjestelmän eri osiin tehtyjen kyberhyökkäysten seurauksena. Tutkimuksessa nähtiin ongelmallisena se, että suuremmissa ja yksityiskohtaisimmissa järjestelmissä (mitä tietojärjestelmät nykyään käytännössä ovat) Petri net -mallista tulee liian monimutkainen. Tutkimuksessa tähän ehdotettiin ratkaisuksi tekemällä useampia Petri net -malleja, jotta luettavuudesta ei tulisi ongelmaa (Chen ym., 2011, s. 8).

Kyseistä mallia käytetään kyberturvallisuuteen liittyen pääasiassa yksittäisissä järjestelmissä tapahtuvien päällekkäisten hyökkäys- tai tapahtumaketjujen analysoinnissa. Tämä malli vaikuttaa hyödylliseltä tilanteissa, joissa järjestelmän suunnitellaan kestämään useampi samanaikaisen, joko tahallinen tai tahaton, tapahtuma. Tällainen tilanne voisi syntyä esimerkiksi kyberhyökkäyksessä, jossa järjestelmä yritetään kaataa useampaan eri solmukohtaan hyökkäämällä. Mallia voisi käyttää järjestelmän koventamisen apuna, mutta kyberoperaatioiden analysointiin ja vertailuun se soveltuu huonommin. Petri net vastaa kysymykseen "miten" jotkin tapahtumat etenevät ottamatta kantaa esimerkiksi hyökkäyksen kestoon, ajankohtaan tai muihin ominaisuuksiin. Mallia voisi todennäköisesti käyttää osana kyberhyökkäyksen analysoinnissa ja ennakoinnissa, mutta ei koko operaatiota analysoitaessa.

4.4.7 Yhteenveto kuvaajamalleista

Kuvaajamallit soveltuvat parhaiten kuvaamaan mahdollisimman montaa hyökkääjän käyttämää reittiä. Eri malleja on lukuisia, ja ne on kehitetty yleensä tietyn

analysointimenetelmän kanssa tai tietyssä tilanteessa käytettäväksi. Tapausten vertailu on myös hankalampaa johtuen puumaisesta rakenteesta – mitä useampi erilainen reitti hyökkääjällä on käytössään, sitä monimutkaisempi puun rakenteesta tulee. Malleja on käytettykin yksittäisten tietojärjestelmien koventamisen apuna, ei laajemman mittakaavan operaatioita analysoitaessa. Näistä syistä kuvaajamallit eivät sovellu kyberoperaatioiden analysointiin ja vertailuun tämän tutkimuksen näkökulmasta.

4.5 Menetelmän valinta

Tässä kappaleessa esitellyistä kyberoperaatioiden mallintamisen menetelmistä yksikään ei sovellu suoraan tämän tutkimuksen operaation mallien analysointiin. Tapauskohtaiset mallit soveltuvat parhaiten järjestelmien ja palveluiden kehittäjille, sillä nämä mallit kuvaavat parhaiten järjestelmiin liittyviä teknisiä ominaisuuksia ja niihin liittyviä riskiä. Ne jättävät käytännössä kokonaan käsittelemättä järjestelmän ulkopuolelta tulevien syiden analysoinnin. Kuvaajamallit taas muodostuvat liian monimutkaisiksi puurakenteensa takia. Nämä mallit soveltuvat myös paremmin ennakointiin, kun useampaa eri vaihtoehtoa pyritään punnitsemaan ja pohtimaan myös sitä, mikä hyökkäysreitti tapahtuu todennäköisimmin. Lallien ym. (2020) esittelemistä kategorioista ajalliset mallit soveltuvat parhaiten operaatioiden analysointiin.

Ajallisista malleista kybertappoketju (engl. Cyber Kill Chain, jäljempänä CKC) ja siitä johdetut mallit vaikuttavat soveltuvan parhaiten operaatioiden analysointiin ja vertailuun. Yhdistetty tappoketju (engl. Unified Kill Chain, jäljempänä UKC) kehittää kybertappoketjua edelleen, paikaten näin CKC:ssa esiintyneitä puutteita. Se ottaa laajimmin huomioon kyberoperaation eri vaiheet. Esimerkiksi timanttimallissa ei ole selkeää operaation jakamista eri vaiheisiin. UKC:ssa huomioidaan tiedon tuhoaminen yhtenä mahdollisena hyökkääjän tavoitteena. Toisin kuin CKC, UKC ei myöskään oleta hyökkäysten eri vaiheiden tapahtuvan tietyssä järjestyksessä. Se jakaa operaation vaiheisiin, joiden sisällä hyökkääjän toimenpiteet voivat toteutua eri järjestyksessä. Malli myös mahdollistaa vähemmän teknisen analyysin tekemisen, mikä on tärkeä vaatimus tämän tutkimuksen analysointityökalulle. CKC:tä ja UKC:tä on myös käytetty aiemmin eri tapausten vertailuun. UKC:n etuna on myös se, että mallissa kuvatun operaation rakenne on sama, mitä esimerkiksi NATO käyttää.

Puutteena UKC:ssä tämän tutkimuksen näkökulmasta on se, että malli ei ota huomioon operaatioon johtaneita syitä. Tämä puute esiintyi muissakin kirjallisuuskatsauksen perusteella löydetyissä operaatioiden ja hyökkäysten mallintamisen menetelmissä. Esitellyissä malleissa analyysi alkaa aina suoraan tilanteesta, jossa hyökkääjä on jo aloittanut operaation suorittamalla tiedustelua tai toimii jo kohteessa. Malleilla ei siis oteta huomioon esimerkiksi uhrin ja hyökkääjän välistä suhdetta, osapuolten aiempaa käytöstä tai muita mahdollisia tekijöitä, jotka ovat saanet hyökkääjän ryhtymään operaation suunnitteluun ja toteuttamiseen. Aiemmin käsitellyistä malleista ainoastaan laajennettu timanttimalli ottaa

jotenkin huomioon sen, miten uhrin ja hyökkääjän välinen sosiopoliittinen suhde vaikuttaa hyökkäyksen tapahtumiseen. Timanttimalli ei kuitenkaan sovellu yhtä hyvin operaatioiden analysointiin ja vertailuun, sillä UKC:n avulla operaatiot pystytään jakamaan systemaattisemmin eri vaiheisiin ja tätä kautta operaatioita pystyy paremmin analysoimaan ja näin myös vertailemaan keskenään.

Edellä mainittuihin syihin pohjaten kyberoperaatioiden analysointiin käytetään UKC-mallia, johon on tehty kirjallisuuskatsauksesta tehtyjen havaintojen perusteella lisäys. Alla olevassa kuviossa (kuvio 24) on esitetty operaatioiden analysointiin käytettävää sovellettua UKC-mallia.

KUVIO 24 Sovellettu yhdistetyn tappoketjun hyökkäysmalli

Malli on rakenteeltaan samanlainen UKC-mallin kanssa. Lisäyksenä malliin on lisätty ”vaihe 0”. Tämä vaihe liittyy operaation alkamista edeltävään vaiheeseen ja niihin syihin, minkä takia operaatioon on alun perin ryhdytty. Vaiheen 0 seurauksena ryhdytään operaatioon, jota mallin muut vaiheet analysoivat. Nämä vaiheet noudattavat alkuperäisen UKC-mallin vaiheistusta. Vaiheessa 1 ollaan siis tilanteessa, johon vaiheessa 0 johtuneiden syiden takia on operaatioon ryhdytty. Vaihe 1 kuvaa operaation valmistautumisvaihetta, jolla vastustaja saa muodostettua operaatiolle suotuisat olosuhteet. Tähän kuuluu muun muassa tiedustelu ja järjestelmiin tunkeutuminen. Vaiheessa 2 hyökkääjä on päässyt tietoverkkoon ja järjestelmään sisälle, ja hyökkääjän tavoitteena on valmistella varsinaista hyökkäystä, joka tapahtuu kolmannessa vaiheessa.

5 ANALYYSI

Tässä kappaleessa esitellään kyberoperaatioiden analysoinnin tulokset. Kappale on jaettu alakappaleisiin, joissa esitellään analyysiin valitut kyberoperaatiot ja tappoketjumallin avulla saadut tulokset. Jokaisesta vaiheesta on esitelty osa-alue, joka on tunnistettu operaatiossa tapahtuneen. Tapahtuneet osa-alueet on avattu tarkemmin tapauksen käsittelyn yhteydessä. Vaiheisiin on siis listattu esimerkiksi ”tiedustelu”, kun kyseinen tapahtuma on mallin perusteella operaatiossa havaittu. Tekstiosuudessa tiedustelun rooli operaatiossa avataan tarkemmin. Analyysissa on myös käsitelty ainoastaan ihmisoperaattoreiden tekemät liikkeet järjestelmiin liittyen. Esimerkiksi poikittaisliike järjestelmien välillä on käsitelty ainoastaan, jos operaattori on tehnyt kyseisen toimenpiteen. Automaattinen haittaohjelman leviäminen järjestelmien välillä on myös rajattu tämän tutkimuksen ulkopuolelle. Operaatioiden tulosten esittelyn yhteydessä käytetään strategisen kulttuurin teoriaa selittämään mallin avulla saatuja tuloksia eli taustalla vaikuttaneita paradigmoja sekä valintoja.

5.1 Viro

Alla olevassa taulukossa (taulukko 1) on esitelty Viroa vastaan kohdistuneen kyberoperaation eri vaiheet.

TAULUKKO 1 Viroa vastaan kohdistuneen kyberoperaation vaiheet

Vaihe	**Osa-alue**
Vaihe 0: Ennen operaatiota	Operaatioon johtaneet syyt (patsaskiista)
Vaihe 1: Valmistautuminen	Tiedustelu, rekrytointi
Vaihe 2: Hallinta	-
Vaihe 3: Toteutus	Rekrytointi, kohteen manipulointi, hyökkääjän tavoitteet

Viron ja Venäjän välille syntyi diplomaattinen kiista, kun Viro ilmoitti siirtävänsä neuvostoliittolaisen sotilaan muistopatsaan toiseen paikkaan. Patsaan siirrosta syntynyt mielipiteiden vastakkainasettelu oli ideologinen (ja tätä kautta historiallinen). Patsaan siirron voidaan nähdä olevan osa Venäjän laajempaa geopoliittista ajattelua, jossa se yrittää pitää vanhoista etupiireistään kiinni. Patsaan siirto oli kuitenkin itsessään pienimuotoinen tapahtuma. Jos kyseessä olisi ollut esimerkiksi venäläisväestön pakkosiirto, olisi tällöin Venäjällä ollut näennäisesti suurempi oikeus reagoida tilanteeseen. Patsasta ei esimerkiksi aiottu tuhota, vaan aikomus oli ainoastaan siirtää se hiljaisempaan paikkaan viereisen hautaus-

maan yhteyteen, pois ruuhkaisemman liikenteen keskeltä. Patsaan siirrosta syntyi isompi tapaus kuin esimerkiksi Liettuan kommunistisymbolien kiellosta, sillä venäläisväestö osoitti Virossa paikoin hyvinkin voimakkaasti mieltään patsaan siirtoa vastaan. Tiedossa ei ole sitä, olivatko mielenosoitukset spontaaneja vai Venäjän hallituksen järjestämiä. Mielenosoitusten avulla tapahtuma sai kuitenkin näkyvyyttä, ja mielenosoitukset olivat Venäjän poliittisten keinojen ohella yksi työkalu, joita käytettiin kybertoimintaympäristössä tehtyjen hyökkäysten rinnalla. Viro ja Venäjä ovat aiemminkin riidelleet ideologisista aiheista. Nämä maat ovat kiistelleet muun muassa siitä, onko Viro itsenäistynyt ensimmäisen kerran vasta Neuvostoliiton hajoamisen jälkeen vai onko kyseessä Viron uudelleen itsenäistyminen (Liik, 2007, s. 71). Ideologinen vaikutus näkyi myös joissain virolaisille nettisivustoille lähetetyissä verkkokyselyiden sisällössä, joissa Viron pääministeriä haukuttiin fasistiksi.

Viron tapauksessa operaation valmistautumisvaiheessa (vaihe 1) toteutetun tiedustelun yksityiskohtia ei ole pystytty selvittämään. Tiedustelua voidaan kuitenkin jossain määrin olettaa tapahtuneen, sillä roskapostihyökkäykset olivat kohdennettuja ja niiden verkkosivujen haavoittuvuudet olivat tiedossa, joille kohdennettiin SQL-hyökkäyksiä. Valmistautumisvaiheeseen lukeutuu myös rekrytointisivujen käyttö, joilla pyrittiin saamaan tavallisia kansalaisia tekemään palvelinestohyökkäyksiä virolaisia järjestelmiä vastaan. Rekrytointi on merkattu osa-alueeksi sekä vaiheeseen 1 että 3, sillä rekrytointi jatkui myös hyökkäysten aikana. Rekrytointiin liittyvää osa-aluetta ei alkuperäisessä mallissa ollut mukana. Se on nostettu kuitenkin yhdeksi osa-alueeksi, sillä rekrytointi esiintyi useammin tässä tutkimuksessa käsitellyissä operaatioissa. Ideologisia syitä korostettiin voimakkaasti venäläisessä retoriikassa ja tätä kautta myös rekrytoinnissa hyödyksi. Moni hyökkäyksissä mukana ollut henkilö lienee ollutkin tavallinen kansalainen, joka on kokenut velvollisuudekseen lähteä puolustamaan Venäjää verkossa. Tässä operaatiossa tehtiinkin tietoisesti päätös käyttää tavallisia kansalaisia operaation ”sotilasvoimana”. Käytännössä kuka tahansa venäläinen, jolla oli pääsy verkkoon, oli potentiaalinen hyökkäysten tekijä. Kokeneemmat hakkerit olivat taas tehneet pohjatyön, eli selvittäneet kohteet ja valmistelleet työkalut etukäteen.

Hyökkäykset jäivät Viron operaatiossa pääosin tietojärjestelmien ulkokehälle. Operaatiossa ei siis toteutettu ollenkaan hallintavaihetta (vaihe 2). Vaiheeseen 2 olisi kuulunut esimerkiksi eri tietojärjestelmiin murtautuminen ja operaatiota edistävien toimenpiteiden toteuttaminen, kuten salasanojen kerääminen järjestelmän sisällä. Tällaisia hyökkäyksiä ei kuitenkaan operaation aikana toteutettu. Operaatio siirtyi siis suoraan toteutusvaiheeseen (vaihe 3). Tämän vaiheen hyökkäykset koostuivat pääosin bottiverkkojen tekemistä palvelinestohyökkäyksistä sekä massiivisista roskapostihyökkäyksistä. Hyökkääjät ylläpitivät hyökkäyksiä usean viikon ajan. Taulukossa olevalla kohteen manipulointi -kohdalla kuvataan tässä tapauksessa sitä, kuinka puolustajan järjestelmiin ja yleiseen mielipiteeseen pyrittiin vaikuttamaan.

Bottiverkkojen ja roskapostihyökkäysten tarkoitus ei ole ollut vahingoittaa tai aiheuttaa pysyvää haittaa ihmisille tai tietojärjestelmille. Nämä hyökkäykset aiheuttivat lähinnä kiusantekoa, kun pääsy joillekin sivustoille estyi hetkellisesti.

Koska hyökkääjää ei ole pystytty varmuudella tunnistamaan, eikä oletettu hyökkääjä tai hyökkäysten tukija (Venäjän valtio) ole tuonut omaehtoisesti julkisuuteen tavoitteitaan, ovat päätelmät operaation tavoitteista lähinnä arvioita. Venäjän tavoitteiksi on veikattu pyrkimystä sulkea Viron verkko osittain tai kokonaan, vaikuttaa poliittisiin päättäjiin patsaskiistan ratkaisemiseksi Venäjän eduksi sekä Venäjän kybertoimintakykyjen testaaminen Viron maaperällä. Venäjän oletetaan myös halunneen näyttää länsimaiden ja Naton suuntaan, että se kykenee tämän tyyppiseen valtiotason vaikuttamiseen. Hyökkääjän voidaan todeta epäonnistuneen kaikissa tavoitteissaan. Vaikka hyökkäyksillä saatiin hetkellisesti häirittyä verkon käyttöä, ei täysimittaisesta verkon sulkemisesta voida puhuakaan. Myöskään patsaan siirtämiseen iskuilla ei ollut vaikutusta. Venäjä sai länsimaat miettimään kyberkykyjen käyttöä politiikan ja sodankäynnin välineenä, mutta lopputuloksena muut valtiot alkoivat kehittää kyberkykyjään.

