Jouni Ritola

KYBERVYÖRY

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Ritola, Jouni
Kybervyöry
Jyväskylä: Jyväskylän yliopisto, 2022, 83 s., 4 liitettä.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Tutkijat pyrkivät selittämään reaalimaailman loogisia tapahtumia syy-seuraussuhteella, jossa toimintaa seuraa vastatoiminta. Syy-seuraussuhteen lisäksi osalle onnettomuuksia on olemassa toinenkin selitys. Tämä selitys perustuu teoriaan, jonka mukaisesti väistämätön katastrofi on sisään rakennettu kompleksisiin järjestelmiin.

Tässä tutkimuksessa osoitetaan, miten kompleksisen järjestelmistä koostuvan kyberjärjestelmän komponentit ovat virittäytyneet itseorganisoidun kriittisyyden (*Self-Organized Criticality, SOC*) tilaan ja miten näiden komponenttien häiriöt aiheuttavat laajavaikutteisen normaalin onnettomuuden (*Normal Accident Theory, NAT*). Tutkimuksessa tätä väistämätöntä kyberonnettomuutta kutsutaan kybervyöryksi.

Tutkimus jakautuu kolmeen loogiseen kokonaisuuteen, joista ensimmäisessä käsitellään kybermaailmaa ja kompleksista järjestelmää monista näkökulmista ja määritetään tutkimuksen kannalta merkittävimmät käsitteet. Luvussa kuvataan kybermaailmaa uhkaavat uhat ja rakennetaan tätä kuvaava viitekehys. Toinen luku sisältää kolme onnettomuuksia kuvaavaa teoriaa, jotka analysoidaan hermeneuttisen käsiteanalyysin keinoin edellisen luvun viitekehyksen kautta katsottuna. Kolmannessa luvussa käsitemallit konstruoidaan yhdeksi kybervyöryä kuvaavaksi kokonaisteoriaksi ja vastataan tutkimuskysymykseen: Miksi kyberonnettomuuksia tapahtuu?

Asiasanat: *kyberympäristö, kyberturvallisuus, onnettomuus, normaalien onnettomuuksien teoria NAT, itseorganisoitunut kriittisyys SOC, voimalaki, kybervyöry*

ABSTRACT

Ritola, Jouni
Cyber Avalanche
Jyväskylä: University of Jyväskylä, 2022, 83 pp., 4 ap
Cyber Security, Master's Thesis
Supervisor(s): Siponen, Mikko

Scientists tries to explain logical events in the real world with a cause-and-effect relationship where action comes with reaction. In addition to the cause-and-effect relationship, there is another explanation for some of the accidents. This explanation is based on the theory that the inevitable catastrophe is built into complex systems.

This study demonstrates how cyber system can be treated like complex system of systems and how components of a that system are tuned into a state of self-organized criticality (*SOC*). Study shows how incidents of these components causes disastrous normal accident (*Normal Accident Theory, NAT*). In this study, this inevitable cyber-accident is called a cyber avalanche.

This study is divided into three logical parts. First one explains the cyberspace and the complex system from many perspectives and defines the most important concepts for this study. It also describes the threats to the cyberspace and builds a framework to describe this. The second part contains three accident theories, which are analyzed using hermeneutic conceptual analysis as a method. Theories are viewed through the framework from the previous part. In the third chapter, the conceptual models are constructed as one overall theory describing the cyber avalanche. At the end study uses this theory of cyber avalanche to answer the research question: Why do cyber accidents happen?

Keywords: *cyberspace, cyber security, accident, normal accident theory NAT, self-organizing criticality SOC, power law, cyber avalanche*

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Suomen kyberturvallisuusstrategia (2019) määrittää kyberturvallisuuden olevan tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristön synonyymina strategiassa käytetään digitaalista toimintaympäristöä, joka kehittyy yhteiskunnan osana ja palveluina nopeasti. Kyberympäristöön kohdistuu kuitenkin ilmiselvien mahdollisuuksien vastapainoksi merkittävä määrä uhkia, kuten perinteiset ihmisen tekemät virheet, mutta myös kehittyvät ja muuttuvat uhat, jotka voivat vaarantaa kriittisen infrastruktuurin kyberrikollisuuden, vakoilun, valtiollisen tiedustelun ja erilaisin hybridivaikuttamisen keinoin. (Turvallisuuskomitea, 2019).

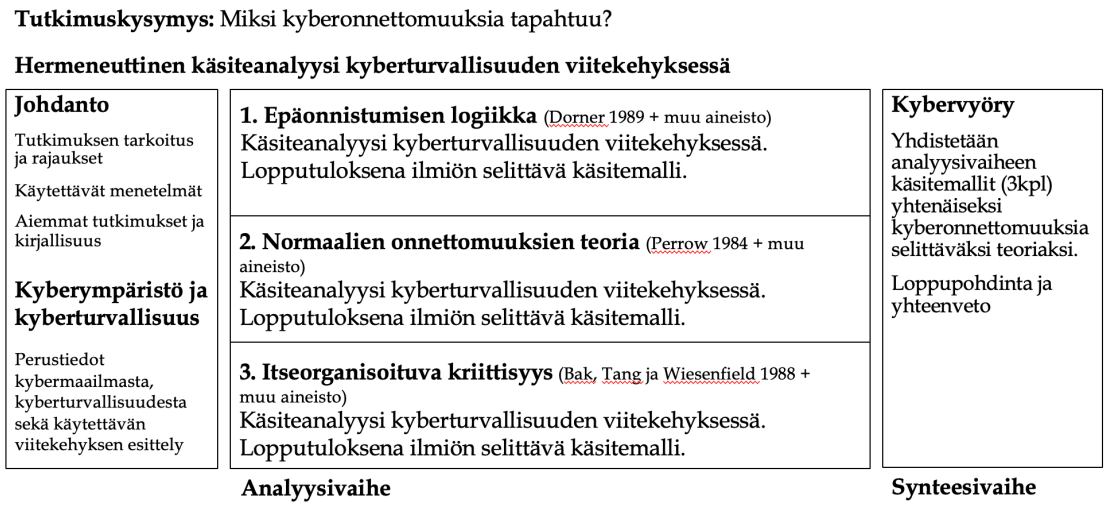
Näihin uhkiin vastataan kyberturvallisuudella, joka on Lehdon (2019a) mukaan *toimenpiteitä, joilla suojaudutaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteutetaan tarvittavia vastatoimenpiteitä*. Sanastokeskuksen (2018) ja Lehdon (2019a) mukaan kyberhyökkäys on käsitteenä synonyymi tietoverkkohyökkäykselle ja verkkohyökkäykselle, jolloin termi antaa kuvan taustalla olevasta tarkoituksenmukaisuudesta ja vihamielisestä toimijasta. Tämä tutkimus käsittelee kompleksisuudesta ja tiukoista kytkennöistä kumpuavaa sisäistä kriittisyyttä järjestelmissä, jolloin Lehdon määritelmää kyberturvasta laajennetaan kattamaan myös muunlaiset kybertapahtumat ja kyberonnettomuudet kuin varsinaiset hyökkäykset.

Jotta kybertuvallisuudella voidaan vastata uhkiin, tulee uhkat ja niiden taustalla olevat ilmiöt tuntea. Tämä tutkimus selvittää mitkä ilmiöt vaikuttavat kyberonnettomuuksien syntyyn. Tutkimuksessa käytetyn määritelmän mukaisesti *kyberonnettomuus on tahallisesti tai tahattomasti toteutunut kyberuhka, joka kohdistuu kybertoimintaympäristöön vaarantaen ympäristön ja siitä riippuvaisen toiminnon osittain tai kokonaan*. Itseorganisoituneen kriittisyyden (engl. *self-organized criticality, SOC*) teorian mukaan kompleksiset ja yhteen liitetyt järjestelmät, kuten kybertoimintaympäristöt, kasvavat, kunnes saavuttavat kriittisen pisteen ja romahtavat. (Bak, Tang ja Wiesenfield 1987).

Kyberympäristö on kompleksinen järjestelmistä koostuva järjestelmä, jonka sisäisiä riippuvuuksia ja vaikutuksia voi olla hankala tunnistaa ulkoapäin. Kybertapahtumat tai häiriöt voivat kohdistua yksittäisiin komponentteihin tai alijärjestelmiin fyysisellä, loogisella tai sosiaalisella kerroksella (Laari, Flyktman,

Härmä, Timonen & Tuovinen, 2019; Perrow, 1984). Tällaisten tapahtumien vaikutukset voivat levitä kerrosten sisällä ja välillä aiheuttaen arvaamattomia ja laajoja kokonaisvaikutuksia, jotka johtavat onnettomuuteen (Bak, 1996). Metaforana tälle on käytetty hiekkakasaa, jossa jokainen yksittäinen hiekanjyvä on merkityksetön, mutta jyvän yhdistyminen kasaan on ratkaisevan tärkeää. Näiden hiekanjyvien, eli kompleksisen järjestelmän yksiköiden ja osien muutoksia tutki Charles Perrow. Perrown (1984) mukaan käytämme elämämme reagoiden ja korjaten normaaleja onnettomuuksia, mutta jokainen korjaus, parannus tai järjestelmän optimointi lisää järjestelmän kompleksisuutta. Dörnerin (1989) tutkimuksen mukaisesti ihmiset eivät kuitenkaan ole kovin hyvä toimimaan kompleksisessa ympäristössä. Kokonaisuudessaan tämä ajaa kyberympäristöä kohti kriittistä pistettä ja vääjäämätöntä kybervyöryä.

Johdannon jälkeisessä luvussa lukijalle esitellään perustiedot kybertoimintaympäristöstä sekä siihen kohdistuvista uhkista ja toimijoista. Luvussa rakennetaan analyysivaiheessa käytettävä kyberturvallisuuden viitekehys. Luvun tarkoitus on antaa lukijalle perustiedot ja ymmärrys miksi kyberympäristöä voidaan käsitellä kompleksisena järjestelmien järjestelmänä, ja mitkä ovat sen erityispiirteet ja merkitys nykyaikaisessa modernissa yhteiskunnassa. Tutkimuksen rakenne on esitelty kuviossa 1.



KUVIO 1 Tutkimuksen rakenne

Analyysivaihe sisältää kolme onnettomuuksia kuvaavaa teoriaa, jotka käsittelevät kompleksisissa järjestelmissä tapahtuvia sisäsyntyisiä väistämättömiä onnettomuuksia. Teorioita tutkitaan harkinnanvaraisella otannalla kerätystä kirjallisuudesta käyttäen hermeneuttista analyysimenetelmää sekä käsiteanalyysiä. Jokaista kolmesta teoriasta analysoidaan edellä mainitun kyberturvallisuuden viitekehyksen kautta ja analyysin lopputuloksena tuotetaan käsitemalli kuvaamaan ilmiötä.

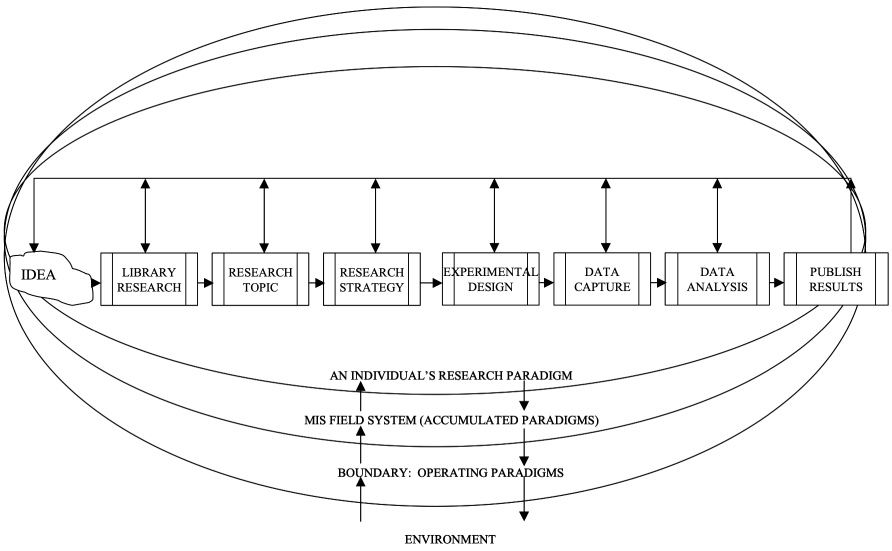
Käsitteellis-teoreettisessa tutkimuksessa analyysivaihetta seuraa synteesivaihe (Järvinen ja Järvinen, 2000), jossa konstruoidaan aiemmin rakennetuista kolmesta käsitemallista yksi yhteinen kyberonnettomuuksia kuvaava käsitemalli ja arvioidaan sen paikkaansa pitävyyttä ja jatkotutkimus mahdollisuuksia.

1.1 Tavoitteet ja menetelmät

Pro Gradu prosessin tavoitteena oli tuottaa aikaa kestävä tutkimus, joka tuottaisi uutta ja tarpeellista tietoa kyberturvallisuuden alueelle. Kyberturvallisuuden keskiössä on nimensä mukaisesti turvallisuus. Mutta ilman tuntemusta uhkista, on mahdotonta määrittää ja toteuttaa suojaavia kontrolleja tai vastatoimia. Turvallisuuden arviointi on myös vaikeaa, jos ei ole tietoa minkälaista uhkaa vastaan ollaan suojautumassa. Perinteiset kyberturvallisuuden hallinnan viitekehykset, kuten esimerkiksi *NIST Cybersecurity framework v1.1* (NIST, 2018), painottavat riskienhallintaa merkittävänä keinona tunnistaa uhat, niiden todennäköisyydet ja vaikutukset. NIST:n viitekehyksessä mainitaan erikseen huomioitaviksi näkökulmiksi järjestelmät, ihmiset, omaisuus, data ja kyvykkyydet. Viitekehyksen mukaisesti tunnistetuilta riskeiltä ja uhilta pyritään suojautumaan, niihin liittyviä tapahtumia pyritään havaitsemaan ja onnistuneisiin tapahtumiin vastaamaan unohtamatta palautumista ja resilienssiä.

Mutta onko asia näin yksinkertainen? Voidaanko uhkat tunnistaa riskienhallinnan keinoin vai onko olemassa jokin kategoria, joka jää järjestäen vaille huomiota? Tämän tutkimuksen tarkoitus on tarkastella kyberympäristöä kompleksisena järjestelmistä koostuvana järjestelmänä ja arvioida onko kyberjärjestelmä altis itseorganisoituneelle kriittisyydelle, normaaleille onnettomuuksille ja ihmisten tunnetuille toimintavirheille liittyen kompleksiseen ympäristöön. Tutkimus vastaa kysymykseen: *Miksi kyberonnettomuuksia tapahtuu*?

Tutkimus noudattaa soveltaen Jenkinsin (1985) tutkimusprosessin mallia, jossa tutkija etenee lineaarisesti ideasta valmiiseen julkaisuun. Huomattavaa prosessissa on kuitenkin takaisinkytkentä, joka mahdollistaa paluun aiempiin vaiheisiin ja huomioi täysin uudet tutkimusideat. Prosessimalli on kuvattu kuviossa 2 ja sisältää vaiheet: *idea, kirjallisuuskartoitus, tutkimusaihe, tutkimusstrategia, koesuunnittelu, tietojen keruu, tietojen analysointi ja tulosten julkaiseminen.*

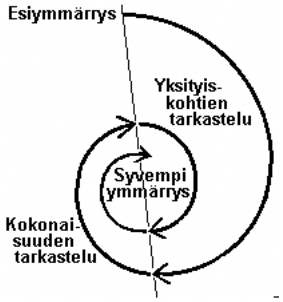


KUVIO 2 Jenkinsin (1985) malli tutkimusprosessista

Mallin mukaisesti tutkimus lähtee ideasta, joka Järvinen ja Järvinen (2000) mukaan on asiantila, joka askarruttaa. Siis jokin ongelma tai kysymys, johon halutaan vastaus. Tämän tutkimuksen osalta idean herätti Eric Saylorsin (2015) artikkeli *Cyber Gravity: The inevitable Collapse of our Technology*, jossa Saylors nostaa esille ajatuksen kybermaailmaa uhkaavasta neljännestä uhasta. Saylorsin mukaan yksilöiden, ryhmittymien ja valtiollisten toimijoiden lisäksi kybermaailmaa uhkaa voima, joka on vahva ja vastustamaton kuin maan vetovoima. Uhka on itseorganisoitunut kriittisyys, joka on sisäänrakennettu kompleksisiin järjestelmiin. Tutkimusprosessin mukaisesti ideasta siirrytään kirjallisuuskartoitukseen, jonka aikana käytiin läpi Saylorsin (2015) artikkelin taustamateriaali. Kirjallisuuskatsaus vahvisti tutkimusidean olevan relevantti tutkimuskohde akateemiseen tarkasteluun.

Valittu tutkimusaihe ja tutkimuskysymys ohjasi tutkimusstrategian valinnan kohti laadullista tutkimusta ja hermeneutiikan filosofista suuntausta. Hermeneutiikka oli alun perin metodi Raamatun selittämiseen ja tulkintaan, josta erotettiin 1600-luvulla kolme käyttöaluetta: Raamattu, klassinen antiikin kirjallisuus ja lakitekstit. Myöhemmin hermeneutiikkaan kehitettiin yleinen tulkintateoria, joka laajensi soveltamisalan minkä tahansa tekstin tulkintaan. (Siponen ja Klaavuniemi, 2021).

Hermeneuttisen tutkimuksen tarkoitus on sama kuin kaikessa humanistisessa tutkimuksessa, ymmärtää tutkittavaa kohdetta syvällisesti. Hermeneuttista kehää käytetään löytämään kirjoitetusta aineistosta asioita, joita siinä ei eksplisiittisesti näy. Tässä menetelmässä tutkija muodostaa tutkittavasta aiheesta esiymmärryksen, jota pyritään syventämään kuvion 3 mukaisesti. Syventämistä voidaan tehdä esimerkiksi näkökulmia vaihtamalla, jolloin ymmärrys aiheesta kasvaa ja palatessa takaisin alkuperäiseen näkökulmaan päästään myös siinä syvemmälle. Toinen käytettävä metodi on tarkastella tutkittavaa aihetta vuoroin kokonaisuutena ja vuoroin yksityiskohtien kautta. (Routio, 2004; Siponen, 2002).



KUVIO 3 Hermeneuttinen kehä, tai spiraali, Roution (2004) mukaan.

Reaalimaailman ilmiöitä tutkiessa hermeneuttiseen menetelmään voidaan yhdistää käsiteanalyysin menetelmä. Käsite-analyysi, eli käsitteellis-teoreettinen tutkimusote kuuluu Järvinen ja Järvinen (2000) esittelemän luokittelun mukaisesti reaalimaailmaa koskeviin tutkimusotteisiin ja on tarkoitettu tutkimaan millainen reaalitodellisuus on. Järvisen (2004) mukaan käsiteanalyysiä voidaan käyttää kahdella lähestymistavalla. Ensimmäinen tapa on lähteä olettamuksista ja johtaa niistä teoria, malli tai viitekehys. Tällöin tutkimuskysymys muotoiltaisiin hakemaan vastausta kysymykseen: *millainen teoria olisi pitävä, mikäli valitut olettamat*

ovat päteviä? Toinen tapa on analysoida aiempien empiiristen tutkimusten taustalla olevia olettamuksia, tunnistaa käytetyt teoriat, mallit ja viitekehykset. Tämän jälkeen näiden yhdistämiseen sovelletaan loogista päättelyä. Tässä tapauksessa tutkimuskysymys voidaan kirjoittaa muotoon: *onko olemassa yleistä teoriaa, joka selittää ilmiön?* Tämä jälkimmäinen vaihtoehto Järvisen (2004) kuvaamista käsiteanalyysin malleista soveltuu tämän tutkimuksen tarpeisiin hyvin yhdessä hermeneuttisen kehän kanssa ja mahdollistaa käytettävän aineiston keräyksen harkinnanvaraisen otannan menetelmällä.

1.2 Kirjallisuus

Monimutkaisten järjestelmien, kuten hiekkakasojen (Bak, Tang, Wiesenfield, 1997), sähkökatkojen (Carreras, Newman, Dobson, & Poole, 2000), maanjäristysten (Scholz, 1990) ja jopa biologisen evoluution (Sole, Manrubia, Benton. & Bak, 1997) muutoskäyttäytymisen ymmärtämisestä on saatu paljon tietoa tutkimusten kautta. Kaikkia näitä järjestelmiä voidaan pitää kompleksisina, koska mikään yksittäinen tapahtuma tai ominaisuus ei voi hallita järjestelmään kohdistuvia muutoksia koko evoluution ajalla. Muutokset kompleksisessa järjestelmässä voivat olla minkä kokoisia tahansa ja tapahtua milloin tahansa. Esimerkiksi sähkökatko voi iskeä kadulle, kaupunkiin, tai vielä laajemmin. Mielenkiintoinen näkökulma kompleksisissa järjestelmissä on, että Bak'sin ja kollegoiden (1987) mukaan niiden tilastollisia ominaisuuksia voidaan mitata voimalain (engl. *power law*) avulla. Samoin Perrow (1984) ja Dörner (1989) esittivät omat teoriansa selittämään syitä muutoksille ja onnettomuuksille kompleksisissa järjestelmissä.

Onnettomuusteorioita käsittelevän analyysivaiheen aineiston keruu pohjautui kolmeen pääteokseen, jota laajennettiin käyttäen näissä teoksissa olleita pohjatutkimuksia ja lähteitä sekä tekemällä verkkohakuja tavoitteena löytää aineistoa, jossa on viitattu samoihin ydinteoksiin. Löydetystä aineistosta rajattiin suoraan pois sellaiset teokset, jotka eivät liity suoraan tutkittavaan kokonaisuuteen tai ovat täysin eriltä toimialalta eivätkä yleistettävissä. Ydinteokset olivat Per Bakin kirja *How Nature Works, the science of self-organized criticality* vuodelta 1996 sekä kirjan pohjalla ollut Bakin, Tangin ja Wiesenfieldin tutkimus *Self-Organized Criticality: an Explanation of the 1/f Noise* vuodelta 1987. Toisena ydinteoksena oli Perrow:n kirja *Normal Accidents: Living With High-Risk Technologies* vuodelta 1984. Kolmas ydinteos oli Dörnerin *The Logic of Failure: Why things Go Wrong and What We Can Do to Make Them Right* vuodelta 1989 sekä tähän pohjautuva samanniminen Dörnerin, Nixonin ja Rosen keskustelupaperi vuodelta 1990.

Aiempaa tutkimusta, jossa tässä tutkimuksessa käsiteltäviä teorioita olisi pyritty syntesoimaan yhdeksi kompleksisten järjestelmien muutoksia kuvaavaksi teoriaksi tai jossa yksittäisten teorioiden sovittamista kyberjärjestelmän laajuuteen olisi tehty, ei löytynyt. Tämän sijaan yksittäisiä teorioita on sovitettu yksittäisiin kyberjärjestelmän alijärjestelmiin, yksiköihin ja osiin.

Onnettomuusteorioita ja kybermaailmaa yhdistäviä aiempia tutkimuksia haettiin digitaalisista lähteistä esimääriteltyjen hakusanojen avulla. Käytetyt hakukoneet olivat *ResearchGate*, *ScienceDirect* ja *Google Scholar*. Käytetyt hakusanat

sisälsivät aina jommankumman pääteorian onnettomuuksien takana sekä viitekehyksestä tulevan hakusanan *ja* -operaattorilla käytettynä. Hakutuloksiin otettiin siis vain sellaiset tulokset, joissa molemmat hakusanat täyttyivät. Käytetyt hakusanat olivat:

- "self-organized criticality" AND security
- "self-organized criticality" AND cyber
- "self-organized criticality" AND internet
- "self-organized criticality" AND “critical infrastructure”
- "self-organized criticality" AND “information systems”
- “normal accident” AND security
- “normal accident” AND cyber
- “normal accident” AND internet
- “normal accident” AND “critical infrastructure”
- “normal accident” AND “information systems”
- “normal accident" AND "self-organized Criticality “

Kokonaisuudessaan hakutulokset tuottivat n. 200 tutkimusta, kirjaa tai muuta akateemista artikkelia. Sama artikkeli nousi tuloksiin kuitenkin useammalla haulla, joten todellinen yksittäisten löydösten määrä lienee noin 100 kpl. Johtuen tulosten suuresta määrästä, menetelmänä päädyttiin käyttämään harkinnanvaraista otantaa (KvantiMOTV, 2013). Hakutuloslista käytiin läpi otsikkotasolla ja mukaan poimittiin sellaiset artikkelit, jotka olivat otsikon perusteella selkeästi aihepiiriltään tutkimukseen soveltuvia, eli tietoturvallisuuteen, kokonaisturvallisuuteen tai kyberturvallisuuteen liittyviä ja joissa käsiteltiin tässä tutkimuksessa käytettyjä teorioita. Niiden aineistojen tiivistelmät luettiin, joiden osalta päätöstä ei voinut tehdä pelkän otsikon perusteella. Valtaosa löydetyistä aineistosta oli kuitenkin toisilta toimialoilta, kuten biologiasta ja lääketieteestä tai aihepiiriltään niin suppeita etteivät ne soveltuneet aineistoksi tähän tutkimukseen. Lopullisia mukaan valittuja aineistoja, joiden pohjalta muodostettiin ymmärrys aiemmasta tutkimuksesta, oli yksitoista kappaletta.

1.3 Aiemmat tutkimukset

Ohjelmistojen evoluutiota sekä ohjelmistokehityksen menetelmiä on tutkittu jonkin verran suhteessa itseorganisoituneeseen kriittisyyteen. Kyberjärjestelmät koostuvat usein yhdistelmästä perinteisiä suljettuja järjestelmiä sekä avoimen lähteen järjestelmiä. Suljetulla järjestelmällä tarkoitetaan ohjelmistoa, joissa lähdekoodi ei ole vapaasti saatavilla ja muokattavissa ja sen käyttöä on rajoitettu lisenssein. Huomattavaa kuitenkin on, että suljettu järjestelmä voi sisältää avoimen lähteen komponentteja, jolloin avoin lähdekoodi ja menetelmät sen kehittämiseen ovat merkittävässä roolissa arvioidessa järjestelmän kokonaisturvallisuutta. Avoimen lähteen järjestelmien suhdetta itseorganisoituneeseen kriittisyyteen on tutkittu projektitasolla, tiedostotasolla ja koodirivientasolla. Seuraavaksi

käydään läpi joitain normaalien onnettomuuksien teoriaa tai itseorganisoitunutta kriittisyyttä koskevia tutkimuksia. Näitä käsitellään luvuissa kolme ja neljä tarkemmin.

Lehmanin (1997) tutkimus ohjelmistoevoluution laeista esittää, että ohjelmistojen tulee jatkuvasti adaptoitua ulkoisten vaatimusten, kuten uusien toiminnallisuuksien, fyysisten komponenttien muutosten ja liiketoiminnan vaatimusten täyttämiseksi. Avoimen lähdekoodin järjestelmiä kehitetään käyttäen vähemmän tiukkoja kontrolleja ja hallintamalleja verrattuna perinteisiin suljettujen ohjelmistojen kehitysmalleihin. Madeyn (2002) ja Kochin (2004) tutkimukset esittävät, että avoimen lähdekoodin projektit voidaan nähdä itseorganisoituneena ilmiönä, jossa toimijat valitsevat itse tehtävänsä ja jossa yhteistyö ja johtajuus on spontaania.

Wu, Spitzer, Hassan ja Holt (2004) osoittivat lähdekoodeja tutkimalla, että *OpenSSH*, *PostgreSQL* ja *Linux k*ernel ovat kehittyneet pitkän ajan kuluessa ja kehityksen elinkaaressa on nähtävissä toistuvia rauhallisia pienten muutosten vaiheita, joita seuraa suurten vyörymäisten muutosten vaiheet. Tämä noudattaa Bak'sin (1996) mallia pisteytetystä tasapainosta (engl. *punctuated equilibrium*), jonka mukaisesti kompleksisten SOC-järjestelmien kehitys ei ole tasaista ja lineaarista kuten Darwinin evoluutioteoria kuvaa, vaan maailma kehittyy romahdusten kautta, jolloin elämä on kulkua katastrofista toiseen epämääräisen pituisten vakaiden ajanjaksojen kautta.

Wu, Holt ja Hassan (2007) tutkivat yhdentoista laajan avoimen lähteen järjestelmän loogisia ja rakenteellisia muutoksia. Tutkimuksen tuloksena esitettiin kaksi voimalakiin liittyvää ilmiötä, joiden mukaan ohjelmistomuutosten todennäköisyysjakauma pienenee muutoskokojen tehofunktiona, ja ohjelmistomuutosten aikasarjat osoittavat pitkän kantaman korrelaatioita teholain käyttäytymisen kanssa. Tällainen spatiaalinen (koko järjestelmän läpäisevä) ja temporaalinen (koko elinkaaren kattava) voimalakia noudattava malli osoittaa Bak's ja kollegoiden (1988) mukaisesti, että itseorganisoitunutta kriittisyyttä esiintyy avoimenlähdekoodin järjestelmissä. Tutkimusten mukaisesti SOC voi olla hyvä konseptillinen viitekehys auttamaan ymmärtämään ohjelmistojen evoluutiota (muutosten ja kasvun syyt ja mekaniikka).

Nunan ja Domenico (2017) tutkivat NAT-teoriaa big datan kautta ja tulivat tulokseen, että organisaatiot, jotka keräävät ja hyödyntävät big dataa, ovat alttiita normaaleille onnettomuuksille johtuen heikkouksista organisaation prosesseissa sekä big datan keräyksen ja käsittelyn mahdollistavista järjestelmistä.

Conrad ja Oman (2007) tutkivat haittaohjelmien leviämistä vuosien 1995 ja 2006 välillä ja löysivät sekä temporaaliset että spatiaaliset todisteet SOC:n mukaiselle käytökselle. Spatiaaliset todisteet tarkoittavat, että viruksen saastuttamien kohteiden määrä noudattaa voimalain mukaista kaavaa. Temporaaliset todisteet puolestaan osoittivat, että yksittäisen viruksen esiintyminen (elinkaari) noudattaa myös voimalain mukaista kaavaa. Voimalaki esitellään luvussa kolme. Kokonaisuudessaan tämä tarkoittaa sitä, että perinteiset tilastolliset jakaumat, kuten Gaussin kellokäyrä, voi aliarvioida tuhoisten virusepidemioiden esiintymistä, sillä Gaussin normaalijakaumalla niiden todennäköisyys on pienempi kuin voimalain mukaisella jakaumalla.

Lewis (2010) on tutkinut SOC ja NAT teorioita pääosin kriittisen infrastruktuurin ja kotimaan turvallisuuden (Yhdysvaltojen) näkökulmasta. Lewisin havainto on, että voimalain mukaista toistuvuutta noudattavien onnettomuuksien taustalla on syy-seuraussuhteen sijaan voimalakia noudattava satunnaisuus. Mauro, Diehl, Marcellin Jr, ja Vaughn (2018) ovat tutkineet työtapaturmia Yhdysvaltojen työvoimaviranomaisen tilastoista. Tutkimuksessa havaittiin, että onnettomuudet, jotka aiheuttavat poissaoloa töistä, noudattavan voimalakijakaumaa sekä onnettomuuksien määrässä että kestossa.

Sähkönsiirtoverkot kehittyvät ajan myötä itseorganisoituneen periaatteen mukaisesti kriittiseen pisteeseen, joka tarkoittaa, että niitä ajetaan lähellä maksimi kapasiteettia, jolloin kuorman kasvaessa ne ovat vaarassa kaatua. Globaalisti kerätty data katkoista ja häiriöistä osoittaakin, että suuret sähkökatkot noudattavat voimalakijakaumaa. (Dobson, Carreras, Lynch & Newman, 2007). Kriittiseen tilaan kehittyneisiin sähköverkkoihin voidaan iskeä myös kybervaikuttamisen keinoin ja aiheuttaa fyysistä tuhoa kuten esimerkiksi Stuxnetin tapauksessa. Stuxnetin tapauksessa kyse oli iskusta ydinmateriaalin rikastusprosessiin ei sähköverkkoon, mutta yhtä lailla kyberiskulla vaikutettiin kineettiseen maailmaan. Kyberiskulla aiheutettu sähkökatko voi olla tutkimuksen arvion mukaan laajempi ja tuhoisampi kuin luonnollisesti aiheutunut. (Sheng, Yingkun, Yuyi, Yong, & Yu, 2011).

Dorner (2014) arvioi analogisen aikakauden NAT ja HRO teorioiden soveltuvuutta digitaaliseen aikakauteen ja tietojärjestelmiin. Tutkimuksen mukaisesti normaaleja onnettomuuksia tapahtuu sekä tietojärjestelmien sisällä yksittäisten alijärjestelmien ja komponenttien vikaantuessa, mutta myös laajemmin organisaatiojärjestelmässä, jossa tietojärjestelmä näyttelee vain yhtä alijärjestelmää. Dornerin mukaan molemmat teoriat soveltuvat myös nykyaikaan ja antavat kaksi tärkeää näkökulmaa onnettomuuksien ehkäisyyn.

Martínez, Eng ja Kim (2012) esittivät tutkimuksessaan, että tietoverkot ovat kompleksisia ja tiukasti yhteen kytkettyjä teknologisia järjestelmiä, jolloin ne täyttävät NAT-teorian ominaispiirteet. Tämän perusteella tutkimuksessa päädytään siihen, että tietoverkot ovat liian kompleksisia, jotta ne voidaan pitää turvallisina ja luotettavina ja että siihen kohdistuvat häiriöt ja onnettomuudet ovat normaaleja, eli odotettavia.