Hyökkäykset eivät aiheuttaneet pysyvää vahinkoa, ja näkyvintä tavoitetta, patsaan siirtoa, Venäjä ei pystynyt estämään. Venäjä onnistui ainoastaan sohaisemaan muurahaispesää saamalla länsimaat varuilleen ja ryhtymään paremmin varautumaan kyberuhkia vastaan. Länsimaiden näkökulmasta operaation toteutumisen voidaan nähdä olevankin hyvä asia, sillä näin saatiin varoittava esimerkki Venäjän mahdollisista ilman vakavampia seurauksia. Venäjän näkökulmasta toimien voidaan nähdä olevan hätäiltyjä, sillä Viro ei taipunut Venäjän painostuksen alla ja nousi tilanteesta lopulta voittajana.

Taustalla tässä operaatiossa vaikuttivat siis ainakin seuraavat strategisen kulttuurin teoriaa mukailevat paradigmat:

- Venäjän halu puolustaa omaa ideologiaansa (ja historiaansa) omien rajojensa ulkopuolella
- Näkemys koko kansan mukanaolosta ulkoista uhkaa vastaan
- Kyberhyökkäysten käyttö muiden vaikuttamiskeinojen rinnalla
- Pysyvän vahingon aiheuttamisen välttäminen kybertoimintaympäristössä
- Hyökkääjän henkilöllisyyden pitäminen hämärän peitossa

Operaatiossa tehtiin seuraavia valintoja edellä oleviin paradigmoihin nojaten:

- Tavallisten kansalaisten käyttö kyberhyökkäysten tekijöinä
- Palvelinestohyökkäysten käyttö, jolla ei haluttu aiheuttaa lyhytaikaisia häiriöitä vakavampia seurauksia
- Roskapostiviestien massamainen käyttö, jolla ei aiheutettu lyhytaikaista häiriötä vakavampia seurauksia
- Mielenosoitusten käyttö kyberoperaation rinnalla
- Poliittisten painostuskeinojen käyttö, kuten diplomaattinen painostus ja raideliikenteen sulkeminen

- Kieltäytyminen avunannosta hyökkääjien henkilöllisyyden selvittämisessä

5.2 Liettua

Liettuaa vastaan tehty kyberoperaatio oli luonteeltaan samankaltainen kuin vuotta aiemmin tapahtunut Viroa vastaan toteutettu kyberoperaatio. Liettuaa vastaan tehty operaatio koostui käytännössä pelkästään palvelinestohyökkäyksistä, joiden intensiteetti ja laajuus olivat pienemmät kuin Viroa kohtaan tehdyt hyökkäykset. Hyökkäykset kestivät silti useamman päivän ajan. Ne keskittyivät pääosin yhteen palvelintarjoajaan ja tämän hallinnoimiin verkkosivuihin. Seuraavassa taulukossa (taulukko 2) on kuvattu Liettuaan kohdistuneen kyberoperaation eri vaiheet.

TAULUKKO 2 Liettuaa vastaan kohdistuneen kyberoperaation vaiheet

Vaihe	**Osa-alue**
Vaihe 0: Ennen operaatiota	Operaatioon johtaneet syyt (kommunististen tunnusten käyttökielto)
Vaihe 1: Valmistautuminen	Tiedustelu
Vaihe 2: Hallinta	-
Vaihe 3: Toteutus	Kohteen manipulointi, hyökkääjän tavoitteet

Venäjällä ja Liettualla on pitkä yhteinen historia. Liettua oli osa Neuvostoliittoa suurimman osan 1900-lukua, ja itsenäistyi uudelleen samoihin aikoihin Viron kanssa. Kuten Viro, myös Liettua alkoi lähestyä länsimaita, mikä on herättänyt Venäjässä närää. Vuoden 2008 operaatio saikin alkunsa Venäjän ja Liettuan välisestä ideologisesta kiistasta, kun Liettua kielsi neuvostoliittolaisten ja kommunistisen symbolien käytön kokonaan. Sekä Venäjä että Valko-Venäjä protestoivat voimakkaasti Liettuan tekemää ratkaisua. Hyökkäykset käynnistyivät pian tämän kiellon jälkeen. Tämän operaation käynnistävänä tekijänä olivat siis ideologiset (ja tätä kautta myös osittain historialliset tekijät).

Kuten Viroa kohtaan tehdyssä kyberoperaatiossa, myöskään Liettuan kyberoperaatiossa ei havaittu operaatiota edeltänyttä tiedustelua. Jonkinlaista tiedustelua voidaan olettaa kuitenkin tapahtuneen, sillä kaikki hyökkäykset osattiin kohdistaa samaa palveluntarjoajaa kohtaan, joka hallinnoi hyökkäyksen kohteeksi joutuneita verkkosivuja. Hyökkääjät olivat siis tiedustelleet kohteensa etukäteen ja myös koordinoineet hyökkäysten tekemisen.

Liettuaa kohtaan tehdyssä kyberoperaatiossa ei ollut varsinaista toteutusvaihetta (vaihe 2). Hyökkääjät pääsivät murtautumaan joillekin verkkosivuille ja muokkaamaan näiden sisältöä, mutta tämä tehtiin vasta operaation toteutusvaiheessa (vaihe 3). Tunkeutuminen on voitu tehdä joko verkkosivuilla olleen haa-

voittuvuuden avulla, tai kaapattuja käyttäjätunnuksia hyväksikäyttäen. Hyökkääjät lisäsivät kohteena olleille sivustoille neuvostosymboleita ja venäläismielistä propagandaa. Kuten Viroa vastaan kohdistuneet kyberhyökkäykset, muut Liettuaa vastaan tehdyt hyökkäykset jäivät pääosin järjestelmien ulkokehälle. Nämä hyökkäykset koostuivat pääosin roskaposti- ja palvelinestohyökkäyksistä. Kyseiset vaikutustoimet menevät mallissa ”kohteen manipulointi” -osa-alueen alle. Tätä operaatiota varten ei perustettu rekrytointisivustoja, eikä Venäjän valtio kohdistanut retoriikkaansa Liettuaa vastaan läheskään yhtä näkyvästi kuin Viron kyberoperaatiossa. Liettuan venäläinen väestö ei osoittanut mieltään lakia vastaan, vaikka kyseessä oli vaikutukseltaan suurempi tapahtuma (uuden lakipykälän voimaantulo vaikuttaa laajemmalti ihmisen elämään kuin yksittäiseen patsaan siirtäminen), eikä Venäjä painostanut yhtä voimakkaasti poliittisella rintamalla Liettuaa kuin aiemmin Viron tapauksessa.

Venäläisten oletetaan halunneen vaikuttaa kyberoperaatiolla Liettuan hallitukseen, jotta se olisi muuttanut mieltään neuvostoliittolaisten ja kommunististen symbolien kiellon suhteen. Muista tavoitteista ei ole esitetty tutkimuskirjallisuudessa arvioita. Omana arviona on, että tavoitteet eivät todennäköisesti olleet samat Viron kyberoperaation kanssa. Hyökkäyksillä on tuskin pyritty vaikuttamaan Liettuan verkkoinfrastruktuuriin laajemmin, sillä hyökkäykset kohdistuivat liian kapealle alueelle kyetäkseen vaikuttamaan laajemmin yhteiskunnan toimintaan. Liettualaiset saivat etukäteen varoituksen tulevasta hyökkäyksestä, mikä vähensi hyökkäysten voimaa entisestään. Ainoastaan katko tiedonkulussa aiheutti sen, että yritykset eivät saaneet varoitusta etukäteen, ja nämä joutuivat kärsimään jonkin verran hyökkäyksistä.

Tässä operaatiossa taustalla vaikuttavat strategisen kulttuurin teorian mukailevat paradigmat olivat siis:

- Venäjän halu puolustaa omaa ideologiaa (ja historiaa) omien rajojensa ulkopuolella
- Pysyvän vahingon aiheuttamisen välttäminen kybertoimintaympäristössä

Operaatiossa tehtiin seuraavia valintoja edellä oleviin paradigmoihin nojautuen:

- Neuvostoliittolais- ja venäläisvaikutteisen materiaalin lisääminen verkkosivuille
- Massamaisen roskapostin käyttö, jolla ei aiheutettu lyhytaikaista häiriötä vakavampia seurauksia
- Palvelinestohyökkäysten käyttö, jolla ei aiheutettu lyhytaikaista häiriötä vakavampia seurauksia

Liettuan operaatio oli huomattavasti pienimuotoisempi kuin vuotta aiemmin Viroa kohtaan suunnattu operaatio. Hyökkäysten volyymi oli huomattavasti pienempi eikä operaatiolla saatu juurikaan tuloksia aikaan. Operaatio oli myös hyvä

esimerkki siitä, miten etukäteen saatu varoitus auttoi liettualaisia estämään vahinkojen syntymisen lähes täysin – operaatio olisi ollut täydellinen epäonnistuminen, jos myös yksityinen sektori olisi osannut varautua vastaavalla tavalla.

5.3 Georgia

Georgiaa vastaan suunnattu kyberoperaatio toteutettiin kahdessa osassa. Ensimmäinen osa toteutettiin kolme viikkoa ennen maahyökkäyksen ja kyberoperaation toisen vaiheen alkua. Ensimmäisessä osassa toteutettiin palvelinestohyökkäyksiä Georgian presidentin verkkosivuja kohtaan. Toinen osa toteutettiin samanaikaisesti Venäjän maahyökkäyksen kanssa. Tämä toinen osa piti sisällään useita erilaisia tietoverkkoja vastaan tehtyjä hyökkäyksiä, jotka olivat muun muassa palvelinestohyökkäyksiä, verkkosivuille tunkeutumisia sekä verkkosivujen häpäisyä. Seuraavassa taulukossa (taulukko 3) on kuvattu Georgiaan kohdistuneen kyberoperaation ensimmäisen osan vaiheet.

TAULUKKO 3 Georgiaan kohdistuneen kyberoperaation ensimmäinen osa

Vaihe	**Osa-alue**
Vaihe 0: Ennen operaatiota	Operaatioon johtaneet syyt (Georgian ja Venäjän sota)
Vaihe 1: Valmistautuminen	Tiedustelu
Vaihe 2: Hallinta	-
Vaihe 3: Toteutus	Kohteen manipulointi, hyökkääjän tavoitteet

Georgia on Viron ja Liettuan tavoin itsenäistynyt Neuvostoliitosta kyseisen valtion hajottua 1990-luvun alussa. Georgian maa-alueelle jäi paljon venäläistaustaista väestöä, jotka olivat siirtyneet maahan neuvostovallan aikana. Esimerkiksi monilla Etelä-Ossetian asukkaalla on venäläinen passi. (Allison, 2009, s. 176.) Georgian ja Venäjän raja-alueella olevat Etelä-Ossetian ja Abkhazian maa-alueet kuuluvat Georgialle, mutta kyseiset alueet ovat historiallisesti olleet aina lähempänä Venäjää. Georgian presidentti lähti ajamaan voimakkaammin näiden alueiden syvempää integroimista osaksi Georgiaa. Tämä johti lopulta georgialaisten sotilasoperaatioon Etelä-Ossetiassa. Venäjä vastasi oman näkemyksensä mukaan georgialaisten invaasioon omien asevoimiensa käytöllä. Venäjän intresseinä koko operaation (kyberoperaatio ja maaoperaatio) taustalla olivat siis pitkälti geopoliittiset syyt.

Kyberoperaation ensimmäisen osan vaiheessa 1 venäläiset hakkerit saivat ujutettua vakoiluohjelman Georgian hallinnon koneille. Vakoiluohjelma löydettiin vasta 2011, mutta oletuksena on, että vakoiluohjelma on ollut georgialaisissa tietokoneissa jo ennen Georgian ja Venäjän sotaa. Tiedossa ei siis ole, saatiinko vakoiluohjelma ujutettua koneille ennen ensimmäiseen vaiheen alkua, ensimmäisen vaiheen aikana vai ennen maahyökkäyksen alkua. On myös mahdollista,

että vakoiluohjelma on asennettu Georgian ja Venäjän sodan jälkeen. Jonkinlaista tiedustelua on operaatioon liittyen kuitenkin tehty, sillä palvelinestohyökkäyksen kohteeksi joutui ainoastaan presidentin verkkosivut. Palvelinestohyökkäyksiä ei siis toteutettu mielivaltaisesti.

Kyberoperaation ensimmäisessä osassa ei ollut hallintavaihetta (vaihe 2), sillä hyökkääjät siirtyivät suoraan toimenpiteisiin kohdetta vastaan (vaihe 3). Kuten Viron kyberoperaatiossa ja suurimmassa osassa Liettuan kyberoperaatiota, myös tässä vaiheessa hyökkäykset jäivät järjestelmän ulkokehälle. Hyökkääjät eivät siis tiedettävästi yrittäneet päästä murtautumaan verkkosivuille ja muokkaamaan tätä kautta sivujen sisältöä. Toimenpiteet kohdetta vastaan koostuivat siis ainoastaan palvelinestohyökkäyksistä presidentti Saakashvilin verkkosivuja kohtaan. Nämä toimenpiteet estivät pääsyn verkkosivulle noin vuorokaudeksi. Lisäksi georgialaisille palvelimille suunnattiin datapaketteja, joissa oli venäläismyönteistä sisältöä. Nämä toimet menevät mallissa ”kohteen manipulointi” -osa-alueen alle. Hyökkääjän tavoitteena on oletettu olleen varsinaisen kyberoperaation valmistelu testaamalla sekä puolustajan reagointia, että hyökkääjän kybervaikuttamiskykyjä. Seuraavassa taulukossa (taulukko 4) on kuvattu Georgiaan kohdistuneen kyberoperaation toisen osan vaiheet.

TAULUKKO 4 Georgiaan kohdistuneen kyberoperaation toinen osa

Vaihe	**Osa-alue**
Vaihe 0: Ennen operaatiota	Operaatioon johtaneet syyt (Georgian ja Venäjän sota)
Vaihe 1: Valmistautuminen	Tiedustelu, rekrytointi
Vaihe 2: Hallinta	-
Vaihe 3: Toteutus	Rekrytointi, kohteen manipulointi, väistötoimenpiteiden suorittaminen, hyökkääjän tavoitteet

Operaation toiseen osaan johtaneet syyt ovat yhtenevät ensimmäisen osan syiden kanssa, sillä kyseessä on saman operaation eri osat. Toisen osan tiedustelu on voinut olla päällekkäistä ensimmäisen osan tiedustelun kanssa. Epätodennäköisempi vaihtoehto on se, että maahyökkäystä tukeneen kyberoperaation sekä Georgian presidentin verkkosivuja vastaan tehtyyn hyökkäykseen liittyvät tiedustelut ovat olleet erillisiä tapahtumia. Tiedustelua voidaan kuitenkin joka tapauksessa olettaa tapahtuneen jossain muodossa, sillä palvelinestohyökkäykset kohdistuivat operaation alkuvaiheessa tiettyjä kohteita, tässä tapauksessa hallituksen ja valtion verkkosivuja vastaan. Jos kohteita ei olisi tiedetty etukäteen, palvelinestohyökkäykset olisivat olleet mielivaltaisempia ja kohdistuneet laajemmalla skaalalla eri tietojärjestelmiä vastaan. Vasta myöhemmin palvelinestohyökkäykset laajenivat myös yrityksiä, julkista hallintoa ja Georgiassa toimineita länsimaisia verkkosivuja kohtaan. Myös verkkosivustojen SQL-haavoittuvuudet

olivat etukäteen tiedossa. Operaation valmisteluun liittyen venäläisillä keskustelupalstoilla puhuttiin siitä, tulisiko Georgiaa vastaan tehdä kyberhyökkäyksiä. Näiden keskustelujen yhteydestä tapahtuneisiin hyökkäyksiin ei ole varmuutta. Venäläiset perustivat kuitenkin verkkosivustoja, joilla tavallisia kansalaisia rekrytoitiin osallistumaan palvelinestohyökkäyksiin georgialaisia verkkosivustoja ja tietojärjestelmiä vastaan. Rekrytointi menee osittain päällekkäin operaation toteutusvaiheen kanssa, sillä rekrytointitarkoitukseen suunnattuja verkkosivuja perustettiin myös maahyökkäyksen alkamisen jälkeen.

Operaation toisella osalla ei ollut varsinaista hallintavaihetta (vaihe 2), vaan hyökkääjät siirtyivät suoraan toteutusvaiheeseen (vaihe 3). Tämä vaihe koostui useista palvelinesto- ja roskapostihyökkäyksistä. Hyökkääjät pääsivät sisään georgialaisille verkkosivuille, ja lisäsivät näille Georgian hallintoa halventavia kuvia ja tekstiä. Hyökkääjät pääsivät lisäämään halventavaa materiaalia SQL-haavoittuvuuksia hyväksikäyttämällä. Poiketen aikaisemmista operaatioista, hyökkääjät suorittivat myös väistötoimenpiteitä operaation toteutusvaiheen aikana. Georgialaisten estäessä venäläisistä osoitteista tulleen verkkoliikenteen, vaihtoivat hyökkääjät osoiteavaruutensa muistuttamaan jonkin toisen maan IP-osoiteavaruutta. Tätä kautta hyökkääjät pystyivät kiertämään georgialaisten asettamat rajoitteet. Alkuperäisestä UKC-mallista poiketen tässä operaatiossa väistötoimia toteutettiin tietojärjestelmien ulkopuolella, ja toisin kuin UKC:ssä, toimenpiteet toteutettiin vaiheessa 3.

Kohteessa tehdyt toimenpiteet rajoittuivat verkkosivujen häpäisemiseen, sillä valtaosa tehdyistä hyökkäyksistä pyrki järjestelmien ylikuormittamiseen ja verkkoliikenteen estämiseen. Tämä on ollut myös yksi osatavoite hyökkääjillä. Muita osatavoitteita on mahdollisesti ollut georgialaisten yleiseen mielipiteeseen vaikuttaminen ja päivittäisen elämän hankaloittaminen. Operaation päätavoitteen oletetaan olleen Venäjän maahyökkäyksen tukeminen kyberoperaatiolla, ja tässä tavoitteessa venäläisten voidaan todeta onnistuneen. Venäläiset onnistuivat myös sulkemaan Georgian hallinnon väliaikaisesti verkon ulkopuolelle. Hyökkäysten seurauksena georgialaiset joutuivat siirtämään palvelintensa toiminnan väliaikaisesti Yhdysvaltoihin. Georgian hallinto ei pystynyt hetkeen kommunikoimaan verkkosivujensa välityksellä, mikä hidasti erityisesti viestintää. Toisaalta georgialaiset eivät olleet vielä samalla tavalla riippuvaisia verkosta kuin esimerkiksi virolaiset, joten päivittäiseen elämään hyökkäyksillä ei ollut samalla tavalla vaikutusta.

Operaation taustalla vaikuttivat seuraavat paradigmat:

- Venäjän geopoliittisten etujen puolustaminen
- Vältettiin pysyvän vahingon aiheuttamista
- Hyökkääjän henkilöllisyyden hämärän peitossa pitäminen
- Kansalaisten osallistuminen hyökkäysten tekemiseen
- Kyberkykyjen käyttö muiden puolustushaarojen rinnalla
- Pitkäjänteisyys operaation suunnittelussa ja toteuttamisessa

Operaatioon liittyen tehtiin seuraavia valintoja edellä mainittuihin paradigmoihin pohjautuen:

- Kyberoperaation yhdenaikaisuus maaoperaation kanssa
- Roskapostihyökkäysten ja palvelinestohyökkäysten käyttö
- Rekrytointisivujen käyttö
- Kyberoperaation aloittaminen ja valmistelu viikkoja, mahdollisesti kuukausia etukäteen
- Vastuun ottaminen maaoperaatiosta, mutta ei kyberoperaatiosta

5.4 Operaatio Armageddon

Operaatio Armageddon edelsi Ukrainan ja Venäjän välistä konfliktia ja Krimin valtausta. Se oli usean vuoden ajan Ukrainaa vastaan toiminut kybervakoiluoperaatio, jonka pääasiallisina kohteina olivat Ukrainan poliitikot sekä asevoimien henkilöstö. Seuraavassa taulukossa esitellään operaatio Armageddonin vaiheet.

TAULUKKO 5 Operaatio Armageddon

Vaihe	**Osa-alue**
Vaihe 0: Ennen operaatiota	Operaatioon johtaneet syyt (Historialliset syyt, poliittinen etu, sotilaallinen etu, uuden teknologian kokeileminen)
Vaihe 1: Valmistautuminen	Tiedustelu, aseistaminen, sosiaalinen manipulointi, kuljettaminen, vastatoimien välttäminen, C&C
Vaihe 2: Hallinta	Suorittaminen
Vaihe 3: Toteutus	Tiedon keräys, tiedon kotiutus, hyökkääjän tavoitteet

Ukrainan historia on tarkoittanut pitkään samaa kuin Venäjän historia. Tämä selittää geopoliittisen kiinnostuksen, joka Venäjällä on entistä Neuvostotasavaltaa kohtaan. Perinteisesti Ukraina onkin ollut Venäjään päin suuntautunut yhteisen historian, kielipohjan sekä väestön samankaltaisuuden takia. Ukrainalaiset ovat kuitenkin olleet tyytymättömiä siihen, miten venäläiset ovat suhtautuneet heihin historian saatossa, sekä millaisia turvallisuuslupauksia venäläiset ovat antaneet. Tästä on seurannut Ukrainan lähestyminen länttä kohti. Tämä on aiheuttanut Venäjässä pelkoa siitä, että Venäjän hallitsema etupiiri pienentyisi entisestään. Ovathan jo Baltian maat hyvin vahvasti kiinnittyneet länteen Euroopan Unionin ja Naton kautta. Operaatio Armageddon alkoikin samaan aikaan, kun neuvotte-

lut Ukrainan ja Euroopan Union välisen yhteistyön syventymisestä alkoivat. Historialliset ja geopoliittiset intressit olivat siis todennäköisesti syyt, jotka johtivat operaation aloittamiseen (vaihe 0).

Operaation tavoitteena oli siis Venäjän pyrkimys ukrainalaisia vaikuttajia vakoilemalla saamaan sellaista tietoa haltuunsa, jotta maa pystyisi reagoimaan tai varautumaan sille haitallisten suhteiden kehittymiseen. Sotilaallisen edun saaminen ei ole ollut päällimmäinen tavoite operaation alkuvaiheessa, sillä vakoilu aloitettiin ennen Krimin operaatiota ja tilanteessa, jossa Ukrainan ja Venäjän välit olivat vielä läheiset. Toinen operaatioon johtanut syy on todennäköisesti ollut uuden teknologian kokeileminen. Hyökkäysmetodit vaihtuivat operaation kuluessa siten, että uhreilla oli suurempia vaikeuksia erottaa aidot sähköpostiviestit ja näiden tiedostot hyökkääjien lähettämistä viesteistä ja saastuneista tiedostoista. Myös vakoilun kohteet vaihtuivat operaation aikana, mikä näyttää hyökkääjien kykenevän muuttamaan toimintatapojaan lyhyenkin ajan sisällä.

Operaation valmistautumisvaiheen (vaihe 1) tiedustelusta ei varsinaista todistusaineistoa ole olemassa. Tiedustelua on kuitenkin jossain muodossa tapahtunut, sillä tietojenkalastelua kohdistettiin vain tietyille Ukrainan hallinnon henkilöille. Henkilöjen yhteystiedot on todennäköisesti saatu julkisista lähteistä tai sosiaalisen manipuloinnin avulla. Haittaohjelmat kuljetettiin kohdejärjestelmiin kohdennettujen sähköpostien avulla, jotka operaation alkuvaiheessa oli varustettu erityyppisillä liitetiedostoilla. Nämä aidolta näyttävät tiedostot pitivät sisällään hyökkääjän räätälöimän haittaohjelman. Hyökkääjät pyrkivät välttämään oman toimintansa havaitsemista alkuvaiheessa naamioimalla sähköpostien liitetiedostot esimerkiksi verkkoselainten päivitystiedostoiksi. Myöhemmässä vaiheessa hyökkääjät käyttivät uhrien koneilta ladattuja aitoja tiedostoja uusissa hyökkäyksissä. Haittaohjelmat lisättiin aitojen tiedostojen yhteyteen, jotka latautuivat uhrien koneille näiden avatessa aidoksi uskomansa tiedoston. Koneille latautuneet haittaohjelmat toimivat joko suoraan etäkäyttötyökaluna tai nämä ottivat yhteyden hyökkääjien hallinnoimille palvelimille, josta etäkäyttötyökalut latautuivat uhrien koneille.

Hallintavaiheesta (vaihe 2) ei kirjallisuuskatsauksesta löytynyt materiaalia. Tähän liittyen hyökkääjän tekemät toimenpiteet jäävät ainoastaan arvailun varaan. Toimenpiteenä on voinut olla esimerkiksi hyökkääjän suorittama poikittaisliike järjestelmässä uusien tietojen löytämiseksi. Hallintavaiheessa on kuitenkin todennäköisesti tehty joitain toimenpiteitä, sillä hyökkääjät ovat saaneet ladattua uhrien järjestelmistä tiedostoja ulos. Tämä vaatii jonkinlaista etäkäyttöohjelmaa, yhteyttä uhrin ja hyökkääjän järjestelmien välillä sekä liikkumista järjestelmissä tarvittavien tiedostojen löytämistä varten.

Operaation toteutusvaihe (vaihe 3) on pitänyt sisällään tietojen siirtämisen uhrien järjestelmästä hyökkääjän järjestelmään. Hyökkääjiä kiinnostivat muun muassa yksityiskohdat erilaisista poliittisista keskusteluista ja päätöksistä (liittyen esimerkiksi Ukrainan ja Euroopan Unionin välisiin neuvotteluihin), tiedot turvallisuuspalveluiden ja armeijan henkilöstöstä, kalustosta ja lukumääristä sekä sellaiset tiedostot, joita hyökkääjät pystyivät käyttämään apuna jatkohyökkäyksissä.

Kybervakoiluoperaation tavoitteena oli ensimmäisen ryhmän vakoiluun liittyen saada todennäköisesti sellaista tietoa selville, jotka edistivät Venäjän poliittisia tavoitteita ja päätöksentekoa. Ukrainassa tapahtuneen vallankumouksen jälkeen kohteet vaihtuivat sotilas- ja turvallisuushenkilöstön vakoiluun. Samalla tavoitteiden voidaan olettaa joko siirtyneen kokonaan tai osittain tukemaan Venäjän sotilaallisia tavoitteita Krimin tilanteeseen ja Itä-Ukrainan konfliktiin liittyen.

Operaatiossa on siis havaittavissa ainakin seuraavat strategisen kulttuurin teoriaa mukailevat paradigmat:

- Venäjän geopoliittisten etujen ajaminen
- Hyökkääjien henkilöllisyyden salassa pitäminen
- Keinovalikoiman laaja käyttö
- Pitkäjänteisyys
- Vältettiin pysyvän vahingon aiheuttamista
- Uuden teknologian ja keinojen kokeileminen

Edellä oleviin paradigmoihin pohjautuen operaatiossa tehtiin seuraavia valintoja:

- Uhrit olivat pääosin poliittisia ja sotilaallisia vaikuttajia
- Aitojen tiedostojen käyttö uhrien hämäämisessä
- Operaation aloittaminen vuonna 2013 ja jatkaminen ainakin vuoteen 2015 saakka
- Tietojärjestelmistä saatujen tietojen käyttäminen ainoastaan tietojen siirtämiseen, ei esimerkiksi tiedostojen tai järjestelmien tuhoamiseen
- Tiedustelu uusi operaatiotyyppi edellisiin operaatioihin verrattuna

5.5 Ukraina, joulukuu 2015

Ukrainan energiayhtiöitä vastaan joulukuussa 2015 kohdistuneen kyberoperaation avulla onnistuttiin vaikuttamaan fyysisesti muuntajien kytkimiin ja aiheuttamaan tätä kautta lyhytkestoinen, alueellinen sähkökatkos. Operaatiota tuettiin puhelinestohyökkäyksillä, jotka vaikuttivat hetkellisesti energiayhtiöiden tilannekuvan muodostamiseen ja yhtiöiden asiakkaisiin. Operaation valmistelu aloitettiin vähintään kuusi kuukautta ennen varsinaisia hyökkäyksiä ja päättyi siihen, kun puhelinestohyökkäykset asiakaspalveluita kohtaan loppuivat. Operaation oletetaan olleen Sandworm-nimisen ryhmän toteuttama, joka oli tehnyt aiemmin yksittäisiä kyberhyökkäyksiä ja kybervakoilua länsimaita kohtaan. Seuraavassa taulukossa (taulukko 6) on esitelty joulukuun 2015 kyberoperaation eri vaiheet.

TAULUKKO 6 Ukrainan energiayhtiöitä vastaan joulukuussa 2015 kohdistunut kyberoperaatio

Vaihe	Osa-alue
Vaihe 0: Ennen operaatiota	Operaatioon johtaneet syyt (Ukrainan ja Venäjän välinen konflikti, kostoisku, teknologian kokeilu)
Vaihe 1: Valmistautuminen	Tiedustelu, sosiaalinen manipulointi, aseistaminen, kuljettaminen, C&C
Vaihe 2: Hallinta	Käyttäjätunnusten kerääminen, poikittainen liike järjestelmässä, haavoittuvuuden hyödyntäminen, vastatoimien välttäminen
Vaihe 3: Toteutus	Kohteen manipulointi, vastatoimien välttäminen, hyökkääjän tavoitteet

Kyberoperaatio toteutettiin samaan aikaan, kun Venäjän ja Ukrainan välit olivat kiristyneet Krimin ja Itä-Ukrainan tilanteen takia. Venäläiset ovat saattaneet ajatella, että kyberoperaatiolla pystyttäisiin vaikuttamaan Ukrainan hallintoon tai yleiseen mielipiteeseen hallintoa kohtaan. Ukrainan hallinto oli saman vuoden aikana suunnitellut Ukrainan alueella olleiden yksityisten energiayhtiöiden kansallistamista. Näistä yhtiöistä moni oli venäläisten oligarkkien omistama. Oligarkit ovat saattaneet kokea ukrainalaisten suunnitelmat uhkaaviksi, ja painostaneet Venäjän hallitusta toimiin kansallistamisen estämiseksi. Kyberkykyjä ei ollut myöskään konfliktissa käytetty tähän mennessä kovin näkyvästi, aiemmin mainittua kybervakoiluoperaatiota lukuun ottamatta. Uuden teknologian testaaminen on todennäköisesti ollut tärkein operatiivisen tason tavoite. Ennen Ukrainaan kohdistunutta kyberoperaatiota ukrainalaisaktivistit tekivät sabotaasi-iskuja Krimin alueella olleita muuntajia vastaan aiheuttaen laajoja sähkökatkoja. Venäläiset ovat saattaneet toteuttaa vastaiskun kostomielessä, mutta tämän voidaan olettaa olleen ainoastaan operaatiota vauhdittanut tekijä. Tiedustelu oli nimittäin alkanut jo kuukausia ennen Krimillä tapahtuneita sähkökatkoja.

Valmisteluvaihe (vaihe 1) alkoi vähintään puolta vuotta ennen varsinaisia hyökkäyksiä. Tiedustelu kohdistettiin soveltuviin henkilöihin, joille lähetettiin haittaohjelmalla varustettuja sähköposteja. Uhrin avattua sähköpostin liitetiedoston hyökkääjät saivat asennettua kohdekoneelle BlackEnergy 3 –nimisen haittaohjelman, joka avasi hyökkääjille pääsyn yhtiön sisäverkkoon. Kohdehenkilöiden tiedustelun lisäksi hyökkääjät selvittivät jossain vaiheessa ennen hyökkäysten alkua asiakaspalvelun yhteystiedot.