Faloutsos, Faloutsos ja Faloutsos (1999) tutkivat internetin fyysistä topologiaa kolmena ajanhetkenä vuosien 1997 ja 1998 välillä ja havaitsivat verkon laajentumisen noudattavan voimalain mukaista jakaumaa. Tulosten perusteella erilaisia verkkokonfiguraatioon liittyviä parametreja voidaan arvioida ja täten rakentaa realistisempia simulaatioita verkosta.

Bibighaus (2015) vertaili artikkelissaan perinteistä kineettistä sodankäyntiä ja kybersodankäyntiä. Tutkijan mukaan kineettisten aseiden tehokkuus noudattaa normaalijakaumaa, kun kyberaseet puolestaan noudattavat voimalain mukaista jakaumaa. Tämä tarkoittaa käytännössä sitä, että kyberaseilla kyetään tekemään iskuja, joiden tehokkuus yllättää toimijat, jotka olettavat perinteistä gaussilaista normaalijakaumaa. Normaalijakauman mukaisesti riittää, että ymmärretään ja arvioidaan vastustajan keskimääräinen voima ja keskihajonta. Voimalain mukaisesti toimiessa ääripäiden voimakkuudet eroavat normaalista merkittävästi.

Tässä luvussa esiteltiin tutkimuksen aihealue, käytettävät tieteelliset menetelmät sekä tutkimuksen rakenne. Luvussa kuvattiin käytettävä kirjallisuus, menetelmät sen hankintaan sekä aiheesta tehty aiempi tutkimus. Seuraavassa luvussa esitellään kybermaailman sen rooli ja vaikutus nykyaikaisessa digitaalisessa maailmassa sekä määritetään tämän tutkimuksen kannalta oleellisimmat käsitteet. Luvussa esitetään kyberjärjestelmiä uhkaavat uhat ja rakennetaan viitekehys, jonka kautta luvun kolme teorioita voidaan tarkastella.

2 KYBERMAAILMA – NEUROMANCERISTA LAZARUKSEEN

Tässä luvussa kuvataan kybertoimintaympäristö sekä sen keskeisimmät termit ja määritelmät. Ensimmäinen kappale kuvaa järjestelmäteorian ja kompleksisuusteorian sekä perustelee, miksi kyberympäristöä voidaan käsitellä kompleksisena järjestelmänä. Toinen kappale käsittelee kyberympäristön roolia osana fyysistä maailmaa, kriittistä infrastruktuuria ja jokapäiväistä elämää. Kolmas kappale kuvaa mitä kyberturvallisuus on ja miten se eroaa tietoturvasta käsitteenä. Kappale esittelee kyberturvallisuusuhat, uhkatoimijat, uhkatoimijoiden motivaatiot ja käyttämät metodit. Kappaleen lopuksi käydään läpi kyberonnettomuuden käsitettä esimerkin kautta.

Kybermaailma on suhteellisen nuori ja voimakkaasti kehittyvä. Tästä johtuen kybermaailmalle ei ole maailmanlaajuisesti hyväksyttyä termistöä ja samalla termillä onkin eri maissa hieman eri tarkoitus tai sävy. Esimerkiksi USA käyttää kyberturvallisuustermiä viittaamaan kriittiseen infrastruktuuriin. Australiassa puolestaan samalla termillä viitataan yleisemmin tieto- ja viestintätekniikkaan, kun saksalaiset puolestaan puhuvat kyberavaruudesta. Kyberavaruus on saksalaisen määritelmän mukaan virtuaalinen tila, jossa kaikki tietojärjestelmät ovat globaalisti kytkeytyneet toisiinsa data tasolla. (Lehto, 2019b). Tässä tutkimuksessa käytetään suomalaista termistöä, joka on kerätty pääosin turvallisuuskomitean ja puolustusvoimien julkaisuista.

Ennen kuin valtiot alkoivat puhumaan vakavissaan kyberavaruudesta, oli termi tuttu lähinnä William Gibsonin 1984 julkaisemasta romaanista *Neuromancer*. Romaanissa kyberavaruus kuvattiin paikaksi, jossa ihminen voi kulkea ja toimia virtuaalisessa toimintaympäristössä yhdessä kehittyneen keinoälyn kanssa. Neljäkymmentävuotta myöhemmin kuvaus alkaa olla kohtalaisen osuva. Sana *kyber* tulee kreikan sanasta *"kybereo" -ohjata, opastaa, hallita*, mutta kuten Laari, Flyktman, Härmä, Timonen ja Tuovinen (2019) totesivat, kyber-sanaa ei käytetä yksistään juuri koskaan, eikä sille ole sellaisenaan mielekästä määritelmää. Sanan merkitys liittyy digitaalisessa muodossa olevan informaation siirtoon, tallennukseen ja käsittelyyn ja yleensä se liitetään toiseen käsitteeseen etuliitteeksi. Näin muodostetulla yhdyssanalla voidaan katsoa olevan oma merkityksensä. Kyberetuliitettä käyttäen, mikä tahansa fyysisen maailman ilmiö voidaan siirtää

kybermaailman viitekehykseen laajentaen sanan alkuperäistä merkitystä. Esimerkiksi kybersota tarkoittaa sotimista digitaalisessa toimintaympäristössä tai kineettisen sodan laajentamista digitaaliseen ympäristöön. (Laari ja kollegat, 2019).

Kybertoimintaympäristö on laaja ja voi olla vaikeasti hahmotettava. Turvallisuuskomitean toimeksiannosta sanastokeskus (2018) määritteli kyberturvallisuuden sanaston ja käsitemallit helpottamaan asian viestintää niin asiantuntijoille kuin suurille yleisöille. Tämän määritelmän mukaisesti kybertoimintaympäristö on yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö. Laari ja kollegat (2019) lisäävät tähän määritelmään fyysiset rakenteet, jotka mielestäni kuuluvat myös oleellisena osana mukaan. Varsinkin kun asiaa tarkastellaan kyberturvallisuuden ja kriittisen infrastruktuurin näkökulmasta. Fyysisiä rakenteita ovat esimerkiksi tietovoimalat, käyttöpisteet, ohjattavat laitteet, päätelaitteet ja kaiken tämän yhdistävä verkko.

Fyysisen ja loogisen digitaalisen kerroksen lisäksi kyberympäristöön kuvataan usein myös toimijat. Näin saadaan kuvion 4 mukainen kolmitasoinen viitearkkitehtuuri kybertoimintaympäristöstä. Esimerkkinä tästä ovat digitaalisella toiminnanohjausjärjestelmällä ohjatut tehtaat ja voimalat, pankki- ja maksujärjestelmät, Logistiikkajärjestelmät (Sanastokeskus, 2018). Lehto (2019a) kuvaa kybermaailmaa viisikerroksisella OSI-mallia mukailevalla jaottelulla, joka eroaa yllä esitetystä kolmikerroksisesta mallista siten, että looginen kerros on jaettu syntaktiseen, semanttiseen ja palvelukerrokseen. Tässä tutkimuksessa käytetään kuvion 4 mukaista kolmitasoista mallia.

KUVIO 4 Kybertoimintaympäristön kolme tasoa

2.1 Kompleksinen järjestelmien järjestelmä

Perrow (1984) määrittää systeemiteorian mukaisesti järjestelmän olevan kompleksinen, kun se sisältää vuorovaikutuksia, joita esiintyy suunnittelemattomissa ja tuntemattomissa jaksoissa ja jotka eivät heti ole ymmärrettäviä. Toisin sanoen kompleksista interaktiivisuutta, kuten tuntemattomia palautesilmukoita esiintyy

silloin kun vuorovaikutusta ei täysin ymmärretä. Kompleksisuusteoria jakaa yhteistä sanastoa systeemiteorian kanssa, mutta tästä huolimatta kyse ei ole samasta asiasta (Phelan, 1999). Kompleksisuusteoria eroaa systeemiteoriasta siinä, että kun systeemiteorian mukaisesti kompleksisuus johtuu komponenttien välisestä vuorovaikutuksesta, niin kompleksisuusteorian mukaisesti kompleksisuus on järjestelmän perusominaisuus. Kompleksiselle järjestelmälle on ominaista, että se sisältää mukautuvia prosesseja, jotka valitsevat tehokkaan toimintatavan monimutkaisessa maailmassa (Murray, 2003; Zwick, 1997; Bar-Yam, 2002). Kompleksinen järjestelmä noudattaa paikallisia sääntöjä, joka tarkoittaa, ettei ole olemassa ylempää tahoa, joka määrittäisi tarkasti erilaiset mahdolliset vuorovaikutukset ja niiden seuraukset (Johnson, 2001).

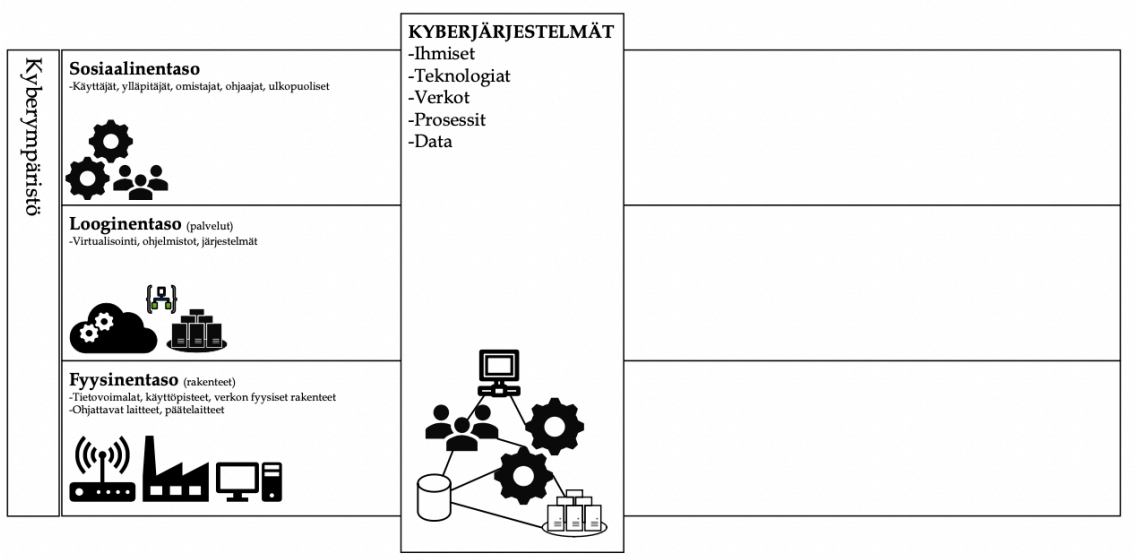
Kompleksinen järjestelmä eroaa kaoottisesta järjestelmästä siten, että kaoottinen järjestelmä muodostuu vakioiden sääntöjen ja säännönmukaisuuksien iteroinnista, kun taas kompleksinen järjestelmä kehittyy ja muuttaa vuorovaikutuksen sääntöjä. Kaoottisen järjestelmän lopputulosta ei voida ennustaa lähtötilanteen perusteella ja sen metaforana käytetään usein perhosvaikutusta, jossa äärimmäisen pieni muutos alkuvaiheessa aiheuttaa suuria muutoksia lopputulokseen. (Aula, 1999). Esimerkiksi perhosen siiven räpäytys Suomessa aiheuttaa tulvan Brasiliassa. Teorioiden käsitteellistä eroavaisuutta on havainnollistettu alla olevalla taulukolla 1.

Taulukko 1 Systeemi-, kompleksisuus- ja kaaosteoria

Systeemiteoria	**Kompleksisuusteoria**	**Kaaosteoria**
Kompleksisuus johtuu komponenttien välisestä interaktiosta	Kompleksisuus on järjestelmän ominaisuus	Kompleksisuus johtuu muuttumattomien sääntöjen ja säännönmukaisuuden iteroinnista

Riippumatta siitä onko kompleksisuus järjestelmän ominaisuus vai vuorovaikutuksen tulos, tarkoittaa kompleksisuus monimutkaisuutta, joka aiheuttaa sen, että kyberjärjestelmä on enemmän kuin osiensa summa. Kompleksiset järjestelmät voidaan purkaa osiin, jotka voidaan edelleen purkaa osiin, kunnes päädytään samoihin alkuainehiukkasiin, joista kaikki eloton ja elollinen on muodostunut. Järjestelmän toimivuus tai toimimattomuus ei siis johdu sen osista, vaan siitä miten osat toimivat yhteen ja tämä on erityistä jokaiselle järjestelmälle (Bar-Yam, 2002).

Yhdestä tai useammasta tietojärjestelmästä koostuva kybertoimintaympäristö voidaan myös purkaa osiin, jotka itsessään ovat kompleksisia järjestelmiä koostuen monimutkaisista sosiofyysisistä ja teknologisista vuorovaikutusverkostoista. Esimerkiksi Raggadin (2010) määritelmän mukaan tietojärjestelmä koostuu ihmisistä, teknologioista, tietoverkoista, prosesseista ja datasta. Tämä määritelmä soveltuu tämän tutkimuksen tarpeisiin ja voidaan lisätä aiemmin esiteltyyn kyberympäristön kolmitasoiseen rakenteeseen (kuvio 5).



KUVIO 5 Kyberjärjestelmät osana kolmitasoista kyberympäristöä

Esimerkkinä kompleksisesta järjestelmien järjestelmästä voidaan esittää perinteisen kolmikerrosarkkitehtuurin mukainen tietojärjestelmä, joka koostuu tietovarannosta, liiketoimintalogiikkakerroksesta sekä käyttöliittymästä. Jokainen näistä kolmesta komponentista voidaan edelleen purkaa osiin, jotka ja ovat yksinään suhteellisen hyödyttömiä. Yhdessä niistä voidaan kuitenkin muodostaa järjestelmä, jolla voidaan hoitaa esimerkiksi sairaalan työvuorolistaa. Työvuorolistajärjestelmä puolestaan voi olla liitetty osaksi sairaalan toiminnanohjausjärjestelmää, jolloin muutokset, viat ja ongelmat yksittäisessä komponentissa voivat aiheuttaa esimerkiksi leikkausoperaation peruuntumisen joka puolestaan voi vaikuttaa kohtalokkaasti potilaaseen.

Tässä kappaleessa esiteltiin kyberympäristön keskeisimmät käsitteet ja niiden määritelmät. Kappaleessa käytiin läpi systeemiteorian ja kompleksisuusteorian taustaa ja perusteltiin, miksi kyberjärjestelmää voidaan käsitellä kompleksisena järjestelmänä. Seuraavassa kappaleessa käsitellään kyberympäristön roolia modernissa yhteiskunnassa.

2.2 Kyberympäristön rooli ja vaikutus modernissa yhteiskunnassa

Digitaalinen ja fyysinen maailma lähentyvät toisiaan kasvavalla vauhdilla, ja voidaankin todeta, että fyysinen maailma on monelta osin riippuvainen digitaalisesta maailmasta. Tämän kappaleen tarkoitus on kuvata esimerkkien kautta, mikä on digitaalisen kyberympäristön rooli ja vaikutus modernissa yhteiskunnassa.

Esineitä, laitteita ja kulkuneuvoja ohjataan yhä enenevissä määrin digitaalista tietoa käsittelemällä. Kybermaailmassa siviili- ja sotilasinfrastruktuurit ovat osittain päällekkäisiä, joka aiheuttaa vastuunjaolle ja valvonnalle haasteita,

mutta tarjoaa myös yhteistoimintamahdollisuuksia. (Liikenne- ja viestintäministeriö, 2001; Laari ja kollegat, 2019). Tämä lisää kyberympäristön kompleksisuutta, tiukkoja kytköksiä, monikäyttöisiä komponentteja sekä niiden välisiä yllättäviä riippuvuuksia ja vaikutuksia. Nämä ovat onnettomuudelle alttiin järjestelmän ominaispiirteitä kuten kolmannessa luvussa tulee esille.

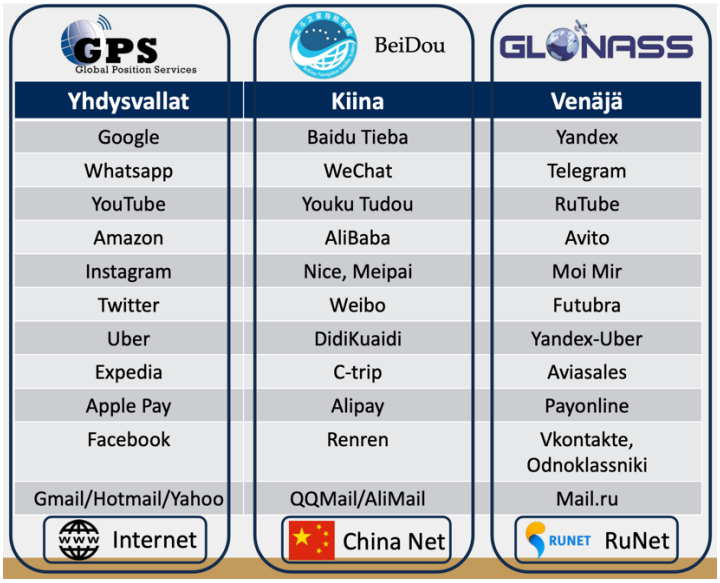
NIS-direktiivi, eli Euroopan verkko- ja tietoturvadirektiivi, määrittää yhteiskunnan kriittisen infrastruktuurin koostuvan *energia, terveydenhuolto, finanssiala, finanssialan infrastruktuuri, liikenne, vesihuolto, digitaalinen infrastruktuuri sekä digitaaliset palvelut* -toimialoista. Direktiivin avulla pyritään luomaan avoimuuteen perustuvaa kyberturvallista yhteiskuntaa. Kriittisen infrastruktuurin palvelut ovat kyberfyysisiä kokonaisuuksia, jotka tarvitsevat fyysisen rakenteen lisäksi turvallisen ja luotettavan digitaalisen kokonaisuuden. (Markopoulou, Papakonstantinou ja De Hert, 2019; Liikenne- ja viestintäministeriö, 2001).

Kuten liitteessä 1 nähdään, ulottuu kybervaikuttamisen ja sodankäynnin keinot moninaisesti läpi kriittisen infrastruktuurin, jossa kybermaailma voi olla kohteena tai välineenä. Esimerkiksi Venäjän 2015 toteuttama kyberhyökkäys ukrainalaiseen voimalaitokseen jätti 235 000 ihmistä ilman sähköä. Pimeässä ja kylmässä odottaminen on jo itsessään ikävää, mutta energian kuuluessa kriittiseen infrastruktuuriin, tarkoittaa sähkökatko samalla sitä, että varavirran loputtua mikään ei enää toimi. Käytännössä lämmitys ja vedentulo lakkaa, bensapumppujen hiljennyttyä logistiikka ja hälytysajoneuvot pysähtyvät, kauppojen sähköovet eivät avaudu eivätkä kassat toimi. Sairaaloiden operaatiot keskeytyvät ja aiheuttavat henkeen ja terveyteen kohdistuvia suoria vahinkoja. Ja monia muita ongelmia. (Greenberg, 2019).

Toisena esimerkkinä kriittistä infrastruktuuria vahingoittaneesta kyberhyökkäyksestä toimii vuoden 2021 Colonial Pipelinen tapaus, jossa rikollisryhmä sai otettua panttivangiksi kriittistä polttoaineputkistoa ylläpitävän infrastruktuurin kiristyshaittaohjelmalla. Linjaston läpi kulkee 45 % Yhdysvaltojen itärannikon polttoaineesta, joten seuraukset olivat mittavat, kun yritys joutui sulkemaan koko 8900 kilometriä pitkän jakelulinjaston. Sulku oli ensimmäinen koko 57 vuoden historian aikana ja kesti kuusi vuorokautta ennen kuin ylösajo aloitettiin. Sulku aiheutti muutoksia ja peruutuksia lentoliikenteeseen, kun välilaskupaikoilla ei ollut polttoainetta, kriisikokouksia valkoisessa talossa sekä ruuhkaa ja bensapulaa huoltoasemilla ihmisten hamstratessa polttoainetta. Kyberhyökkäyksen mahdollisti yksi menetetty salasana, jonka avulla hyökkääjät pääsivät sisälle verkkoon. Hyökkäys päättyi Colonial Pipelinen maksaessa Bitcoin-lunnaat, jotka olivat sen hetkisellä kurssilla n. 5 miljoonaa. Muutaman tunnin kuluttua maksusta he saivat ohjelmistotyökalun, jolla infrastruktuurin palautus voitiin tehdä. Palautustyökalun suorituskyky oli kuitenkin niin vaatimaton, että palautuksessa ja operaation uudelleen käynnistyksessä kesti vielä useita päiviä. (Energy.gov, 2021; Turton & Mehtrotra, 2021)

Kybertoimintaympäristö nähdään niin tärkeänä osana kriittistä infrastruktuuria, että sen saatavuuteen ja hallintaan kiinnitetään paljon huomioita. Tämä on ohjannut kehityskulkuun, jossa yhteinen globaali internet on jakautumassa geopolitiikan ja arvojen mukaisesti useaan verkkoon, jotka eivät keskustele enää keskenään. Kiina on panostanut voimakkaasti Afrikan tietoliikenneinfrastruktuurin kehittämiseen ja suodattaa kansalaisten yhteyksiä globaaliin internettiin

digitaalisenajan kiinanmuurilla, joka estää mm. Facebookin, Googlen, Twitterin ja BBC:n käytön. Venäjä on rakentanut digitaalisen rautaesiripun idän ja lännen väliin ja pyrkinyt vähentämään riippuvuuttaan länsimaisesta informaatioteknologiasta kehittämällä omia kansallisia tietojärjestelmäratkaisujaan. (the Guardian 2018; the Guardian, 2019; Laari ja kollegat, 2019; Hruby, 2021). Verkon ja sen palveluiden omavaraisuudella pyritään vastaamaan huoltovarmuuden tuomiin saatavuuden ja jatkuvuuden vaatimuksiin, mutta myös suojaamaan kansaa informaatiovaikuttamiselta. Samalla tämä on karhunpalvelus kansalle, jolta evätään pääsy vapaaseen tutkittuun tietoon. Kuviossa 6 Lehto (2019b) on esittänyt Yhdysvaltojen (lännen), Venäjän ja Kiinan käyttämät kyberympäristöt sekä esimerkkejä niiden palveluista.



KUVIO 6 Yhdysvaltojen, Kiinan ja Venäjän verkot ja palvelut vertailussa (Lehto, 2019b).

Kuten kuviosta 6 näkee, lännessä tutuille hakukoneille, sosiaalisen median palveluille ja monille muille löytyy vastineet Runetista ja China netistä. Vaikka nämä äkkiseltään voidaan mieltää ei-kriittiseksi infrastruktuuriksi, on niillä suuri vaikutus yhteiskunnan toimintaan. Ne voidaan myös luokitella kaksoiskäyttökomponenteiksi, joilla on siviilikäytön lisäksi merkittävä sotilaallinen ulottuvuus niin tiedustelun kuin operaatioiden toteuttamisen näkökulmasta. Sosiaalisen median palvelut ovat tärkeitä kollaboraatioalustoja, joiden kautta tieto välittyy nopeasti ja globaalisti. Esimerkiksi Krimin ja Donetskin alueen asukkailta saatiin tutkinnan kannalta tärkeää kuva- ja videomateriaalia tapahtumista, joiden avulla saatiin osoitettua, että Malaysia Airlinesin lento MH17 ammuttiin alas Itä-ukrainassa BUK-ilmatorjuntaohjuksella (Dutch Safety Board, 2015). Varsinainen Musta Joutsen tapahtui kuitenkin helmikuussa 2022 Ukrainan sodan käynnistyessä, kun Ukrainan varapääministeri Mykhailo Fedorov ilmoitti Twitterissä Ukrainan perustavan vapaaehtoisista hakkereista koostuvan IT-armeijan. Mukaan pyydettiin kaikkia halukkaita avustamaan Ukrainan kyberympäristön puolustuksessa sekä tiedustelemaan Venäjän armeijan sotilaita. Pian perustetulla Telegram-viestintäkanavalla olikin jo 300 000 vapaaehtoista ja tehtävälista laajeni

koskemaan hyökkäyksellisiä operaatioita. Seuraavien viikkojen aikana heidän raportoitiin hyökänneen onnistuneesti useisiin Venäläisiin kyberjärjestelmiin. (Reuters, 2022; Yle, 2022).

Kyberjärjestelmien rauhanomainen siviilikäyttö on hyvin tärkeässä roolissa. Verkkokaupat korvaavat kivijalkakauppoja, e-kirjat ja audiokirjat korvaavat perinteisiä medioita, videovuokraamot ovat jääneet striimauspalveluiden jalkoihin. Jopa terveydenhuolto on lähtenyt etätyötrendin mukaisesti tuottamaan palveluitaan virtuaalisesti (Yle, 2021). Digitaalisilla palveluilla, etäohjauksella, automatiikalla ja tekoälyllä on valtavasti käyttökohteita, kun puhutaan työnteon tehostamisesta tai ihmistyön korvaamisesta. Tämä on monessa suhteessa hyvä asia, joka vähentää osaltaan materialismia ja mahdollistaa palveluiden tuoton alueelle, jossa niitä ei muutoin olisi kannattavaa tuottaa.

Automaatio soveltuu helposti toistettaviin ja ohjelmoitaviin tehtäviin sekä suurten tietomassojen käsittelyyn. Tämä parantaa työnlaatua ja vähentää virheitä jättäen ihmiselle sellaiset tehtävät, joissa ihminen on parempi kuin kone (Barbieri, Mussida, Piva ja Vivarelli, 2019). Tämä lisää kuitenkin riskiä sille, että perinteiset palvelut katoavat. Näin on käynyt suurelta osin jo esimerkiksi fyysisille pankkipalveluille. Digitaalisten internetpalveluiden taustalla on tiukasti yhteen kytketty infrastruktuuri, joka on rakennettu suurten tietomäärien käsittelyyn, tallennukseen ja siirtämiseen ja josta yhä useammat ovat riippuvaisia (Nunan ja Domenico, 2017). Tämä lisää kokonaisjärjestelmän kompleksisuutta ja tiukkoja yhteyksiä sekä teknologian, että organisaatioiden välillä. Toisaalta modernit teknologiat ja hyperskaalatut pilvipalvelut mahdollistavat hajautettujen ja resilienttien järjestelmien toteuttamisen nopeasti ja tehokkaasti, mutta toisaalta lisäävät riippuvuutta ja riskiä yllättäville tapahtumille.

Esimerkiksi jouluna 2012 sattui tapaus, jossa maailman suurimman pilvipalveluinfrastruktuurin Amazonin ylläpitäjä poisti vahingossa muutaman rivin koodia kuormanjakolaitteesta. Amazon tuotti tuolloin siirtoverkkoa (CDN) Netflixille, jolloin tämän virheen seurauksena Netflixin videopalvelut eivät olleet käytettävissä jouluaamuna. (Cockroft, 2012). 2021 Microsoftilla sattui vahinko rutiininomaisessa avaintenvaihto-operaatiossa. Tämän seurauksena maailman toiseksi suurin pilvipalvelualusta oli saavuttamattomissa 14 tunnin ajan. Ongelma koski Azure Active Directoryä (AAD), Microsoft 360 -palveluita, Xbox live -palvelua ja monia muita. (Pulsifier 2021). Entistä laajemman ongelmasta teki se, että Microsoft AAD on laajasta käytetty identiteettipalvelu (IDP), jolloin katkos tarkoitti sitä, että käyttäjät eivät voi kirjautua mihinkään palveluun, johon ovat rekisteröityneet käyttäen Microsoft tiliä.

Oleellinen osa digitaalista kybermaailmaa on esineiden internet. Maailma on nykyisin pullollaan laitteita (IoT), joihin on sisällytetty sensoreita ja teknologiaa joko asiakkaan tai valmistajan eduksi. Käytännössä nämä verkkoon kytketyt televisiot, leivänpaahtimet, valvontakamerat, autot ja jopa bioniset implantit ovat tietokoneita, joihin voidaan hyökätä ja joita voidaan väärin käyttää. Koti- tai yritysverkkoon kytketty IoT-laite on usein tietoturvaltaan heikko tai olematon. Laitteiden päivittäminen voi olla hankalaa tai mahdotonta ja usein se vain unohtuu käyttäjältä. Tämä mahdollistaa kuitenkin verkkoon tunkeutumisen näiden laitteiden kautta tai laitteiden haltuunoton ja kytkennän esimerkiksi osaksi bottiverkkoa. (Trafikom, 2021; Lehto, 2019b; Cloudflare, 2022).

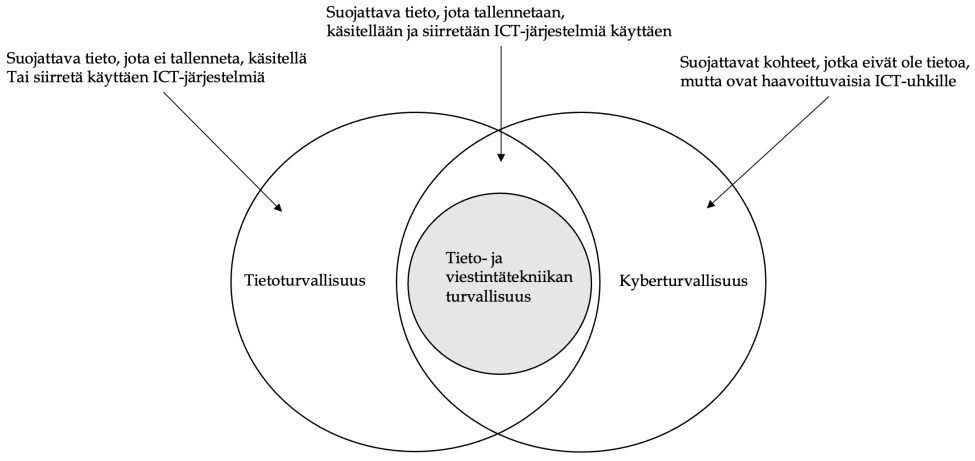
OT-laitteet (*operational technology*), ovat teollisuuden laitteisiin ja rakenteisiin kytkettyjä digitaalisia laitteita, joiden tarkoitus on ohjata, mitata ja valvoa kohdetta ja prosessia. IoT- ja OT-laitteita käytetään paljon osana tuotantotaloutta ja logistiikka, joka on johtanut siihen, että uhkatoimijat ymmärtävät niiden roolin globaalissa toimitusketjussa, jolloin niihin kohdistuvat häiriöt aiheuttavat kerrannaisvaikutuksia, jotka ovat omiaan lisäämään painetta esimerkiksi lunnaiden maksuun. IoT- ja OT-laitteisiin kohdistuvat hyökkäykset ovatkin kasvaneet joka vuosi (IBM, 2022).

Tässä kappaleessa on esitelty digitaalisen kyberympäristön roolia osana fyysistä maailmaa, kriittistä infrastruktuuria ja jokapäiväistä elämää. Seuraavassa kappaleessa tutkitaan mikä kyberympäristöä uhkaa ja miten sitä suojataan.

2.3 Kyberturvallisuus

Tässä kappaleessa kuvataan mitä on kyberturvallisuus ja miten se eroaa käsitteenä tietoturvasta. Kappale esittelee kyberturvallisuusuhat, uhkatoimijat, uhkatoimijoiden motivaatiot ja käyttämät metodit. Kappaleen lopuksi käydään läpi kyberonnettomuuden käsitettä esimerkin kautta.

Arkikielessä kyberturvallisuus mielletään helposti tietoturvan synonyymiksi vaikkakaan nämä kaksi konseptia eivät ole suoraan verrannollisia keskenään. Kuviossa 7 kuvataan Von Solmsin ja Van Niekerin (2013) mukaisesti tietoturvallisuuden, ICT-turvallisuuden ja kyberturvallisuuden kolminaisuus, josta ilmenee että, tietoturvalla on analogisen ja fyysisen maailman ulottuvuus, joka ei kuulu digitaaliseen maailmaan, kun taas kyberturvallisuudessa on digitaalinen ja fyysinen ulottuvuus, joka ei liity suoraan tiedon suojaamiseen tai turvaamiseen. Näiden leikkauskohdassa on tieto- ja viestintätekniikan turvallisuus.



KUVIO 7 Kyberturvallisuuden ja tietoturvan alueet

Tietoturvan perimmäinen tarkoitus on nimensä mukaisesti turvata tietoa. Sanastokeskus (2018) määrittää ISO 27002 standardin mukaisesti tietoturvan olevan järjestelyitä, joilla pyritään varmistamaan tiedon saatavuus (engl. *availability*), eheys (engl. *integrity*) ja luotettavuus (engl. *confidentiality*). Tietoturva liitetään

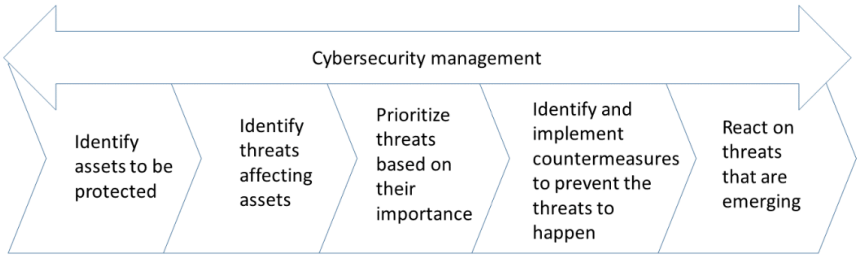
usein digitaaliseen tietojen käsittelyyn, mutta täytyy muistaa, että sitä on kuitenkin tehty jo paljon ennen digitaalista aikaa. Asioiden kirjoittaminen kivitauluun on omalta osaltaan turvannut viestin muuttumattomuuden, eheyden ja saatavuuden. Sallimanin (2019) mukaan historiallisesti tietoturvassa painotettiin fyysisiä menetelmiä, kuten ensimmäiset lukot 2000 vuotta eaa. sekä Julius Caesarin käyttämä *Caesar Cipher* -salausmenetelmä 100 vuotta eaa. Tietoturva itsessään on laaja käsite ja sitä sekä sen historiaa tutkitaan usealla tieteenalalla kukin hieman omasta näkökulmastaan. Matemaatikot tutkivat mm. kryptologiaa, tietojärjestelmätieteissä tietojärjestelmäturvallisuutta, ohjelmistotekniikassa turvallisia kehitysmenetelmiä, tietojenkäsittelyssä tietojen mallinnusta ja turvallista säilytystä (Siponen, 2005).

Kyberturvallisuus puolestaan on suomalaisen termistön mukaisesti *tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan* (Turvallisuuskomitea, 2019). Lehdon (2019a) määritelmän mukaisesti kyberturvallisuus on toimenpiteitä, joilla suojaudutaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteutetaan tarvittavia vastatoimenpiteitä. Huomattavaa on, että tietoturvallisuuta ja kyberturvallisuutta voidaan määritellä monilla tavoin (Von Solms ja Van Nieker, 2013). Tämän tutkimuksen pohjana käytettävät kyberturvallisuuden ja tietoturvan käsite-erot on tiivistetty alla olevaan taulukkoon 2.

Taulukko 2 Tietoturvan ja kyberturvallisuuden käsitteet

Tietoturva	**Kyberturvallisuus**
Järjestelyitä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luotettavuus. Ei ota kantaa siihen onko tiedonkäsittely digitaalista, analogista tai niiden yhdistelmä.	Toimenpiteitä, joilla suojaudutaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteutetaan tarvittavia vastatoimenpiteitä. Kyberturvallisuus kattaa tiedon suojaamisen lisäksi kyberympäristön ja siitä riippuvaisten toiminteiden turvaamisen.

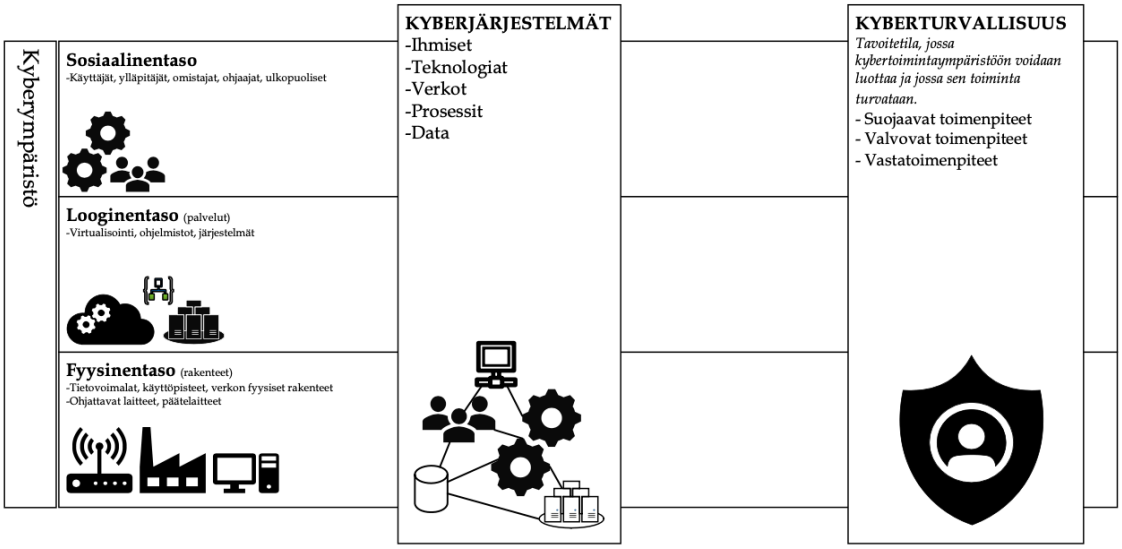
Baskerville (1991) suhtautuu riskien arviointiin ja analysointiin kriittisesti, mutta tunnustaa sen käytettävyyden ennen kaikkea kommunikaatiovälineenä johdon ja turvallisuusasiantuntijoiden välillä. Rajamäki ja kollegat (2018) ovatkin kuvanneet kyberturvallisuuden hallinnan kuvion 8 kaltaisena riskienhallintaa muistuttavana jatkuvana prosessina, joka koostuu NIST:n (2018) kyberturvallisuuden viitekehyksen mukaisesti suojattavien kohteiden tunnistamisesta, niitä kohtaavien uhkien tunnistamisesta, uhkien priorisoinnista suhteessa todennäköisyyteen, vaikuttavuuteen sekä suojattavan kohteen prioriteettiin. Kaksi viimeistä vaihetta sisältävät vastatoimien tunnistamisen ja toteuttamisen sekä eteen tuleviin uhkiin vastaamisesta. Malli tukee Baskervillen (1991) ajatusta, jonka mukaisesti riskienhallinta on menetelmänä väärin ymmärretty ja onnistuvan riskianalyysin tulisi kehittyä kvantitatiivisesta, tilastoihin perustuvasta arviosta kohti asiantuntija-arviota.



KUVIO 8 Kyberturvallisuuden hallinta riskienhallintaprosessina (Rajamäki ja kollegat, 2018)

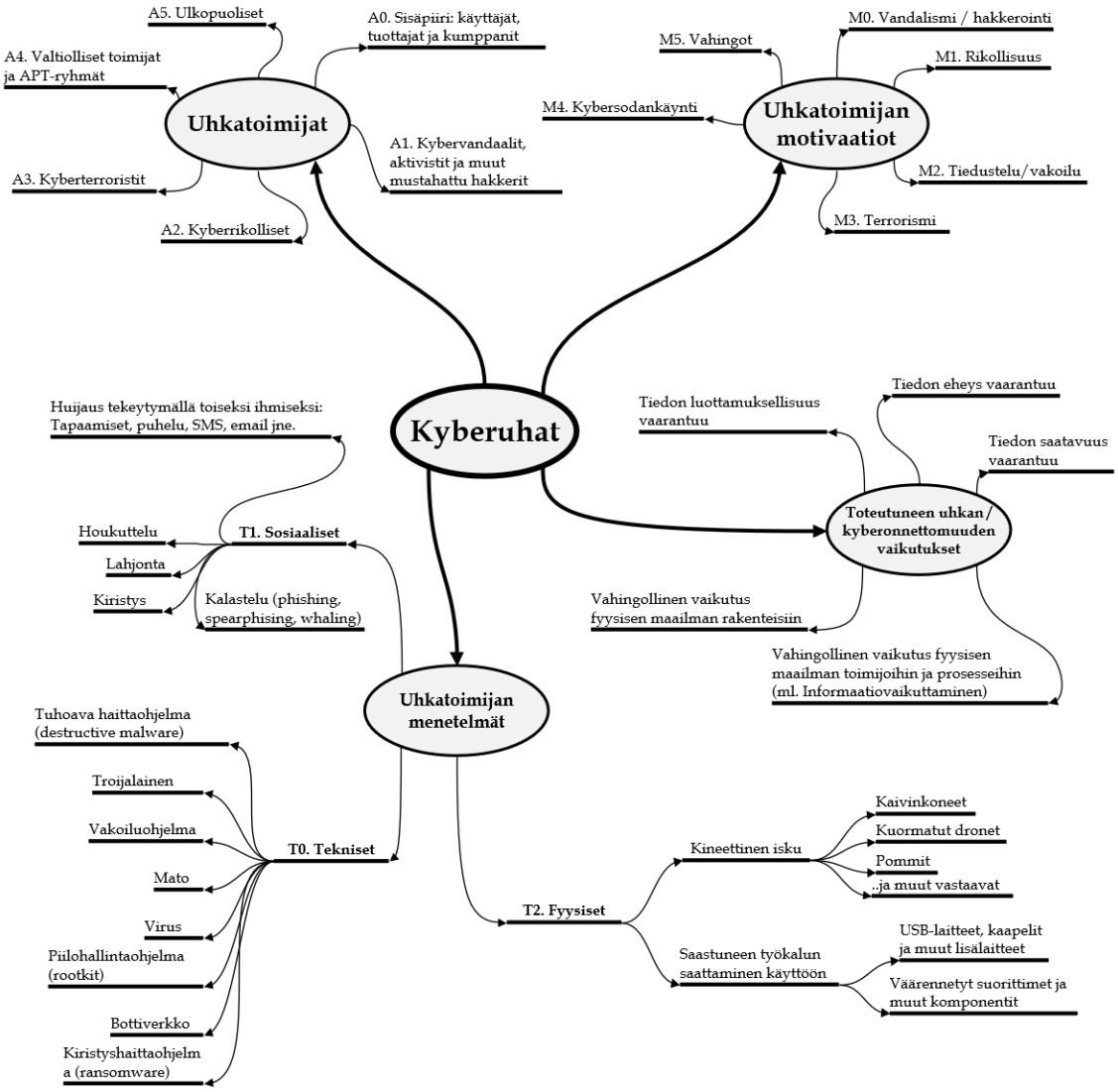
Toinen kuvaava määritelmä on Yhdysvaltalaisen CISA:n (*Cybersecurity and Infrastructure Security Agency*) käyttämä, jonka mukaisesti kyberturvallisuuden hallinta valvoo tietojärjestelmän tai verkon kyberturvallisuusohjelmaa, jonka tulee kattaa strategiset henkilöstö ja infrastruktuuriresurssit, vaatimukset ja politiikat sekä niiden täytäntöönpanon, hätäsuunnittelun ja turvallisuustietoisuuden.

Tässä kappaleessa on käyty läpi tietoturvaa ja kyberturvallisuutta käsitteenä sekä kuvattu mitä kyberturvallisuuden hallinta on. Kyberturvallisuus voidaankin lisätä osaksi aiemmin rakennettua kolmitasoista kuvausta kyberympäristöstä (kuvio 9).



KUVIO 9 Kyberympäristön viitearkkitehtuuri täydennettynä kyberturvallisuuden käsitteellä

Seuraavissa alikappaleissa avataan asiaa tarkemmin kuvion 10 mukaisesti. Kappaleet käsittelevät kyberturvallisuutta uhkaavia uhkia, toimijoita, motivaatioita sekä menetelmiä. Luvun lopuksi käsitellään kyberonnettomuutta käsitteenä sekä esimerkkien kautta.



KUVIO 10 Käsitekaavio kyberturvallisuuden uhkakentästä

2.3.1 Kyberuhat

Edellisen kappaleen lopussa kyberturvallisuudella täydennetty kyberympäristön viitearkkitehtuuri kuvasi kyberturvallisuustoimina *suojauksen*, *valvonnan* ja *vastatoimet*. Jotta nämä toimet ovat oikeasuhtaisia ja tehokkaita, tulee kyberuhkien kohteet tuntea. Laajasti katsottuna tärkeimmät suojattavat kohteet löytyvät kriittisen infrastruktuurin piiristä. Nämä ovat välttämättömiä yhteiskunnan jatkuvalle toiminnalle ja siihen kuuluvat fyysisen maailman rakenteet kuten laitokset, käyttöpisteet, tietovoimalat, fyysiset verkkorakenteet, laitteet ja sensorit sekä digitaaliset toiminteet ja palvelut (Lehto, 2019a). Tarkemmin katsottuna niin kriittisen infrastruktuurin kuin muidenkin kyberjärjestelmien suojattavat kohteet voidaan jakaa tässä tutkimuksessa käytettävään kuvion 10 mukaiseen määritelmään, jossa kyberuhkat on jaettu viiteen kategoriaan niiden tuottamien vaikutusten perusteella. Kategoriat kyberuhkille ovat:

- Fyysisen maailman rakenteisiin kohdistuvat

- Fyysisen maailman toimijoihin ja prosesseihin kohdistuvat
- Tiedon luottamuksellisuuteen kohdistuvat
- Tiedon eheyteen kohdistuvat
- Tiedon saatavuuteen kohdistuvat

Kyberfyysisen maailman uhat ovat haitallisia tapahtumia tai kehityskulkuja, jotka kohdistuvat fyysisten rakenteiden, ihmisten ja prosessien vahingoittumiseen siten, että siitä riippuvainen toiminto häiriintyy tai keskeytyy (Lehto, 2019a). Tämä tarkoittaa esimerkiksi tahallisia ja tahattomia onnettomuuksia kuten avainhenkilön sairastuminen, tietovoimalan sähkökatko tai yhteiskunnan poikkeustila, joka johtaa ennakoimattomiin priorisointeihin. Tähän kategoriaan kuuluvat myös kaivinkoneella katkaistut kaapelit, kiristyshaittaohjelmilla lukitut koneet, heikosta tietoturvakulttuurista johtuva käyttäjien huolimattomuus tai välinpitämättömyys sekä inhimilliset virheet.

Tietoon liittyvät uhkakuvat voidaan määrittää aiemmin kuvatun CIA-kolmion (engl. *confidentiality-integrity-availability*) kautta. Ensimmäinen uhka on luottamuksen menetys, joka tarkoittaa sitä, että luottamuksellista tietoa on päätynyt ulkopuolisen käsiin vahingon tai rikoksen myötä. Eheys menetetään silloin kun tietoon ei voida enää luottaa. Uhkan taustalla voi olla esimerkiksi vihamielinen toimija, jonka epäillään muuttaneen tietoa tai järjestelmävirheestä aiheutunut virheellinen tiedonkäsittely. Eheys voidaan menettää myös laiterikon seurauksena, jos esimerkiksi tallennus on epäonnistunut. Saatavuus vaarantuu silloin kun tieto ei ole niiden henkilöiden saataville, joilla tietoihin on lupa ja tarve. Saatavuus voi vaarantua esimerkiksi palvelunestohyökkäyksen kautta tai järjestelmän vikaantuessa tahallisen tai tahattoman toimen seurauksena kuten vaikka edellä mainittu laiterikko, johon ei ollut varauduttu. Oleellista uhkien osalta on tunnistaa kyseiseen kohteeseen kuuluvat komponentit ja priorisoida niiden kriittisyys.

Kaikkia konkreettisia uhkia ei voida yksiselitteisesti luokitella kuulumaan vain yhteen kategoriaan ja onkin tyypillistä, että yksi uhka aiheuttaa useampia vaikutuksia. Esimerkiksi tietomurto vaarantaa ensisijaisesti tiedon luottamuksellisuuden, mutta jättää myös epäilyksen eheyden vaarantumisesta. Samoin tietoon kohdistuvat uhkat vaikuttavat usein myös prosesseihin ja voivat keskeyttää esimerkiksi rikostiedusteluun liittyvän peiteoperaation, mikäli on epäilys, että operaatioturvallisuus on menetetty esimerkiksi tietomurron seurauksena. Listalta on tarkoituksella jätetty pois uhka, joka kohdistuu tietojärjestelmään itseensä. Tämän tutkimuksen näkökulmasta uhka kohdistuu aina arvoon, jota tietojärjestelmällä tuotetaan, jolloin se on pääsääntöisesti tietoa, prosessia, ihmishenkiä tai vaikeasti korvattavaa materiaa.

2.3.2 Uhkatoimijat

Uhkatoimijan määritelmä riippuu katsantokannasta. Toiselta puolelta katsottuna jokin ryhmä voi tuottaa uhkaa, mutta toiselta puolelta katsottuna sama ryhmä tuottaa mahdollisesti onnistuneen operaation. Uhkatoimija voi siis olla pahantahtoinen hyökkääjä, viranomainen suorittamassa laillista operaatiota tai

tietoturvatestaaja suorittamassa luvallista testausta. Tässä tutkimuksessa toimijan uhkaavuutta katsotaan kohdejärjestelmän näkökulmasta, jolloin laillinenkin operaatio uhkaa sitä toimintaa, joka on riippuvainen kohteena olevasta järjestelmästä.

Esimerkkinä laillisesta viranomaisoperaatiosta toimii tullin operaatio, jolla laiton kauppapaikka suljettiin takavarikoimalla fyysiset palvelimet (Yle, 2020). Toinen esimerkki on ANOM-viestintäsovelluksen tapaus. ANOM oli FBI:n ja DEA:n operaatio, jossa valmistettiin salaa kovennettu Android-puhelin, joka sisälsi turvalliseksi ja anonyymiksi markkinoidun viestintäsovelluksen, jolla voi viestiä vain toiseen ANOM-puhelimeen. Viestintäsovellus otettiinkin rikollisryhmissä laajaan käyttöön (12 000 puhelinta), joka aiheutti sen, että FBI sai pääsyn viestiliikenteeseen ja keräsi alustalta 27 miljoonaa viestiä ja jakoi nämä yhteistyöviranomaisille. Tämän seurauksena käynnistyi valtava operaatio, johon osallistui 9000 viranomaista 33 maassa. Operaation lopputuloksena pidätettiin 800 ihmistä 16 maassa, takavarikoitiin useita tonneja huumausaineita sekä lähes 150 miljoonan edestä rahaa ja kryptovaluuttaa. Rikostutkinnat ja oikeudenkäynnit jatkuvat edelleen. (Department of Justice, 2021). Perinteisemmin uhkatoimijana pidetään kuitenkin toimijaa, joka toiminnallaan rikkoo lakia samalla kuin aiheuttaa uhkaa kohteena olevalle toiminnalle. Näitä toimijoita käydään läpi kappaleessa myöhemmin.

Kirjallisuudessa uhkatoimijoita ei selkeästi ole määritetty ja *"cyber threat actors"* -haulla löytyykin useita listoja. Yleistä näille on, että toimijat luokitellaan motivaation mukaisesti ja näkökulmana on hyökkäykselliset kybertapahtumat. Tämän tutkimuksen, eli kyberonnettomuuksien, näkökulmasta toimijoiden osalta tulee huomioida myös vahingon ja sattuman mahdollisuus. Näin ollen tämä tutkimus määrittää uhkatoimijat Lehdon (2019a) kyberuhkien rakennemallia mukailevalla kategorisoinnilla viiteen ryhmää:

- Sisäpiiri, käyttäjät, tuottajat ja kumppanit
- Kybervandaalit, aktivistit ja mustahattuhakkerit
- Kyberrikolliset
- Kyberterroristit
- Valtiolliset toimijat ja APT-ryhmät
- Ulkopuoliset

Sisäpiiriläinen tarkoittaa toimijaa, jolla on laillinen pääsy kohteena olevaan järjestelmään jossain käyttäjän tai palveluntuottajan roolissa. Mukaan lasketaan myös palveluntuottajan toimitusketjuun kuuluvat kumppanit. Kybervandaalit, haktivistit ja mustahattuhakkerit ovat opportunistisia yksilöitä tai pieniä ryhmiä, joiden luokittelu tulee motivaation kautta. Ryhmittävänä tekijänä voi olla maineenhankinta, ilkivalta, mielenilmaus, ajattelematon kokeilunhalu tai jokin muu ideologia, jota pyritään levittämään käyttäen kyberympäristöä (Laari ja kollegat, 2019).

Rikollisryhmät ovat toimijana selkeästi yleisin ja IBM (2022) mukaan vastasi jopa 97 % kaikista 2021 havaituista kyberhyökkäyksistä. Tämä ryhmän luokittelua ohjaa motivaatio taloudellisen edun saavuttamisesta rikoksen keinoin. Kyberrikollisille kyberjärjestelmät voivat olla kohteita itsessään, mutta niitä voidaan

käyttää myös välineinä perinteisten rikosten suorittamiseen. Tunnettuja kyberrikollisryhmiä ovat esimerkiksi *REvil*, *Ryuk* ja *Conti*. Vuoden 2021 yleisin kyberrikollisuuden muoto oli kiristyshaittaohjelmat, joiden osuus kaikista hyökkäyksistä oli IBM:n tuottaman tilaston mukaan 21 %. Näistä puolet yhdistetään *REviliin* (37 %) ja *Ryukiin* (13 %). Kyberrikollisryhmien keskimääräiseksi elinikä on 17 kuukautta, jonka jälkeen ne uudelleen brändäävät tai lopettavat toimintansa (IBM, 2022). Kyberrikosten kohteet valikoituvat hyötytuotto suhteen mukaisesti painottuen helppoihin kohteisiin. (Laari ja kollegat, 2019) Kohteena voi olla yksittäinen kansalainen tai organisaatio. Keinovalikoima on laaja petoksista ja kiristyksistä aina murtoihin ja varkauksiin (Lehto, 2019a). Keinoista lisää myöhemmässä kappaleessa.

Kyberterroristit ovat perinteisiä terroristiryhmiä, jotka ovat laajentaneet toimintansa fyysisestä digitaaliseen maailmaan. Kuten kyberrikollisuudessa myös terrorismissa kyberjärjestelmä voi olla kohteena tai välineenä. Yhdistävä tekijä tälle ryhmälle tulee motivaation kautta. Kyberterrorismi on toistaiseksi ollut vähäistä, mutta sen odotetaan olevan yksi lähitulevaisuuden vakavimmista turvallisuusuhista (Lehto, 2019a).

Valtiolliset toimijat hyödyntävät kyberympäristöä tiedustelun ja sodankäynnin alustana. Suuresta mediahuomiosta huolimatta kyse on suhteessa pienestä ja harvoihin kohdistuvasta uhkatoiminnasta. IBM:n IR-ryhmän (*incident response*) 2021 havaitsemista ja tilastoimista kyberhyökkäyksistä 2 % oli johdettavissa valtiolliseen toimijaan. Valtiolliset toimijat jakautuvat virallisten toimijoiden lisäksi yleensä useisiin offensiivisiin APT-ryhmiin, joiden osalta attribuutioongelma on todellinen (Laari ja kollegat, 2019). APT tulee sanoista Advanced (*kehittynyt*), Persistent (*sitkeä*), Threat (*uhka*), joka kuvaa ryhmän toimintaa hyvin. APT-ryhmien operaatiot voivat olla vuosien kestoisia ja ovat menetelmiltään pitkälle kehittyneitä. Ryhmät nimetään yleisesti APT- *ja jokin numero*, mutta ryhmille annetaan usein myös erillisiä kutsumanimiä. Kutsumanimen antaa tunnistanut taho, joka usein on jokin tietoturvayhtiö. Tämä johtaa siihen, että samalla ryhmällä voi olla useita nimiä (Suojelupoliisi, 2022d). Useat tietoturvayhtiöt nimeävät ryhmät eläinten mukaan, siten että mm. Kiinasta tulevat ryhmät ovat pandoja, Venäjältä tulee karhuja ja Iranista kissoja. Esimerkiksi APT28 tunnetaan myös nimellä *Fancy Bear* ja APT29 nimellä *Cozy Bear*. Muita tunnettuja Venäläisryhmiä ovat esimerkiksi *Sandworm*, jonka oletetaan olleen Ukrainan sähköverkon lamauttaneen hyökkäyksen takana (liite1) sekä hyökänneen 2018 talviolympialaisia vastaan *OlympicDestroyer* -madolla. Sandworm on Venäjän sotilastiedustelu GRU:n ryhmä *Unit 74455*. (Greenberg, 2019).

Lazarys-ryhmä tulee Pohjois-Koreasta ja tunnetaan sisäisesti nimellä *414 Liaison Office.* Lazarus muistuttaa toimintatavoiltaan ja motivaatioiltaan rikollisryhmää ja on tunnettu kyberpankkiryöstöistä, joiden arvellaan olevan tapa kerätä Pohjois-Korean valtiolle varallisuutta. Muita Lazarus-ryhmän tekemiä hyökkäyksiä ovat mm. 2014 hyökkäys Sony Picturesia kohtaan, jossa varastettiin suuri määrä dataa, joka myöhemmin vuodettiin internettiin sekä palvelunestohyökkäyksiä Etelä-Koreaa kohtaan. Tunnetuin tämän ryhmän hyökkäys on kryptomadolla toteutettu WannaCry, joka saastutti globaalisti yli 200 000 tietokonetta 150 maassa. WannaCry kryptasi saastuttamansa koneen tiedostot ja vaati 300 dollarin lunnaita kryptausavainta vastaan. Lunnasvaatimus tuplaantui kolmen

päivän kuluessa ja tiedostot tuhoutuivat viikon kuluttua, mikäli lunnaita ei maksettu. Madosta löydettiin kuitenkin tappokytkin, jolla eteneminen saatiin lopulta pysäytettyä. Lazaruksen näkökulmasta operaatio ei onnistunut, sillä arvioidaan, että laajasta saastutuksesta huolimatta lunnaita saatiin kerättyä vain 160 000 dollarin edestä. Osasyynä tähän oli WannaCryn heikko laatu, joka aiheutti sen, ettei tiedostoja saatu palautettua, vaikka lunnaat maksettiin. Tämän tultua julki ei uusilla uhreilla ollut enää motivaatiota maksaa lunnaita. Toisaalta tämä nostaa epäilystä siitä oliko perimmäinen motiivi kuitenkaan raha vai pelkästään kaaoksen aiheuttaminen. (Mohurle & Patil, 2017; Park, 2021; Kaspersky, 2022a)

Kolmantena esimerkkinä on rikollisryhmä Conti, joka on käytännössä rikollisten ICT-palvelun tarjoaja (engl. *ransomware-as-a-service*). Conti tekee hyökkäysoperaatioita ja vuokraa infrastruktuuriaan asiakkaille käytettäväksi rikollisiin tarpeisiin. Contin vuosittainen liikevaihto on yli 100 miljoonaa dollaria (USD) ja se työllistää yli 100 kuukausipalkkaista rikollista. Conti julkaisee kuukausittaista uutiskirjettä, jossa se julkaisee varastettua dataa niiltä organisaatioilta, jotka eivät ole maksaneet lunnaita. Lunnaat maksaneille ”asiakkaille” Conti tarjoaa asiakaspalvelua auttamaan järjestelmien palautuksessa. Conti toimii siis kuin mikä tahansa globaali suuryritys, jonka toimialana sattuu olemaan kyberrikollisuus. Conti on tehnyt omaan tai asiakkaidensa laskuun useita kiristysoperaatioita yrityksiä ja kriittistä infrastruktuuria kohtaan. Contin hyökkäyksillä on ollut vakavia seurauksia kuten esimerkiksi Irlannin terveydenhuoltopalveluiden järjestelmien alasajoon maanlaajuisesti. Conti on lähtöisin Venäjältä ja sen uskotaan olevan läheisessä tekemisessä Venäjän tiedustelupalveluiden kanssa. Conti on osoittanut julkisesti tukensa Venäjälle Ukrainan sotaan liittyen. (Microsoft, 2021a; Grebs, 2022; Gupta, 2022; Whittaker, 2022).

Viimeisenä uhkatoimijaryhmänä ovat *ulkopuoliset*, joka tarkoittaa harmaan joutsenen (Taleb, 2007) kaltaisia toimijoita. Harmaat joutsenet ovat tapahtumia tai toimijoita, jotka ovat harvinaisia, mutta merkityksellisiä. Niiden ilmaantumista voidaan ennustaa jonkin tilastollisen mallin mukaisesti, mutta tämä vaatii, että niihin ollaan valmistautuneita ja että organisaatiolla on työkaluja niiden ymmärtämiseen. Nämä toimijat eivät kuulu kyberjärjestelmän suunniteltuihin käyttäjiin tai palveluntuottamiseen osallistuviin henkilöihin, eivätkä he kuulu mihinkään muuhunkaan edellä mainittuun vihamieliseen ryhmään. Nämä ovat satunnaisia toimijoita, joiden toimilla on yllättävä vaikutus järjestelmään. He ovat kaivinkoneenkuljettajia, kahvin läikyttäjiä ja muita, joilla on mahdollisuus tehdä tuhoa vahingossa muttei usein motivaatiota tähän.

Tässä kappaleessa käytiin läpi kyberuhan taustalla olevia toimijoita ja kuten edeltä tulee esille, APT-ryhmät toimivat usein lähellä valtiota, jolloin on vaikea todistaa, onko kyseinen ryhmä valtion ohjaama vai suojelema. Kyberhyökkäysten selvityksessä törmätään usein attribuutio-ongelmaan, sillä hyökkääjät käyttävät usein kaapattuja palvelimia ja hyökkäysohjelmat saattavat sisältää hämäystarkoituksessa jätettyjä vihjeitä tekijästä. Osa APT-ryhmistä toimii rikollisryhmän tavoin, mutta kohteet voivat olla sellaisia, että todellinen motivaatio voi olla muutakin kuin taloudellisen edun tavoittelu. Usein paras ja vahvin tapa selvittää hyökkääjä on tarkastella motivaatiota.

2.3.3 Motivaatiot

Lehto (2019a) jakaa kyberuhkien motivaatiot kuuteen tasoon, josta 5. taso on kybersodankäynnin ja terrorismin väliin sijoittuva kybersabotaasi. Kybersabotaasin kuvataan olevan valtiollisen toimijan tai sen tukeman ryhmän toteuttamaa operointia sotaa alemmalla tasolla tarkoituksenaan epävakauden aiheuttaminen kohteessa tai hyökkäys- tai puolustuskyvykkyyksien testaus. Kuitenkin Ukrainan sodan ja sitä edeltävien kybermaailman tapahtumien (liite1) kautta välittyy kuva, jossa kybersodankäynti ja vandalismi sekoittuvat toisiinsa. Attribuutio-ongelman takia on vaikea vetää linjaa mitkä tapahtumat ovat sotaoperaatioita ja mitkä vandalismia tai terrorismia. Tästä johtuen, sekä tämän tutkimuksen tavoitteiden näkökulmasta, tässä tutkimuksessa käytetään kuusikohtaista motivaatioluokittelua, josta kybersabotaasi on sulautettu muihin luokkiin ja mukaan on lisätty uusi motivaatioluokka, *vahinko*. Vahinkoa lukuun ottamatta samat motivaatioluokat ovat tunnistettavissa EU:n kyberturvallisuusstrategiasta (EU, 2013) sekä kyberturvallisuuden sanaston uhkia kuvaavasta käsitemallista (Sanastokeskus, 2019). Tutkimuksessa käytettävät motivaatioluokat ovat:

- Vandalismi
- Rikollisuus
- Tiedustelu ja vakoilu
- Terrorismi
- Kybersodankäynti
- Vahingot

Kybervandalismilla tarkoitetaan toimintaa, jonka tavoitteena on aiheuttaa häiriötä, tuhoa tai kasvattaa toimijan mainetta (Sanastokeskus, 2019). Toimijaa voi motivoida digitaalinen kanava ideologiansa levittämisessä tai osaamisensa esittelyssä. (Laari ja kollegat, 2019). Koska kybervandalismin on yleensä tarkoitus herättää huomiota, koostuu operaatiot usein näyttävistä kampanjoista kuten verkkosivustojen hakkerointi ja sisällön korvaamista toisella tai kohteen häiritsemistä palvelunestohyökkäyksillä. Kybervandalismille on ominaista, että hyökkäyksen motivaatioista ei löydy piirteitä, jotka viittaisivat taloudellisen hyödyn tavoitteluun tai poliittiseen (valtiolliseen) toimintaan. Kybervandalismi on kuitenkin useimmiten kyberuhkista harmittominta (JYU, 2022).

Kyberrikos on käsitteenä laaja ja käsittää kaiken tietoverkoissa tapahtuvan tai tietoverkkoja hyödyntävän rikollisuuden. Kyberrikokset jaetaan yleensä kahteen kategoriaan sen mukaan, onko kyse tietoverkkosidonnaisesta (engl. *cyber dependent*) vai tietoverkkoavusteisesta (engl. *cyber enabled*) rikoksesta. Tietoverkkosidonnaiset kohdistuvat verkkoihin ja tietojärjestelmiin, kun tietoverkkoavusteiset ovat perinteisiä rikoksia, joissa verkkoja ja järjestelmiä on käytetty välineinä. (Poliisi, 2022a). Yhdistävä tekijä molemmissa on rikoksen teko, jolla voidaan tavoitella taloudellista etua, uhkailla, kiristää, harjoittaa laitonta vakoilua tms. Huomattavaa onkin, että riippumatta motivaatiosta, kyberhyökkäys on lähes aina rikollinen toimi. Poikkeuksena tähän on kyberharjoittelu, sovittu hyökkäystestaus ja muu vastaava kohteen omistajan hyväksymä toimi.

Kyberhyökkäysten näkökulmasta rikosta pidetään motivaationa silloin kun kyse on taloudellisen edun tavoittelusta esimerkiksi kiristämällä tai huijaamalla ja kohteena voi olla yksittäiset ihmiset tai organisaatiot. Motivaatioltaan kyberrikoksia ovat myös tietomurrot, joissa rikollisesti saatuja tietoja, kuten esimerkiksi käyttäjätunnuksia myydään edelleen pimeässä verkossa käytettäväksi muissa kyberoperaatioissa. Esimerkkinä kyberhyökkäyksestä, jossa motivaationa on ollut puhtaasti rikollinen toiminta, on aiemmin kuvattu Lazarus-ryhmä ja heidän kyberpankkiryöstönsä (Park, 2021). Toinen ikävä esimerkki on Vastaamon tapaus, jossa hyökkääjä sai varastettua arkaluonteiset potilastiedot heikosti suojatusta potilasrekisteristä ja kiristi tällä murron kohteena ollutta organisaatiota. Kun organisaatio ei suostunut vaadittuihin lunnaisiin, ryhtyi hyökkääjä kiristämään asianomistajapotilaita, joiden tiedot oli varastettu. Lopulta hyökkääjän virheen kautta varastetut tiedot julkaistiin vahingossa kokonaisuudessaan TOR-verkossa, josta ne kopioitiin useisiin muihin paikkoihin. Tämän jälkeen hyökkääjällä ei ollut enää millä kiristää ja tekijä katosi verkosta. (Ralston, 2020).