Hallintavaiheessa (vaihe 2) järjestelmään päästyään hyökkääjät alkoivat laajentaa käyttöoikeuksiaan. Hyökkääjien työtä helpottivat järjestelmässä olleet haavoittuvuudet. Esimerkiksi VPN-yhteydet eivät vaatineet kaksivaiheista tunnistautumista, jolloin salasanojen murtaminen oli helpompaa. Hyökkääjät välttivät vastatoimia sekä passiivisesti että aktiivisesti. Hyökkääjien suorittamat passiiviset vastatoimet olivat lähinnä vahinko, sillä yhtiön tietojärjestelmissä ei ollut

minkäänlaisia valvontajärjestelmiä, joiden avulla luvaton tunkeutuminen ja järjestelmien käyttö olisi havaittu. Aktiivisiin toimenpiteisiin lukeutui erillisen KillDisk-ohjelman käyttö, joka poisti lokitiedoista hyökkääjien jättämät jäljet. Tällä tavoin hyökkääjät pystyivät toimimaan täysin näkymättömissä operaation toteutusvaiheeseen saakka.

Edeltävissä vaiheissa tehdyt valmistelut huipentuivat toteutusvaiheessa (vaihe 3). Tällöin hyökkääjät sammuttivat etäkäyttöyhteydellä sähköyhtiöiden käyttämien muuntajien kytkimet. Hyökkäyksen toteutusvaihetta tuettiin samanaikaisilla puhelinestohyökkäyksillä. Nämä hyökkäykset kohdistettiin energiayhtiöiden asiakaspalveluita kohtaan, jotta asiakkaat eivät päässeet soittamaan keskukseen ja selvittämään sähkökatkon syytä. Hyökkäykset eivät kestäneet kovin kauaa, ja niiden lopullinen vaikutus jäi pieneksi. Puhelinestohyökkäyksillä saatiin silti viivytettyä tilannekuvan muodostamista. Hyökkäyksen taktiset tavoitteet ovat todennäköisesti olleet pyrkimykset vaikuttaa energiayhtiöiden sähkönjakeluun. Hyökkäyksen strategisiksi tavoitteiksi on veikattu halu testata kyberkykyjä sekä pyrkimys vaikuttaa ukrainalaisiin päättäjiin. Todennäköisesti hyökkääjät ovat itsekin tienneet, että hyökkäysten varsinainen vaikutus jäisi vähäiseksi. Sähkökatkot ovat kohtalaisen tavanomaisia ukrainalaisten elämässä, joten pienen alueen sähköjen katkeaminen ei vaikuta ukrainalaisten elämään juurikaan. Tästä syystä uuden teknologian kokeilu on ollut todennäköisemmin päällimmäisenä tavoitteena.

Hyökkääjät onnistuivat taktisen tasan tavoitteissaan, mutta vaikutukset jäivät lyhytaikaisiksi. Sähkönjakelu saatiin keskeytettyä, mutta tilanne palautui normaaliksi muutaman tunnin sisällä. Tavallisiin kansalaisiin tilanne ei juuri vaikuttanut, sillä aiemmin kappaleessa 2.7.3 mainitussa haastattelussa moni ukrainalainen kertoi, etteivät he olleet kuulleet joulukuun 2015 kyberhyökkäyksistä tai niiden vaikutuksista. Tätä kautta ei myöskään poliittista vaikutusta saatu aikaiseksi.

Operaatiossa on siis havaittavissa ainakin seuraavat strategisen kulttuurin teoriaa mukailevat paradigmat:

- Venäjän geopoliittisten etujen ajaminen
- Keinovalikoiman laaja käyttö
- Vältettiin pysyvän vahingon aiheuttamista
- Pitkäjänteisyys
- Uuden teknologian ja keinojen kokeileminen

Operaatiossa tehtiin seuraavia valintoja edellisiin paradigmoihin pohjautuen:

- Fyysinen järjestelmiin vaikuttaminen lamauttavasti
- Aktiivisten väistötoimien käyttö (KillDisk-ohjelma)
- Kytkimet laitettiin pois päältä, niitä tai muita järjestelmiä ei tuhottu
- Operaation osana tehtiin puhelinestohyökkäyksiä

5.6 Ukraina, kesäkuu 2017

Sandworm-ryhmä yhdistettiin myös NotPetya –nimiseen haittaohjelmaan, joka aiheutti vuoden 2017 aikana maailmanlaajuisesti satojen miljoonien eurojen vahingot. Tunkeuduttuaan ukrainalaisen Linkos Group -nimisen ohjelmistoyrityksen järjestelmiin ryhmä onnistui ujuttamaan NotPetyan kyseisen yrityksen palvelimille. Linkos Groupin asiakkaina oli useita ukrainassa toimineita paikallisia ja kansainvälisiä yrityksiä. Nämä yritykset latasivat päivitykset omiin järjestelmiinsä Linkos Groupin palvelimilta. Samassa yhteydessä haittaohjelma latautui päivitystiedoston mukana asiakkaiden järjestelmiin. Tästä seurasi ketjureaktio, jonka seurauksena NotPetya levisi ympäri maailmaa, ja jonka takia lukuisten ukrainalaisten sekä kansainvälisten yritysten tiedot ja tietojärjestelmät tuhoutuivat. Näiden tietojen tuhoutuminen aiheutti satojen miljoonien eurojen vahingot. Ukrainassa sijainneet yritykset kärsivät eniten haittaohjelman aiheuttamista tuhoista. Seuraavassa taulukossa (taulukko 7) on esitelty kyberoperaation eri vaiheet.

TAULUKKO 7 Ukrainaan vuonna 2017 kohdistunut kyberoperaatio

Vaihe	**Osa-alue**
Vaihe 0: Ennen operaatiota	Operaatioon johtaneet syyt (Ukrainan ja kansainvälisten yritysten vahingoittaminen, teknologian kokeilu)
Vaihe 1: Valmistautuminen	Tiedustelu, aseistaminen, sosiaalinen manipulointi, kuljettaminen, C&C
Vaihe 2: Hallinta	Suorittaminen, poikittainen liike järjestelmässä, käyttäjätunnusten keräys
Vaihe 3: Toteutus	Vastatoimien välttäminen, tiedon manipulointi, hyökkääjän tavoitteet

Operaatio tapahtui aikana, jolloin Venäjän ja Ukrainan välit olivat edelleen kireät. Krimin operaatiosta ei ollut kulunut montaa vuotta, ja taistelut Itä-Ukrainassa jatkuivat. Taustalla vaikuttivat siis todennäköisimmin geopoliittiset syyt, sillä Sandworm-ryhmä on muiden APT-ryhmien ohella liitetty Venäjän hallintoon. Koska lopulliset iskut kohdistuivat pääosin ukrainalaisia ja Ukrainassa olleita yrityksiä ja yhteisöjä vastaan, on operaatiolla pyritty todennäköisesti vaikuttamaan ensisijaisesti Ukrainaan. Operaatiolla on todennäköisesti myös pyritty kokeilemaan uutta teknologiaa sekä menetelmiä ja nähdä, millaista vaikutusta tämän tyyppisellä haittaohjelmalla saadaan aiheutettua.

Operaation valmistautumisvaiheeseen (vaihe 1) liittyen tiedustelua ei yksiselitteisesti havaittu. Tiedustelua voidaan kuitenkin olettaa tapahtuneen, sillä hyökkääjät osasivat suunnata kohdennetun sähköpostikampanjan oikean yrityk-

sen (Linkos Groupin) henkilöstölle. Sosiaalisen manipuloinnin avulla ohjelmistoyrityksen henkilökunnasta yksi tai useampi henkilö saatiin avaamaan hyökkääjien sähköpostin kautta lähettämä Word-liitetiedosto, johon oli sisällytetty etäkäyttöohjelma. Tätä kautta hyökkääjät saivat etäyhteyden yrityksen verkkoon.

Operaation hallintavaiheessa (vaihe 2) hyökkääjät alkoivat valmistella operaation toteutusvaihetta. Tällöin hyökkääjät latasivat etäkäyttöyhteyden avulla Linkos Groupin palvelimille NotPetya-haittaohjelman. Asiakkaat latasivat tietämättä tämän haittaohjelman omiin tietoverkkoihinsa hakiessaan ohjelmistopäivityksiä Linkos Groupin palvelimilta. Operaatioon liittyen hyökkääjät ovat oletettavasti liikkuneet sisäverkon kautta järjestelmästä toiseen, riippuen onko sähköpostin liitetiedoston avanneella työntekijällä ollut riittävät käyttöoikeudet ja yhteys yrityksen palvelimille. Jos hyökkääjien on täytynyt liikkua järjestelmästä toiseen, on tähän liittyen kerätty myös käyttäjätunnuksia käyttöoikeuksien laajentamista varten.

Hyökkääjät eivät käynnistäneet itse operaation toteutusvaihetta (vaihe 3). Tämä vaihe käynnistyi, kun asiakkaat latasivat päivitystiedostot omiin järjestelmiinsä. Tällöin NotPetya levisi eri organisaatioiden ja yritysten tietoverkkojen läpi lukiten koneet ja niihin tallennetut tiedot. Perinteisesti koneiden lukitsemisella pyritään kiristämään uhreilta rahaa. Tässä tapauksessa hyökkääjien tarkoitus ei ollut alun perinkään palauttaa lukittuja tietoja uhreille, ainoastaan aiheuttaa mahdollisimman paljon tuhoa poistamalla tärkeitä tiedostoja. Tätä ei kuitenkaan alussa tiedetty, sillä uhrien koneille ilmestyi teksti, joka kehotti maksamaan rahat hyökkääjien tilille, jotta tiedot saataisiin takaisin. Tilinumero, joka uhreille annettiin, oli luotu satunnaisgeneraattorilla, ja maksu katosi bittiavaruuteen. Tämän toimenpiteen voidaan ajatella olevan vastatoimien välttämistä, sillä näin hyökkääjien tavoite pyrittiin pitämään pitempään hämärän peitossa. Hyökkääjien taktisen tasan tavoite ei siis ollut rahallisen edun saaminen, vaan maksimaalisen vahingon aiheuttaminen. Esimerkiksi tavallisten ihmisten elämä vaikeutui maksuliikenteen pysähdyttyä kokonaan. Strategisemman tasan tavoitteiksi on veikattu Venäjän halua pelotella Ukrainassa toimivia yrityksiä sekä vaikuttaa Ukrainan hallintoon ja talouselämään.

Operaatiossa on havaittavissa ainakin seuraavat strategisen kulttuurin teoriaa mukailevat paradigmat:

- Venäjän geopoliittisten etujen ajaminen
- Uuden operaatiotavan kokeileminen
- Pysyvän vahingon aiheuttaminen

Operaatiossa tehtiin edellä mainittuihin paradigmoihin nojaten seuraavia valintoja:

- Laajalle levinneen, vahinkoa aiheuttaneen haittaohjelman käyttö
- Mahdollisimman suuren vahingon aiheuttaminen
- Välinpitämättömyys siitä, kenelle vahinkoa aiheutuu

6 DISKUSSIO

Tässä kappaleessa esitetään edellisessä kappaleessa tehdyn analyysin perusteella löydettyjen havaintojen yhteenveto. Tuloksia verrataan aiempaan tutkimuskirjallisuuteen. Samassa yhteydessä pohditaan, mistä erot ja yhtäläisyydet voivat johtua. Kappaleessa nostetaan esille tutkimuksen aikana havaittuja puutteita sekä mahdollisia jatkotutkimuskohteita.

6.1 Analyysin perusteella tehdyt havainnot

Venäjän toteuttamien tai tukemien kyberoperaatioiden tekotapa ja laajuus ovat muuttuneet paljonkin, kun verrataan Viroa vastaan toteutettua operaatiota tuoreimpaan, NotPetya-haittaohjelman aiheuttamiin vahinkoihin. Ensimmäiset operaatiot olivat pitkälti lyhyen ajan sisällä suunniteltuja ja toteutettuja (vaikka Viron operaatio kestikin pitkään, ei sen pitkäkestoisesta suunnittelusta ole viitteitä). Nämä ensimmäiset operaatiot koostuivat palvelinesto- ja roskapostihyökkäyksistä, jotka aiheuttivat ennemminkin kiusaa. Sama tilanne näkyi vielä Georgiankin operaatiossa. Georgian kyberoperaatiolla oli lamauttava vaikutus georgialaishallinnon toimiin, mutta pohjimmiltaan hyökkäykset olivat samanlaisia kuin esimerkiksi Viroa vastaan toteutetut palvelinesto- ja roskapostihyökkäykset. Aidosti uusi operaatiotyyppi oli vasta operaatio Armageddon, jossa kybervakoilua kohdistettiin ukrainalaisia vaikuttajia kohtaan usean vuoden ajan. Uudenlainen operaatiotyyppi oli myös ukrainalaisiin voimaloihin vaikuttaminen, kun hyökkääjät kykenivät sulkemaan fyysiset kytkimet verkon välityksellä. Myös NotPetyan tapauksessa hyökkääjät toteuttivat operaation uudella tavalla. Haittaohjelmalla haluttiin ensimmäistä kertaa aiheuttaa pysyvää vahinkoa, eikä ainoastaan haitata väliaikaisesti uhrien toimintaa. Operaatioissa näkyy siis alun kyberoperaatioiden jälkeen selvä pyrkimys kokeilla erilaisia toimintatapoja ja teknologioita.

Operaatioiden erilaisuus on näkyvissä jo operaatioihin johtaneiden syiden muuttumisessa. Ensimmäisissä toteutetuissa operaatiossa taustalla vaikuttaneet syyt olivat ideologispainotteisia. Viron ja Liettuan tapauksessa Venäjä ei alun pitäenkään ollut saamassa geopoliittista hyötyä, jos operaatiot olisivat onnistuneet hyökkääjän näkökulmasta. Operaatioissa puolustettiin ennemminkin venäläistä historiaa ja ajattelutapaa. Tilanne muuttui Georgian sodassa, jossa kyberoperaatiolla tuettiin samanaikaisesti toteutetun maaoperaation kulkua. Tämän operaation avustuksella Venäjä sai geopoliittista hyötyä erottamalla Georgiasta sille kuuluvia maa-alueita ja liittämällä ne lähemmäs omaa etupiiriään. Sama lähestymistapa näkyi Ukrainan operaatioissa: kyberoperaatioilla pyrittiin saavuttamaan etulyöntiasema joko hankkimalla Venäjän tarkoitusperiä edistäviä tietoja tai pyrkimällä vaikuttamaan pitkäkestoisemmin ja monimutkaisemmin, kuin

aiemmissa operaatioissa. Ideologia ei hävinnyt kuitenkaan operaatioihin johtaneista syistä täysin, vaan siirtyi ennemminkin yhdeksi osatekijäksi geopoliittisten tekijöiden rinnalle tai taustalle. Esimerkiksi voimalaitoksia vastaan toteutetuissa hyökkäyksissä yhtenä syynä operaation toteuttamisessa oletetaan olleen halu kostaa ukrainalaisaktivistien aiheuttamat Krimin alueen sähkökatkot. Georgian operaatiosta eteenpäin geopoliittiset tekijät olivat kuitenkin selkeämmin vaikuttamassa operaatioiden aloittamiseen.

Myös valmistautumisvaihe kehittyi operaatioiden edetessä. Tiedustelu on yksi esimerkki. Jokaisessa operaatiossa oletetaan tapahtuneen jonkinasteista tiedustelua, sillä esimerkiksi verkkosivujen haavoittuvuudet olivat selvillä operaatioiden alkaessa. Tiedustelu muuttui kuitenkin hienovaraisemmaksi, esimerkiksi Georgian operaatioon liittyen löydettiin jälkikäteen haittaohjelma, joka oli keränyt tietoa operaatiota edeltäneeltä ajalta. Samalla kyberoperaatiot myös muodostuivat monimutkaisimmiksi ja pitkäkestoisimmiksi. Ennen varsinaista hyökkäystä Georgian operaatioon liittyen toteutettiin erillinen palvelinestohyökkäys, ja Ukrainassa toteutettuja operaatioita valmisteltiin useiden kuukausien ajan. Hyökkääjät olivat siis pitkäjänteisiä, ja siirtyivät hienovaraisempiin keinoihin pelkän raa'an voiman käyttämisen sijasta. Rekrytointia toteutettiin näkyvästi ainoastaan Viron ja Georgian operaatioissa, tämän jälkeen ulkopuolisten rekrytointi on joko lakannut tai se on siirtynyt näkymättömiin muiden kanavien kautta toteutettavaksi. Operaatioiden monimutkaistuminen näkyi myös valmistautumisvaiheen laajenemisessa. Ensimmäisissä operaatioissa (Viro, Liettua ja Georgia) toteutettiin valmistautumisvaiheeseen liittyen ainoastaan tiedustelua. Operaatio Armageddonista lähtien valmistautumisvaiheessa mukaan tulivat kyberhyökkäyksiin liittyen esimerkiksi sosiaalinen manipulointi, haittaohjelman aseistaminen ja vastatoimien välttäminen.

Mallin mukaista hallintavaihetta ei tehty ensimmäisten operaatioiden (Viro, Liettua ja Georgia) aikana ollenkaan. Tämän voi nähdä olevan yhteydessä operaatioiden monimutkaistumiseen. Ensimmäiset operaatiot (Viro, Liettua, Georgia) olivat yksinkertaisemmin toteutettuja, ja ne koostuivat pääosin roskaposti- ja palvelinestohyökkäyksistä. Ukrainassa toteutetut operaatiot taas olivat monimutkaisempia ja yksityiskohtaisempia. Esimerkiksi voimalaitoksia vastaan tehdyssä operaatiossa hyökkääjät suorittivat toimenpiteitä pitemmällä ajanjaksolla saadakseen paremman jalansijan järjestelmissä, ja kybervakoiluoperaatiossa saadakseen tiedot ulos kohdejärjestelmistä.

Toteutusvaihe muuttui monimutkaisemmaksi verrattaessa aiemmin toteutettuja operaatiota myöhemmin toteutettuihin operaatioihin. Viron, Liettuan ja Georgian tapauksissa hyökkäykset koostuivat pääosin roskaposti- ja palvelinestohyökkäyksistä, joilla aiheutettiin pääosin lyhytaikaista haittaa. Kybervakoiluoperaatiossa päätavoite ei ollutkaan enää järjestelmiin vaikuttaminen, vaan tietojen saaminen ulos järjestelmistä poliittisten ja sotilaallisten etujen ajamista varten. Sekä voimalaitoksia vastaan tehdyissä hyökkäyksissä että NotPetya-haittaohjelman asentamiseen liittyen hyökkääjät myös pyrkivät pysymään pitempään järjestelmissä ja haittaamaan puolustajien toimintaa käyttämällä aktiivisesti väistötoimenpiteitä sekä operaation aikana että operaation jälkeen.

NotPetyan aiheuttamia vahinkoja lukuun ottamatta operaatioilla ei ollut kovinkaan pitkäkestoisia vaikutuksia, ja suhteessa nähtyyn vaivaan hyödyt vaikuttavat olleen hyvinkin pieniä. Esimerkiksi voimalaitoksia vastaan toteutettua operaatiota suunniteltiin vähintään puoli vuotta, mutta vaikutukset jäivät muutaman tunnin mittaisiksi. Todennäköisempänä vaihtoehtona voidaan nähdä Venäjän halu kokeilla erilaisia kyberkykyjä Ukrainassa, ja laajentaa näin omaa keinovalikoimaansa varautumalla tulevaisuudessa tapahtuviin konflikteihin.

6.2 Pohdinta

Miten tutkimuksen analyysista saadut tulokset käyvät yhteen olemassa olevan tutkimuskirjallisuuden kanssa? Yhtenä tuloksena analyysissa havaittiin, että kyberoperaatioihin johtuneet syyt olivat alkuvaiheessa ideologisia, muuttuen sitten pääosin geopoliittisiksi ja teknologisiksi syiksi. Vastaavat syyt ovat olleet Venäjän toimintaa ohjaavia myös aiemmin maan historiassa. Erityisesti geopolitiikkaan liittyen Venäjälle on ominaista sen jatkuva turvattomuuden tunne, ja tästä kumpuava piiritetyn linnakkeen ajattelutapa. Kyseinen ajattelutapa sai alkunsa kommunisteilta, jotka ylläpitivät mielikuvaa muurien ympäröimästä Neuvostoliitosta, joiden takana vihollinen oli jatkuvasti hyökkäysvalmiina (Kennan, 1947, s. 575). Putinin Venäjä on jatkanut samankaltaista vastakkainasettelua, jossa länsimaista ja erityisesti Yhdysvalloista on tehty valtion vihollisia, jotka pyrkivät horjuttamaan Venäjälle kuuluvaa valta-asemaa kansainvälisessä politiikassa (Lipman, 2015, s. 111; Sinovets, 2016, s. 419). Turvattomuuden tunnetta on Eitelhuberin (2009) mukaan aiheuttanut erityisesti Neuvostoliiton hajoaminen. Venäjä on tästä syystä erityisen herkkä länsimaiden tekemille päätöksille ja toimille (Eitelhuber, 2009, s. 1). Näistä syistä länsimaiden ja Naton vaikutusvallan leviäminen Venäjän aiemmin hallitsemaan etupiiriin koetaan Venäjällä uhkaavana. Venäjä haluaakin puolustaa etujaan vedoten geopoliittisiin syihin, kuten kansalaistensa etujen puolustamiseen ja vanhaan etupiiriajatteluun.

Ideologiset syyt ovat olleet aiemminkin operaatioiden osasyinä Venäjän ja Neuvostoliiton suorittamissa sotilasoperaatioissa. Esimerkiksi yksi syy, minkä takia Neuvostoliitto soti Afganistanissa lähes vuosikymmenen ajan, oli marxistisen hallituksen ja kommunistisen ideologian puolustaminen (Collins, 1987, s. 200). Geopolitiikka on kuitenkin ollut ideologiaa tärkeämpi osa Venäjän toimintaa. Esimerkiksi Venäjän kiinnostus Tšetšeniaa kohtaan ja lopulta sotaan Tšetšenian alueella johtui pitkälti geopoliittisista syistä (Celestan, 1996; Kramer, 2005). Sama tilanne on Krimillä, jossa Venäjän tekemisiä ajavat alueelliset intressit (Norberg & Westerlund, 2014). Yksi Georgian sotaan johtaneista syistä oletetaan olleen uusien teknologioiden käyttöönoton testaaminen (Shakarian, 2012), mutta Bartlesin ja McDermottin mukaan sotaan ajauduttiin myös Venäjän ja Georgian eriytyneiden geopoliittisten intressien vuoksi (2015, s. 47).

Yhtenä havaintona oli, että kyberoperaatioissa käytettiin ideologispainotteista retoriikkaa erityisesti tavallisen kansan rekrytoinnissa apuna. Tätä keinoa on aiemminkin käytetty Venäjällä. Venäläisten poliitikkojen retoriikassa on ollut

pyrkimys käyttää koko kansaa yhdistäviä kielikuvia, kun maassa on tapahtunut jonkinasteisia kriisejä. Esimerkiksi Beslanin kouluiskun jälkeen Putin puhui koko Venäjän olevan hyökkäyksen kohteena, ja että valtiota uhkasi totaalinen sota (Lynch, 2005, s. 141) Venäjä on käyttänyt paljon rahaa erilaisiin isänmaallisiin ohjelmiin, kuten nuorison sotilaskoulutukseen, historiallisiin merkkipäiviin ja muistotilaisuuksiin (Goode, 2018, s. 266). Retoriikan ja resurssien kohdistaminen tavalliseen kansaan on loogista, sillä Venäjällä on paljon väkeä, joilla on matemaattista ja teknisen alan osaamista. Tätä kautta Venäjällä on käytössään paljon tietotekniikkataustaisia ja patrioottishenkisiä kansalaisia (Thomas, 2014, s. 107).

Ihmetystä herätti Liettuan operaatio. Se oli käytännössä hiilikopio Viron operaatioon liittyen, mutta toteutuksen laajuudelta huomattavasti pienempi. Esimerkiksi Viron operaatiossa käytettiin poliittisia ja fyysisiä painostuskeinoja (kuten diplomaattisuhteiden katkaisulla uhkaamista ja mielenosoituksia), kun taas Liettuaa kohtaan tehtiin ainoastaan palvelinesto- ja roskapostihyökkäyksiä. Operaatiotaktiikka ei siis muuttunut parempaan suuntaan kuin vuotta aiemmassa Viron operaatiossa, päinvastoin. Tilanne muuttui Georgian ja erityisesti Ukrainan alueilla toteutetuissa kyberoperaatioissa, joiden yhteydessä käytettiin myös muita kuin kybervaikuttamistapoja. Tämän voi selittää osittain strategisen kulttuurin muuttumisen hitaudella. Kuten aiemmin teorian esittelyn yhteydessä mainittiin, strateginen kulttuuri muuttuu hitaasti. Ainoastaan tietyt tekijät, kuten ulkopuolelta tullut heräte, voivat muuttaa strategista kulttuuria nopeammin. Cassidy (2003) on tutkinut Venäjän toimia Afganistanissa ja Tšetšeniassa, ja hänen havaintojensa mukaan osasyy Venäjän huonoon menestykseen näissä maissa tehdyissä sotilasoperaatioissa oli sotilaskulttuurin hidas muuttuminen. Sotilaskulttuurilla kestää hänen mukaansa normaalisti 5 – 10 -vuotta muuttua. Tämä sama kulttuurin hidas muuttuminen on voinut näkyä myös kyberoperaatioiden hitaassa kehittymisessä. Liettuan tapauksessa on voitu yrittää toteuttaa samanlainen operaatio, kuin Viroa vastaan toteutettiin. Epäonnistuminen Liettuassa on voinut ajaa Venäjää kehittämään kyberoperaatioiden rakennetta ja toteutustapaa. Kyberoperaatioita ei toteutettukaan enää samalla tavalla ainoana vaikutuskeinona kuin Liettuassa, vaan kybervaikuttaminen toteutettiin muiden vaikuttamiskeinojen rinnalla (kuten maaoperaation tukeminen Georgiassa) tai operaatioiden rakenne ja kohteet muuttuivat täysin (kuten operaatio Armageddonissa ja NotPetya-haittaohjelman levittämisessä).

Analyysin operaatioita yhdistivät useat paradigmat ja näistä johdetut hyökkäystapojen valinnat. Yksi näistä paradigmoista oli haluttomuus aiheuttaa pysyvää vahinkoa. NotPetyaa lukuun ottamatta operaatioiden vaikutukset kyberympäristössä jäivät verrattain lyhytaikaisiksi ja vähän vahinkoa aiheuttaneiksi. Tämä ajattelutapa ei noudata venäläisten perinteisissä sotilasoperaatioissa noudattamaa toimintatapaa. Esimerkiksi Tšetšeniassa venäläiset eivät välittäneet sivullisista uhreista pommittaessaan kaupunkeja ja kyliä tavoitteenaan ajaa kapinalliset ulos piilopaikoistaan. Samanlainen suhtautumistapa on ollut Syyriassa, jossa Venäjän ilmapommitukset olivat vuoteen 2016 mennessä aiheuttaneet noin 2000 siviilin kuoleman. (Williams &

Souza, 2016, s. 49.) Ukrainassa vuoden 2017 aikana tuhoa levittänyt NotPetya-haittaohjelma taas noudattaa tätä sotilasoperaatioiden ajattelutapaa. NotPetyan ainoana tavoitteena oli levitä mahdollisimman moneen tietojärjestelmään ja laitteeseen ja aiheuttaa mahdollisimman paljon tuhoa näissä kohteissa. Jensen ym. (2019, s. 229) ovat löytäneet saman piirteen (haluttomuuden aiheuttaa pysyvää vahinkoa) Venäjän toteuttamista kyberoperaatioista. Toinen heidän havaintonsa on, että iskut ovat kohdistuneet pääosin siviili-infrastruktuuria vastaan. Tämän tutkimuksen perusteella kyseinen havainto ei pidä täysin paikkaansa, sillä kyberkykyjä on käytetty sekä sotilas- että siviilikohteita vastaan. Sotilaat olivat kybervakoilun kohteena operaatio Armageddonissa, ja Naton verkkosivuja vastaan on tehty palvelinhyökkäyksiä. Suurempi osa kohteista tosin oli siviilien ylläpitämiä palvelimia ja verkkosivuja. Tämä on voinut johtua siitä, että siviilikohteisiin on helpompi vaikuttaa, koska asevoimien verkot ovat todennäköisemmin paremmin suojattuja. Parhaimmallakaan suojakeinolla ei ole toisaalta merkitystä, jos tietojärjestelmiä käyttävät yksilöt tekevät vääriä ratkaisuja. Operaatio Armageddonissa päästiin sosiaalisen manipuloinnin avulla myös asevoimien järjestelmiin sisälle, kun näitä järjestelmiä käyttäneet sotilaat saatiin avaamaan hyökkääjien lähettämät sähköpostien saastuneet liitetiedostot.

Operaatioissa tehdyt valinnat eroavat erityisesti Karin (2019, s. 77) väitöskirjassa esitellyistä valinnoista. Nämä olivat:

- Kansainvälisten sopimusten käyttö
- Kriittisen verkkoinfrastruktuurin suojelu
- Venäjän suvereniteetin kasvattaminen kyberympäristössä
- Tiedon säilyttäminen
- RuNetin valvonta
- RuNetin sensurointi
- Anonymiteetin kieltäminen
- Erityisvalmisteisen verkkojen käyttö
- Ulkomailta tuotujen verkkolaitteiden korvaaminen kotimaisella tuotannolla

Erot voidaan osittain selittää ainakin sillä, millaista dataa tässä tutkimuksessa on käytetty verrattuna Karin väitöskirjassa käyttämään dataan. Kari käytti tutkimuksessaan venäläisiä virallisia asiakirjoja, jotka selittävät, millaisia uhkia Venäjää vastaan kohdistuu kyberympäristössä. Tässä tutkimuksessa taas käytetään lähdemateriaalina toteutetuista operaatioista saatuja tietoja. Neuvostoliitto on aikaisemmin toiminut samalla tavalla, sillä se on toiminut eri tavalla, kuin mitä maan tuottamat asiakirjat antoivat ymmärtää. Neuvostoliitolla oli käytössään defensiivispainotteisemmat poliittiset doktriinit, kun taas sotilasstrategiat olivat pitkälti hyökkäykselliset (Cassidy, 2003, s. 9-10). Tämän voi nähdä vaikuttavan myös kyberympäristössä: kybervaikuttamiseen liittyvät asiakirjat ovat kirjoitusasultaan puolustuksellisempia (kuten Karin väitöskirjassa todetaan), kun taas todellinen, kyberoperaatioissa käytetty strategia on

hyökkäyksellisempi (kuten tässä tutkimuksessa käsitellyistä operaatioista käy ilmi).

Toinen operaatioita yhdistävä tekijä oli vastuun välttäminen ja yritys pitää operaation tekijän varsinainen henkilöllisyys piilossa. Esimerkiksi Viron operaatioon liittyen Venäjä kielsi olevansa vastuussa operaatiosta, mutta esti silti tutkijoiden pääsyn maahan haitaten tätä kautta ratkaisevasti tutkimuksen kulkuun. NotPetyan tapauksessa venäläiset ovat sanoneet itse olleen uhrin asemassa ja perustelleet tätä sillä, että haittaohjelma levisi myös venäläisiin tietojärjestelmiin. Jensenin ym. (2019, s. 226) mukaan Venäjän on käyttänyt Ukrainassa niin kutsuttua false-flag-operaatiotaktiikkaa, joissa tekijän henkilöllisyys pyritään pitämään epäselvänä tai vastuu hyökkäyksistä yritetään siirtää toisen osapuolen syyksi. Tällainen operaatiotaktiikkaa on ollut aikoinaan käytössä myös Neuvostoliitossa, ja sen voidaan epäillä olleen vaikuttavana taktiikkana myös kyberoperaatioissa.