Tiedustelulle ei ole kyetty luomaan yleisesti hyväksyttyä määritelmää vaan jokainen tiedustelua harjoittava toimija määrittelee toimensa esimerkiksi prosessin kautta (Kari, 2019). Tiedustelu ja vakoilu ovat käytännössä saman asian kaksi puolta. Tiedustelun ollessa valtiollista toimintaa tai toimivaltaisen viranomaisen harjoittamaa, on se usein tiedustelutoimijan näkökulmasta laillista tiedustelutoimintaa, mutta samaan aikaan kohteen näkökulmasta laitonta ja haitallista vakoilua. Suojelupoliisin (2021a) mukaan kybervakoilu ei korvaa perinteistä tiedustelua vaan toimii lisänä ja uutena kanavana. Kybertiedustelun etuja verrattuna perinteisiin tiedustelulajeihin on lähes rajoittamaton maantieteellinen ulottuvuus (Laari ja kollegat, 2019), edullisuus ja harjoittajan näkökulmasta operaatioturvallisuus. Kari (2019) määrittää tiedustelun seuraavasti ”*Tiedustelu tuottaa tietoa vastustajasta ja olosuhteista päätöksenteon tueksi*”. Näin ollen kyberuhkan motivaatioksi kybervakoilu määritetään silloin kun esimerkiksi tietomurrossa saaduilla tiedoilla ei kiristetä kohdetta eikä niitä myydä tai julkaista, vaan tarkoitus on nimenomaan saada tietoa kohteesta.

Tiedustelu voi kohdistua myös organisaatioihin, jolloin puhutaan usein liiketoimintasalaisuuksien vakoilusta. Samaan kategoriaan menevät myös yksilöihin kohdistuva urkinnat ja laittomat katselut. Tunnettuja kotimaisia kybervakoilutapauksia ovat mm. vuoden 2020 kybervakoiluyritys, jossa Kiinaan yhdistetty APT31 -ryhmä yritti murtautua eduskunnan tietojärjestelmiin sekä ulkoministeriön tapaus, jossa 2013 ministeriön verkkoon ja tietojärjestelmiin tunkeuduttiin vieraan valtion toimesta. Viimeisin julkisesti uutisoitu ulkoministeriöön kohdistunut kybervakoilutapaus on vuodelta 2022 kun suomalaisten diplomaattien puhelimista löydettiin NSO Groupin Pegasus -vakoiluhaittaohjelma. (Suojelupoliisi, 2021b; Yle, 2014; Ulkoministeriö, 2022).

Kyberterrorismi on motivaationa silloin kun hyökkääjä pyrkii aiheuttamaan vakavaa pelkoa väestön keskuudessa, pyrkii vaikuttamaan oikeudettomasti valtion toimintaan, aiheuttaa merkittävää vahinkoa valtiolle tai kansainväliselle järjestölle. Kyberterrorismi on siis terrorismia, jossa fyysisten iskujen lisäksi tai sijaan käytetään kohteena tai välineenä kyberympäristöä. Hyökkäys voi kohdistua esimerkiksi tietojärjestelmien kautta toteutettuna kansalaisiin, liikeelämään, kriittiseen infrastruktuuriin tai muihin kohteisiin (Sanastokeskus,

2019). Kyberterrorismia ei ole toistaiseksi nähty paljon, mutta sen uskotaan olevan yksi tulevaisuuden suurimmista kyberuhista (Lehto, 2019a). Kyberterrorismilla voidaan aiheuttaa perinteiseen terrori iskuun lisätuhoa esimerkiksi siten, että pommi-iskun ohessa toteutetaan jokin lamauttava isku hätäkeskustietojärjestelmiin (Laari ja Kollegat, 2019).

Kybersodankäynnille ei ole olemassa yksiselitteistä määritelmää. Joillekin se tarkoittaa sotimista digitaalisessa kybermaailmassa ja toisille se on vastakohta kineettiselle sodankäynnille (Lehto, 2019a). Käytännössä kybersodankäynnistä tuli osa kaikkea sodankäyntiä, kun NATO julisti Varsovan kokouksessa 2016 kyberympäristön olevan sotilaallinen toimintaympäristö, jossa on kyettävä taistelemaan kuten maa-, meri-, ilma- ja avaruustoimintaympäristöissä (Penttilä, 2019). Kuten jo aiemmin tuli ilmi, ja liitteestä 1 nähdään, on kybersabotaasin ja kybersodankäynnin välinen ero veteen piirretty. Ukrainassa on nähty jatkuvia yhteiskuntaa häiritseviä ja lamaannuttavia operaatioita kohta kymmenen vuoden ajan samaan aikaan kun kineettinen sodankäynti on ollut välillä kiivaampaa ja välillä rauhallisempaa. Kybersodankäynti voidaan katsoa olevan motivaationa silloin kun hyökkääjä ja kohde ovat valtioita tai niiksi rinnastettavia toimijoita ja kun tarkoitus on vaikuttaa toisen toimintaan oikeudettomasti aiheuttaen vakavaa vahinkoa.

Viimeisenä motivaatioluokkana on vahinko. Kyseinen luokka ei varsinaisesti ole motivaatio vaan toimii kyberonnettomuuksien kannalta tärkeänä tekijänä silloin kun onnettomuus aiheutuu vahingosta. Tällöin toimijalla ei välttämättä ole tarkoitusta tai erityistä motivaatiota aiheuttaa vahinkoa, vaan se vain sattuu tapahtumaan. Esimerkkinä tästä on tapaus, jossa maarakennusurakoitsija katkaisi kaivinkoneella runkoverkkokaapelin ja hyydytti valtion it-järjestelmät (HS, 2021).

2.3.4 Menetelmät

Kyberhyökkäyksissä käytettävät menetelmät voidaan jakaa kolmeen tasoon kuten kybertoimintaympäristökin. Fyysisen tason menetelmillä pyritään aiheuttamaan vahinkoa tai murtautumaan järjestelmään. Menetelmät koostuvat kineettisistä iskuista fyysisiä kohteita kohtaan vastaan sekä fyysisten laitteiden käytöstä välineinä tai kohteina. Fyysisen tason kineettinen isku voi olla esimerkiksi edellisessä kappaleessa mainittu kaivinkone, jolla verkkokaapeli katkaistiin, pommi, joka vahingoittaa fyysistä infrastruktuuria tai vaikka drone, jonka kantamalla kuormalla häiritään tai vahingoitetaan kyberjärjestelmän toimintaa. Kineettisen tason iskuilla pyritään aiheuttamaan vahinkoa.

Toinen fyysisen tason menetelmäkokonaisuus on saastuneen välineen käyttöön saattaminen. Tämä tarkoittaa esimerkiksi muistitikkua, näyttökaapelia tai muuta lisälaitetta, joka sisältää haittaohjelman. Väärennetyt kaapelit tai komponentit ovat vaikeasti havaittavia menetelmiä ja kuuluvat lähinnä APT-ryhmien työkaluihin. Saastuneilla välineillä pyritään pääsemään sisään kyberympäristöön, jossa voidaan muiden menetelmien avulla saavuttaa tukeva jalansija ja piiloutua tai jatkaa liikkumista verkon sisällä. Saastuneiden välineiden kautta suoritetut hyökkäykset ovat merkittäviä uhkia sellaisten ilmatiiviiden kyberjärjestelmien osalta, jotka eivät ole liitettyjä internettiin. Tätä hyödynnettiin mm.

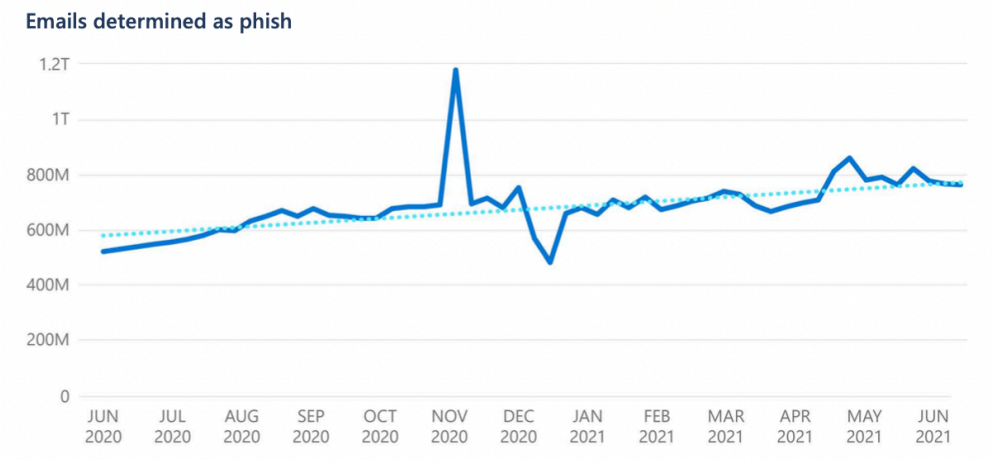
Iranissa, kun Stuxnet-mato ujutettiin saastutetulla USB-tikulla ydinvoimalaan (Zetter, 2014; Laari ja kollegat, 2019).

Väärennettyjä komponentteja on löydetty mm. Yhdysvaltojen asevoimien navigointilaitteista, pimeänäkölaitteista ja helikoptereista (BBC, 2012). 2019 Tietoturvatutkija Monta Elkins osoitti onnistuneella kokeella, miten kotikutoisilla työkaluilla ja 200 $ investoinnilla voidaan toteuttaa Bloombergin raportoima hyökkäys, jossa Yhdysvaltalaisen Supermicron Kiinassa valmistamista emolevyistä löydettiin ylimääräinen komponentti (Wired, 2019). Väitetysti tämä komponentti mahdollisti salaisen takaportin avaamisen verkkoon, jossa tämä saastutettu laite sijaitsee. Raportin mukaan Supermicro on yksi maailman suurimmista komponenttivalmistajista, jolloin näitä väärennettyjä komponentteja löytyi laajasti mm. Amazonin palvelinkeskuksista, pankeista, Yhdysvaltojen puolustusministeriön ja CIA:n laitteista, merivoimien sota-aluksista sekä tuolloin maailman arvokkaimman yhtiön Applen palvelinkeskuksesta. (Robertson ja Riley, 2018). Supermicro, Apple ja NSA ovat kieltäneet tapauksen (Cyperscoop, 2018). Edward Snowdenin vuotamien tietojen mukaan myös NSA käyttää samankaltaisia menetelmiä (The Intercept, 2019).

Sosiaalisen tason hyökkäykset (*social engineering*) ovat yleisimpiä menetelmiä, joilla hyökkääjä pyrkii saamaan hyökkäyksen ensivaiheen käyntiin. Nämä menetelmät kattavat mm. sähköpostilla levitettävän haittaohjelman tai sen latauslinkin sekä massana tehtävän sähköposti ja tekstiviestikalastelun. Tietojen kalastelun tarkoitus on saada harhautettua käyttäjää siten, että käyttäjä luovuttaa hyökkääjälle suojattavaa tietoa kuten luottokorttitietoja, pankkitunnuksia tai käyttäjätunnuksia ja salasanoja. Kalastelukampanjat voidaan jakaa ryhmiin sen mukaan, miten ne on kohdennettu. Tavallinen kalastelu (engl. *phishing*) on kohdentamatonta koputtelua ja kokeilua, jossa kalasteluviestiä jaetaan laajasti ja operaation onnistuminen perustuu tilastolliseen faktaan, jossa joka aina menee vipuun. (Laari ja kollegat, 2019; IBM, 2022).

Kohdennettu kalastelu (engl. *spear phishing*) tarkoittaa sitä, että kampanja on kohdistettu johonkin tiettyyn ryhmään kuten organisaatioon tai jonkin palvelun käyttäjiin. Tällaisissa kampanjoissa kalasteluviestit voidaan räätälöidä ja lokalisoida huomattavan pitkälle, jolloin niiden uskottavuus paranee. IBM:n tilastojen mukaan vuonna 2021 17,8 % käyttäjistä klikkasi kalasteluviestin linkkiä. Kalastelukampanjaan voidaan yhdistää muitakin sosiaalisia menetelmiä, kuten vaikka puhelu, jossa uhrille kerrotaan tulevasta sähköpostista ja pyydetään hoitamaan se eteenpäin. Tämä nostaa edelleen kampanjan uskottavuutta ja IBM:n tilastojen mukaisesti lisää klikkauksen todennäköisyyden kolminkertaiseksi verrattuna pelkkään kalasteluviestiin. Valastelusta (engl. *Whaling*) puhutaan kun kalastelu kohdistetaan ylimpään johtoon tai muuhun merkittävään kohteeseen (Laari ja kollegat, 2019; Microsoft, 2021a; IBM, 2022).

Kalastelupostit ovat yksittäisenä luokkanaan suurin haittapostikategoria ja niitä lähetetään kuukausitasolla satoja miljoonia (kuvio 11). Määrä on merkittävästi suurempi kuin esimerkiksi sähköpostilla levitettävien haittaohjelmien määrä, joka oli samaan aikaan keskimäärin n. 10 miljoonaa viestiä kuukaudessa. Vuonna 2021 kalastelu oli mukana 41 % kaikista kyberhyökkäyksistä sen ollen haavoittuvuuksien hyväksikäytön ohella käytetyin menetelmä, jolla kohteeseen päästiin sisään. (Microsoft, 2021a; IBM, 2022)



KUVIO 11 Kuukausittain globaalin Microsoft Exchangen läpi kulkevat kalasteluviesti

Sosiaalisiin menetelmiin lukeutuvat myös muut petosrikokset kuten esimerkiksi yrityksiin kohdistuvat toimitusjohtajahuijaukset (Poliisi, 2022b), kiristykset, lahjonnat ja houkuttelut. (Laari ja kollegat, 2019). Sosiaalisten menetelmien ominaispiirre on siis huijata, hämätä tai muutoin manipuloida ihmisiä jonkin motivaation takia ja sitä voidaan tehdä monin teknisin keinoin kuten sähköpostilla, soittamalla, viesteillä, mutta myös reaalimaailmassa kasvokkain. Yksi esimerkki tällaisesta on Ylen tekemä testi, jossa remonttimieheksi pukeutunut henkilö pääsi kulkemaan tikkaiden kanssa läpi usean kriittisen organisaation kulunvalvonnan (Yle, 2018). Tämä mahdollistaisi hyökkäyksen syventämisen muilla menetelmillä.

Vaikka sosiaaliset menetelmät ovat tänä päivänä yleisimpiä, ovat tekniset menetelmät kuuluisimpia. Tekniset hyökkäysmenetelmät, joilla pyritään pääsemään sisään kohteeseen myöhempiä operaatioita varten, perustuu jonkin kohteessa olevan heikkouden eli haavoittuvuuden hyväksikäyttöön. Haavoittuvuus tarkoittaa alttiutta tietoturvaan kohdistuvaan uhkaan (Sanastokeskus, 2018) ja niitä on lähes kaikissa käyttämissämme digitaalisissa järjestelmissä. Kaikki haavoittuvuudet eivät kuitenkaan ole kriittisiä (Laari ja kollegat, 2019). Haavoittuvuus voi olla laitteessa, ohjelmistossa tai prosessissa ja tarkoittaa käytännössä toiminnallisuutta, joka aiheuttaa kohteessa suunnittelemattomia vaikutuksia. Tämä voi olla esimerkiksi ohjelmistossa oleva virhe, jota hyödyntämällä hyökkääjä saa käyttöönsä vahvat käyttöoikeudet tai prosessissa oleva aukko, joka mahdollistaa väärinkäytön. Haavoittuvuudet ovat kalastelun jälkeen yleisin tapa, jolla hyökkääjä pääsee kohteeseen sisään. Vuonna 2021 näiden osuus kasvoi edellisestä vuodesta 33 % ollen kaikista hyökkäyksistä 34 %. Löydettyjen teknisten haavoittuvuuksien määrä on noussut tasaisesti jo yli viiden vuoden ajan (IBM, 2022). Nollapäivähaavoittuvuus, tarkoittaa haavoittuvuutta, jolle on olemassa hyökkäysmenetelmä muttei korjausta.

Sisään päästyään hyökkääjä voi käyttää laajaa joukkoa eri menetelmiä, joiden tarkoitus on tuhota tai varastaa tietoa tai aiheuttaa tuhoa kohteena olevalle järjestelmälle tai toimintaympäristölle, johon se on liitetty. Ensimmäiset tunnetut tietokonevirukset olivat suhteellisen harmittomia ja niitä kirjoitettiinkin lähinnä koodarin omaksi huviksi. Tällaisia oli esimerkiksi 1986 Pakistanissa kirjoitettu

Brain, joka muutti kiintolevyn nimeksi © brain ja kirjoitti tartutetun levyn käynnistyssektorille terveiset sisältäen jopa tekijän yhteystiedot. (Hyppönen, 2021). Virus on tarkoitettu asentamaan kohdekoneeseen hyökkääjän haluamaa koodia. Sen määritelmä on, että se osaa suorittaa ja monistaa itseään ja leviää tietokoneesta toiseen. Madoksi se puolestaan määritellään silloin kun se kykenee leviämään ilman ihmisen toimia (F-Secure, 2022a). Yksi tunnetuimpia ja tuhoisimpia matoja oli WannaCry (Kaspersky, 2022a).

Rootkitin, eli piilohallintaohjelman ja vakoiluohjelman (engl. *spyware*) tarkoitus on piiloutua järjestelmään ja toimia käyttäjän huomaamatta. Vakoiluohjelmassa kerätään ja lähetetään suojattavia tietoja hyökkääjälle, kun rootkitiä puolestaan käytetään usein osana muita menetelmiä. Sen rooli on antaa hyökkääjälle hallinta kohdejärjestelmään sekä piilottaa ja häivyttää hyökkääjän toimia kuten käynnistettyjä prosesseja. Rootkit voi olla yksittäinen ohjelmisto, mutta usein se koostuu useista komponenteista, joilla on erilaisia kyvykkyyksiä ja jotka mahdollistavat kohteena olevan järjestelmän täyden haltuunoton ja etähallinnan. Piilohallintaohjelmat toimivat hyvin matalalla tasolla järjestelmää esimerkiksi kernel-tasolla. (Kaspersky, 2022b). Norton (2022) jakaa rootkitit viiteen alaluokkaan: rauta/firmwarerootkit, käynnistysrootkit, muistirootkit, sovellusrootkit ja kernelrootkit.

Bottiverkko on useasta hyökkääjän haltuun saamasta järjestelmästä (tietokoneista, IoT-laitteista, palvelimista) koostuva järjestelmä kokonaisuus, jonka hajautettua tehoa hyökkääjä voi käyttää esimerkiksi palvelunesto hyökkäyksiin tai kryptovaluutan louhimiseen. Tunnettuja bottiverkkoja ovat mm. *Mirai* ja *Mozi*. Mozi on p2p (peer-to-peer) botnet, joka hyökkää verkkolaitteita kohtaan käyttäen hyödykseen kohdelaitteen heikkoa telnet-salasanaa sekä laitteiden tunnettuja haavoittuvuuksia. Infektoinnin jälkeen Mozi kykenee säilyttämään saamansa jalansijan laitteissa antaen laitteen hyökkääjän käyttöön myöhempiä operaatioita varten. Suojelupoliisin mukaan ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun. (Microsoft, 2021a; IBM, 2022; Suojelupoliisi, 2021d)

Digitaaliset Troijan hevoset ovat huolella valmistettuja ohjelmistoja, jotka on pyritty tekemään luotettavaksi ja houkuttelevaksi. Taustalla nämä harmittomalta vaikuttavat ohjelmat tekevät kuitenkin jotain käyttäjälle tai laitteelle haitallista. Ne voivat toimia ladata hyökkääjän seuraavan työkalun kohteeseen, ne voivat toimia vakoiluohjelmina ja varastaa käyttäjän tietoja ja toimia ja välittää ne eteenpäin. (F-Secure, 2022b).

Viimevuosien kuuluisin ja käytetyin haittaohjelmakategoria on kiristyshaittaohjelmat (engl. *ransomware*). Ensimmäiset kiristyshaittaohjelmat kryptasivat saastutetun koneen tiedostot ja vaativat lunnaita vastineeksi avaimesta, jolla tiedostot voitiin jälleen avata. Nykyisin näihin kiristyshaittaohjelmiin on lisätty toiminnallisuuksia, jotka ensin tutkivat ympäristön, varastavat arvokkaiksi tunnistetut tiedot ja vasta tämän jälkeen kryptaavat tiedostot. Hyökkääjät voivat näin tehostaa hyökkäystä uhkaamalla julkaista tiedot, mikäli uhri ei maksa lunnaita. Tunnettuja kiristyshaittaohjelmia ovat mm. *WannaCry*, *Petya* ja *Darkside*. (Greenberg, 2019; kaspersky, 2022a; IBM, 2022).

Kiristyshaittaohjelmat ovat rikollisille pieniriskisiä ja tuottavia, jolloin on loogista, että niiden kehittämiseen panostetaan. Monenlaista kokeilua mm. eri

ohjelmointikielillä ja salaustekniikoilla onkin nähtävissä. Näiden tarkoitus on hankaloittaa hyökkäystyökalujen takaisinmallinnusta ja salauksen purkamista ilman salausavainta. Hyökkäyskohteiden osalta on nähtävissä myös muutos siinä, että hyökkäyksiä kohdistetaan suoraan virtualisointikerrokseen, jonka kautta on mahdollista ottaa kohteeksi ja salata kokonaisia virtuaalikoneita sen sijaan että hyökättäisiin käyttöjärjestelmän läpi ja salattaisiin yksittäisiä tiedostoja. Kiristyshaittaohjelmat ovat ottaneet kohteikseen myös Dockerkontteja, jotka ovat yleisiä komponentteja pilvipalveluiden PaaS-ratkaisuissa (Cimpanu, 2021; Microsoft, 2021a, IBM, 2022).

Viheliäisin haittaohjelmista on tuhoava haittaohjelma (engl. *destructive malware*), joka nimensä mukaisesti kykenee tuhoamaan kohteena olevan laitteen tai järjestelmän. Tällaisia ovat mm. WhisperGate ja HermeticWiper, joilla Venäjä hyökkäsi Ukrainaa kohtaan alkuvuodesta 2022 (liite 1). HermeticWiper on kohdistettu Windows-käyttöjärjestelmiä ajaviin laitteisiin ja se muokkaa pääkäynnistystietueen rikki, jolloin laite ei enää käynnisty. WhisperGatesta on tunnistettu samankaltaisuutta NotPetyan kanssa ja se pyrkii naamioitumaan kiristyshaittaohjelmaksi. Kryptaamisen sijaan se kuitenkin tuhoaa pääkäynnistystietueen (CISA, 2022; Microsoft, 2022).

Teknisellä menetelmällä voi olla useita edellä mainittuja ominaisuuksia ja niitä yhdistellään toisiinsa tarpeen mukaan. Esimerkiksi troijalaista voidaan käyttää lataamaan kohteeseen rootkit, jolla hyökkääjä saavuttaa kohteesta pysyvän jalansijan ja saa rakennettua tarvittavan komentokanavan. Tämän jälkeen hyökkääjä voi tutkia järjestelmää, varastaa tietoa ja viedä sinne varsinaisen kiristyshaittaohjelman, joka vastaa tietojen salaamisesta. Matomaisesti leviävä tuhoava haittaohjelma, joka hyödyntää laajasti käytetyn ohjelmiston, kuten esimerkiksi Windows-käyttöjärjestelmän nollapäivähaavoittuvuutta on yksi pahimpia uhkakuvia.

Tunnettu ja maailmaa muokannut hyökkäystyökalu on Yhdysvaltojen NSA:n kehittämä EternalBlue, jonka Shadow Broker -ryhmä varasti ja julkaisi 2017. Työkalu hyödynsi Microsoftin SMB-protokollan haavoittuvuutta, joka kuitenkin paikattiin kuukautta ennen EternalBluen julkaisua. Tätä ennen työkalu ehti olla NSA:n käytössä viiden vuoden ajan. Julkaistusta korjauspäivityksestä huolimatta haavoittuvuus oli paikkaamatta laajasti, jolloin tätä työkalua hyödyntäneet WannaCry ja Petya tekivät yli miljardin arvosta tuhoa 65 maassa. (Greenberg, 2019).

Toinen esimerkki hyvin edistyneestä tietokonemadosta on Stuxnet, joka vakoilee ja uudelleen ohjelmoi teollisuusjärjestelmiä. Stuxnet hyödynsi neljää haavoittuvuutta, joista kaksi oli aiemmin tuntemattomia nollapäivähaavoittuvuuksia. Mato oli kohdennettu Iranilaiseen Natanzin rikastuslaitokseen, jossa sen oli tarkoitus kulkeutua matomaisten kykyjensä avulla koneeseen, jolla ohjattiin sentrifugeja. Madolla oli kyvykkyys tutkia ympäristöä, jossa se oli, jolloin se aktivoitui vain ollessaan oikeassa kohteessa. Mato kykeni seuraamaan ympäristöä ja ymmärtämään sentrifugien normaalitilan, jonka jälkeen se alkoi ohjata sentrifugien toimintaa ja syöttää monitoroiville järjestelmille normaalitilaa muistuttavaa metriikkaa. (Zetter, 2014).

Tässä kappaleessa on esitelty kyberturvallisuutta uhkaavia uhkia, toimijoita, motivaatioita ja menetelmiä. Kyseinen aihe alue kehittyy ja muuntuu koko

ajan ja luokittelua voidaan tehdä eri näkökulmista. Kappaleen ei ole tarkoitus olla täydellinen listaus yllä mainituista asioista, vaan antaa lukijalle hyvä yleiskatsaus yleisimmistä tekijöistä. Seuraavassa luvussa vedetään yhteen aiempi ja määritellään, mikä on kyberonnettomuus ja miten se voisi tapahtua.

2.4 Kyberonnettomuus

Tutkimuksessa käytetyn määritelmän mukaisesti *kyberonnettomuus on tahallisesti tai tahattomasti toteutunut kyberuhka, joka kohdistuu kybertoimintaympäristöön vaarantaen ympäristön ja siitä riippuvaisen toiminnon osittain tai kokonaan*. Käytännössä määritelmällä tarkoitetaan onnistunutta kyberhyökkäystä, yllättämään päässyttä harmaata tai mustaa joutsenta tai muuta vahinkoa. Kyberonnettomuus voidaan kuvata edellisen kappaleen esille nostamien elementtien (taulukot 3-6) kautta kaavana: *toimija(t) + motivaatio(t) + menetelmä(t) = vaikutukset*.

Taulukko 3 Yhteenveto uhkatoimijoista

Toimijat
Sisäpiiri
Kybervandaalit, haktivistit ja muut mustahattu hakkerit
Kyberrikolliset
Kyberterroristit
Valtiolliset toimijat ja APT-ryhmät
Ulkopuoliset

Taulukko 4 Yhteenveto uhkatoimijoiden motivaatioista

Motivaatiot
Vandalismi/hakkerointi
Rikollisuus
Tiedustelu/vakoilu
Terrorismi
Kybersodankäynti
Vahingot

Taulukko 5 Yhteenveto uhkatoimijoiden menetelmistä

Menetelmät
Fyysiset: kineettinen isku, saastuneen työkalun käyttöön saattaminen
Sosiaaliset: Kalastelu, kiristys, hujaus. lahjonta, houkuttelu
Tekniset: virus, mato, spyware, rootkit, botnet, troijalaiset, kiristyshaittaohjelmat, tuhoavat haittaohjelmat

Taulukko 6 Yhteenveto uhkien vaikutuksista

Vaikutukset
Vahingollinen vaikutus fyysisen maailman rakenteisiin
Vahingollinen vaikutus fyysisen maailman toimijoihin ja prosesseihin
Tiedon saatavuus vaarantuu
Tiedon eheys vaarantuu
Tiedon luottamuksellisuus vaarantuu

Tämän kaavan kautta mukaisesti voidaan käydä läpi kolme esimerkkitapausta. Ensimmäinen tapauksista on NotPetya, joka on maailman historian toistaiseksi tuhoisin haittaohjelma taloudellisten vaikutusten kautta mitattuna. NotPetya hyödynsi EternalBlue ja Mimikatz hyökkäysohjelmia ja levisi itsenäisesti niissä verkoissa, joihin sai jalansijaa. NotPetya oli todella tehokas ja saastutti esimerkiksi suuren ukrainalaisen pankin 45 sekunnissa. Tutkijoiden mukaan hyökkäys oli venäläisen APT-ryhmän tekemä ja kohdennettu Ukrainaan. Alun perin sitä levitettiin piilotettuna ohjelmistoon, jolla Ukrainassa toimivien yritysten piti hoitaa verotus. NotPetya pääsi kuitenkin tahallisesti tai tahattomasti leviämään 65 maahan ja saastutti n. 50 000 tietokonetta useilta toimialoilta mm. ydinvoimalan valvontajärjestelmä, terveydenhuollon järjestelmiä, logistiikkaa. Tuhojen aineelliset kustannukset arvioidaan olevan n. 10 miljardia dollaria. Yksi pahiten kärsineistä sivullisista uhreista oli Maersk. NotPetya kryptasi peruuttamattomasti lähes koko Maerskin infrastruktuurin ja pysäytti liiketoiminnan kokonaan. Maersk hoitaa viidenneksen globaalista logistiikasta. (Greenberg, 2019)

Taulukko 7 Kyberonnettomuuden esimerkkitapaus

Tapaus 1	NotPetya hyökkäyksen vaikutukset Maerskille
Toimija	**Ulkopuoliset**: Valtiolliset toimijat ja APT-ryhmät
Motivaatio	**Vahinko**: Maerskia pidetään sivullisena uhrina.
Menetelmä	**Tekninen haittaohjelma.** Matomaisesti levinnyt kiristyshaittaohjelma
Vaikutukset	**Tiedon saatavuus** menetettiin. **Tiedon eheys** menetettiin. Vahingollinen vaikutus **fyysisen maailman toimijoihin ja prosesseihin** Vahingollinen vaikutus **fyysisen maailman rakenteisiin**. Maerskin liiketoiminta pysähtyi. Globaali logistiikka pysähtyi suurelta osin. Tietojärjestelmäpalvelut ei olleet käytössä ja peruuttamattomasti kryptatut tiedot menetettiin.

Toisena tapauksena on onnettomuus, jossa ministeriöiden ja virastojen tietoliikenneyhteydet katkesivat lähes vuorokaudeksi. Onnettomuuden seurauksena useat tietojärjestelmäpalvelut, kuten sähköposti ja etäyhteydet eivät olleet viranomaisten käytettävissä eivätkä kansalaiset voineet käyttää digitaalisia

julkispalveluita kuten omaveri ja suomi.fi. Onnettomuus johtui siitä, että kaivinkone katkaisi vahingossa Telian runkoverkkokaapelin. Toinen osa onnettomuutta oli arkkitehtuurinen, jossa sovitusta poiketen varayhteydet kulkivat samassa kaapelikourussa kuin pääyhteys, jolloin onnettomuuden seurauksena menetettiin myös varayhteys. Tietoliikenteestä vastaa Valtion tieto- ja viestintätekniikkakeskus Valtori, joka on hankkinut palvelun Tieto-Evryltä, joka ostaa valokuituyhteyden Telialta. (HS, 2021; verkkouutiset, 2021)

Taulukko 8 Kyberonnettomuuden esimerkkitapaus 2

Tapaus 2	Valtionhallinnon tietoliikenneyhteyksien katkeaminen
Toimija	**Ulkopuoliset**: kaivinkoneurakoitsija
Motivaatio	**Vahinko**: Teki tilattua kaivuu työtä eikä tiennyt kaapelista. Pää- ja varayhteys kulki samassa kaapelikourussa.
Menetelmä	**Kineettinen isku**: Kaapelin katkaisu kaivinkoneella
Vaikutukset	**Tiedon saatavuus** menetettiin. Vahingollinen vaikutus **fyysisen maailman toimijoihin ja prosesseihin** Useat valtionhallinnon käyttämät IT-palvelut olivat poissa viranomaisten käytöstä usean tunnin ajan. Kansalaisten digitaaliset palvelut eivät olleet käytettävissä katkona aikana.

Kolmas tapaus psykoterapiakeskus Vastaamon tietomurto vuodelta 2021. Tapauksen taustalla on vuonna 2015 toteutettu potilastietojärjestelmä, jonka tietokanta rakentuu Linux-käyttöjärjestelmästä ja MySQL -tietokantaohjelmistosta. Potilastietokannan on toteuttanut itseoppinut koodari, joka toimi murron aikana Vastaamon toimitusjohtajana. 2017 potilastietojärjestelmään tehtiin muutoksia, joiden yhteydessä palvelimen portti 3306 jäi avoimeksi. Tietomurron aikana palvelin oli suojattu heikolla salasanalla ja siihen oli avoin yhteys internetistä. Tämän seurauksena tekijä sai varastettua arkaluonteiset potilastiedot ja kiristi tällä Vastaamoa. Kun Vastaamo ei suostunut vaadittuihin lunnaisiin, ryhtyi hyökkääjä kiristämään suoraan potilaita. Lopulta hyökkääjä julkaisi vahingossa kaikki tiedot TOR-verkkoon hetkellisesti, mutta sen aikana ne ehdittiin jo kopioida useisiin muihin paikkoihin. Tämän jälkeen hyökkääjällä ei ollut enää millä kiristää ja tekijä katosi verkosta. (Jyu, 2022; Ralston, 2020).

Taulukko 9 Kyberonnettomuuden esimerkkitapaus 3

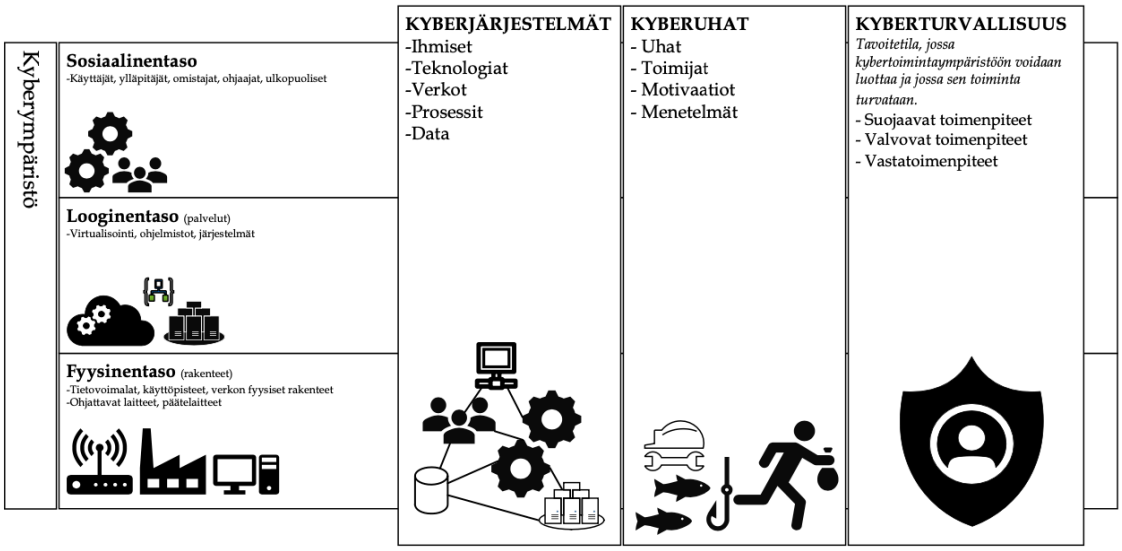
Tapaus 3	Vastaamon tietomurto
Toimija	**Sisäpiiri**, huolimaton ylläpitäjä **Kyberrikollinen**
Motivaatio	**Vahinko**, huolimattomuudella mahdollistettiin tietomurto. (palvelin tarpeettomasti yhteydessä julkiseen internettiin ja heikko salasana) **Rikollisuus**: Kyberrikollinen pyrki saamaan taloudellista etua kiristämällä Vastaamoa ja uhreja.

Menetelmä	Tekninen: heikkosalasana murrettiin todennäköisesti brute force -menetelmällä tai sanakirjahyökkäyksellä
Vaikutukset	**Tiedon luottamuksellisuus menetettiin**. Kymmenien tuhansien potilaiden luottamukselliset potilastiedot ovat kenen tahansa luettavissa edelleen. **Vahingollinen vaikutus fyysisen maailman toimijoihin ja prosesseihin.** Muutamia esimerkkejä: - Tietomurron uhreilla murto aiheutti monenlaisia kärsimyksiä sekä henkisesti että fyysisesti (identiteetti varkaudet). - Rikosilmoitukset ruuhkauttavat poliisin esitutkintaprosessin (yli 25000 rikosilmoitusta). - Vastaamo meni konkurssiin.

Tässä kappaleessa on käyty läpi kyberonnettomuuden käsitettä kolmen esimerkin kautta ja vedetty yhteen edellisen kappaleen kyberuhat, toimijat, motivaatiot ja menetelmät yhdeksi taulukoksi. Huomioitavaa kyberonnettomuuden käsitteessä on, että se kattaa tarkoituksellisen hyökkäyksen lisäksi myös vahingot.

2.5 Kybertoimintaympäristön viitekehys

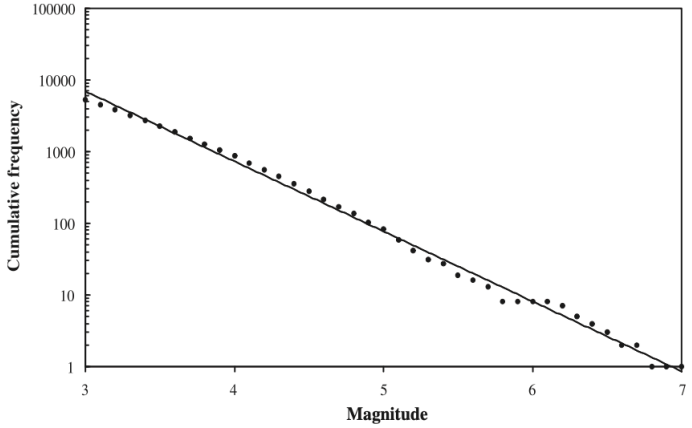
Tämän luvun aikana on rakennettu kyberympäristön viitekehys palapalalta ja johon nyt täydennetään mukaan vielä edellisessä kappaleessa läpikäydyt kyberuhat (kuvio 12). Viitekehys koostuu nyt kyberjärjestelmistä, niitä uhkaavista uhista sekä uhkilta suojaavilta kyberturvallisuuden toimilta. Viitekehyksen mukaisesti nämä kolme tekijää jakautuu kolmelle tasolle: sosiaalinen, looginen ja fyysinen. Seuraava luku kuvaa teorioita, jotka pyrkivät selittämään tekijöitä onnettomuuksien taustalla. Jokaisesta teoriaa peilataan kybertoimintaympäristön viitekehykseen ja käsitellään siitä nousevien esimerkkien kautta.



KUVIO 12 Kybertoimintaympäristön viitekehys

3 MIKSI ONNETTOMUUKSIA TAPAHTUU?

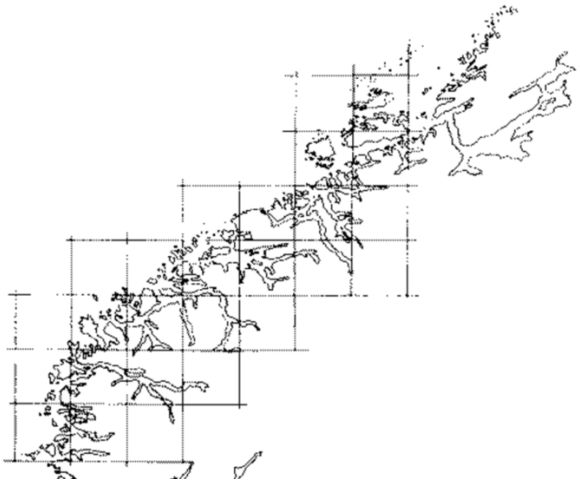
Per Bakin (1996) mukaan katastrofit ja onnettomuudet seuraavat yksinkertaisia malleja, joita on löydettävissä kaikkialta. Maanjäristykset noudattavat yksinkertaista jakaumafunktiota nimeltään Gutenberg-Richter laki. Tämän lain mukaan maanjäristysten laajuus ja teho noudattaa kaavaa, joka voidaan kuvata kuvion 13 mukaisella logaritmisella asteikolla suorana. Käytännössä tämä tarkoittaa sitä, että kun tapahtuu esimerkiksi 1000 maanjäristystä 4 richterin voimakkuudella, tapahtuu myös 100 maanjäristystä voimakkuudella 5, 10 kpl voimakkuudella 6 ja yksi voimakkuudella 7. (Gutenberg & Richter, 1955).



KUVIO 13 Gutenberg–Richter laki maanjäristysten jakautumisesta SGI tietokannan tietojenpohjalta. Aineistosta poistettu esi- ja jälkijäristykset. (Morales-Esteban, A., Martínez-Álvarez, F., Troncoso, A., Justo, J. L. & Rubio-Escudero, C. (2010).

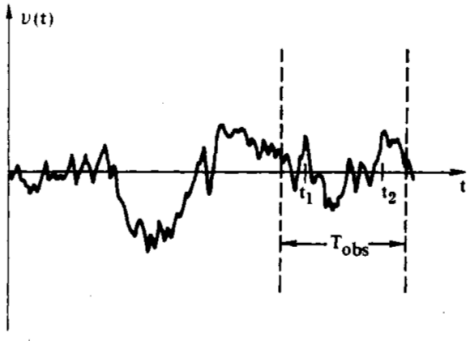
Mandelbrot (1982) havaitsi fraktaalien olemassaolon yrittäessään laskea Britannian rannikon pituutta. Asiaa tutkiessaan hän huomasi luonnon koostuvan fraktaaleista muodoista, jotka ovat itsesimilaareja mittasuhdevapaita muotoja. Tarkoittaen sitä, että ne näyttävät samalta riippumatta siitä miltä suurennostasolta niitä katsotaan. Esimerkiksi kuvion 14 Norjan vuonot ovat vuonoja, jotka koostuvat vuonoista, jotka koostuvat vuonoista. Keskimääräistä vuononpituutta ei voida laskea koska fraktaalissa mittaustarkkuuden kasvaessa pituus kasvaa rajatta, eli äärettömäksi. Mandelbrotin tutkimuksessa mittaustapana käytettiin kuvan 2 mukaisesti määräkokoisia neliöitä, joilla valittu kartta-alue

peitettiin. Tutkimuksessa huomattiin, että mittakaavasta riippumatta mitatun alueen vuonojen pituuden suhde tarvittavien neliöiden määrään noudattaa funktiota, joka voidaan kuvata logaritmisen asteikon suorana. Samaa mallia noudattavia fraktaalimuotoja ovat mm. pilvet, vuoristot ja galaksit.



KUVIO 14 Fraktaaleista koostuva Norjan rannikko peitettynä mittausneliöillä (Man-delbrot, 1982).

1/f-kohina, vaaleanpunainenkohina, on ilmiönä yksi fysiikan suurimmista mysteereistä. Sitä on havaittu laajasti erilaisista järjestelmistä kuten Niilin joen virtauksesta, kvasaarien valosta, moottoritien liikenteestä tai maapallon lämpötilan vaihteluista. Jopa ihmisaivoista ja musiikista löytyy vaaleanpunaista kohinaa. (Keshner, 1982). Kohinasignaali on visuaalisesti luonnollisen näköinen ja sisältää vaihtelua niin taajuudessa kuin amplitudissa (kuvio 15). Signaali on mittasuhdevapaa fraktaali, joka muistuttaa vuoristomaisemaa laaksoine ja tasankoineen. Soitettuna se kuulostaa tuulelta tai merenkohinalta. (Per Bak, 1996).



KUVIO 15 Näyte 1/f-kohinasta. Kuvassa näkyy koko näyte sekä siitä erotettu lyhyen ajan näyte. (Keshner, 1982).

1949 professori George Kingsley Zipf Harvardin yliopistosta julkaisi kirjan *Human Behaviour and the Principle of Least Effort*, joka sisälsi merkittäviä huomioita säännöllisyydestä ihmisten rakentamissa järjestelmissä. Hän tutki vuoden 1920 kaupunkien kokoja. Raportin mukaan yli 8 miljoonan asukkaan kaupunkeja oli pari kappaletta, miljoonan asukkaan kaupunkeja oli 10 kappaletta ja 200 000 asukkaan kaupunkeja 100 kappaletta. Kaupunkien lukumäärät suhteessa

väestömääriin voidaan kuvata jälleen logaritmisen asteikon suoralla viivalla. Zipf teki vastaavia havaintoja monesta muustakin asiasta kuten esimerkiksi englannin kielen yleisimmistä sanoista, jotka voidaan piirtää logaritmiselle suoralle esiintymistiheyden mukaisesti. Tulokset ovat samoja riippumatta mistä lähteestä sanat otettiin (kirja, keskustelu jne.) ja pätee kaikille kielille. (Wentian 2002).

Nämä neljä, *Gutenberg-Richter laki*, *fraktaalit*, *1/f-kohina* ja *Zipf'sin laki* ovat luonteeltaan tilastollisia havaintoja. Gutenberg-Richter laki osoittaa montako erikokoista maanjäristystä tapahtuu, mutta se ei kerro milloin ja missä nämä tapahtuvat. Zipfin havainnot kertovat montako minkäkin kokoista kaupunkia on, mutta ei selitä miksi. (Bak 1996). Kaikki nämä havainnot voidaan esittää logaritmisen asteikon suoralla, mutta mitä se tarkoittaa? Matematiikassa tällaista log-log suoraa kutsutaan Zipfin laiksi. Zipfin lain mukaisen logaritmisen asteikon kuvaaja on normaaliasteikolla nimeltään voimalaki, joka kuvaa satunnaisuutta. Voimalain ja Zipfin lain mukaiset kuvaajat on esitetty kuviossa 25. Voimalain mukaista käytöstä pidetään itseorganisoituneen kriittisyyden ominaispiirteenä (Bak, 1996; Lewis, 2010; Bibighaus, 2015).

Tämän pitkän aasinsillan kautta tutkimuksessa esitetään seuraavaksi onnettomuuksia ja katastrofeja selittäviä teorioita ja miten ne liittyvät edellä kuvattuihin luonnosta löytyviin malleihin. Kappale 3.1 kertoo miksi ihmiset tekevät virheitä. Kappale 3.2 kertoo, miksi virheistä aiheutuu onnettomuuksia ja miten tämä rapauttaa järjestelmää. Kappale 3.3 kuvaa teorian itseorganisoituneen kriittisyyden taustalla sekä tästä aiheutuvat tapahtumat.

3.1 Epäonnistumisen logiikka

Toisin kuin muut elävät olennot, ihmiset osaavat adaptoitua epävarmuuteen. Ihmiset osaavat tunnistaa epävarmuutta aiheuttavat tekijät ja muodostaa näistä hypoteeseja, joiden kautta ikäviä vaihtoehtoja voidaan ennakoida ja pyrkiä välttämään. Ihmiset osaavat odottaa odottamatonta ja valmistautua tähän. Vai osaavatko? Tämän kaltaista toimintastrategiaa tutkittiin Dörnerin (1989) julkaisemassa kirjassa *The logic of Failure: Why Things Go Wrong and What We Can Do To Make Them Right.*

Kirjassa kuvataan tutkimusta, jossa tietokoneohjelma simuloi Länsi-Afrikkaan sijoittuvan Moron kylän elämää 20 virtuaalisenvuoden aikana. Järjestelmällä on tarkoitus testata henkilöiden toteuttamia toimintastrategioita ja se on erittäin kompleksinen sisältäen suuren määrän muuttujia, kuten syntyvyys, kuolleisuus, vedenmäärä jne. Muuttujilla voidaan vaikuttaa simulaation kulkuun. Testattaville Moro-järjestelmä on dynaamisen päätöksenteon ongelma. Testi toimii siten, että testattavat voivat kerran vuoronsa aikana kerätä tiedot järjestelmän tilasta, päättää uusista toimista ja toteuttaa ne. Yksi vuoro tarkoittaa yhtä virtuaalista vuotta simulaatiossa. Seuraavalla kierroksella testattavilla on käytettävissä tiedot edellisen kierroksen toimenpiteiden vaikutuksista, joiden perusteella testattavat voivat päättää seuraavista toimenpiteistä. Toimenpiteet

voivat olla esim. traktoreiden hankinta tai kaivojen kaivaminen. Järjestelmässä on mahdollista luoda hyvät elinmahdollisuudet Morolaisille pitkällä aikavälillä.

Testin tarkoitus oli saada yleinen näkemys toiminnan sääntelyn psykologiasta kompleksisessa todellisuudessa. Testissä oli mukana 45 johtajaa, joiden suoriutumista verrattiin opiskelijoiden suoriutumiseen. Kokonaisuudessaan johtajat pärjäsivät hyvällä johtamisellaan testissä paremmin kuin opiskelijat. Heidän kansansa rikastui, karjan määrä oli suurempi, kasvillisuuden peitto oli laajempi kuten myös väestön määrä. Ylipäätään katastrofeja oli vähemmän.

Testissä huomattiin kuitenkin suuri määrä erilaista virheellistä käyttäytymistä, jotka johtivat epäonnistumiseen kompleksissa tilanteissa. Pääasialliset virheet, jotka tunnistettiin, olivat:

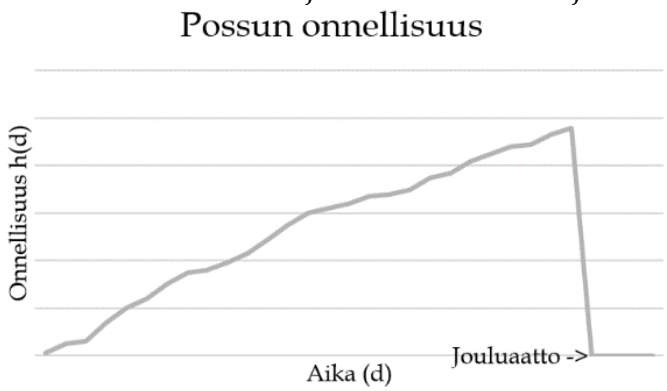
- Riittämätön tavoitteiden asetanta, jolloin toimenpiteet kohdistuvat akuuttiin ongelmaan eivätkä pitkäaikaiskehitykseen.
- Riittämättömät hypoteesit järjestelmän rakenteesta, jolloin sivu- ja pitkäaikaisvaikutukset jätetään huomioimatta.
- Riittämätön ja oikea-aikainen kuva järjestelmän käyttäytymisestä johti kehityssuuntausten laiminlyöntiin.
- Riittämätön koordinaatio eri toimenpiteiden välillä johti törmäyksiin.
- Vääriä hypoteeseja ja sopimattomia strategioita ei havaittu.
- Itsereflektion puute, jolloin vääriä hypoteeseja ja sopimattomia strategioita ei korjattu

Yhteenvetona Dörnerin (1990) tutkimuksessa todettiin, että testaajat eivät käsitelleet järjestelmää kompleksisena järjestelmänä vaan kasana irrallisia muuttujia, joita voidaan käsitellä erikseen. Testattavat eivät esimerkiksi huomioineet, että veden nostaminen kaivoista vaikuttaa pohjaveden korkeuteen. Testattavat olettivat lineaarista kehitystä, vaikka tilanne selvästi näytti, että kehityksen täytyy olla epälineaarista. Testattavat eivät ottaneet huomioon epälineaarista kehitystä eivätkä yllättäviä katastrofisia kehityksiä.

Vaikka edellä esiteltyjen virheiden mukainen toiminta ei ole riittävää, jotta sillä selviydytään kompleksisessa järjestelmässä, soveltuu se erittäin hyvin johonkin muuhun. Ihmisen tietoinen ajattelu on hidasta eikä kykene käsittelemään suurta määrää tietoa aikayksikköä kohti. Pyrkimys käyttää rajoitettua resurssia taloudellisesti voi siis olla järkevää. Dörnerin (1990) mukaan tämä kuitenkin johtaa rajoitettuun tiedonkeruuseen, lineaariseen ekstrapolointiin ja rajoitettuun hypoteesin muodostamiseen. Lineaarinen ekstrapolointi olettaa asioiden jatkuvan samalla tavalla. Käytännössä tämä tarkoittaa, että ihminen ei kykene vastaanottamaan ja käsittelemään niin paljoa tietoa kuin olisi tarve, jolloin ihminen muodostaa väärän hypoteesin vajaisiin tietoihin pohjaten ja olettaa kaiken jatkuvan vanhaa rataa. Saman ilmiön Taleb (2007) nosti esille puhuessaan Mustalle Joutsenelle altistavista ulkoisista mekanismeista.

Tällaista kutsutaan induktio-ongelmaksi, joka tarkoittaa induktiiviseen päättelyyn liittyvää ongelmaa siitä kuinka paljon tulevaa voidaan päätellä menneestä. Induktio-ongelmaa voidaan havainnollistaa Talebin (2007) mallia mukaillen possuesimerkin kautta, jossa possun onnellisuus ja luottamus ihmiseen kasvaa tasaisesti päiväpäivältä, kun sitä ruokitaan. Tasainen kehitys päättyy kuitenkin romahdukseen jouluviikolla (kuvio 16). Induktiivisesti pääteltynä possu

odotti onnellisuuden ja huolenpidon jatkuvan loputtomiin eikä se menneen perusteella osannut kuvitella joutuvansa uuniin jouluna.



KUVIO 16 Possun onnellisuus esimerkkinä induktio-ongelmasta.

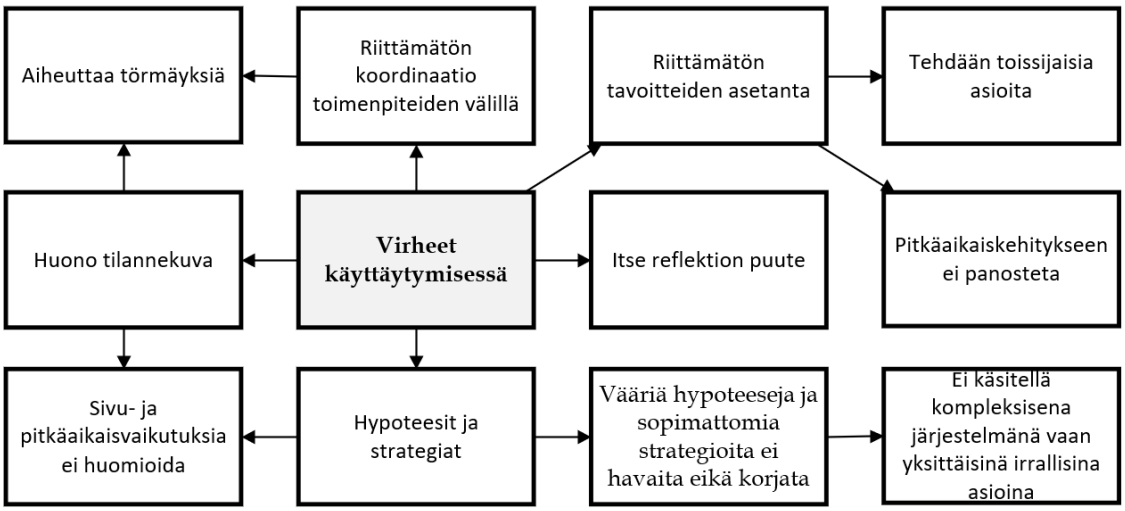
Kuten Dörner (1990) ja Taleb (2007) havainnoivat, ihmiset käyttävät myös induktiivista päättelyä ja olettavat että tulevaisuus muistuttaa nykyisyyttä. Induktiivinen päättely ei kuitenkaan ole luotettavaa, sillä menneestä voidaan tehdä monenlaisia yleistyksiä, jotka ennakoivat tulevaa eri tavalla. Talebin (2007) mukaan tämä altistaa meidät Mustille Joutsenille, eli ennustamattomille tapahtumille, joilla on valtavat vaikutukset.

Muut ongelmalliset käyttäytymistavat johtuvat taipumuksesta suojella omaa osaamistaan. Ihmisillä on vahva taipumus suojata mielipiteensä omasta osaamisestaan toimia. Tällä on tietyssä määrin järkeä, koska joku, joka pitää itseään toimintakyvyttömänä, tuskin toimii. Oman mielipiteen vartioiminen osaamisestaan on tärkeä motivaatio. Säilyttääkseen korkean olettamuksen omasta osaamisestaan, ihmiset eivät huomaa dataa, joka kaataa hypoteesin. Henkilöt käsittelevät ongelmia, jotka heillä on käsillä nyt, eivätkä niitä, joita heillä ei vielä ole. Henkilön koko keskittyminen ei kuitenkaan pitäisi olla käsillä olevassa asiassa vaan osittain myös tulevassa. Toisaalta unohtaminen on luonnollista ja aiheuttaa sen, että vain osa vanhasta datasta on käytettävissä. (Dörner, 1990).

Huomattavaa on, että tutkimuksen mukaan johtajien tilannekuva ei ollut yhtään parempi kuin opiskelijoiden, mutta he osasivat adaptoitua tilanteeseen paremmin ja tuntevat toimintamalleja eri tilanteisiin. Tätä Dörner (1989) kutsuu strategiseksi joustavuudeksi, joka on opittavissa mutta sitä on vaikea opettaa.

Kuviossa 17 on kuvattu Dörnerin tutkimustuloksista avaintekijät, jotka selittävät virheellistä käytöstä. Virheellisellä käytöksellä voidaan aiheuttaa

kriittisen järjestelmän keikahtaminen reunan yli ja komponenttien vikaantuminen. Seuraavassa kappaleessa tutkitaan normaalien onnettomuuksien teoriaa.



KUVIO 17 Virheet käyttäytymisessä Dörnerin (1990) tutkimuksen mukaisesti.

3.2 Normaalien onnettomuuksien teoria

Seuraavassa kappaleessa kerrotaan mikä on normaali onnettomuus ja miksi se on odotettavissa oleva ja väistämätön. Kappale esittelee kompleksisen järjestelmän sellaisena kuin se NAT-teoriassa kuvataan, perehdyttää teoriaan ja kuvaa kaksi oleellista tekijää, jotka teorian mukaisesti johtavat väistämättömiin onnettomuuksiin. Näitä ovat interaktiivinen kompleksisuus ja tiukat kytkennät. Teoriaa kuvataan kyberjärjestelmästä tuttujen komponenttien ja tapahtumien kautta esimerkein.

Tervetuloa korkean riskin teknologioiden maailmaan. Näin aloitti Charles Perrow (1984) kirjansa *Normal Accident Theory*, jossa esiteltiin samoin nimetty teoria (engl. *normal accident theory, NAT, normaalien onnettomuuksien teoria*). Teorian juuret juontavat aikaan, jolloin sosiologi Charles Perrow'ta pyydettiin toimittamaan taustaraportti Presidentin toimikunnalle Three Mile Islandin (*TMI*) ydinvoimalaonnettomuudesta 1979. Perrown näkökulma onnettomuustutkintaan oli organisatorinen ja tämä näkyy myös teorian muotoilussa. Teorian tarkoitus ei siis ole yksittäisen syyllisen selvittämisessä, vaan selittää, kuinka organisaatiojärjestelmät ovat kehittyneet tällaisten onnettomuuksien mahdollistamiseksi (Nunan & Domenico, 2017). Normaalit onnettomuudet ovat normaaleja siinä mielessä, että nämä negatiiviset tapahtumat ovat väistämättömiä ja tapahtuvat siellä, missä organisaatiot ovat sekä kompleksisia että tiiviisti kytkettyjä. Kirjassaan Perrow (1984) käsitteli teoriaa TMI-onnettomuuden lisäksi useiden teknologioiden ja toimialojen kautta, kuten ilmailu, ydinaseet, DNA-muokkaus, avaruusraketit jne. Oleellista teorian soveltamisessa oli, että Perrow käsitteli näitä kaikkia kokonaisuuksia järjestelminä. Tämän jälkeen teoriaa on laajennettu useiden tutkijoiden toimesta ja sovellettu fyysisten onnettomuuksien lisäksi mm. digitaalisen maailman dataonnettomuuksiin, tietoverkkojen fyysisiin rakenteisiin ja IT-

järjestelmiin. (Martínez, Eng & Kim, 2012; Dorner, 2014; Nunan & Domenico, 2017).

Normaalit onnettomuudet ovat onnettomuuksia, jotka ovat odotettavissa ja väistämättömiä kun tietyt reunaehdot täyttyvät. Tätä on helpoin selventää seuraavalla esimerkillä. Eräänä aamuna jäät kotiin töistä koska sinulla on tärkeä tapaaminen kaupungilla ja sinne on nopeampi mennä suoraan kotoa. Puolisosi on keittänyt aamulla kahvia ja jättänyt lähtiessään keittimen päälle. Heräät kuitenkin vähän myöhemmin, jolloin lasinen kahvipannu on kiehunut tyhjäksi ja haljennut. Olet kahviaddikti, joten kaivat kaappia, kunnes löydät vanhan keittimen. Alkaa olla jo kiire, mutta kahvia on saatava. Odottelet kelloa katsoen kahvin tippumista ja vihdoin kun se on valmista, nappaat kupillisen mukaan ja lähdet. Autolle päästyäsi huomaat kiireessä unohtaneesi kaikki avaimet sisälle. Mutta ei hätää, sinulla on vara-avain piilossa tällaisia tapauksia varten. Muistit kuitenkin antaneesi tämän avaimen edellisellä viikolla kaverillesi lainaan, jotta hän voi käydä lainaamassa muutaman kirjan poissa ollessasi. Tämä on ensimmäinen turvakontrollisi, joka pettää.

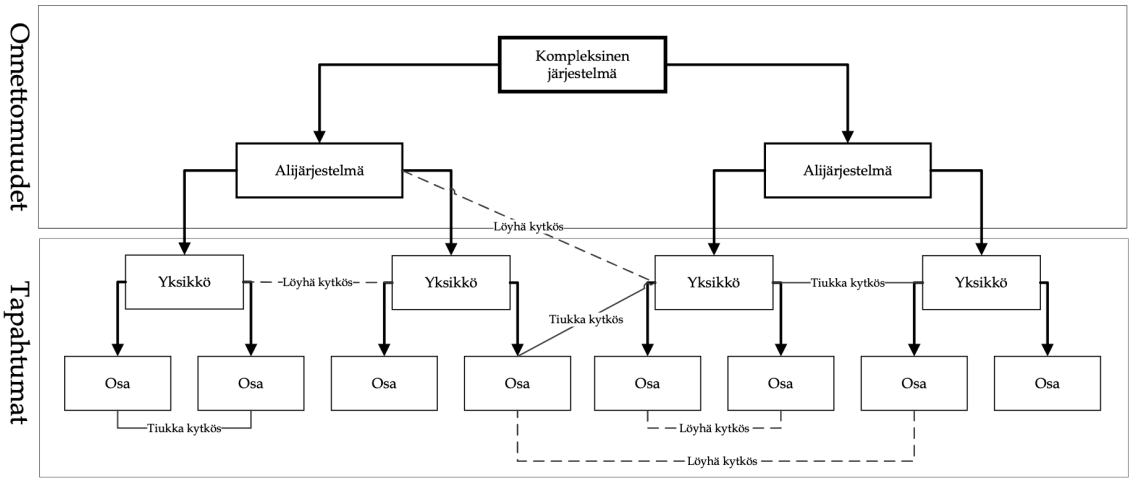
Alat olla myöhässä, mutta onhan naapurilla onneksi auto. Koputat naapurisi ovelle ja hän kertoo auton jäähdyttimen rikkoutuneen eivätkä varaosat ole vielä saapuneet. Jo toinen turvakontrolli pettää, mutta tällä ei ole mitään suoraa kytköstä toimintaasi. Avain ja jäähdytin ovat yksittäisiä komponentteja, joilla ei ole suoraa tekemistä keskenään, joten niiden välillä ei ole kytkentää (engl. *uncoupled*). No, mutta onhan aina olemassa bussi. Paitsi, että naapuri, jonka ovella seisot edelleen, kertoo bussinkuljettajien menneen lakkoon. Nyt kolmas turvajärjestelmäsi petti. Soitat naapurisi puhelimesta taksin, mutta ne ovat kaikki varattuja johtuen bussinkuljettajien lakosta. Neljäs turvakontrolli petti juuri. Tässä tapauksessa lakon ja taksien puutteen välillä on tiukka kytkentä koska toinen laukaisee toisen (engl. *tightly coupled*).

Soitat henkilölle, jota olit menossa tapaamaan ja kerrot, että tilanne on uskomaton, mutta kaikenlaista sattui etkä pääse paikalle ja pyydät uutta tapaamisaikaa. Uutta tapaamista ei kuitenkaan koskaan tapahdu, joten koit henkilökohtaisen onnettomuuden. NAT-teorian mukaan onnettomuuden syynä ei ollut inhimillinen virhe (*kahvipannu ja avaimet*), eikä syynä ollut mekaaninen vika tai ympäristö. (*jäähdytin, bussit ja taksi*). Kyseessä ei ollut myöskään suunnitteluvika, vaikka saitkin lukittua avaimet sisään. Teorian mukaan kyseessä oli monimutkaisesta järjestelmästä johtuva normaali onnettomuus. Yksittäiset tapahtumat olivat sellaisia, että niiden odotetaankin tapahtuvan satunnaisesti, jolloin niillä ei ole suurta vaikutusta ja niiden varalle on olemassa varmistuksia ja korvaavia vaihtoehtoja. Pienistä tapahtumista kasvaa suuri ongelma, kun ne ovat vuorovaikutuksessa toisiinsa. Ja tämä selittää onnettomuuden. (Perrow, 1984).

3.2.1 Perrow:n kompleksinen järjestelmä

Perrow (1984) kuvaa kirjassaan kompleksisen järjestelmän mallina, jossa järjestelmä koostuu *alijärjestelmistä*, jotka koostuvat *yksiköistä*, jotka koostuvat *osista*. Vikatilanteet, jotka kohdistuvat osiin ja yksiköihin ovat teorian mukaisesti tapahtumia (engl. *incident*) kun taas alijärjestelmiin ja järjestelmiin kohdistuvat häiriöt

ja viat ovat onnettomuuksia (engl. *accident*). Esimerkki rakenteesta on kuvattu kuviossa 18.



KUVIO 18 Perrow:n (1984) järjestelmärakenne ja onnettomuuksien taso.