Yhteenvetona voidaan todeta, että Venäjä on toteuttanut useita erilaisia kyberoperaatioita 2000-luvun aikana, joista tässä tutkimuksessa käsiteltiin kuutta eri operaatiota (Viro, Liettua, Kirgisia sekä kolme Ukrainassa tteutettua operaatiota). Viron, Liettuan ja Georgian kyberoperaatiot olivat samankaltaisia rakenteeltaan. Georgian kyberoperaatio tosin erosi aiemmista operaatioista siten, että sillä tuettiin samanaikaisesti suoritettua maaoperaatiota. Georgian kyberoperaatiolla oli siis strategisemmat tavoitteet, kuin Viron ja Liettuan kyberoperaatioilla. Myös operaatioon johtaneet syyt vaihtuivat ideologisista syistä geopoliittisiin syihin. Ukrainassa toteutetut kyberoperaatiot ovat jokainen olleet erilaisia rakenteeltaan. Venäläiset ovat toteuttaneet ja kokeilleet sekä kybervakoilua, fyysisiin järjestelmiin vaikuttamista sekä maksimaalisen vahingon aiheuttamista. Hyökkääjän henkilöllisyys on pyritty pitämään piilossa kaikissa kyberoperaatioissa. Yleensä on tiedetty, että toteuttajana ovat olleet venäläiset, mutta Venäjän hallituksen rooli on jäänyt epäselvemmäksi (vaikkakin kansainvälisesti ollaan sitä mieltä, että Venäjän hallitus on vastuussa näistä operaatioista).

Kyberhyökkäyksen mallintamisen menetelmiä on kehitetty lukuisa määrä. Nämä voidaan jakaa kolmeen kategoriaan (tapauskohtaiset, ajalliset ja visuaaliset mallit), joiden alakategorioihin useimmat hyökkäysmallit voidaan lokeroida. Mallien valtaisasta lukumäärästä johtuen kaikkia malleja ei tämän tutkimuksen rajoissa voitu käsitellä. Tärkeintä oli löytää soveltuvin malli kyberoperaatioiden analysointia varten. Varsinaisia kyberoperaatioiden analysointimenetelmiä löydettiin yllättävän vähän eivätkä löydetyt mallit olleet soveltuvia operaatioiden analysointiin. Täten lopullisena analysointityökaluna käytettiin hieman muutettua sovellettua yhdistettyä tappoketjua.

6.3 Tutkimuksen validiteetti ja reliabiliteetti

Tämän tutkimuksen tuloksia voidaan pitää luotettavana. Luotettavuutta kasvattaa erityisesti kirjallisuuskatsauksen laajuus. Operaatioista etsittiin kaikki

saatavilla oleva mahdollinen tieto, ja operaatioihin liittyneet väitteet ja löydöt pyrittiin varmistamaan useamman kuin yhden lähteen kautta. Kirgisiaan liittynyt kyberoperaatio jätettiin juuri siitä syystä analyysiosiosta pois, koska kyseisen operaation tekijästä ei löytynyt riittävästi yksityiskohtaista tutkimustietoa. Kuuden operaation analysointi on riittävän laaja, mutta kuitenkin yksityiskohtainen, jotta yleistyksiä operaatioiden rakenteesta pystyttiin löytämään. Tutkimuksen analysointiosuus oli myös moneen muuhun kirjallisuuskatsauksen tutkimukseen verrattuna parempi. Tämä johtui siitä, että tämän tutkimuksen tulokset saatiin käyttämällä jokaisen operaation analysoinnissa samaa kyberhyökkäysten mallintamisen menetelmää. Tällöin operaatiot saatiin purettua osiin, ja rakennetta pystyttiin analysoimaan ja vertailemaan tarkemmin. Useassa muussa tutkimuksessa analysointi pohjautui ainoastaan tutkijoiden omiin havaintoihin.

Tuloksia analysoitaessa tulee kuitenkin muistaa, että yhteisen menetelmän käytöstä huolimatta havainnot perustuvat pohjimmiltaan tutkijan omiin havaintoihin. Kirjallisuuskatsauksen aikana on voinut jäädä jokin lähde tai tutkimus huomaamatta, josta olisi voinut nousta esiin tärkeitä, operaatioihin liittyviä yksityiskohtia. Esimerkiksi Kirgisiaan liittyen on voitu tehdä tutkimus, joka käsittelee yksityiskohtaisemmin operaatiota kuin mitä tämän tutkimuksen kirjallisuuskatsaukseen nostetuissa lähteissä tehdään.

6.4 Tutkimuksen aikana esiin nousseet haasteet ja jatkotutkimus

Tutkimuksen edetessä suurimpana puutteena esiin nousi tähän tutkimukseen sopivan kyberoperaation mallintamisen menetelmän puuttuminen. Varsinaisista kyberhyökkäysten mallintamisen menetelmistä ei ole puutetta, päinvastoin. Tämän tutkimuksen kirjallisuuskatsauksessa ei käsitelty kuin osaa tällaisista menetelmistä. Ongelmana oli, että kyseiset työkalut oli pääosin kehitetty yksittäisten kyberhyökkäysten teknisempää analysointia varten. Graafiset mallit (kuten kybertappoketju) soveltuivat myös kyberoperaatioiden analysointiin, mutta tällöinkin mallit olivat teknispainotteisempia. Lisäksi yhdessäkään mallissa ei otettu kunnolla huomioon operaation juurisyitä. Timanttimalli käsitteli hyökkääjän ja uhrin välistä suhdetta, mutta analyysi hyökkäyksen tai operaatiota edeltäneistä syistä puuttui. Yhdistettyyn tappoketjuun lisäämäni vaihe 0 korjasi tätä puutetta hieman. Kyseessä ei ole kuitenkaan tutkimustulokseen pohjautuva vaihe, joten kyseisen vaiheen olemassaolo tulisi jatkotutkimusten avulla perustella paremmin.

Käytin myös yhdistettyä tappoketjua hieman eri tavalla kuin sitä oli alun perin tarkoitettu. Eri vaiheiden sisällä olleet osa-alueet eivät omien havaintojeni mukaan olleet täysin kiinteitä, vaan jotkut osa-alueet tapahtuivat useammassa kuin yhdessä vaiheessa. Esimerkiksi vastatoimien välttämistä toteutettiin sekä operaation valmistautumisvaiheessa (hyökkääjien ollessa tietojärjestelmissä sisällä), että operaation toteutusvaiheessa (kun hyökkääjät pyrkivät hidastamaan puolustajien havaintojen tekemistä ja toimenpiteitä). Rekrytointi oli yksi osa-alue,

joka puuttui kokonaan alkuperäisestä mallista. Tätä osa-aluetta ei esiintynyt jokaisessa operaatiossa, mutta kuvastaa sitä, että mallia voisi käyttää joustavammin ja muunnella sitä operaation mukaan.

Ensimmäisten operaatioiden aikana mallin käytössä korostuivat sen tekniset lähtökohdat. Viron, Liettuan ja Georgian operaatioissa ei ollut havaittavissa mallin mukaista operaation hallintavaihetta. Ne kyberoperaatiot, joissa oli osana esimerkiksi sosiaalista manipulointia ja järjestelmien sisällä liikkumista, malli kykeni yksityiskohtaisemmin kuvaamaan. Tarve kuitenkin on mallille, joka olisi suunniteltu erikseen tämän kaltaiselle kyberoperaatioiden analysoinnille. Tällaisen mallin avulla pystyttäisiin analysoimaan saman toimijan toteuttamia kyberoperaatioita, ja mahdollisuuksien mukaan ennakoimaan tulevien operaatioiden tapaa ja ajankohtaa.

Joistain kyberoperaatioista oli myös saatavilla yllättävän vähän yksityiskohtaisempaa tutkimuskirjallisuutta. Aiemmin mainittu Kirgisiaan liitetty kyberoperaatio jouduttiin jättämään pois juuri puutteellisten tietojen vuoksi. Liettuaan liitetylle kyberoperaatiolle oli käydä sama, mutta kirjallisuudesta löytyi onneksi tutkimus, jonka ansiosta operaatio pystyttiin ottamaan analyysivaiheeseen mukaan. Operaatioista saatavilla olevat tiedot olivat myös painottuneet teknisempään suuntaan. Tämä on ymmärrettävää, kun kyseessä on tietojärjestelmiä vastaan kohdistuneet hyökkäykset, ja operaatiokohtaisilla analyyseillä pyritään antamaan ohjeistusta ja neuvoja, jotta vastaavanlaisia hyökkäyksiä vastaan pystytään paremmin valmistautumaan. Tarve olisi kuitenkin myös vähemmän teknispainotteisemmille analyyseille. Tällaiset tiedot auttaisivat esimerkiksi hyökkääjien käyttäytymisen ymmärtämisessä ja ennustamisessa. Lisäksi valtiotasolla tehtävät päätökset kyberoperaation analyyseista pohjautuvat tämän tutkimuksen perusteella muihinkin kuin pelkästään teknisiin syihin.

LÄHTEET

Abraham, S., & Nair, S. (2015). A predictive framework for cyber security analytics using attack graphs. *International Journal of Computer Networks & Communications, 7(1),* 1-17.

Aguessy, F-X. (2016). *Évaluation dynamique de risque et calcul de réponses basés sur des modèles d'attaques bayésiens* (Väitöskirja). Institut National des Télécommunications. Haettu osoitteesta https://tel.archives-ouvertes.fr/tel-01408035/document

Ahmad, T. (2018, 15. helmikuuta). Foreign Office Minister condemns Russia for NotPetya attacks. Haettu 10.2.2020 osoitteesta https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

Alexander, D. (2014). Cyber threats against the North Atlantic Treaty Organization (NATO) and selected responses. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, 1(2),* 1-36.

Alfonsi, A., Rabiti, C., Mandelli, D., Cogliati, J., Kinoshita, R. & Naviglio, A. (2013). *Dynamic event tree analysis through Raven* (No. INL/CON-13-29344). Idaho National Laboratory (INL).

Allison, R. (2008). Russia resurgent? Moscow's campaign to 'coerce Georgia to peace'. *International Affairs, 84(6),* 1145-1171.

Amor, N., Benferhat, S. & Elouedi, Z. (2004). Naive bayes vs decision trees in intrusion detection systems. Teoksessa *Proceedings of the 2004 ACM symposium on Applied computing*, Nicosia, Cyprus, March 14-17, 2004.

Andress, J. & Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. (2. uud. painos). Waltham: Elsevier.

Andrews, J. & Dunnett, S. (2000). Event-tree analysis using binary decision diagrams. *IEEE Transactions on Reliability, 49(2),* 230-238.

Arias, J., & Stern, R. (2011). Review of risk management methods. *Business Intelligence Journal, 4(1),* 51-78.

Arlow, J. (1998). Use cases, UML visual modelling and the trivialisation of business requirements. *Requirements Engineering, 3(2),* 150-152.

Artz, M. (2002). *Netspa: A network security planning architecture* (Väitöskirja). Massachusetts Institute of Technology. Haettu osoitteesta https://dspace.mit.edu/bitstream/handle/1721.1/29899/51072296-MIT.pdf?sequence=2&isAllowed=y

Ashmore, W. (2009). Impact of alleged Russian cyber attacks. *Baltic Security & Defence Review, 11(1),* 4-40.

Aslanoğlu, R. & Tekir, S. (2012). *Recent cyberwar spectrum and its analysis.* Izmir Institute of Technology.

Bajpai, K. (2002). Indian strategic culture. Teoksessa M. Chambers (toim.), *South Asia in 2020: Future Strategic Balances and Alliances (245-304)*.

Barik, M. & Mazumdar, C. (2011). A novel approach to collaborative security using attack graph. Teoksessa *2011 IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application*, Bangalore, India, December 12-13, 2011.

Bartles, C. & McDermott, R. (2014). Russia's military operation in Crimea: Road-testing rapid reaction capabilities. *Problems of Post-Communism, 61(6),* 46-63.

Baxter, P. & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13(4),* 544-559.

BBC. (2018, 15. Helmikuuta). UK and US blame Russia for 'malicious' NotPetya cyber-attack. Haettu 10.2.2020 osoitteesta https://www.bbc.com/news/uk-politics-43062113

Beim, G. & Hobbs, B. (1997). Event tree analysis of lock closure risks. *Journal of Water Resources Planning and Management, 123(3),* 169-178.

Bonner III, E. (2014). Cyber power in 21st-century joint warfare. *Joint Force Quarterly, 74(3),* 102-109.

Booth, K. (1990). The concept of strategic culture affirmed. Strategic Power: USA/Ussr. Teoksessa C. Jacobsen (toim.), *Strategic Power: USA(USSR (121-128).* London: Palgrave Macmillan.

Boudali, H., Crouzen, P. & Stoelinga, M. (2007). Dynamic fault tree analysis using input/output interactive markov chains. Teoksessa *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07),* Edinburgh, Uk, June 25-28, 2007.

Blank, S. (2017). Cyber war and information war a la russe. *Understanding Cyber Conflict: Fourteen Analogies, 18(1)*, 81-98.

Braynov, S. & Jadliwala, M. (2003). Representation and analysis of coordinated attacks. Teoksessa *Proceedings of the 2003 ACM workshop on Formal methods in security engineering (CCS03),* Washington DC, The United States of America, October, 2003.

Bryant, B. & Saiedian, H. (2017). A novel kill-chain framework for remote security log analysis with SIEM software. *Computers & Security, 67*, 198-210.

Bucci, P., Kirschenbaum, J., Mangan, L., Aldemir, T., Smith, C. & Wood, T. (2008). Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliability Engineering & System Safety, 93(11),* 1616-1627.

Bumgarner, J. & Borg, S. (2009). *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*. US-CCU Special Report.

Bunda, J. (2020). *APT28 : tapaustutkimus Venäjään yhdistettyjen kyberoperaatioiden kehittymisestä vuosina 2007 – 2016* (Pro gradu -tutkielma). Jyväskylän yliopisto.

Caltagirone, S., Pendergast, A. & Betz, C. 2013. *The Diamond Model of Intrusion Analysis* (Report 0704-0188). US Department of Defense.

Cassidy, R. (2003). *Russia in Afghanistan and Chechnya: military strategic culture and the paradoxes of asymmetric conflict*. Strategic Studies Institute: DIANE Publishing.

Cavaye, A. (1996). Case study research: a multi ‐ faceted research approach for IS. *Information systems journal, 6(3),* 227-242.

Celestan, G. (1996). *Wounded Bear: The Ongoing Russian Military Operation in Chechnya* (FMSO 4). Department of Defense, Foreign Military Studies Office

Čepin, M. & Mavko, B. (2002). A dynamic fault tree. *Reliability Engineering & System Safety, 75(1),* 83-91.

Chaufette, N. & Haag, T. (2007). Vulnerability cause graphs: a case of study.

Chen, T., Sanchez-Aarnoutse, J. & Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on smart grid, 2(4),* 741-749.

Cheng, P., Wang, L. & Long, T. (2010). Compressing attack graphs through reference encoding. Teoksessa *2010 10th IEEE International Conference on Computer and Information Technology, (1026-1031)*, Bradford, UK, June 29 – July 1, 2010.

Clark, D. & Landau, S. (2011). Untangling attribution. *Harvard National Security Journal, 2,* 323-353.

Clemen, R. & Reilly, T. (2013). *Making hard decisions with DecisionTools.* (15. uud. painos). Mason: South-Western.

Collins, J. (1987). Soviet policy toward Afghanistan. *Proceedings of the Academy of Political Science, 36(4),* 198-210.

Corbin, K. (2009, 12. maaliskuuta). Lessons From The Russia-Georgia Cyberwar. internetnews. com: Real time IT News, 12. Haettu 5.2.2020 osoitteesta http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm

Cornell, S. & Starr, S. (2009). *The guns of August 2008*. London: ME Sharpe.

Covington, S. (2016). *The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare.* Harvard Kennedy School, Belfer Center for Science and International Affairs.

Czosseck, C., Ottis, R. & Talihärm, A. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT), 1(1),* 24-34.

Darczewska, J. (2014). *The anatomy of Russian information warfare. The Crimean operation, a case study*. Warsaw: Ośrodek Studiów Wschodnich.

Daricili, A. (2014). Rusya Federasyonu Kayanakli Olduğu İddia EdİIen Siber Saldiridalin Analizi. *International Journal of Social Inquiry, 7(2).*

Davis, J. (2007, 21. elokuuta). Hackers take down the most wired country in europe. Haettu 28.4.2020 osoitteesta https://www.wired.com/2007/08/ff-estonia/

Dehlawi, Z. & Abokhodair, N. (2013). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. Teoksessa *2013 IEEE International Conference on Intelligence and Security Informatics, (73-75),* Seattle, Washington, June 4-7, 2013.