Se, mikä on muuttunut Perrown ajoista, on digitaalisuuden nousu ja uudenlaisten toimijoiden ja liiketoimintojen syntyminen. Hallitusten rooli tiedon kerääjinä on aina ollut tärkeä valtion turvallisuuden ja keskeisten palveluiden kannalta, mutta nykyisin on nähtävissä kaupallisten toimijoiden kasvava merkitys sekä tiedonkeruun että -analyysin veturina. Informaatioteknologian aiempia sukupolvia hallitsivat yritykset, joilla oli asiantuntemusta laitteistosta tai ohjelmistoista ja muutamilla harvoilla molemmista. Nyt monilla johtavilla Internet-yrityksillä on kaupalliset strategiat, jotka perustuvat tietojen keräämiseen. Googlen, Facebookin ja muiden yritysten kaltaisille organisaatioille tiedon keräämisestä on tullut päämäärä itsessään, eikä tukipalvelu muiden liiketoimintatavoitteiden saavuttamiseksi. (Li, Nirei ja Yamana, 2018).

Nunan ja Domenicon (2017) artikkelissa esitetään, että moderneilla organisaatioilla, jotka keräävät ja hyödyntävät big dataa, on organisaatiojärjestelmässään ominaisuuksia, jotka ovat NAT:lle ominaisia. Normaalien onnettomuuksien seuraukset näissä datakeskeisissä organisaatioissa ovat kuitenkin vähemmän välittömästi konkreettisia kuin fyysisen katastrofin, mikä tekee tunnistamisesta ja korjaamisesta vaikeampaa. Käytännössä tämä tarkoittaa sitä, että dataonnettomuuden tapahtuma aikaa voi olla vaikea todentaa ja voi olla, että se havaitaan vasta pitkän ajan kuluttua esimerkiksi tilanteessa, jossa varastetut tiedot julkaistaan internetissä. Näin kävi esimerkiksi Vastaamon tapauksessa (Ralston, 2020).

3.2.2 NAT perusteet

Järjestelmäonnettomuuteen johtavat viat alkavat itsenäisistä yksiköistä tai alijärjestelmistä ja johtuvat jonkin komponentin vikaantumisesta tai käyttäjän virheestä. Kuten aiemmin tuli esille, perussyy normaalille onnettomuudelle on useiden vikojen käsittämätön vuorovaikutus tapauksessa, jossa viat eivät ole suorassa prosessin mukaisessa järjestyksessä. Käytännössä tämä tarkoittaa tilannetta, jossa toisistaan riippumattomista syistä tapahtuu useita vikoja, tapahtumia tai

onnettomuuksia ja joiden yhteisvaikutus on merkittävä ja aiheuttaa järjestelmäonnettomuuden. Käsittämättömyydellä tarkoitetaan tässä yhteydessä sitä, että tapahtumat ja niistä syntyneet tapahtumaketjut vaikuttavat käsittämättömiltä ja huonolta tuurilta. (Perrow, 1984).

Tunnettuja esimerkkejä kybermaailmaa kohdanneesta NAT:sta on Bradley Manningin ja Edward Snowdenin tapaukset, joissa tekijät onnistuivat keräämään ja julkaisemaan suuren määrän salassa pidettävää ja turvaluokiteltua tietoa. Manning julkaisi 260 000 diplomaattisähkettä Wikileaksissa (Leigh, 2010) ja Snowden vuoti suuren määrän NSA:n luokiteltua materiaalia medialle analysoitavaksi ja julkaistavaksi (Zetter, 2013). Tämä Pro Gradu -tutkimus ei ota kantaa olivatko vuodot laillisesti, eettisesti tai ihmiskunnan näkökulmasta oikein vai väärin, mutta kun asiaa tarkastellaan puhtaasti järjestelmän ja sen omistavan organisaation näkökulmasta, niin kyseessä on kyberonnettomuus. Nunan ja Domenico (2017) tutkivat asiaa NAT:n kautta katsottuna, ja esittivät että teoriaan peilaten kumpikaan tapahtumista ei johtunut Manningista tai Snowdenista itsestään, vaan järjestelmäonnettomuudesta kompleksisessa organisaatiossa, jonka sisäisissä järjestelmissä oli tiukkoja kytkentöjä. Nämä tiukat kytkennät aiheuttivat vikaantuessaan odottamattomia vaikutuksia muihin komponentteihin. Käytännössä organisaation turvakontrollit ja järjestelmät, jotka on kehitetty suojamaan tällaisilta tietovuodoilta, pettivät ja aiheuttivat onnettomuuden. Esimerkiksi Snowdenin tapauksessa pettivät sekä tietoturvapolitiikat ja sen toteutukset (*turvatyöasemassa voi käyttää usb-muisteja*), tietoturvavalvonta (*suurten datamäärien lataaminen ja tallentaminen ei laukaissut hälytyksiä tai niihin ei reagoitu*), fyysisen turvallisuuden kontrollit (*tiloihin kuljettiin läpivalaisun ja turvatarkastuksen kautta, mutta siitä huolimatta usb-muisti saatiin salakuljetettua ulos*) ja todennäköisesti myös vähimmän pääsyn periaate, jonka mukaisesti käyttäjällä tulisi olla pääsy vain sellaiseen tietoon jota työssään tarvitsee juuri sillä hetkellä. Vaikea nähdä, että järjestelmäylläpitäjä tarvitsisi pääsyä näin laajaan joukkoon luokiteltua operatiivista tiedustelutietoa. Tapahtumat sisälsivät siis paljon Perrown NAT:lle määrittämää ominaispiirrettä: käsittämättömyyttä.

Käsittämättömyyden lisäksi Perrow (1984) esittää kaksi ominaispiirrettä, jotka altistavat järjestelmän normaalille onnettomuudelle. Ne sisältävät komponenttien välistä *interaktiivista kompleksisuutta* ja *tiukkoja kytkentöjä*.

3.2.3 Kompleksisuus

NAT määrittää kuvion 19 mukaisesti kompleksisen järjestelmän olevan vastakohta lineaariselle järjestelmälle. Kompleksinen järjestelmä sisältää vuorovaikutuksia, joita esiintyy suunnittelemattomissa ja tuntemattomissa jaksoissa, ja jotka eivät ole näkyvissä tai heti ymmärrettävissä. Toisin sanoen kompleksista interaktiivisuutta, kuten tuntemattomia palautesilmukoita, esiintyy silloin, kun vuorovaikutusta ei täysin ymmärretä. Tämä on kriittistä silloin kun on tehtävä aikakriittisiä päätöksiä onnettomuuksien ehkäisemiseksi. Kompleksinen järjestelmä sisältää usein monikäyttöisiä komponentteja sekä erikoistuneen henkilöstön. Monikäyttöinen komponentti voi olla esimerkiksi sosiaalinen media, jota voidaan käyttää viestintään ja yhteydenpitoon, mutta myös tiedusteluun. Toinen esimerkki on vapaasti saatavilla olevat hyökkäystyökalut, kuten metasploit, joita

voidaan käyttää tietoturvatestaukseen tai kyberhyökkäykseen. Snowdenin tapaukseen viitaten esimerkki voisi olla turvatarkastus, jonka tehtävä on estää vaarallisen materiaalin tuonti turvatiloihin, mutta toisaalta estää luvaton tietojen vienti pois turva-alueelta.

TABLE 3.1
Complex vs. Linear Systems

Complex Systems	*Linear Systems*
Tight spacing of equipment	Equipment spread out
Proximate production steps	Segregated production steps
Many common-mode connections of components not in production sequence	Common-mode connections limited to power supply and environment
Limited isolation of failed components	Easy isolation of failed components
Personnel specialization limits awareness of interdependencies	Less personnel specialization
Limited substitution of supplies and materials	Extensive substitution of supplies and materials
Unfamiliar or unintended feedback loops	Few unfamiliar or unintended feedback loops
Many control parameters with potential interactions	Control parameters few, direct, and segregated
Indirect or inferential information sources	Direct, on-line information sources
Limited understanding of some processes (associated with transformation processes)	Extensive understanding of all processes (typically fabrication or assembly processes)

Summary Terms

Complex Systems	*Linear Systems*
Proximity	Spacial segregation
Common-mode connections	Dedicated connections
Interconnected subsystems	Segregated subsystems
Limited substitutions	Easy substitutions
Feedback loops	Few feedback loops
Multiple and interacting controls	Single purpose, segregated controls
Indirect information	Direct information
Limited understanding	Extensive understanding

KUVIO 19 Perrown (1986) kompleksisen ja lineaarisen järjestelmän ominaispiirteet.

Internet toimii hyvänä arkkiesimerkkinä kompleksisesta järjestelmästä, jonka sisällä nähtiin mielenkiintoinen vuorovaikutus sekä protokollien välillä (*NAT:osat*) että palveluiden välillä (*NAT:alijärjestelmä*) lokakuussa 2021. Facebookin ylläpitäjä teki muutoksen reitittimen konfiguraatioon, joka virheellisesti kadotti Facebookin DNS ja BGP reititystiedot. Tämän seurauksena palvelut eivät olleet saatavilla 3,5 miljardille käyttäjälle kuuteen tuntiin. Suorat vaikutukset tällä palvelukatkolla oli useiden miljoonien menetykset mainostuloissa. Yllättävät vaikutukset katkosta tulivat kuitenkin muille somepalveluille kuten Twitterille, Telegramille ja TikTokille, jonne Facebookin kävijät siirtyivät nopealla aikataululla ja aiheuttivat odottamattoman määrän palvelupyyntöjä ja tukkivat nämäkin palvelut (Kuvio 20) (Cloudflare, 2021; Janardhan, 2021). Järjestelmien suunnittelijat pyrkivät tietenkin estämään tahattomien vuorovaikutusten mahdollisuudet ja

lisäävät mukaan puskureita ja muita turvatekijöitä. Nämä turvatekijät kuitenkin lisäävät järjestelmän kompleksisuutta itsessään (Perrow, 1982).

KUVIO 20 Tilasto verkkoliikenteestä Facebookin häiriön ajalta.

3.2.4 Tiukka kytkentä

Toinen normaalin onnettomuuden komponentti, joka itsessään on riippumaton kompleksisesta vuorovaikutuksesta, on tiukan kytkennän vaatimus. Tiukka kytkentä tarkoittaa kompleksisen järjestelmän sisäisten prosessien, toimijoiden ja komponenttien välistä tiukkaa yhteistoimivuutta, jossa vuorovaikutus tapahtuu nopeasti ja esteettömästi. Tiukasti yhteen kytketyillä järjestelmillä on usein aikakriittisiä muuttumattomia prosesseja ja ne on suunniteltu tuottamaan lopputuotetta vain yhdellä tavalla. Usein tämä on tehokkuuskysymys, mutta joskus tuotantoprosessiin liittyvä asia. Esimerkiksi Internet on löyhästi kytketty kompleksinen järjestelmä, joka on suunniteltu kylmän sodan aikana selviytymään, vaikka osa siitä tuhoutuisi. Internet-yritysten liiketoiminnan takana on puolestaan tiukasti yhteen kytketty infrastruktuuri ja palveluntuottajat, jotka yhdistävät kaikki organisaatiot, jotka ovat riippuvaisia tästä teknologiasta (Nunan ja Domenico, 2017). Esimerkiksi verkkokauppayrittäjä on riippuvainen muista verkkopalveluista, kuten maksujärjestelmät (luottokortit, applepay, paypall), integraatiot sosiaaliseen mediaan, sisällön siirtoverkkopalvelun (CDN) tarjoajiin, asiakkuudenhallintaan ja varastojärjestelmiin, web-analytiikkaan ja moneen muuhun. Tiukasti yhteen liitettyjen järjestelmien sekvenssit ovat usein muuttumattomia, jossa B-tapahtuma ei voi tapahtua ennen tapahtumaa A. Käytännössä siis verkkokaupan asiakas ei voi ostaa tuotetta käyttäen maksuliikennejärjestelmää ennen kuin asiakas on tunnistettu. Tässä esimerkissä sekä identiteetin- ja pääsynhallinnanjärjestelmä että maksuliikennejärjestelmä ovat irrallisia alijärjestelmiä ja voivat olla kolmannen osapuolen tuottamia. Kuviossa 21 on kuvattuna Perrown (1984) mukaisesti tiukan ja löysän kytkennän ominaispiirteet.

TABLE 3.2
Tight and Loose Coupling Tendencies

Tight Coupling	*Loose Coupling*
Delays in processing not possible	Processing delays possible
Invariant sequences	Order of sequences can be changed
Only one method to achieve goal	Alternative methods available
Little slack possible in supplies, equipment, personnel	Slack in resources possible
Buffers and redundancies are designed-in, deliberate	Buffers and redundancies fortuitously available
Substitutions of supplies, equipment, personnel limited and designed-in	Substitutions fortuitously available

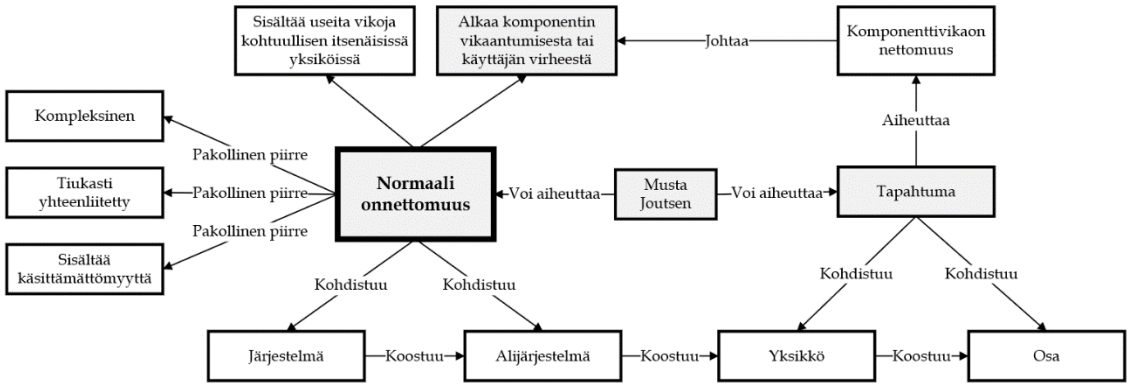
KUVIO 21 Perrown (1986) tiukan ja löyhän kytkennän ominaispiirteet

Eräänlainen normaalien onnettomuuksien vastateoria on HRO (High Reliability Organization). HRO:t ovat organisaatioita, jotka toimivat vaativissa ja/tai vihamielisissä ympäristöissä ja ovat kompleksisesta rakenteestaan huolimatta onnistuneet välttämään onnettomuudet. HRO:t vaativat toiminnaltaan täydellisyyttä, mutta ymmärtävät ettei sitä voida saavuttaa. NAT:n ja HRO:n suurin ero on tapa, jolla vakavia onnettomuuksia pyritään ennalta estämään. HRO:n malli perustuu jatkuvaan henkilöstön ja prosessien parantamiseen, kun taas NAT malli suosittaa kompleksisuuden ja tiukkojen kytkösten vähentämistä tai ääritapauksessa järjestelmästä luopumista (Sutcliffe, 2011).

NAT ja HRO välinen depatti on jatkunut kauan (Sagan, 1993; Rijpma, 1997; Shrivastava, Sonpar & Pazzaglia, 2009). Perrown vastaus tähän on, että useita onnettomuuksia, jopa kompleksisiin järjestelmiin liittyviä voidaan ennalta estää, mutta normaaleja onnettomuuksia ei. Tästä johtuen NAT ei oikeastaan ole riskienhallintaa, vaan vääjäämättömien onnettomuuksien seurausten kanssa selviytymistä eli resilienssiä. Samaan tapaan asia on määritetty myös kyberturvallisuuden sanastossa: "*Resilienssin lähtökohtana on ajatus siitä, että turvallisuutta vaarantavat tilanteet syntyvät toimintojen odottamattomista yhdistelmistä, eivät niinkään toimintavirheistä tai häiriöistä, joita voidaan hallita suunnittelulla. Turvallisuuden hallinta onnistuu, jos toimintatavat joustavat tilanteiden ja olosuhteiden mukaisesti.*" (Sanastokeskus STK ry., 2018).

Edellä kuvattiin, että normaalit onnettomuudet ovat onnettomuuksia, jotka ovat odotettavissa ja väistämättömiä kun tietyt reunaehdot täyttyvät. Teorian mukaisesti onnettomuudet tapahtuvat siellä missä epälineaariset organisaatiojärjestelmät ovat sekä kompleksisia että tiivisti kytkettyjä. Normaali onnettomuus alkaa usein useiden itsenäisten komponenttien vikaantuessa. Komponenttivika voi aiheutua myös käyttäjän virheestä, joita käsiteltiin edellisessä

kappaleessa. Normaalin onnettomuuden keskeisimmät käsitteet on kuvattu kuviossa 22.



KUVIO 22 Normaalin onnettomuuden keskeisimmät käsitteet ja vuorovaikutukset

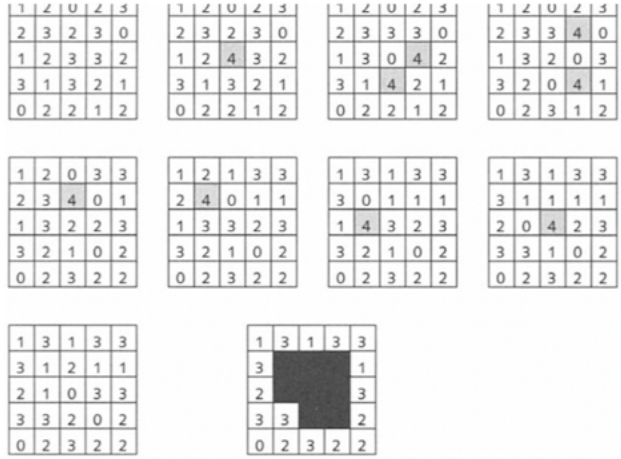
3.3 Itseorganisoitunut kriittisyys

Tässä kappaleessa esitellään itseorganisoituneen kriittisyyden teoria, sen suhde voimalakiin ja zipf'sin lakiin sekä fraktaalien olemassaoloon. Kappale esittää Bak'sin pisteytetyn tasapainon (engl. *punctuated reality*) sekä tähän liittyvää tutkimusta kyberlinssin läpi katsottuna.

Per Bakin 1996 julkaisema kirja *How Nature Works, the science of self-organizing criticality* alkoi vahvalla väitteellä, jonka mukaisesti itseorganisoitunut kriittisyys on uusi tapa katsoa maailmaa. Kirja oli jatkoa Bak, Tang ja Wiesenfieldin 1987 julkaisemalle lyhyelle tutkimuspaperille, jossa he esittelivät teorian, joka tunnetaan mm. nimillä *BTW Experiment, BTW Sandpile, Bak's Sandpile*. Teoria pyrkii selittämään ja numeerisesti todistamaan kuinka epälineaariset, kompleksiset järjestelmät käyttäytyvät. Teorian mukaan järjestelmillä on luonnollinen tapa organisoitua kriittiseen pisteeseen, jossa yksikin muutos järjestelmässä aiheuttaa ketjureaktion, joka edelleen vaikuttaa kasvavaan määrään komponentteja. Metaforana tälle käytetään hiekkakasaa. Kun hiekkakasa on saavuttanut kriittisen pisteen, yhden hiekanjyvän lisääminen voi olla turvallista, mutta se voi myös aiheuttaa koko kasan tuhoutumisen. Tutkijat kutsuivat tätä itseorganisoituneeksi kriittisyydeksi.

Tutkimuksessa simuloitiin matemaattisesti tuhansia vyöryjä asettamalla lukuja yksi-, kaksi- ja kolmeulotteisiin matriiseihin. Kokeessa käytetyn kaksiulotteisen matriisin voi ajatella shakkilaudan kaltaiseksi pinnaksi, jossa hiekanjyviä, eli lukuja, tiputeltiin sattumanvaraisiin ruutuihin. Jossain vaiheessa lukuja alkoi kasaantua samaan ruutuun ja kun niiden summa saavutti kaavassa määritetyn kriittisenpisteen (3), romahti tämä luku (-4) ja levisi solujakauman kaltaisesti viereisiin ruutuihin. Joissain vastaanottavissa ruuduissa tämä aiheutti kyseisen ruudun summan kasvamisen kriittiseen pisteeseen, jolloin tuloksena oli uusi vyöry. (Bak, Tang ja Wiesenfield 1987). Esimerkki simulaatiosta näkyy alla olevassa kuviossa 23. Kuvion toisessa kuvassa keskimmäinen ruutu kasvaa yli romahduspisteen (3 -> 4), jolloin seuraavassa kuvassa näkyy tämän luvun romahtaneen

nollaan samalla kun naapurisolujen luvut ovat kasvaneet yhdellä. Samalla tämä nosti kaksi uutta lukua yli kriittisen pisteen ja seuraavat vyöryt olivat valmiina. Viimeinen kuva esittää lopputulosta, jossa tilanne on jälleen tasapainotilassa. Vyöryn laajuus näkyy mustalla ja se on koskettanut kahdeksaa solua. Yhtä solua muutettiin kaksi kertaa, jolloin tämän vyöryn tilastollinen koko oli 9.

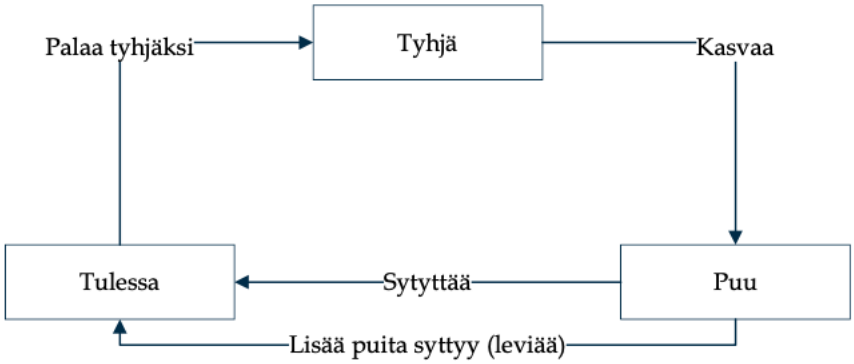


KUVIO 23 Esimerkki Bak'sin (1997) hiekkakasa simulaatiosta.

Bak'sin (1996) mukaan kompleksisessa järjestelmässä on paljon sisäisiä riippuvuuksia ja vuorovaikutuksia, joita on hankala nähdä. Kriittisessä pisteessä olevan hiekkakasan sisältä on tunnistettavissa sisäistä vuorovaikutusta, jonka kautta keskelle kasaa putoavan hiekanjyvän vaikutukset yltävät ennustamattomasti kaikkialla kasassa. Ajattele pöydälle kasautuvaa hiekkakasaa. Jossain vaiheessa kasa saavuttaa kriittisen pisteen ja tapahtuu suuri vyöry. Riippumatta mihin kohtaan kasaa uusi hiekan jyvä pudotetaan, pudottaa se samalla osan hiekanjyvistä lattialle. On kuitenkin mahdoton ennustaa etukäteen mitkä jyvät putoavat. Kriittinen kasa pyrkii aina kohti tasapainotilaa, joka on lähellä kriittistä pistettä mutta kuitenkin sen alla. Esimerkiksi Bak'sin ja kollegoiden alkuperäisessä tutkimuksessa (1987) "hiekkakasan" kriittiseksi korkeudeksi määritettiin 3, jolloin koko alueen kasojen keskimääräinen korkeus oli hieman yli 2.

Metsäpalomalli (engl. *forest fire model, FFM*), on hyvin dokumentoitu SOC-malli, jota on käytetty laajasti muillakin aloilla. FFM-malli on satunnaisesti ajettava soluautomaatio ja noudattaa soveltaen Bak'sin ja kollegoiden (1987) koetta. FFM-mallia on tutkittu 1–6 ulottuvuudessa ja yksinkertaistettu esimerkki on 2-ulotteinen matriisi, jonka ruudut kuvaavat maata. Tämä esimerkin tilakone on havainnollistettu kuviossa 24. Esimerkki menee näin: osa kentistä on tyhjiä, joihin voi kasvaa puita. Puita sisältävät kentät voivat pienellä todennäköisyydellä syttyä tuleen itsekseen (salama tms.) ja mikäli viereinen ruutu on tulessa syttyvät ne hieman todennäköisemmin. Tulessa olevat ruudut voivat palaa tyhjäksi, jolloin niihin voi jälleen kasvaa uusia puita. FFM-malli noudattaa voimalakia palojen keston (temporaalinen) ja palavien alueiden koon osalta (spatiaalinen). FFM-mallia voidaan säätää syttymisen todennäköisyyttä muuttamalla lähemmäksi tai kauemmaksi kriittisyydestä. Tämä antaa ymmärtää, että todellisen maailman metsäpaloja voitaisiin mahdollisesti säätää kauemmaksi kriittisyydestä, jolloin

suurten ja tuhoisien palojen todennäköisuus laskisi. (Conrad ja Oman, 2007). FFM-mallin muista sovellutuksista keskustellaan luvussa 4.



KUVIO 24 Metsäpalomalli (FFM) on laajasti käytetty SOC-malli

Hiekkavyöryn ennustaminen on Bak'sin (1996) mukaan kuin meteorologin työtä. Paikallista ilmastoa voidaan seurata ja ennustaa kohtuullisen tarkasti, mutta siitä huolimatta ennakoimattomat katastrofit yllättävät. Taustalla on osittain sama syy, jonka Dörner (1989) nosti esille omassa tutkimuksessaan. Tutkittavan aiheen ympärille luotavat hypoteesit ovat vääriä ja puutteellisia. Niissä ei huomioida sivu- ja pitkäaikaisvaikutuksia ja asioita käsitellään yksittäisinä tapahtumina eikä ymmärretä oman paikallisen hiekkakasan olevan osa laajempaa järjestelmää. Paikallinen hiekkakasameteorologi voisi laatia ennusteen, jonka mukaisesti yönaikana hiekkakasan koordinaateissa (3,3) on huomattu kasvaneen lähelle kriittistä pistettä ja siitä seuraava vyöry uhkaa nostaa kasojen (3,4), (3,2), (2,3) ja (4,3) korkeutta, joka taas aiheuttaisi monenlaista harmia. Vastatoimena aamulla otetaan lapiot käteen ja käydään tasoittamassa hiekkakasat. Paikallinen uhka on poistettu siltä kertaa ja ostettu hieman lisäaikaa. Teorian mukaisesti kuitenkin kriittiseen pisteeseen kasvanut järjestelmä sortuu jossain vaiheessa ja sortuma voi alkaa mistä tahansa. Lopputulos on kuitenkin sama. Sortuma kulkee järjestelmän läpi ja tasoittaa tilanteen tasapainotilaan. Vyöry kulkee myös hiekkakasameteorologin alueen läpi ja tulee yllätyksenä.

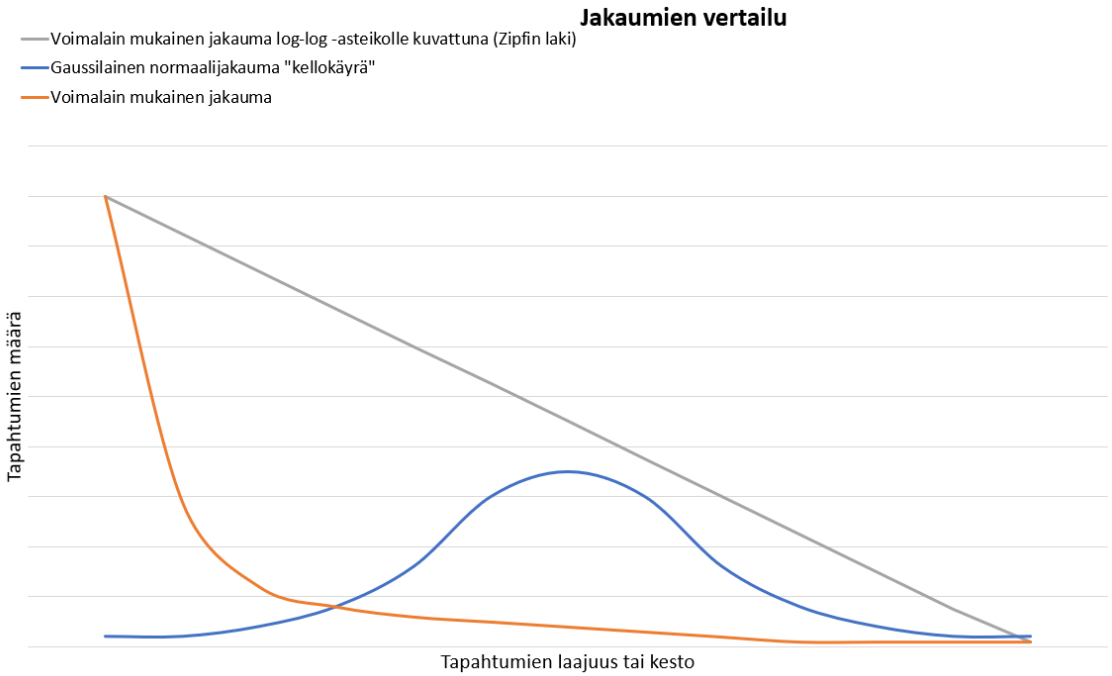
3.3.1 Voimalaki

Mielenkiintoinen näkökulma kompleksisissa järjestelmissä on, että Bak'sin ja kollegoiden (1987) mukaan niiden tilastollisia ominaisuuksia voidaan mitata voimalain avulla. Edellä esitellyn BTW-kokeen yhteydessä tilastoitiin vyöryjen tiheyttä ja kokoa, josta havaittiin, että pienet vyöryt ovat merkittävästi yleisempiä verrattuna suuriin vyöryihin ja että vyöryjen tuhoisuuden todennäköisyys seuraa kasvua kuvaavaa voimalakifunktiota (engl. *power law*). Samaa voimalain mukaista jakaumaa havaittiin myös metsäpalomallissa sekä työtapaturmien määrissä ja vakavuuksissa, tietoverkon topologian levinneisyydessä, haittaohjelmahyökkäyksissä, kyberaseiden tehoissa ja monissa muissa kohteissa (Mauro, Diehl,

Marcellin Jr, ja Vaughn, 2018; Faloutsos, Faloutsos ja Faloutsos, 1999; Conrad ja Oman, 2007; Bibighaus, 2015).

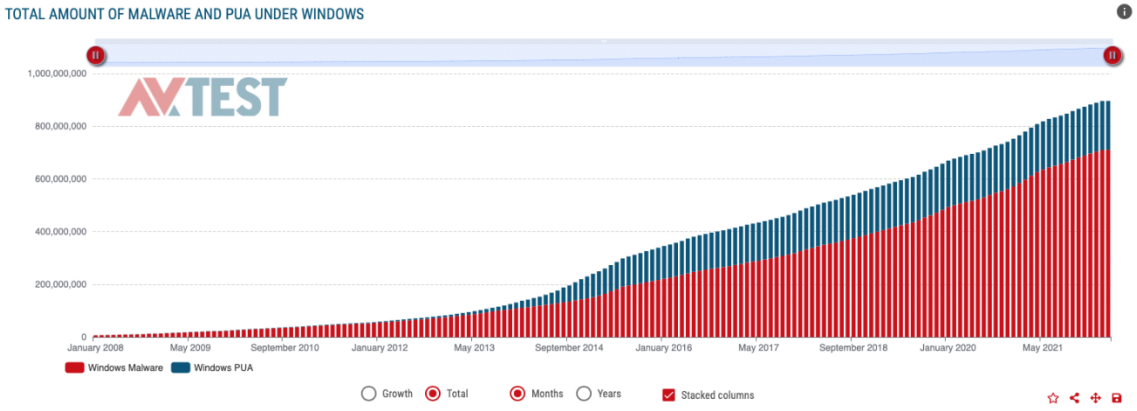
Voimalaki kuvaa kahden suureen välistä riippuvuutta, jossa muutos toisessa suureessa aiheuttaa merkittävän muutoksen toisessa suureessa. (ScienceDirect, 2013). Esimerkiksi neliön sivun pituuden kaksinkertaistaminen aiheuttaa pinta-alan nelinkertaistumisen. Muutoksen suuruuteen ja kuvaajan käyrän jyrkkyyteen vaikuttaa eksponentti q (y = 1/x^q). BTW-kokeen simulaatiossa eksponentin arvot olivat n. 1. Funktiosta voidaan päätellä, että *mitä pienempi eksponentti, sitä yleisempiä suuret onnettomuudet ja mitä suurempi eksponentti, sitä tuhoisampia onnettomuudet ovat*. (Bak, Tang ja Wiesenfield 1988).

Voimalaki kuvaa satunnaisuutta, joka on tyypillinen kriittiseen tilaan virittyneille järjestelmille. Tämä satunnaisuus noudattaa Gaussilaisen normaalijakauman sijaan voimalain mukaista jakaumaa (kutsutaan myös Mandelbrottilaiseksi normaalijakaumaksi). Jakaumien välinen eroavaisuus on esitetty kuviossa 25, jota voidaan havainnollistaa noppapeli esimerkillä. Gaussilaisen normaalijakauman mukainen kellokäyrä saadaan perinteisellä satunnaisuudella pelissä, jossa pelaaja heittää muutamaa noppaa yhtä aikaa ja noppien luvut lasketaan yhteen. Kun tätä toistetaan jonkin aikaa ja tulokset piirretään kuvaajalle, alkavat noppien yhteenlasketut luvut noudattavat normaalijakaumaa. Mandelbrottilaisen voimalain mukainen jakauma saadaan hieman erilaisella noppapelillä. Tässä pelissä pelaaja heittää noppaa ja peli päättyy aina kun tuloksena on parillinen luku. Kun pelaaja heittää parittoman, hän saa pisteen. Joka kerta kun pelaaja saa parittoman, pisteet tuplataan ja pelaaja saa uuden heittovuoron. Lopputulos on, että puolet pelaajista ei saa yhtään pistettä ja muutamat erittäin onnekkaat saavat suuria pistemääriä. (Lewis, 2010; Bibighaus, 2015). Kuviossa 25 esitettävä Zipfin laki esitellään seuraavassa alikappaleessa.