DeVries, E. J. (2005). Episyemology and Methodology in Case Research: A Comparison Between European and American IS Journals. *ECIS 2005 Proceedings, 145, 4-25.* Haettu osoitteesta https://www.researchgate.net/profile/Erik_De_Vries3/publication/221408643_Epistemology_and_Methodology_in_Case_Research_A_Comparison_between_European_and_American_IS_Journals/links/5469d3cc0cf20dedafd10b27.pdf

Dragos, I. (2017). *Crashoverride: Analysis of the threat to electric grid operations.* Dragos Inc.

Duffy, R. (2018, 29. toukokuuta). The U.S. military combined cyber and kinetic operations to hunt down ISIS last year, general says. Cyberscoop. Haettu 22.1.2020 osoitteesta https://www.cyberscoop.com/u-s-official-reveals-military-combined-cyber-kinetic-operations-hunt-isis/

Durkota, K., Lisy, V., Kiekintveld, C. & Bosansky, B. (2015). Game-theoretic algorithms for optimal network security hardening using attack graphs. Teoksessa *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, (1773-1774),* Istanbul, Turkey, May 4-8, 2015.

Eitelhuber, N. (2009). The Russian Bear: Russian strategic culture and what it implies for the West. *Connections, 9(1),* 1-28.

Eisenhardt, K. (1989). Building theories from case study research. *Academy of management review, 14(4),* 532-550.

Ermarth, F. (2006). Russia's strategic culture: Past, Present, and… in Transition? *Defense Threat Reduction Agency, 2*, 234-256.

Fanelli, R. & Conti, G. (2012). A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict. Teoksessa C. Czosseck, R. Ottis & K. Ziolkowski (toim.), *2012 4th International Conference on Cyber Conflict (CYCON 2012) (319-332),* Tallinn, Estonia, June 5-8, 2012.

Feng, C. & Jin-Shu, S. (2008). A flexible approach to measuring network security using attack graphs. Teoksessa *2008 International Symposium on Electronic Commerce and Security, (426-431),* Guangzhou City, China, August 3-5, 2008.

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P. & Veitch, B. (2009). Handling data uncertainties in event tree analysis. *Process safety and environmental protection, 87(5),* 283-292.

Firesmith, D. (2003). Security use cases. *Journal of object technology, 2(3).*

Franke, U. (2015). *War by non-military means: Understanding Russian information warfare* (FOI-R--4065—SE). Stockholm: Totalförsvarets Forskningsinstitut (FOI).

Friedl, M. & Brodley, C. (1997). Decision tree classification of land cover from remotely sensed data. *Remote sensing of environment, 61(3),* 399-409.

Freire, M. (2017). Ukraine and the Restructuring of East-West Relations. Teoksessa R. Kanet (toim.), *The Russian Challenge to the European Security Environment, (189-209).* United Kingdom: Palgrave Macmillan.

Fussell, J. (1973). *Synthetic tree model: A formal methodology for fault tree construction* (No. ANCR-1098). Idaho: Aerojet Nuclear Co.

Gao, N., He, Y. & Ling, B. (2018). Exploring attack graphs for security risk assessment: a probabilistic approach. *Wuhan University Journal of Natural Sciences, 23(2),* 171-177.

Geers, K. (2015). *Cyber war in perspective: Russian aggression against Ukraine.* NATO, Cooperative Cyber Defence Centre of Excellence.

Giles, K. (2016). *Handbook of Russian Information Warfare*. Rome: DeBooks Italia srl.

Giles, K. & Hagestad II, W. (2013). Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. Teoksessa K. Podins, J. Stinissen & M. Maybaum (toim.), *2013 5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications.

Giuliano, E. (2005). Islamic identity and political mobilization in Russia: Chechnya and Dagestan compared. *Nationalism and Ethnic Politics, 11(2),* 195-220.

Goel, S. (2011). Cyberwarfare: connecting the dots in cyber intelligence. *Communications of the ACM, 54(8),* 132-140.

Goode, J. (2018). Everyday patriotism and ethnicity in today's Russia. *Russia before and after Crimea: Nationalism and Identity, 2010–2017*, 258-281.

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice? *Strategic Studies Quarterly, 4(3),* 102-135.

Grant, T., Burke, I. & van Heerden, R. (2012). Comparing Models of Offensive Cyber Operations. Teoksessa V. Lysenko (toim.), *Proceedings of the 7th*

International Warfare and Security, (108-121), Seattle, The United States of America, March 22-23, 2012.

Gray, C. (1988). *The Geopolitics of Super Power.* Lexington: University Press of Kentucky.

Green, J. (2016). *Cyber Warfare - A Multidisciplinary Analysis.* Abingdon: Routledge.

Greenberg, A. (2017, 12. kesäkuuta). 'Crash Override': The Malware That Took Down a Power Grid. Haettu 23.2.2020 osoitteesta https://www.wired.com/story/crash-override-malware/

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. Haettu 28.4.2020 osoitteesta https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hamilton, S. & Hamilton, W. (2008). Adversary Modeling and Simulation in Cyber Warfare. Teoksessa S. Jajodia, P. Samarati & S. Cimato (toim.) *Proceedings of the IFIP TC 11 23rd International Information Security Conference vol 278 (461-475),* Milano, Italy, September 7-10, 2008.

Harrison, H., Birks, M., Franklin, R. & Mills, J. (2017). Case study research: Foundations and methodological orientations. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research 18(1).* Haettu osoitteesta http://www.qualitative-research.net/index.php/fqs/article/view/2655/4080

Hollis, D. (2011). *Cyberwar case study: Georgia 2008*. Small Wars Journal.

Hutchins, E., Cloppert, M. & Amin, R. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Teoksessa *Proceedings of the 6th International Conference on i-Warfare and Security, (113-125),* Washington D.C., March 17-18, 2011.

Hämäläinen, J., Åkesson, B., & Lappi, E. (2013). Combining Research and Education in Tactical Combat Modelling. Teoksessa- 5 th Sandis Workshop. *Information Warfare and Security,* 106-111.

Jasiul, B., Szpyrka, M. & Śliwa, J. (2014). Detection and modeling of cyber attacks with petri nets. *Entropy, 16(12),* 6602-6623.

Jensen, B., Valeriano, B. & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies, 42(2),* 212-234.

Jensen, J. & Rodgers, R. (2001). Cumulating the intellectual gold of case study research. *Public Administration Review, 61(2),* 235-246.

Johnston, A. (1995). Thinking about strategic culture. *International security, 19(4),* 32-64.

Johnston, A. (1998). *Cultural realism: Strategic culture and grand strategy in Chinese history*. Princeton: Princeton University Press.

Joubert, V. (2012). *Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?* NATO Defense College: Research Division.

Kallberg, J. (2018). Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations. *The Cyber Defense Review, Spring 2016,* 101-116

Kamiński, B., Jakubczyk, M. & Szufel, P. (2018). A framework for sensitivity analysis of decision trees. *Central European Journal of Operations Research, 26(1),* 135-159.

Karaman, M., Catalkaya, H., Gerehan, A. & Goztepe, K. (2016). Cyber Operation Planning and Operational Design. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 5(1),* 21-29.

Kari, M. (2019a). *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture–a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats* (Väitöskirja). JYU Dissertations 122. Jyväskylän Yliopisto. Haettu osoitteesta https://jyx.jyu.fi/bitstream/handle/123456789/65402/978-951-39-7837-2_vaitos_2019_10_11_jyx.pdf?sequence=4&isAllowed=y

Kari, M. (2019b). Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception. Teoksessa N. van der Waag-Cowling & L. Leenen (toim.), *Proceedings of the 14th International Conference on Cyber Warfare and Security (528-535),* Stellenbosch, South Africa, February 28 – March 1, 2019.

Karpati, P., Sindre, G. & Opdahl, A. (2010). Visualizing cyber attacks with misuse case maps. Teoksessa R. Wieringa & A. Persson (toim.), *International Working Conference on Requirements Engineering: Foundation for Software Quality (262-275)*, Essen, Germany, June 30 – July 2, 2010.

Kasemsri, R. (2006). *A survey, taxonomy, and analysis of network security visualization techniques* (Pro gradu –tutkielma). Georgia State University.

Katta, V., Karpati, P., Opdahl, A., Raspotnig, C. & Sindre, G. (2010). Comparing Two Techniques for Intrusion Visualization. Teoksessa P. Van Bommel, S. Hoppenbrouwers, S. Overbeek, E. Proper & J. Barjis (toim.), *IFIP Working Conference on The Practice of Enterprise Modeling (1-15),* Delft, The Netherlands, November 9-10, 2010.

Kealey, J. & Amyot, D. (2007). Enhanced Use Case Map Traversal Semantics. *Lecture Notes in Computer Science (volume 4745).*

Kenarangui, R. (1991). Event-tree analysis by fuzzy probability. *IEEE transactions on reliability, 40(1),* 120-124.

Kennan, G. (1947). The sources of Soviet Conduct. *Foreign Affairs, 25(4),* 566-582.

Korns, S. & Kastenberg, J. (2009). Georgia's Cyber Left Hook. *Parameters Winter 2008-2009, Volume XXXVIII, No. 4,* 60-76.

Kotenko, I. & Chechulin, A. (2013). A cyber attack modeling and impact assessment framework. Teoksessa M. Maybaum (toim.), *5th International Conference on Cyber Conflict, (1-24),* Tallinn, Estonia, Jun 4 – 7, 2013.

Kramer, M. (2005). Guerrilla Warfare, Counterinsurgency and Terrorism in the North Caucasus: The Military Dimension of the Russian–Chechen Conflict. *Europe-Asia Studies, 57(2),* 209-290.

Kontio, J. (1997). *The Riskit Method for Software Risk Management, version 1.00* (CS-TR-3782). University of Maryland, Department of Computer Science.

Kozlowski, A. (2014). Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal, 3,* 237-245.

Kukkola, J., Kuikka, V. & Nikkarila, J-P. (2017). Modelling the imbalance of cyber operations between closed and open national networks. Teoksessa *International Society for Military Sciences (ISMS 2017), (123-130),* Oslo, Norway, November 15–17, 2017.

Kumar, R., Ruijters, E. & Stoelinga, M. (2015). Quantitative attack tree analysis via priced timed automata. Teoksessa S. Sankaranarayanan, E. Vicario (toim.), *International Conference on Formal Modeling and Analysis of Timed Systems (156-171),* Madrid, Spain, September 2-4, 2015.

Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T. & Butler-Purry, K. (2011). Towards Modelling the Impact of Cyber Attacks on a Smart Grid. *International Journal of Security and Networks, 6(1),* 2-13.

Laari, T., Flyktman, J., Härmä, K., Timonen, J., & Tuovinen, J. (2019). *#kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle* (Julkaisusarja 3: Työpapereita nro 12). Maanpuolustuskorkeakoulu: Sotataidon laitos.

Lacasse, S., Eidsvik, U., Nadim, F., Hoeg, K. & Blikra, L. (2008, May). Event tree analysis of Åknes rock slide hazard. *Geoscience Canada, 35(1),* 20-27.

Laliberte, M. (2016, 21. syyskuuta). A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack [blogikirjoitus]. Haettu 3.3.2020 osoitteesta https://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952

Lallie, H., Debattista, K. & Bal, J. (2020). A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review, 35.*

Lantis, J. (4.4.2006). Presentation on theme: Strategic Culture and Threat Assessment [PowerPoint-esitys]. Haettu 1.3.2020 osoitteesta http://slideplayer.com/slide/4271931/

Lantis, J. (2002). Strategic culture and national security policy. *International studies review, 4(3),* 87-113.

Lazar, M. (2012). The 2008 Russian Cyber Campaign Against Georgia. Teoksessa *International Scientific Conference "Strategies XXI" (500-505)*. Bucharest: National Defence University.

Lee, R., Assante, M. & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Washington, D.C.: Electricity Information Sharing and Analysis Center.

Lee, R., Assante, M. & Conway, T. (2014). German Steel Mill Cyber Attack. *Industrial Control Systems, 30,* 62-76.

Lee, W., Grosh, D., Tillman, F. & Lie, C. (1985). Fault Tree Analysis, Methods, and Applications ☍ A Review. *IEEE transactions on reliability, 34(3),* 194-203.

Lemos, R. (2009, 30. tammikuuta). Cyber attacks disrupt Kyrgyzstan's networks. Haettu 6.2.2020 osoitteesta https://www.securityfocus.com/brief/896

Lemos. R. (2014, 14. lokakuuta). Suspected Russian "Sandworm" cyber spies targeted NATO, Ukraine. Haettu 9.2.2020 osoitteesta https://arstechnica.com/information-technology/2014/10/suspected-russian-sandworm-cyber-spies-targeted-nato-ukraine/

LeVine, S. (2009, 24. elokuuta). Cyber-Attack Strategy: Part of Russian Attack on Georgian Pipelines: Report Finds. Hatti 8.2.2020 osoitteesta https://www.resilience.org/stories/2009-08-24/cyber-attack-strategy-part-russian-attack-georgian-pipelines-report-finds/

Lewis, J. (2015). *Operation Armageddon: Cyber espionage as a strategic component of Russian modern warfare*. LookingGlass Cyber Threat Intelligence Group.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica: Rand Corporation.

Liik, K. (2007). The "Bronze Year" of Estonia-Russia relations. *Estonian Ministry of Foreign Affairs Yearbook,* 71-76.

Lin, H. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy, 4*, 63-86.

Lincoln, Y., Lynham, S. & Guba, E. (2011). Paradigmatic Controversies, Contradictions, and Emerging Confluences, Revisited. *The Sage Handbook of Qualitative Research, 4,* 163-188.

Lipman, M. (2015). Putin's 'besieged fortress' and its ideological arms. Teoksessa N. Petrov & M. Lipman (toim.), *The State of Russia: What Comes Next? (110-136)*. London: Palgrave Pivot.

Lippmann, R., Ingols, K., Scott, C., Piwowarski, K., Kratkiewicz, K., Artz, M. & Cunningham, R. (2005). *Evaluating and Strengthening Enterprise Network Security Using Attack Graphs* (Project Report IA-2). Lexington: Massachusetts Institute of Technology.

Liu, X., Li, Z., Shuai, Z. & Wen, Y. (2016). Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution. *IEEE Transactions on Smart Grid, 8(2),* 1023-1025.

Lo, E. & Au, T. (2010). Improving the Kill Chain for Prosecution of Time Sensitive Targets. Teoksessa A. Brito (toim.), *Dynamic Modelling, (93-110)*. Rijeka: InTech.

Lobel, H. (2011). Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. *Texas International Law Journal, 47(3),* 617-640.

Luck, L., Jackson, D. & Usher, K. (2006). Case Study: A Bridge Across the Paradigms. *Nursing Inquiry, 13(2),* 103-109.

Lynch, D. (2005). 'The enemy is at the gate': Russia after Beslan. *International Affairs, 81(1),* 141-161.

Lynch, A. (2002). The Evolution of Russian Foreign Policy in the 1990s. *The Journal of Communist Studies and Transition Politics, 18(1),* 161-182.

Mackey, R. (2009, 5. helmikuuta). Are 'cyber-militias' attacking Kyrgyzstan. Haettu 6.2.2020 osoitteesta http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan

Malone, S. (2016, 4. elokuuta). Using an expanded cyber kill chain model to increase attack resiliency [PowerPoint-esitys]. Haettu osoitteesta https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf

Mauw, S. & Oostdijk, M. (2005). Foundations of attack trees. Teoksessa D. Won & S. Kim (toim.), *International Conference on Information Security and Cryptology, (186-198).* Heidelberg, Berlin, December 1-2, 2005.

Maybaum, M. & Ziolkowski, K. (2013). Technical Methods, Techniques, Tools and Effects of Cyber Operations. *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, (103-131),* Tallinn: NATO CCD COE Publication.

McDermott, R. (2010). Decision Making Under Uncertainty. Teoksessa *Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy, (227-241).* Washington, D.C.: National Academics Press.

McLaughlin, D. (2008, 2. heinäkuuta). Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites. Haettu 2.2.2020 osoitteesta https://www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155

Mehta, V., Bartzis, C., Zhu, H., Clarke, E. & Wing, J. (2006). Ranking Attack Graphs. Teoksessa *International Workshop on Recent Advances in Intrusion Detection, (127-144),* Heidelberg, Berlin, September 20-22, 2006.

Metsämuuronen, J. (2011). *Tutkimuksen tekemisen perusteet ihmistieteissä: tutkijalaitos.* Helsinki: International Methelp Ky.

Mishra, B. & Prajapati, A. (2013). Modelling and Simulation: Cyber War. Teoksessa A. Mukhopadhyay (toim.), *International Conference on*

Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013, (987-997), Kalyani, India, September 27-28, 2013.

Mixia, L., Qiuyu, Z., Hong, Z. & Dongmei, Y. (2008). Network Security Situation Assessment Based on Data Fusion. Teoksessa Q. Luo, M. Gong, F. Xiong & F. Yu (toim.), *First International Workshop on Knowledge Discovery and Data Mining (WKDD 2008), (542-545),* Adelaide, Australia, January 23-24, 2008.

Modderkolk, H. (2018, 25. tammikuuta). Dutch agencies provide crucial intel about Russia's interference in US-elections. Haettu 12.5.2020 osoitteesta https://cyber-peace.org/wp-content/uploads/2018/11/Dutch-agencies-provide-crucial-intel-about-Russias-interference-in-US-elections-_-De-Volkskrant.pdf

Monaghan, A. (2013). Putin's Russia: Shaping a 'Grand Strategy'? *International Affairs, 89(5),* 1221-1236.

Morrison, J. (1993). Pereyaslav and After: the Russian—Ukrainian relationship. *International Affairs, 69(4),* 677-703.

Mshvidobadze, K. (2015). *Georgia Cyber Barometer Report*. Tbilisi: Rondeli Foundation.

Mwiki, H., Dargahi, T., Dehghantanha, A. & Choo, K-R. (2019). Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. Teoksessa D. Gritzalis, M. Theocharidou & G. Stergiopoulos (toim.), *Critical Infrastructure Security and Resilience (221-244).* Cham: Springer.

Nachreiner, C. (2015, 10. helmikuuta). Kill Chain 3.0: Update the cyber kill chain for better defense. Haettu 11.3.2020 osoitteesta https://www.helpnetsecurity.com/2015/02/10/kill-chain-30-update-the-cyber-kill-chain-for-better-defense/

Nakashima, E. (2018, 12. tammikuuta). Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. The Washington Post, 12. Haettu 10.2.2020 osoitteesta https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html#comments-wrapper

Nanda, S., & Deo, N. (2007). A Highly Scalable Model for Network Attack Identification and Path Prediction. Teoksessa *Proceedings 2007 IEEE SoutheastCon, (663-668),* Richmond, The United States, March 22-25, 2007.

National Cyber Security Centre. (2018, 15. lokakuuta). Annual Review 2018. Haettu 1.5.2020 osoitteesta https://www.ncsc.gov.uk/annual-review/2018/ncsc/docs/ncsc_2018-annual-review.pdf

NATO. (2013). *Allied Command Operations Comprehensive Operations Planning Directive, COPD Interim V2.* Belgium.

Owens, W., Dam, K. & Lin, H. (2009). *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*. Washington, D.C.: National Academies Press.

Nazario, J. (2009). Politically Motivated Denial of Service Attacks. *The Virtual Battlefield: Perspectives on Cyber Warfare,* 163-181.

Newman, L. (2019, 7. toukokuuta). The Biggest Cybersecurity Crises of 2019 So Far. Haettu 11.2.2020 osoitteesta https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/

Nguyen, T., Wright, M., Wellman, M. & Baveja, S. (2017). Multi-stage Attack Graph Security Games: Heuristic Strategies, With Empirical Game-theoretic Analysis. Teoksessa H. Okhravi & X. Ou (toim.), *Proceedings of the 2017 Workshop on Moving Target Defense, (87-97),* Dallas, Texas, October, 2017.

Nichols, W., Hawrylak, P., Hale, J. & Papa, M. (2017). Introducing Priority Into Hybrid Attack Graphs. Teoksessa J. Trien, S. Prowell & J. Goodall (toim.), *Proceedings of the 12th Annual Conference on Cyber and Information Security Research, (1-4),* Oak Ridge, Tennessee, April, 2017.

Noel, S. & Jajodia, S. (2004). Managing Attack Graph Complexity Through Visual Hierarchical Aggregation. Teoksessa C. Brodley, P. Chan, R. Lippman & B. Yurcik (toim.), *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, (109-118),* Washington D.C., The United States of America, October, 2004.

Norberg, J. & Westerlund, F. (2014). *Russia and Ukraine: Military-strategic options, and possible risks, for Moscow* (Project No: A14101). Stockholm: Swedish Defence Research Agency.

Norvanto, E., Ruotsalainen, H. & Schroderus, J. (2019). *Venäjän vaikuttamistoimet Ukrainassa: paikallisväestön näkökulmia ja tulkintoja.* Tiede ja ase 77, 71-99.

Ortalo, R., Deswarte, Y. & Kaâniche, M. (1999). Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security. *IEEE Transactions on Software Engineering, 25(5),* 633-650.

Osawa, J. (2017). The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review, 24(2),* 113-131.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. Teoksessa D. Remenyi (toim.), *Proceedings of the 7th European Conference on Information Warfare, (163-168),* Plymouth, United Kingdom, June 30 – July 1, 2008.

Park, D., Summers, J. & Walstrom, M. (2017). *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*. University of Washington, Henry M Jackson School of International Studies.

Pernik, P. (2018). The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine. Teoksessa N. Popescu & S. Secrieru (toim.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies.* Paris: Institute for Security Studies.

Petersen, K. & Gencel, C. (2013). Worldviews, Research Methods, and Their Relationship to Validity in Empirical Software Engineering Research. Teoksessa *2013 Joint Conference of the 23rd International Workshop on Software Measurement and the 8th International Conference on Software Process and Product Measurement, (81-89),* Ankara, Turkey, October 23-26, 2013.

Pols, P. (2017). *The Unified Kill Chain: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks* (Väitöskirja). Cyber Security Academy. Haettu osoitteesta https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf

Press Secretary. (2018, 15. helmikuuta). Statement from the Press Secretary. Haettu 10.2.2020 osoitteesta https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

Quinlan, J. (1987). Generating Production Rules From Decision Trees. Teoksessa *Proceedings of the 10th international joint conference on Artificial intelligence - Volume 1 (304-307),* August 23-28, 1987.

Raitasalo, J. (2018). Hybridisota ja hybridiuhat-paljon vanhaa… onko mitään uutta? *Tiede ja ase, 76,* 27-53.

Rantapelkonen, J. & Koistinen, L. (2016). *Pohdintoja sotatieteellisistä käsitteistä* (Julkaisusarja 2: Tutkimusselosteita Nro 1). Maanpuolustuskorkeakoulu, Sotataidon laitos.

Raptis, D., Dimitrakos, T., Gran, B. & Stølen, K. (2002). The CORAS approach for model-based risk management applied to e-commerce domain. Teoksessa B. Jerman-Blazic & T. Klobucar (toim.), *Advanced Communications and Multimedia Security, (169-181)*, Portorož, Slovenia, September 27-27, 2002.

Reidy, P. & Randal, K. (2013). Combating the Insider Threat at the FBI: Real World Lessons Learned. Teoksessa *RSA Conference 2013*, San Francisco, California, February 25 – March 1, 2013.

Rhoads, C. (2009, 28. tammikuuta). Kyrgyzstan Knocked Offline. Haettu 6.2.2020, osoitteesta https://www.wsj.com/articles/SB123310906904622741

Rhodin, S. (2008, 1. heinäkuuta). Hackers tag Lithuanian web sites with Soviet symbols. Haettu 8.2.2020 osoitteesta http://www. nytimes. com/2008/07/01/world/europe/01baltic. html.

Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38(1-2),* 4-37.

Rios, B., Czosseck, C. & Geers, K. (2009). Sun Tzu was a hacker: An examination of the tactics and operations from a real world cyber attack. *The Virtual Battlefield: Perspectives on Cyber Warfare, 3,* 143-156

Roy, A., Kim, D. & Trivedi, K. (2010). Cyber security analysis using attack countermeasure trees. Teoksessa F. Sheldon, S. Prowell & R. Abercrombie (toim.), *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, *(1-4),* Oak Ridge, Tennessee, April, 2010.

Scarfone, K. & Mell, P. (2009). An analysis of CVSS version 2 vulnerability scoring. Teoksessa *2009 3rd International Symposium on Empirical Software Engineering and Measurement, (516-525),* Lake Buena Vista, Florida, October 15-16, 2009.

Sanghvi, H. & Dahiya, M. (2013). Cyber Reconnaissance: An Alarm Before Cyber Attack. *International Journal of Computer Applications, 63(6),* 36-38.

Schneier, B. (1999). Attack Trees. *Dr. Dobb's journal, 24(12),* 21-29.

Schroder, R. (1969). *Fault Trees For Reliability Analysis* (No. BNWL-SA-2522; CONF-700215-1). Richland: Pacific Northwest Lab.

Šešelgytė, M. (2010). Security Culture of Lithuania. *Lithuanian Foreign Policy Review, (24),* 23-40.

Shackelford, S. (2009). Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks. *Journal of Internet Law, November 4.*

Shakarian, P. (2011). The 2008 Russian cyber campaign against Georgia. *Military Review, 91(6),* 63-68.

Simos, M. (2018, 5. helmikuuta). Overview of Petya, a rapid cyberattack. Haettu 12.3.2020 osoitteesta https://www.microsoft.com/security/blog/2018/02/05/overview-of-petya-a-rapid-cyberattack/

Sindre, G. & Opdahl, A. (2005). Eliciting Security Requirements With Misuse Cases. *Requirements Engineering, 10(1),* 34-44.

Sinovets, P. (2016). From Stalin to Putin: Russian Strategic Culture in XXI Century, its Continuity and Change. *Philosophy Study, 7(6),* 417-423.

Snegovaya, M. (2015). *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Russia Report, 1). Washington, D.C.: Institute for the Study of War.

Snyder, J. (1977). *The Soviet Strategic Culture: Implications for Limited Nuclear Operations* (R-2154-AF). Santa Monica: Rand Corporation.

Staheli, D., Yu, T., Crouser, R., Damodaran, S., Nam, K., O'Gwynn, D., ... Harrison, L. (2014). Visualization Evaluation for Cyber Security: Trends and Future Directions. Teoksessa *Proceedings of the Eleventh Workshop on Visualization for Cyber Security (49-56).* New York: Association for Computing Machinery.

Stake, R. (2013). *Multiple Case Study Analysis*. (2. uud. painos). London: The Guilford Press.

Stake, R. 1995. *The Art of Case Study Research*. (9. uud. painos). London: SAGE Publications Ltd.

Stamatiou, Y.., Skipenes, E., Henriksen, E., Stathiakis, N., Sikianakis, A., Charalambous, E., … Papadaki, K. (2003). The CORAS Approach for Model-based Risk Management Applied to a Telemedicine Service. Teoksessa R. Baud, M. Fieschi, P. Le Beux & P. Ruch (toim.), *Medical Informatics Europe (MIE'2003) (206-211)*. Amsterdam: IOS Press.

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A. & Thomas, C. (2018). MITRE ATT&CK: Design and Philosophy (Project No.: 01ADM105-PI). Bedford: The MITRE Corporation.

Strom, B., Battaglia, J., Kemmerer, M., Kupersanin, W., Miller, D., Wampler, C., … Wolf, R. (2017). *Finding Cyber Threats With ATT&CK-based Analytics* (Project No.: 0716MM09-AA). Bedford: The MITRE Corporation.

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

Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. *Loyola of Los Angeles International and Comparative Law Review, 32,* 303-333.

Thomas, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies, 27(1),* 101-130.

Thomas, T. (2009). The Bear Went Through The Mountain: Russia Appraises Its Five-Day War in South Ossetia. *Journal of Slavic Military Studies, 22(1),* 31-67.

Tikk, E., Kaska, K. & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE).

Olin, P., Koivuniemi, M., Lehto, M., Luukkainen, K., Magd, N., Nevaste, N., … Suhonen, S. (2018). *Kyberturvallisuuden sanasto*. Helsinki: Sanastokeskus TSK ry.

Valdes, A. & Skinner, K. (2000). Adaptive, Model-based Monitoring for Cyber Attack Detection. *Teoksessa International Workshop on Recent Advances in Intrusion Detection, LNCS 1907 (80-93).* Berlin: Springer.

Vasquez, J. (1986). Capability, Types of War, Peace. *Western Political Quarterly, 39(2)*, 313-327.

Varuttamaseni, A., Bari, R. & Youngblood, R. (2017). *Construction of a Cyber Attack Model for Nuclear Power Plants* (No. BNL-113640-2017-CP). Upton: Brookhaven National Laboratory.

Volz, D. & Finkle, J. (2016, 12. tammikuuta). U.S. helping Ukraine investigate power grid hack. Haettu 9.2.2020 osoitteesta https://www.reuters.com/article/us-ukraine-cybersecurity-usa-idUSKCN0UQ24020160112

Waldo, D. (1980). *The Enterprise of Public Administration: A Summary View.* Novato: Chandler & Sharp.

Watson, F. (2017). Petya/NotPetya: Why It Is Nastier Than WannaCry and Why We Should Care. *ISACA Journal, Vol. 6*, 1-6.

Whitehead, D., Owens, K., Gammel, D. & Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. Teoksessa *2017 70th Annual Conference for Protective Relay Engineers (CPRE) (1-8),* College Station, Texas, April 3-6, 2017.

Williams, B. & Souza, R. (2016). Operation "Retribution": Putin's Military Campaign in Syria, 2015–16. *Middle East Policy, 23(4),* 42-60.

Xie, A., Cai, Z., Tang, C., Hu, J., & Chen, Z. (2009). Evaluating Network Security with Two-layer Attack Graphs. Teoksessa *Proceedings of the 2009 Annual Computer Security Applications Conference (127-136).* Washington D.C.: IEEE Computer Society.

Zetter, K. (2016, 3. maaliskuuta). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Haettu 9.2.2020 osoitteesta https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zoller, R. (2010). *Russian Cyberspace Strategy and a Proposed United States Response* (Pro gradu –tutkielma). U.S. Army War College.

Yadav, T. & Mallari, R. (2015). Technical Aspects of Cyber Kill Chain. Teoksessa J. Abawajy, S. Mukherjea, S. Thampi & A. Ruiz-Martínez (toim.) *International Symposium on Security in Computing and Communication, (438-452),* Kochi, India, August 10-13, 2015.

LIITE 1 KYBERHYÖKKÄYKSET VUOSINA 2007 - 2017

Vuosi	Kohteena ollut maa	Hyökkäyksen kohde
2007	Viro	Hallinto, media, liiketalous
2008	Liettua	Hallinto, yksityinen sektori
2008	Yhdysvallat	Vakoilu
2008	Georgia	Hallinto, media, liiketalous
2009	Kirgisia	ISP
2009	Etelä-Korea ja Yhdysvallat	Hallinto
2009	Google	Järjestelmät
2010	Iran	Ydinvoimalaitos
2011	Japani	Puolustussektori
2011	Japani	Hallinnon jäsen
2011	Yhdysvallat	Liiketalous
2012	Saudi-Arabia	Energiasektori
2013	Yhdysvallat	Media, ajatushautomot
2014	Etelä-Korea ja Yhdysvallat	Media, liiketalous
2014	Ukraina	Hallitus, viestintäsektori
2014	Belgia	Ulkoministeriö
2014	Yhdysvallat	Yksityinen sektori
2014	Yhdysvallat	Valkoinen talo
2014	Yhdysvallat	Sony Pictures
2015	Ranska	TV5
2015	Yhdysvallat	Hallinto
2015	Saksa	Hallinto
2015	Japani	Eläkejärjestelmä
2015	Ukraina	Energiasektori
2016	Bangladesh	Keskuspankki
2016	Ruotsi	Media
2016	Liettua	Parlamentti
2016	Vietnam	Lentokentät
2016	Saudi-Arabia	Hallinto, yksityinen sektori
2016	Yhdysvallat	Demokraattipuolue
2016	Ukraina	Energiasektori
2017	Japani	Kybervakoilu
2017	Maailmanlaajuinen	Lukuisat järjestelmät
2017	Maailmanlaajuinen	Lukuisat järjestelmät

Kyberhyökkäykset maailmalla (mukaillen Osawa, 2017, s. 116–117)