KUVIO 25 Satunnaisjakaumien vertailu

Voimalain ja Gaussilaisen satunnaisuuden suurin ero on siinä, että voimalain mukaisessa satunnaisuudessa äärimmäisen suuret tapahtumat (onnettomuudet) ovat mahdollisia. Normaalijakauman mukaisessa satunnaisuudessa ääripäät eivät eroa keskimääräisestä kovinkaan paljoa. Reaalimaailman esimerkki voimalain mukaisesta tapahtumasta on haittaohjelmaepidemia. Uusia haittaohjelmia kirjoitetaan vuosittain miljoonia (kuvio 26), mutta valtaosa niistä on harmittomia ja nähdään vain muutaman kerran (AV-Atlas, 2022). Pieni osa sen sijaan aiheuttaa suurta tuhoa ja on kuuluisampia kuin toiset (esim. WannaCry ja NotPetya).



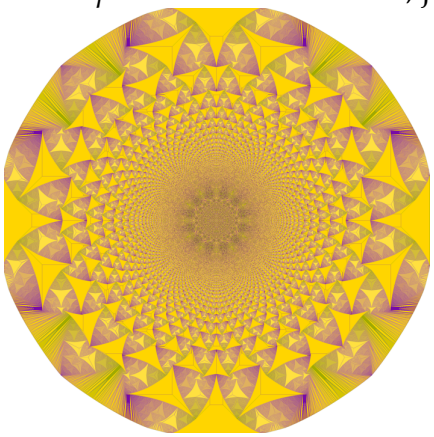
KUVIO 26 Haittaohjelmien määrä 2008–2022 (AV-Atlas, 2022)

Voimalain mukaista jakaumaa esiintyy järjestelmissä, jotka voivat kasvaa ja muuttua siten, että se vahvistaa järjestelmän onnistumista. Voimalain mukainen käytös spatiaalisesti ja temporaalisesti on tärkein tunnusmerkki itseorganisoituneelle kriittiselle järjestelmälle. Voimalakia ja satunnaisuutta käsitellään lisää 4. luvussa.

3.3.2 Zipfin laki ja fraktaalit

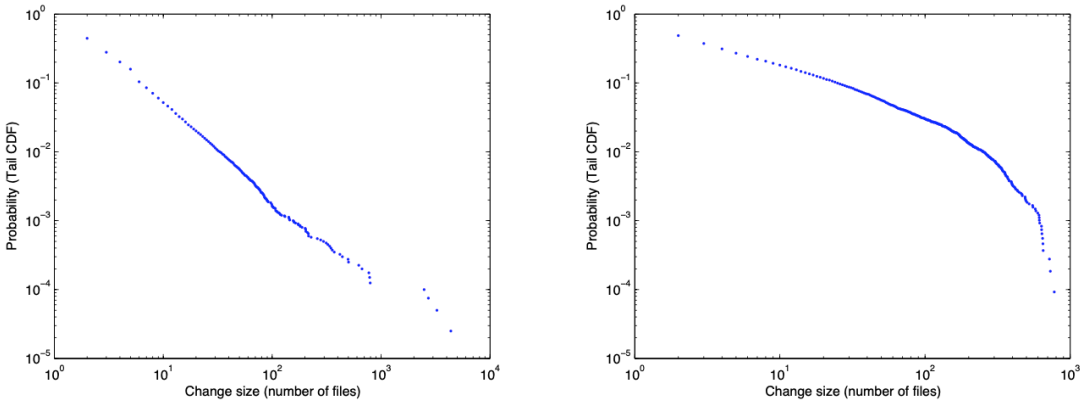
Zipfin laki tarkoittaa sitä, että koska vyöryjen tiheys ja koko noudattavat voimalakia, voidaan se kuvata log-log asteikolla suorana kuten luvun alussa esitetyt havainnot. Voimalain mukainen käytös indikoi järjestelmän olevan kriittisessä tilassa ja että vyöryt noudattavat Zipfin lakia, jossa jokaista suurta järistystä vastaa kymmenen pienempää (kuten maanjäristys ja kaupunkien koko esimerkeissä luvun alussa). Järjestelmän vyöryttyä ja rauhoituttua jälleen tasapainotilaan, voidaan ”hiekkakasat”, eli luvut, värittää siten että jokaisella luvulla on oma väri.

Kun tätä värikoodattua hiekkakasaa katsotaan ylhäältä päin, muodostuu tästä *Abelian sandpile* -niminen fraktaali, jonka esimerkki on nähtävissä kuvassa 27.



KUVIO 27 Kuvassa on pudotettu 30 miljoonaa hiekanjyvää äärettömän kokoiselle alustalle BWT kokeen mukaisesti. Kuvan värit tarkoittavat korkeusvaihtelua.

Wun, Holtin ja Hassannin (2007) tutkimuksessa avoimen koodin fraktaalirakenteita mitattiin koko ohjelmiston elinkaaren ajalta käyttäen voimalakia Bak'sin ja kollegoiden (1987) mukaisesti. Tutkimuksessa tutkittiin ohjelmistoon kohdistuneita muutoksia loogisessa ja rakenteellisessa tasossa. Tutkimuksen kohteena oli käyttöjärjestelmiä, tietokantoja, kääntäjiä ja kooditulkkeja sekä hyötyohjelmia. Ohjelmistomuutos määritettiin olevan tapaus, jossa joukkoa tiedostoja on muokattu yhdessä tietyn syyn perusteella. Tutkimusaineisto kerättiin suoraan versionhallinta repositoreista kuten GIT ja CVS. Tutkimus selittää avoimenkoodin itseorganisoituneen kriittisyyden ja luonnossa esiintyvien fraktaalirakenteiden olemassaolon. Kuvio 28 esittää muutosten laajuuden ajallista jakaumaa, joka noudattaa Zipfin lakia ja samalla kertoo taustalla olevan voimalain mukaisen satunnaisuuden. Kuvion 28b lopussa nähtävä notkahdus johtuu GCC-ohjelmistosta, jonka lähdekoodiin ei ole tehty rakenteellista muutosta, joka kohdistuisi yli 800 tiedostoon.



(a) Size distribution of logical changes ($\beta = 1.3237$)

(b) Size distribution of structural changes ($\beta = 0.7482$)

KUVIO 28 Voimalain mukaista käytöstä avoimen lähdekoodin ohjelmistoissa

Wu, Holt ja Hassan (2007) mukaan tämä korreloi myös avoimen lähdekoodin ohjelmistokehitykseen, jossa pieniä muutoksia tehdään jatkuvasti, mutta laajempia koko arkkitehtuuria muuttavia harvemmin.

3.3.3 Pisteytetty tasapaino

Hiekkakasa metafora on kulkenut pitkän matkan ja se on otettu hyvin vastaan eri tieteenaloilla kompleksisia rakenteita tutkivien tutkijoiden kesken. Teoriaan pohjautuvaa tutkimusta tehdään mm. geofysiikan, kosmologian, evoluutiobiologian, ekonomian ja neurobiologian alueilla (Wikipedia, 2022a). Se sisältää kaiken tarpeellisen: useiden yksiköiden yhteen toimivuuden, pisteytetyn tasapainon, satunnaisuuden, arvaamattomuuden ja kohtalon. Itseorganisoitunutta kriittisyyttä pidetään yhtenä perusmekanismeista, joka selittää luonnossa havaittavan kompleksisuuden. Bak, Tang ja Wiesenfield julkaisivat tutkimuksestaan laajemman raportin 1988 ja Bakin julkaistessa kirjansa 1996, oli alkuperäistä artikkelia viitattu yli 2000 kertaa sen olleen viitatuin artikkeli tuolla aikavälillä (Bak, 1996).

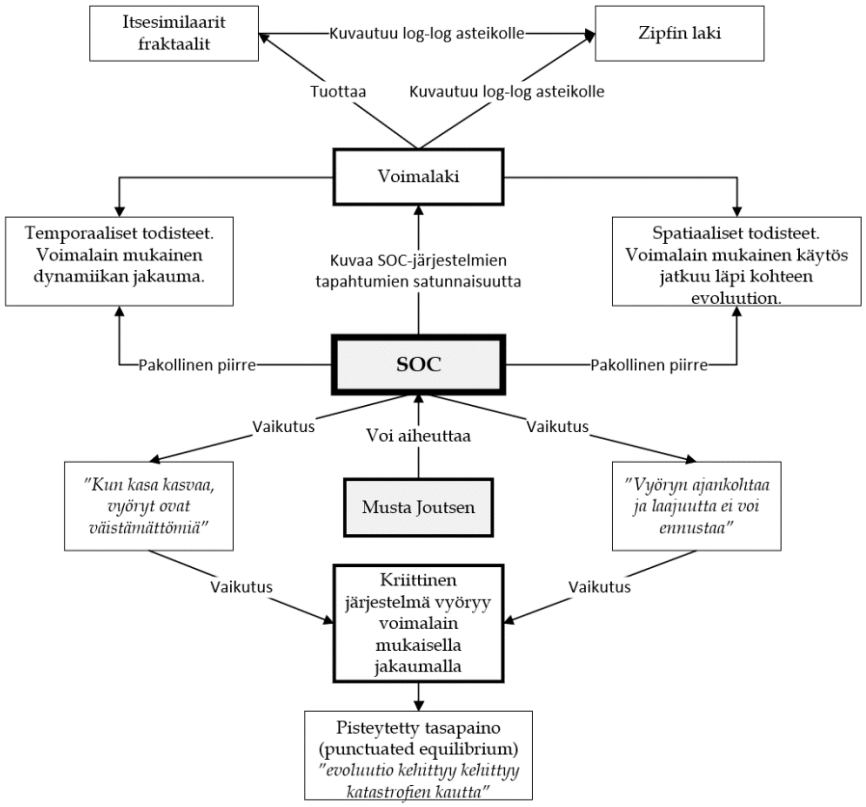
Bak'sin (1996) mukaan teoria pätee järjestelmiin, jotka voivat tallentaa historiaa. Metaforassa käytetty hiekkakasa voi tallentaa siihen piirretyt kirjaimet tai kuvat, kun taas tasapainoiset järjestelmät kuten vesi eivät kykene vastaavaan. Hiekkakasojen evoluutio kulkee katastrofien kautta ja suuria muutoksia tapahtuu suurten vyöryjen yhteydessä eikä vähitellen.

Kirjassaan Bak (1996) esitteli ajatuksen, jota hän kutsui pisteytetyksi tasapainoksi (engl. *punctuated equilibrium*), ja vei alkuperäistä teoriaa merkittävästi eteenpäin kohti ajatusta, että järjestelmät ja maailma kehittyy vain katastrofien kautta. Hänen mukaansa todellisuus on muutakin kuin sarja pieniä tapahtumia, jotka äityvät välillä suuriksi ja tuhoisiksi. Sen sijaan eksistentiaalinen kello on pysähdyksissä tasapainon aikana ja hyppää eteenpäin katastrofin kautta. Kehitys ei ole tasaista vaan satunnaista. Itseorganisoitunut kriittisyys on luonnon tapa tehdä valtavia muutoksia lyhyessä ajassa. (Bak, 1996). Tämän Bak's kiteytti kahteen periaatteeseen: *vyöryn ajankohtaa ja laajuutta ei voi ennustaa* ja *kun kasa kasvaa, vyöryt ovat väistämättömiä*. Ajatusta pisteytetystä tasapainosta tukee myös SOC:n mukainen Amaral-Meyer-verkosto ekologisesta ruokaketjusta, jossa eliöiden ja niiden välisten yhteyksien määrä kasvaa alkuun nopeasti, mutta tasoittuu rauhalliseksi ennen yllättävää romahdusta (Nakazako ja Arita, 2004).

Useat aiemmat tutkimukset osoittavat pisteytetyn tasapainon näkyvän myös ohjelmistojen evoluutiossa. Esimerkiksi Wu, Spitzer, Hassan ja Holt (2004) osoittivat, että *OpenSSH*, *PostgreSQL* ja *Linux kernel* kehittyivät pitkällä aikavälillä, jossa oli toistuvia pienten muutosten vaiheita sekä suurten vyörymäisten muutosten kohtia. Tämä noudattaa Bak'sin mallia pisteytetystä tasapainosta, jossa kehitys ei ole tasaista ja lineaarista kuten Darwinin evoluutioteoria, vaan kehitys ottaa suuria harppauksia yksittäisten tapahtumien kautta, jolloin niiden välinen aika on rauhallista eikä kehitystä juuri tapahdu. Verrattuna tavanomaiseen suljettuun järjestelmään, avoimen lähteen järjestelmät on kehitetty käyttäen vähemmän tiukkoja kontrolleja ja hallintamalleja. Spontaania yhteistyötä edistää ja tukee hajautettu kehittäjäyhteisö ympäri internettiä. (Raymond, 1999). Madeyn, Freehin ja Tynanin (2002) ja Kochin (2004) tutkimukset ehdottavat, että avoimen koodin projektit voidaan nähdä itseorganisoituneena ilmiönä sisältäen

itsevalittuja tehtäviä, spontaania yhteistyötä ja johtajuutta. Merkittävin empiirinen todiste on voimalain mukainen jakauma avoimen koodin projektien koon (kehittäjien määrä projektissa) ja tuottavuuden välillä (tallennusten määrä repositoriossa).

Tässä luvussa esiteltiin itseorganisoituneen kriittisyyden (SOC) teoria ja osoitettiin aiempien tutkimusten kautta sen esiintyvän myös kybermaailman rakenteissa. Itseorganisoitunutta kriittisyyttä kuvaava käsitemalli on nähtävissä kuviossa 29. Bak'sin mukaan SOC on selitys kaikkialla luonnossa esiintyville fraktaaleille muodoille. Itseorganisoituneella kriittisyydellä on kaksi tärkeää tunnusmerkkiä: voimalain mukainen dynamiikan (muutosten) jakauma ja pitkän aikavälin korrelaatio voimalain mukaiselle käytökselle ajan funktiona. Yksinkertaisesti sanottuna suurta määrää pieniä muutoksia SOC-järjestelmässä seuraa satunnaisesti suuret vyörymäiset muutokset.



KUVIO 29 Käsitekartta itseorganisoituneen kriittisyyden keskeisimmistä komponenteista ja termeistä

4 KYBERVYÖRY

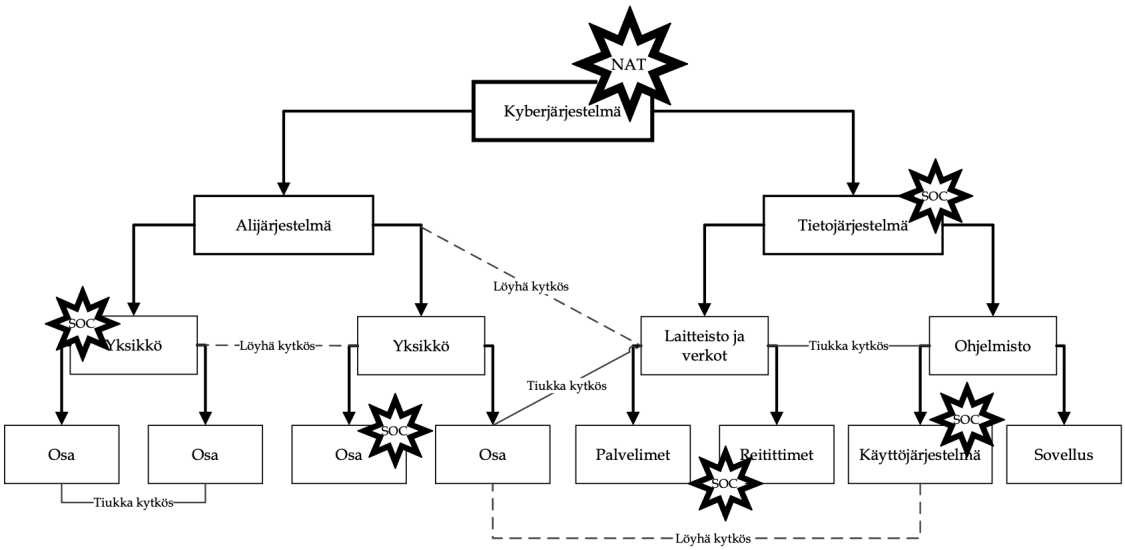
Tutkijat pyrkivät selittämään reaalimaailman loogisia tapahtumia aina syy-seuraussuhteella, jossa toimintaa seuraa vastatoiminta. Mutta voidaanko suuria onnettomuuksia, kuten Yhdysvaltojen itärannikon suuri sähkökatkos 2003 tai WannaCryn leviäminen 2017 selittää syy-seuraussuhteella vai ovatko ne vain satunnaisia tapahtumia maailman historiassa? (Carreras, Newman, Dobson, & Poole, 2000; Lewis, 2010; Greenberg, 2019).

Tässä luvussa kuvataan kybervyöryn teoria ja sitä tukevat evidenssit. Luku alkaa johdatuksella aiheeseen ja kertaa teorialle kriittisen ainesosan, voimalain, ominaispiirteet. Toinen alikappale esittelee varsinaisen teorian ja tätä seuraava kappale pohtii mitä asialle voidaan tehdä. Luvun lopussa on yhteenveto ja pohdinta.

4.1 Kohti kybervyöryä

Tutkimuksessa käytetyn määritelmän mukaisesti *kyberonnettomuus on tahallisesti tai tahattomasti toteutunut kyberuhka, joka kohdistuu kybertoimintaympäristöön vaarantaen ympäristön ja siitä riippuvaisen toiminnon osittain tai kokonaan*. Tutkimus määrittää *kybervyöryn olevan laajavaikutteinen tai pitkäkestoinen kyberjärjestelmäonnettomuus*. Kyberjärjestelmäonnettomuudella tarkoitetaan tässä Perrown (1986) teorian mukaista *normaalia onnettomuutta, joka määritelmän mukaan on onnettomuus, joka on sekä odotettavissa että väistämätön kun tietyt reunaehdot täyttyvät.*

Järjestelmäonnettomuuteen johtavat viat alkavat itsenäisistä yksiköistä tai alijärjestelmistä ja johtuvat jonkin komponentin vikaantumisesta tai käyttäjän virheestä. Komponentin vikaantuminen voi johtua sen virittymisestä itseorganisoituneeseen kriittiseen tilaan. Kriittisen pisteen saavutettua komponentti vikaantuu aiheuttaen erikokoisia "*SOC-vyöryjä*" ja kun tämä vyöryvä komponentti on tiukasti yhteen liitetty järjestelmän toiseen komponenttiin, voi tämä laukaista normaalin onnettomuuden (NAT). Kuviossa 30 on havainnollistettu Perrown järjestelmämallia sekä mihin komponentteihin SOC ja NAT kohdistuu. Teoria käydään läpi tarkemmin myöhemmässä kappaleessa.



KUVIO 30 Normaalien onnettomuuksien teorian mukainen järjestelmä (NAT), jossa alijärjestelmät, yksiköt ja osat ovat virittäytyneet kriittiseen tilaan (SOC).

4.1.1 Voimalaki ja satunnaisuus

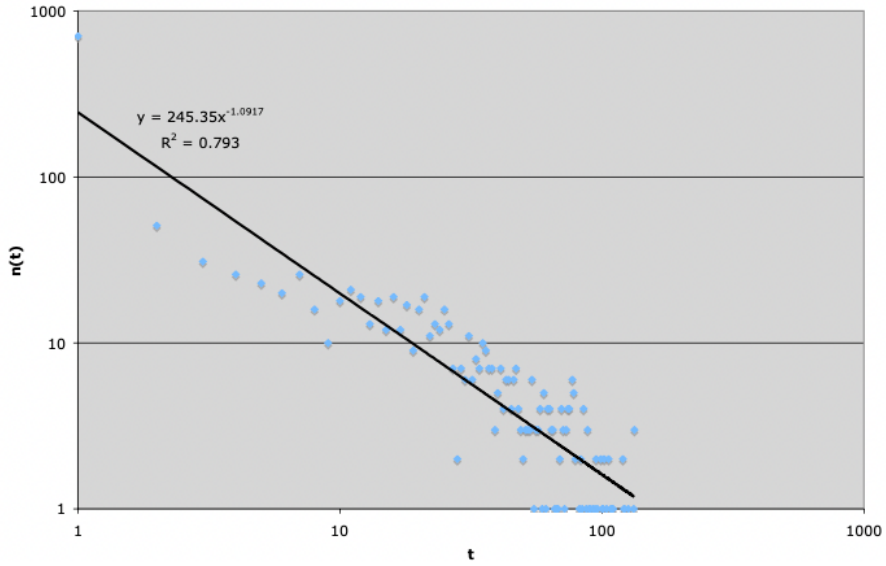
Kybervyöryn, eli kyberjärjestelmään kohdistuvan normaalin onnettomuuden tärkeä ainesosa on itseorganisoitunut kriittisyys. Itseorganisoituneen kriittisyyden tärkeimmät tunnusmerkit ovat voimalain mukainen dynamiikan (muutosten) jakauma ja pitkän aikavälin korrelaatio voimalain mukaiselle käytökselle ajan funktiona. Voimalakia käsiteltiin kolmannessa luvussa, mutta koska se on oleellinen todiste kriittisistä järjestelmistä, on siihen tehtyä tutkimusta hyvä tutkia tarkemmin.

Conrad ja Oman (2007) tutkivat Virus Bulletinin arkistoja 11 vuoden ajalta (1995–2006). Arkistot sisältävät kuukausittaisen raportin haittaohjelmien aktiivisuudesta. Koska datan kattavuudesta ei ole täyttä varmuutta, otettiin tutkimuksen lähtökohdaksi kaksi olettamusta:

- Saman aikaikkunan sisältä kerätyt näytteet ovat keskenään vertailukelpoisia.
- Näytteistysprosessi muuttuu niin hitaasti, että sillä ei ole merkitystä yksittäisen näytteen elinkaaren aikana

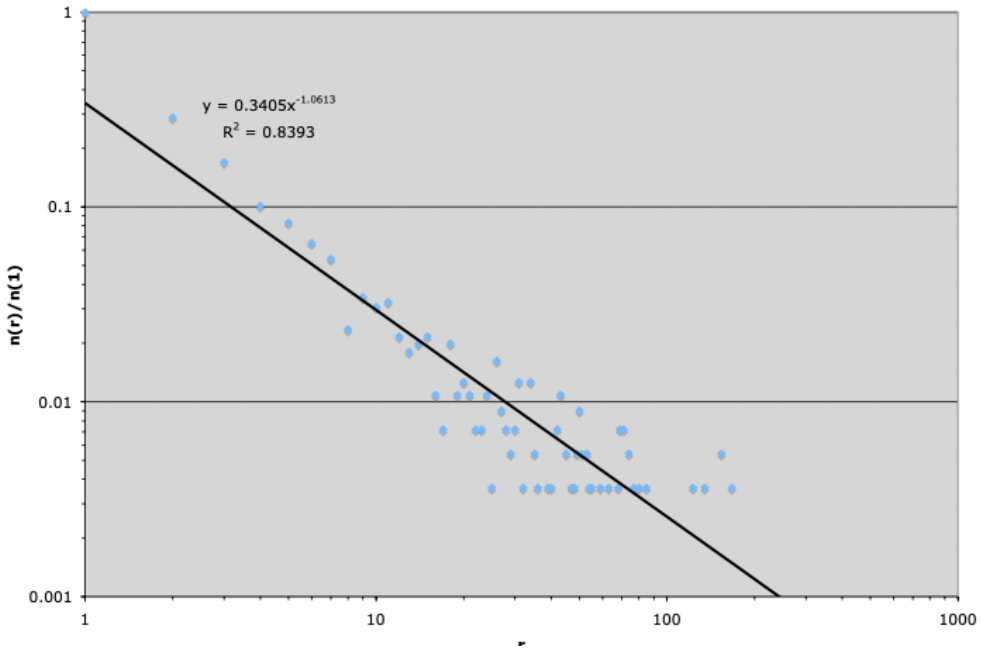
Tutkimustulokset osoittavat hyvää voimalain mukaisuutta sekä temporaalisissa että spatiaalisissa todisteissa. Mielenkiintoisen aineistosta tekee se, että vuosien 1995 ja 2006 välillä, internet kasvoi muutamasta palvelimesta n. 325 miljoonaan palvelimeen. Tämän ajanjakson aikana koettiin myös muutoksia internetiin kytkeytymisessä, tietokoneiden käyttöjärjestelmissä, jatkuvasti kehittyneissä haittaohjelmissa ja suojausteknologioiden nousussa. Tutkimuksessa havaittiin kuvion 31 mukaisesti temporaaliset todisteet hyökkäysten kestoissa. Kuvio 31 kuvaa, haittaohjelmatapausten määrää ajan funktiona, eli käytännössä sitä aikaa, jonka yksittäinen haittaohjelma on ollut aktiivisena. Zipfin lain mukaisesta log-log

kuvaajasta voidaan lukea, että suurin osa haittaohjelmista oli hetkellisiä ja vain pieni osa toimi pidemmän aikaa.



KUVIO 31 n(t) kuvaa haittaohjelmatapausten määrää ajan t funktiona

Saman tutkimuksen spatiaaliset tulokset osoittavat, että haittaohjelman laajuus noudatti samaa Zipfin lain mukaista log-log kuvaajaa (kuvio 32), jossa suuri osa haittaohjelmista oli paikallisia ja vain pieni osa saastutti laajemman joukon kohteita. Haittaohjelman levinneisyyttä mitattiin sen toistumisella raporteissa.

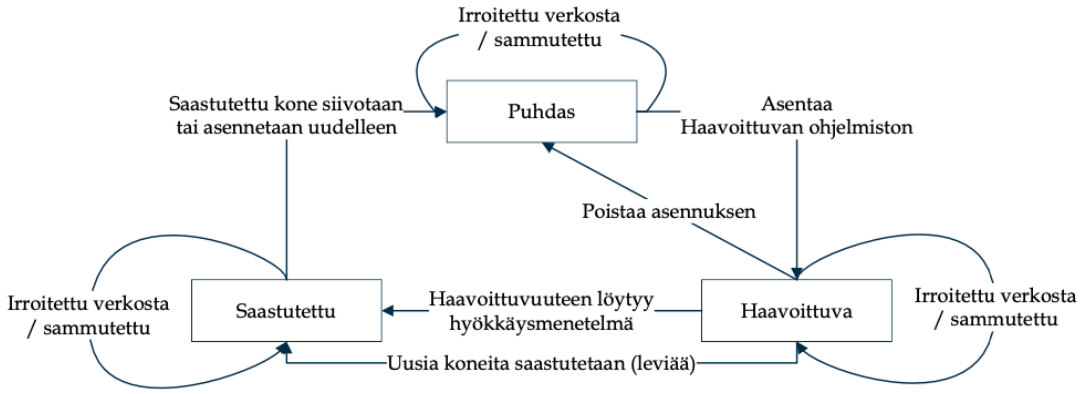


KUVIO 32 Vertikaali-akseli (n(r)/n(1) esittää haittaohjelma havaintojen normalisoidun toistuvuuden ja havainnon koko (r) esitetään horisontaali-akselilla.

Ja kuten luvussa kolme käytiin läpi, tarkoittaa log-log asteikolle piirretty Zipfin lain mukainen kuvaaja voimalain mukaista satunnaisuutta. Tulokset väittävät

siis, että valtaosa haittaohjelmista on elinkaareltaan lyhyitä ja levinneisyydeltään pieniä. Voimalain mukainen jakauma tarkoittaa kuitenkin myös sitä, että äärimmäisen tuhoisat ja pitkäkestoiset haittaohjelma epidemiat ovat mahdollisia. Onneksi kuitenkin harvinaisia.

Conrad ja Oman (2007) mallinsivat haittaohjelma epidemiaa käyttäen kolmannesta luvusta tuttua metsäpalomallia. Tilamalliin lisättiin muutamia tälle sovellutukselle tarpeellisia tilasiirtymiä, kuten palvelimen irrotus verkosta tai haavoittuvan ohjelmiston poistamisen (kuvio 33). Mallin kautta ajetut simulaatiot olivat yhteneviä Virus Bulletin datasta saatujen tutkimustulosten kanssa.



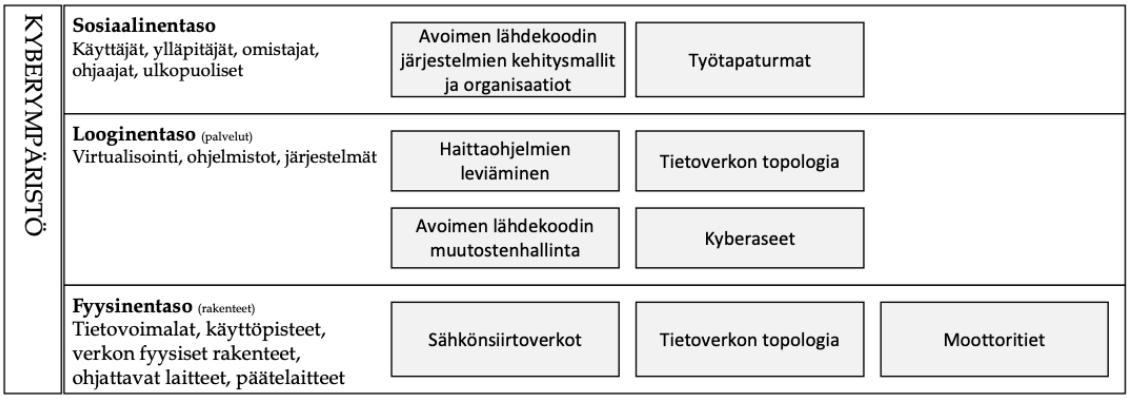
KUVIO 33 Haavoittuvuuden hyväksikäyttöä kuvaava FFM-malli

Samaa aihetta tutki Bibighaus (2015), mutta kybersodankäynnin näkökulmasta ja esitti että kyberaseet toimivat voimalain mukaisella satunnaisuudella. Kyberaseet ovat pohjimmiltaan kehittyneitä haittaohjelmia, joten tämä on linjassa Conradin ja Omanin (2007) tutkimuksen kanssa. Bibighaus painotti tutkimuksessaan voimalain mukaista satunnaisuutta sekä hyökkääjän että puolustajan näkökulmasta ja tuo esille, että epävarmuus, jota kybersodankäynnissä koetaan (*voimalain mukainen satunnaisuus*) on erilaista kuin perinteisen kineettisen sodankäynnin Gaussian normaalijakauman mukainen satunnaisuus. Kellokäyrän mukaista normaalijakaumaa ymmärtääkseen tarkkailijan tulee ymmärtää keskiarvo ja keskihajonta. Voimalakia ymmärtääkseen tulee ymmärtää mitä ääripäissä tapahtuu.

Kellokäyrän normaalijakaumalle on tyypillistä, että keskimääräisestä voidaan poiketa vain vähän. Esimerkiksi 220 cm pitkä ihminen on poikkeuksellisen pitkä, mutta sopii vielä kuvaan ollen n. 1.5 kertaa keskimääräistä ihmistä pidempi. Kellokäyrällä tulee kuitenkin raja vastaan, jonka jälkeen kaikki on astronomisen harvinaisia, kuten vaikka viisimetrinen mies. Voimalain mukaisessa jakaumassa sen sijaan on täysin mahdollista, että jokin tapahtuma poikkeaa tuhat kertaisesti normaalista. Jos ihmisten pituus (joka noudattaa normaalijakaumaa) suhteutettaisiin varallisuuteen (noudattaa voimalakia) olisi maailma täynnä kääpiöitä, joiden rinnalla olisi kourallinen Bill Gatesin kaltaisia jättiläisiä. (Taleb, 2007). Sama analogia pätee, kun perinteisiä aseita verrataan kyberaseisiin. Kineettisen aseen, olipa se kivääri tai pommi, tehoa mitataan sen kantamalla ja tuotetulla kineettisellä iskuvoimalla. Asetta voidaan parantaa lisäämällä

räjähdysainetta, sirpaloitumista tai parantamalla tarkkuutta. Parannuksia voidaan tehdä kuitenkin rajallisesti, koska kineettisen aseen iskuvoima noudattaa normaalijakaumaa. Kyberase sen sijaan noudattaa voimalakia, jolloin voidaan olettaa, että useat kyberaseet tehoavat vain harvoihin kohteisiin, mutta jotkin taas hyvin suureen määrään kohteita. Jotkin kyberaseet aiheuttavat rajallista tuhoa, mutta jotkin voivat aiheuttaa hyvinkin laajaa tuhoa. (Bibighaus, 2015)

Kuviossa 34 on kuvattu esimerkkinä joitakin kybermaailmasta ja kriittisestä infrastruktuurista tuttuja järjestelmiä, joiden on todettu käyttäytyvän voimalain mukaisesti. Nämä järjestelmät sisältävät siis kyberaseiden ja haittaohjelmien lisäksi itseorganisoituneen kriittisyyden tunnusmerkit ja noudattavat sen mukaista satunnaisuutta.



KUVIO 34 Esimerkkejä voimalain mukaisesta käytöksestä kyberympäristössä

Avoimen lähdekoodin järjestelmiä löytyy jokaisesta kyberympäristöstä. Tähän kategoriaan menevät kaikki Linux-käyttöjärjestelmästä yksittäisiin kirjastoihin, joita on sisällytetty esimerkiksi kaupalliseen tuotteeseen. Hyvä esimerkki tällaisesta kirjastosta on log4j, joka on laajasti käytetty lokitusta hoitava ohjelmakirjasto. Log4j-kirjastosta löytyi kriittinen haavoittuvuus joulukuussa 2021 joka uhkasi olla koko internetin tuhoava tapahtuma. Haavoittuvuudelle annettiin nimeksi Log4Shell ja se oli äärimmäisen helposti hyökättävä. Käytännössä riitti, että hyökkääjä sai sopivasti muotoillun lauseen haavoittuvan kirjaston käsiteltäväksi, jonka jälkeen tämä mahdollisti oman koodin suorittamisen kohteessa. Koska kyseessä oli lokituskirjasto, oli sille helppo syöttää hyökkäyskoodia, vaikka internet-sivun kirjautumislomakkeen tai jonkin muun lokitettavan kentän kautta.

Haavoittuvuus oli Talebin termistön mukaisesti Harmaa Joutsen, harvinainen, mutta odotettavissa oleva tapahtuma, jolla on laajat vaikutukset. Harmaa Joutsen yllättää ne, jotka eivät ole siihen valmistautuneita. Internet- ja tietoturvayhteisön yhteisellä ponnistuksella haavoittuvuudelle saatiin pikaisesti korjaus ja päivitysasennukset liikkeelle. Esimerkiksi Yhdysvalloissa *US Cybersecurity and Infrastructure Agency* (CISA) antoi hätädirektiivin valtionhallintoon, joka velvoitti tunnistamaan ja korjaamaan kaikki haavoittuvat järjestelmät 7 vrk kuluessa ja raportoimaan toimista 14 vrk kuluttua. Tällä kertaa Log4Shell-haavoittuvuuden tuhot jäivät kohtuullisen pieniksi. (Taleb, 2007; CISA, 2021)

Wu, Holt ja Hassan (2007) tutkivat yksitoista laajaa avoimenlähdekoodin järjestelmää. Tutkimuksessa esitettiin kaksi voimalakiin liittyvää ilmiötä:

ohjelmistomuutosten todennäköisyysjakauma pienenee muutoskokojen tehofunktiona ja ohjelmistomuutosten aikasarjat osoittavat pitkän kantaman korrelaatioita teholain käyttäytymisen kanssa. Käytännössä tämä tarkoittaa sitä, että mitä suuremmasta muutoksesta ohjelmistoon on kyse, sitä harvinaisempia nämä ovat. Tulokset pätevät tutkittujen ohjelmistojen osalta koko elinkaaren ajan. Tutkittavat ohjelmistot olivat: *NetBSD, FreeBSD, OpenBSD, Linux, PostgreSQL, GCC, KSDK, Koffice, OpenSSL, PHP ja Ruby*. Tällainen spatiaalinen (koko järjestelmän läpäisevä) ja temporaalinen (koko elinkaaren kattava) voimalakia noudattava malli osoittaa Bak's ja kollegoiden mukaisesti, että itseorganisoitunutta kriittisyyttä esiintyy avoimenlähdekoodin järjestelmissä. Avoimen koodin järjestelmien projektiorganisaation koosta, tehtävien jakautumisesta ja monesta muusta kehittämiseen liittyvästä mallista on tunnistettu myös voimalain mukaista jakaumaa. Avointen ohjelmistojen liike on itsessään itseorganisoitunut kriittinen yhteistyötä tekevä sosiaalinen verkosto (Wu, Spitzer, Hassan ja Holt, 2004).

Myös työtapaturmien, jotka ovat vakavuudeltaan sellaisia, että vaativat poissaoloa töistä, on tutkittu noudattavan voimalain mukaista jakaumaa. Lyhyet poissaolot ovat siis tavallisia, mutta laajemmatkin ovat mahdollisia (Mauro, Diehl, Marcellin Jr ja Vaughn, 2018). Voimalakijakauma on kuitenkin tyypillinen 80–20 tapaus, jossa 80 prosenttia vaikuttavista asioista syntyy 20 prosentin toimesta, jolloin organisaatiolla on suuri mahdollisuus kompastua vahvistusharhaan ja ludiseen harhaan. Vahvistusharha tarkoittaa, että korostamme sitä mitä näemme ja unohdamme näkymättömät todisteet kuten luvun kolme possulle kävi. Ludinen harha tarkoittaa järjestelmän sisällä olevaa näkökulmaa, joka ei hahmota järjestelmän ulkopuolisia vaikuttavia tekijöitä. Käytännössä tämä tarkoittaa sitä, että työturvallisuutta suunnitellessa keskitytään 80 % tapahtumista, jotka ovat suhteellisen harmittomia. Gaussilaisessa normaalijakaumassa tämä olisi absoluuttisen oikein. Voimalain mukaisessa järjestelmässä täytyy kuitenkin muistaa, että ääripäät eli se 20 % voi olla tuhatkertaisesti tuhoisampia, jolloin yksikin tällainen voi tuhota organisaation. Tällainen voisi olla esimerkiksi organisaation avainhenkilöiden joutuminen onnettomuuteen yhteisellä työmatkalla.

Sähkönsiirtoverkot ovat osa kriittistä infrastruktuuria ja välttämätön digitaalisten kyberpalveluiden tuottamiseen. Sähköllä on kybermaailman suhteen kaksi roolia ja vaikutusketjua. Fyysisellä iskulla sähköverkkoon voidaan aiheuttaa vaikutuksia digitaaliseen kyberympäristöön, jonka palveluiden tuottamiseen ja ylipäätään kyberympäristön käynnissä pitämiseen sähkö on välttämätöntä. Toinen vaikutusketju menee toisinpäin koska kyberympäristö ulottuu myös voimaloihin ja sähköverkon solmupisteisiin, joissa sitä käytetään ohjaamaan sähköverkon toimintaa. Tällöin digitaalisella kyberiskulla voidaan aiheuttaa vaikutuksia fyysiseen maailmaan. Sähköverkot ovat kehittyneet ajan saatossa kriittiseen pisteeseen noudattaen itseorganisoituneen kriittisyyden periaatetta. Tämä tarkoittaa sitä, että niitä ajetaan lähellä niiden maksimikapasiteettia, jolloin kuorman kasvaessa ne ovat vaarassa kaatua. Teoriaa tukee globaalisti kerätty data, joka osoittaa, että suuret sähkökatkot noudattavat voimalakijakaumaa. (Dobson, Carreras, Lynch & Newman, 2007).

Suurten sähkökatkojen taustalla on usein peräkkäisten häiriöiden suma, jonka tuloksena verkko kaatuu kuin dominopalikat. Näin kävi esimerkiksi 1996 Yhdysvaltojen lounaiskulmassa, jossa 7,5 miljoonaa asiakasta jäi sähköttä. 2003

Yhdysvaltojen koillisosassa sähköttä jäi 50 miljoonaa asiakasta kahdeksan osavaltion alueelta. (Dobson, Carreras, Lynch & Newman, 2007). Ylikuormituksen lisäksi sähköverkot voivat kaatua myös komponenttivian tai kyberhyökkäyksen johdosta. Kyberhyökkäyksellä voidaan vaikuttaa fyysisiin rakenteisiin ja aiheuttaa tuhoa kuten esimerkiksi Stuxnetilla Iranin ydinrikastamossa 2010 tai Ukrainan sähköverkkoon kohdistuneella iskulla 2015. Sähköverkkoon kohdistettuna tämä voi ajaa kriittiseen tilaan virittyneen infrastruktuurin tilaan, jossa se kaatuu osa kerrallaan. Tutkimuksen arvion mukaan kyberiskulla tehty sähköverkon kaataminen voi aiheuttaa luonnollista onnettomuutta laajemmat vahingot. (Sheng, Yingkun, Yuyi, Yong, & Yu, 2011; Zetter, 2014).

Tietoverkkoja tutkittiin marraskuun 1997 ja joulukuun 1998 välisenä aikana. Tutkimuksessa käytettiin kolmea instanssia verkosta ja se sijoittui ajanhetkeen, jonka aikana verkot kasvoivat arviolta 45 %. Tutkimuksessa internetin topologiasta löydettiin yllättävän yksinkertaisia voimalain mukaisia rakenteita. Voimalaki kuvaa verkoston noodien ominaisuutta, joka auttaa ennustamaan miltä verkko näyttää tulevaisuudessa tai pitkään vaivannutta ongelmaa, kuinka realistisia tietoverkkosimulaatioita voidaan suunnitella. Voimalain mukainen jakauma antaa kuitenkin viitteitä myös järjestelmän mahdollisesti kriittisyydestä. Tutkimuksen lyhyt aikajänne ei kuitenkaan esitä pitkän aikavälin korrelaatiota dynamiikan muutokselle, joten itseorganisoituneen kriittisyyden todistaminen vaatisi lisää tutkimusta. (Faloutsos ja kollegat, 1999)

Näiden esimerkkien kautta esitettiin kybermaailmasta tuttujen komponenttien sisältävän itseorganisoituneen kriittisyyden merkkejä. Tämä tarkoittaa SOC-teorian mukaisesti, että kyseisten komponenttien vyöryt ovat väistämättömiä vaikkakaan vyöryn ajankohtaa tai laajuutta ei voida ennustaa. Seuraava kappale esittää miten itseorganisoituneet kriittiset järjestelmät aiheuttavat kokonaisjärjestelmän järjestelmäonnettomuuden. Tätä tutkimuksessa kutsutaan kybervyöryksi.

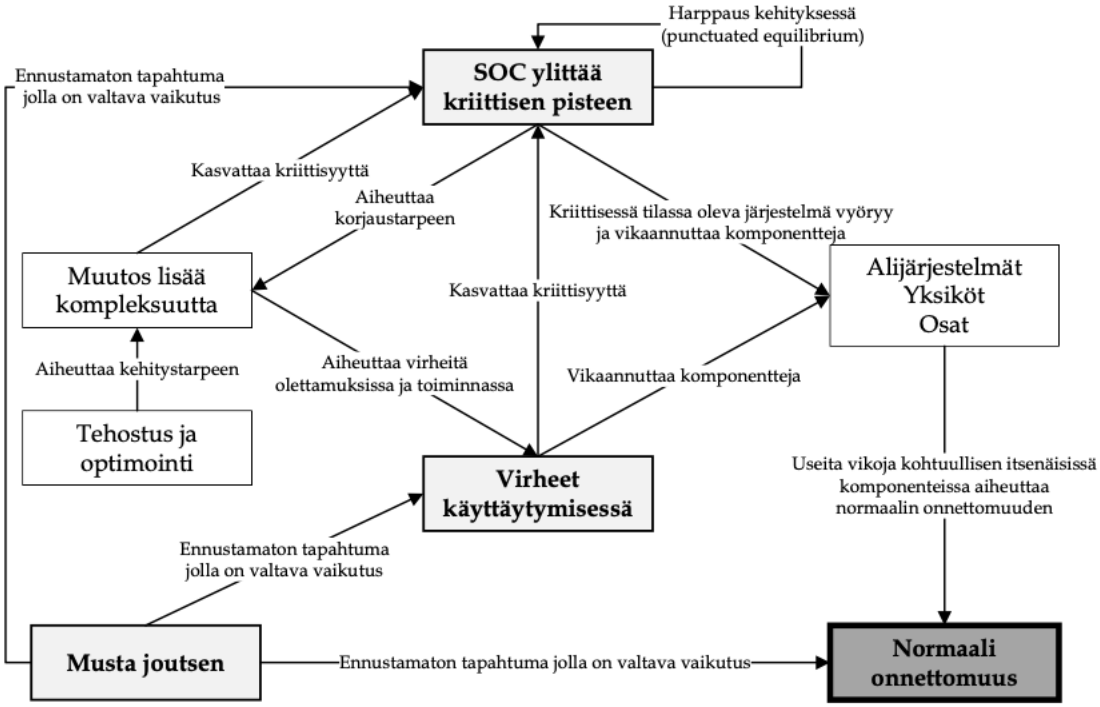
4.2 Teoria kybervyörystä

Bakin ja kollegoiden (1987) yksinkertaisella ja selkeällä itseorganisoituvuutta kuvaavalla mallilla ei ollut mitään tekemistä nykyisen kybermaailman tai riskiperustaisen päätöksenteon kanssa. Tutkijat halusivat ymmärtää miksi kompleksiset järjestelmät romahtavat yllättäen ja ilman selkeää syytä. Perrow (1984) lupautui kirjoittamaan Presidentin toimikunnalle lyhyen analyysiin sosiaalisesta ja organisatorisesta näkökulmasta Three Mile Islandin ydinvoimalaonnettomuuteen, joka vaikutti kaikin puolin olleen puhtaasti tekninen. Aihe vei mennessään ja pian kasassa oli neljäkymmentä sivua ja pohja normaalien onnettomuuksien teorialle. Dörner (1990) pohti kolme vuotta Tšernobylin ydinvoimalaonnettomuuden jälkeen missä määrin ihmiskunnalla on varaa teknologioihin, joihin liittyvillä epäonnistumisilla on niin pitkät seuraukset.

Jokaisesta teoriasta (virheet käyttäytymisessä, NAT, SOC) tuotettiin luvussa kolme käsitemallit, joissa kuvattiin teorioiden keskeisimmät termit ja vaikutusketjut. Nämä käsitemallit on kuvattu kokonaisuudessaan liitteessä 2. Tässä

kappaleessa esitellään edellä mainitun käsitemallin yksinkertaistettu ja yleistetty versio, joka kuvaa miten kyberjärjestelmä on altis normaaleille onnettomuuksille ja miten onnettomuus lähtee liikkeelle yksittäisten toisiinsa kytkettyjen komponenttien vikaantuessa. Komponenttien vikaantumisen voi aiheuttaa SOC-vyöry, ihmisten virheellinen käytös tai Musta Joutsen. Tämä malli on teoria kybervyörystä.

Kybervyöry (kuvio 35) kuvaa neljää keskeistä komponenttia (Musta Joutsen, SOC-vyöry, virheet käytöksessä sekä normaalin onnettomuuden). Näiden lisäksi kuviossa on kolme oleellista käsitettä sekä näiden välisiä relaatioita.



KUVIO 35 Teoria kybervyörystä

Teorian perusperiaate on, että kompleksinen ja tiukasti yhteen kytketty kyberjärjestelmä koostuu komponenteista, jotka ovat normaalin teorian käsitteissä alijärjestelmiä, yksiköitä ja osia. Osa komponenteista voi olla virittynyt kriittiseen tilaan, jolloin sen vyöryminen on väistämätöntä. Vyöryn voi aiheuttaa monet tekijät. Esimerkiksi komponenttiin kohdistuva muutos kasvattaa järjestelmän kompleksisuutta, joka nostaa kriittisyyttä ja voi jossain vaiheessa aiheuttaa vyöryn. Yksittäisen komponentin vyöryminen johtaa yleensä kyseisen komponentin korjaamiseen (muutokseen), joka lisää jälleen kompleksisuutta. Järjestelmän tehostaminen ja optimointi aiheuttavat myös muutostarpeita, jotka voivat johtaa edellä kuvattuun kriittisyyttä kasvattavaan kierteeseen. Muutokset järjestelmään aiheuttavat lisääntyneen kompleksisuuden lisäksi riskiä inhimillisille virheille käyttäytymisessä, jotka johtavat epäonnistumiseen.

Epäonnistumiseen johtaneet virheet käytöksessä voivat kasvattaa komponenttien kriittisyyttä tai aiheuttaa suoraan vikaantumista. Kuten luvussa kolme todettiin, ihmiset ovat huonoja toimimaan kompleksisissa tilanteissa ja luonnostaan käsittelevät järjestelmää kasana irrallisia muuttujia sen sijaan että

käsittelisivät sitä kompleksisena järjestelmänä, jossa on syy-seuraussuhteita, mutta myös voimalain mukaista satunnaisuutta.

Kolmas elementti teoriassa on Talebin (2007) kuvaama Musta Joutsen. Musta Joutsen on metafora tapahtumalle, joka on ennustamaton ja jolla on valtavat vaikutukset. Samasta ilmiöstä käytetään kirjallisuudessa myös termiä tuntematon-tuntematon (engl. *unknown-unknown*). Kybervyöryteoriassa Mustat Joutsenet voivat aiheuttaa virheitä käyttäytymisessä tai kriittisen komponentin vyörymisen, mutta ne voivat myös aiheuttaa suoraan normaalin onnettomuuden. Talebin (2007) mukaan Mustille Joutsenille altistaa samankaltaiset ominaisuudet, joita myös Dörner (1990) havainnoi tutkimuksessaan. Mustan Joutsenen sokeudessa on kaksi sisäistä mekanismia: *vahvistusharha* ja *narratiivinen harha*. Vahvistusharhassa kasautuvat tiedot vahvistavat alkuperäistä ajatusta ja vaikeuttaa muiden totuuksien näkemistä. Narratiivinen harha yksinkertaistaa näkemystämme todellisuudesta pakottaen tapahtumat syy-seuraus suhteisiin, jolloin satunnaisuuden merkitys katoaa. Narratiiviseen harhaan liittyy myös tarve selittää asioita, jolloin syitä kehitellään, jotta tarinat tuntuisivat järkeville. Ulkoiset mekanismit liittyvät tapaamme ottaa vastaan ja ymmärtää tapahtumia sekä puutetta tavassamme toimia niiden perusteella. Emme siis huomaa mitä on tulossa, tai jos huomaamme niin emme usko. Ja vaikka huomattaisiin ja uskottaisiin, niin ei siltikään uskota niin paljon että toimisimme siten, että se keventäisi tulevaa iskua (Taleb, 2007; Dörner 1990).

Kybervyöryteoriaa tukee Amaral-Meyer-verkosto, joka simuloi Perrown normaalien onnettomuuksien teoriaa useissa luonnollisissa ja ihmisten rakentamissa kompleksissa järjestelmissä. Yksinkertainen esimerkki verkostosta on ekologinen ruokaketju, jossa eliöt pikkuhiljaa mutatoituvat ja liikkuvat verkostossa rakentaen riippuvuussuhteita toisiinsa. Pitkässä juoksussa eliöiden määrä kasvaa tasaisesti, kunnes kasvu hidastuu ja alkaa rauhallinen tasainen jakso. Yllättäen verkosto ja eliöiden määrä kuitenkin romahtaa. (Nakazako ja Arita, 2004) Mielenkiintoista kokeessa on, että vaikka siinä simuloidaan Perrow NATtia vuodelta 1986, seuraa romahdus samalla Bakin ja kollegoiden (1987) määrittämää SOC-mallia, jossa romahdukset ovat ennustamattomia, mutta seuraavat kuitenkin voimalain mukaista jakaumaa temporaalisesti ja spatiaalisesti. Tämä havainto nostaa esille ehdotuksen, että verkoston romahduksen taustalla ei ole yksittäisen eliön katoaminen vaan SOC:n mukainen satunnaisuus. (Lewis, 2010).

Kybervyöry teoria pohjautuu vahvasti SOC ja NAT teorioihin, jolloin sen voidaan olettaa olevan pitävä vain, jos näiden kahden teorian tunnusmerkit täyttyvät. Näin olleen kybervyörylle alttiin järjestelmän tulee olla kompleksinen ja sen sisäisten komponenttien välillä tulee olla tiukkoja kytkentöjä. Tämän lisäksi joidenkin sisäisten komponenttien tulee noudattaa voimalain mukaista käytöstä dynamiikan osalta koko komponentin elinkaarenajalta havainnoituna.

4.3 Mikä neuvoksi?

Oletamme että jos ymmärrämme syyn maanjäristyksille, tulville tai kyberiskuille, voimme tehdä asialle jotain. Käytännössä syyn selvittäminen kuitenkin

tapahtuu onnettomuuden jälkeen. Jälkikäteen katsottuna useimmat tapahtumat vaikuttavatkin loogisilta, jotka olisi voitu tunnistaa ja estää ennalta. Syyn ja seurauksen ymmärtäminen onkin ensiaskel kohti suojautumista, joten on tärkeää ymmärtää, miksi onnettomuuksia tapahtuu. Kuten tutkimuksessa on tuotu esille, syy-seuraussuhteen lisäksi osalle onnettomuuksia on olemassa toinenkin selitys. Tämä selitys perustuu teoriaan, jonka mukaisesti väistämätön katastrofi on sisään rakennettu kompleksisiin järjestelmiin. Voimalain mukaiset tapahtumat johtuvat satunnaisuudesta, joka on riippumaton syy-seuraus suhteesta. Koska syy ei ole itsestään selvä (ennen kybervyöryä) tulee vyöry shokkina ja on psykologisesti yllättävä suuruutensa vuoksi. Luonteeltaan tällainen normaali onnettomuus tai kriittisen järjestelmän romahdus on arvaamaton niin ajassa kuin paikassa, jolloin sen ennalta estäminen on mahdotonta. (Perrow, 1986; Bak ja kollegat, 1987; Lewis, 2010).

Organisaation on siis ymmärrettävä kompleksisten järjestelmien muodostama riski ja ennen kaikkea sen voimalakia noudattava satunnaisuus. Voimalain mukaisesti 20 % onnettomuuksista on tuhoisimpia, jolloin Lewisin (2010) mukaan organisaatioiden tulisi keskittää onnettomuuksia estävät (engl. *prevent*) strategiat näihin korkean riskin haittoihin, joilla on potentiaalinen mahdollisuus tuhota koko järjestelmä. 80 % onnettomuuksista on matalamman riskin tapahtumia, jolloin niihin tulisi kohdistaa vastaava (engl. *response*) strategia. Suojautuakseen Mustilta Joutsenilta ja kompleksiseen järjestelmään liittyviltä haasteilta (esim. luvun kolme mukaisesti väärät hypoteesit, sopimattomat strategiat, sivu- ja pitkäaikaisvaikutusten huomiotta jättäminen) organisaatioiden tulisi tuntea induktio-ongelma ja ymmärtää ettei mennyt ole tae tulevasta. Tuntea ludinen harha ja tutkia riskejä laatikon ulkopuolelta, eli suojautua tuhoisalta 20 prosentilta. Pyrkiä välttämään narratiivisen harhan ominaisuus selitellä asioita ja keksiä syitä tapahtumille, jotta ne tuntuisivat järkeviltä. Narratiivinen harha ajaa vahvistusharhaan, jossa alkuperäinen ja ehkä väärä ajatus vahvistuu, jolloin organisaatio sokeutuu tilanteelle. Organisaation koko henkilöstön tulisi tunnistaa henkilökohtainen biasoituminen, joka estää hiljaisten todisteiden havainnoimisen ja tuhoisiin riskiskenaarioihin liittyvien indikaattorien tunnistamisen ja hyväksymisen. Tämä vaatii organisaation kulttuurin muutosta ja henkilöstön kouluttamista. (Dörner, 1990; Taleb, 2007). On myös hyvä muistaa, että asioita arvioidessa keskimääräinen asiantuntija osuu oikeaan likimain yhtä usein kuin tikkaa heittävä simpanssi. (Tetlock & Gardner, 2015).

Itseorganisoitunutta kriittisyyttä voidaan madaltaa myös useilla teknisillä keinoilla. Järjestelmiin voidaan rakentaa puskureita, välttää kaksoiskäyttöisiä komponentteja ja vähentää ylipäätään tiukkoja kytköksiä ja järjestelmän sisäistä interaktiivisuutta. Tällä pyritään vähentämään järjestelmän kompleksisuutta. Kaikilla näillä ratkaisuilla on kuitenkin korkea hinta, sillä samalla täytyy kustannustehokkuus unohtaa arvona. Tällainen malli on lähellä HRO mallia, jossa suurin arvo on luotettavuudella, johon pyritään jatkuvalla toiminnan mittaamisella ja kehittämisellä. Jatkuvalla kehittämisellä ja keinotekoisella puskureiden rakentamisella on vaarana kuitenkin nostaa järjestelmän kompleksisuutta sen sijaan että se laskisi sitä. Vaarana on, että järjestelmään rakentuu uudenlaista kapeikkoa esimerkiksi riittävän ja osaavan henkilöstön muodossa tai harvinaisen teknologian kautta. Keskustelu NAT ja HRO teorioiden välillä on käynyt teorioiden

alusta lähtien. Perrown näkemys asiasta on, että vaikka HRO:n tai muiden keinojen kautta kompleksisuutta saadaan laskettua, niin mikäli NAT ominaispiirteet täyttyvät on normaali onnettomuus väistämätön. Tästä johtuen NAT ei oikeastaan ole riskienhallintaa, vaan vääjäämättömien onnettomuuksien seurausten kanssa selviytymistä eli resilienssiä. (Sagan, 1993; Rijpma, 1997; Shrivastava, Sonpar & Pazzaglia, 2009).

Resilienssi lieneekin lopulta tärkein huomioitava asia kompleksisten kriittisten järjestelmien kanssa toimiessa. Kuten edellä on moneen kertaan tuotu esille, on vyöry väistämätön ja joskus vyöry tulee olemaan iso. Tällöin on hyvä olla olemassa suunnitelma toiminnalle. Keinoja on monia ja niiden tunnistaminen lähtee kyberturvallisuuden hallintamallin mukaisesti tunnistamalla ja priorisoimalla suojattavat kohteet. Kun tiedetään mitkä osat järjestelmästä on sellaisia, joita ilman organisaatio ei voi toimia, voidaan näiden suojaaminen ja jälleen rakentaminen suunnitella. Yksinkertaisimmillaan tämä voi olla, vaikka huolella laadittu ja testattu varmistus- ja palautussuunnitelma, joilla järjestelmä saadaan rakennettua uudelleen, olipa tuhon syy haittaohjelmahyökkäys, maanjäristys tai irtisanottu järjestelmäylläpitäjä.

4.4 Yhteenveto ja pohdinta

Tässä Pro Gradu tutkimuksessa esitetty kybervyöryteoria on rajallisen ajan ja resurssien vuoksi pintapuolinen raapaisu kokonaisuuteen, joka vaikuttaa jo tämän perusteella lupaavalta mallilta selittämään useita kyberjärjestelmiin liittyviä ilmiöitä ja ehkä tuomaan uutta näkökulmaa riskienhallintaan ja suojautumiseen ja sitä kautta lieventämään onnettomuuksien vaikutuksia.

Tutkimus jakautui kolmeen loogiseen kokonaisuuteen, joista ensimmäisessä käsiteltiin kybermaailmaa ja kompleksista järjestelmää monista näkökulmista ja määritettiin tutkimuksen kannalta merkittävimmät käsitteet. Luvussa kuvattiin kybermaailmaan uhkaavat uhat ja rakennettiin viitekehys kuvaamaan kybertoimintaympäristöä.

Seuraavassa luvussa käytiin läpi kolme onnettomuuksia kuvaavaa teoriaa hermeneuttisen analyysin keinoin. Luvun jokaisessa kappaleessa käsiteltiin yhtä teoriaa edellisessä luvussa rakennetun viitekehyksen kautta ja se kuvattiin käsitemallina.

Kolmannessa luvussa konstruktoitiin edellisen luvun käsitemallit yhdeksi kybervyöryä kuvaavaksi kokonaisuudeksi. Luvussa kerrattiin pohjateorioiden keskeisimmät asiat ja syvennettiin ymmärrystä voimalain mukaisen jakauman tuottamaan satunnaisuuteen. Tämän jälkeen luku esitteli varsinaisen kybervyöryteorian ja toi esille muutamia keinoja, joilla väistämättömän vyöryn vaikutusta voi pyrkiä keventämään. Luvun lopussa on tämä yhteenveto sekä ajatuksia jatkotutkimuksesta.

Tutkimusaiheena onnettomuudet ja kybermaailma ovat äärimmäisen mielenkiintoinen kokonaisuus, jonka taustalta avautui monitieteinen kokonaisuus. Informaatioteknologia ja kyberturvallisuus on itsessään jo niin laaja-ala, että sen eri näkökulmia tutkitaan useilla tieteen aloilla. Onnettomuuksia, niiden syitä ja

seurauksia, tutkitaan ihmisen toimintaa selittävistä näkökulmista kognitiotieteiden, psykologian ja kriminologian aloilla. Järjestelmiä, systeemejä ja kompleksisia rakenteita tutkitaan useilla aloilla kuten myös organisaatioita ja verkostoja. Kybervyöry tutkimusta olisikin mahdollista jatkaa horisontaalisti mihin suuntaan tahansa ja syventää vertikaalisti lähes loputtomiin.

Jatkotutkimusta aiheesta voisi tehdä esimerkiksi pitkäaikaistapaustutkimuksena kohdistuen johonkin laajaan kyberjärjestelmään. Tutkimuksessa kohdejärjestelmä voitaisiin purkaa komponentteihin ja havainnoida jokaisen komponentin osalta merkkejä itseorganisoituneesta kriittisyydestä, selvittää ja tilastoida komponentteihin ja koko järjestelmään kohdistuneita tapahtumia ja onnettomuuksia ja arvioida tätä kautta empiirisen aineiston tuottamaa kuvaa kybervyöry teoriasta. Tutkimuksessa voitaisiin esimerkiksi mitata uhkien ilmaantumistiheyttä ja verrata tätä yksittäisen uhkan aiheuttamien muutosten määrään. Asiaa voitaisiin tarkastella samanaikaisesti useassa ulottuvuudessa, kuten muutokset fyysiseen kerrokseen (uusien tai kovennettavien turvakontrollien määrät), muutokset loogiseen kerrokseen (ohjelmistojen päivitykset) ja muutokset sosiaaliseen kerrokseen (poliitikoiden ja ohjeiden päivitykset, henkilöstön ja käyttäjien koulutukset). Teoreettisesta näkökulmasta tutkimusta voitaisiin jatkaa syventämällä ja laajentamalla kirjallisuusanalyysia ja hakemalla tätä kautta evidenssiä eri komponenttien itseorganisoituneesta kriittisyydestä.

LÄHTEET

Aula, P. (1999) *Organisaation kaaos vai kaaoksen organisaatio? Dynaamisen organisaatioviestinnän teoria.* Helsinki: Loki-kirjat, 1999.

AV-Atlas. (2022). *Total amount of Malware and PUA Under Windows*. Haettu 3.4.2022 osoitteesta : https://portal.av-atlas.org

Bak, P., Tang, C. & Wiesenfield, K. (1987). Self-Organized Criticality: An Explanation of the 1/F Noise. *The American Physical Society, 59*, 381.

Bak, P., Tang, C. & Wiesenfield, K. (1988). Self-Organized Criticality. *The American Physical Society*, *38*, 364.

Bak. (1996). *How Nature Works, the science of self-organized criticality*. New York : Springer-Verlag Inc.

Barbieri, L., Mussida, C., Piva, M. & Vivarelli, M. (2019). Testing the employment impact of Automation, Robots and AI : A Survey and Some Methodolgcal issues. *IZA Discussion Paper No. 12612.*

Bar-Yam, Y. (2002). *General Features of Complex Systems*. UNESCO Encyclopedia of Life Support Systems.

Barabási, A-L. & Frangos. J. (2002). *Linked*. New York: Basic Books

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems* 1(2): 121-130

BBC. (2012). *China fake parts "used in US military equipment"*. Haettu 21.3.2022 osoitteesta: https://bbc.com/news/world-us-canada-18155293

Bibighaus, D. L. (2015). How Power-Laws Re-Write The Rules Of Cyber Warfare. *Journal of Strategic Security 8, no. 4, 39-52.*

Carreras, B., Newman, D. E., Dobson, I & Poole, A. B.. (2000). Initial evidence for self-organized criticality in electric power system blackouts. *Proceedings of Hawaii International Conference on System Sciences*, January 4-7, 2000, Maui, Hawaii.

CISA. (2021). *Emergency directive 22-02 mitigate apache log4j vulnerability*. Haettu 3.4.2022 osoitteesta : https://www.cisa.gov/emergency-directive-22-02

CISA. (2022). *Destructive Malware Targeting Organizations in Ukraine*. Haettu 25.3.2022 osoitteesta : https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

Cimpanu, C. (2021). *Conti ransomware group adopts log4Shell exploit*. haettu 25.3.2022 osoitteesta : https://therecord.media/conti-ransomware-group-adopts-log4shell-exploit/

Cloudflare. (2021). *Understanding how facebook disappeared from the internet*. Haettu 7.3.2022 osoitteesta https://blog.cloudflare.com/october-2021-facebook-outage/

Cloudflare. (2022). *What is the Mirai Botnet?* Haettu 15.3.2022 osoitteesta : https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Cockcroft, A. (2012). *The Netflix tech blog: A closer look at the Christmas Eve outage.* Haettu 15.3.2022 osoitteesta : http:// techblog.netflix.com/2012/12/a-closer-look-at-christmas-eve-out age.html.

Conrad, J. & Oman, P. (2007). *Evidence for self-organized criticality in Internet attacks.* Noudettu 14.2.2022 osoitteesta https://www.researchgate.net/publication/228933655_Evidence_for_self-organized_criticality_in_Internet_attacks

Cyperscoop. (2018). *DHS, Apple push back on Bloomberg supply chain story.* Haettu 1.4.2022 osoitteesta : https://www.cyberscoop.com/dhs-bloomberg-supply-chain-story-apple-amazon-denial/

Department of Justice (2021). *FBI's encrypted phone platform infiltrated hundreds criminal syndicates.* Haettu 19.3.2022 osoitteesta : https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

Dutch Safety Board. (2015). *Crash MH17, 17 july 2014*. Haettu 15.3.2022 osoitteesta : https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014

Dobson, I., Carreras, B.A., Lynch, V.E. & Newman, D.E. (2007). Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization. *Chaos : An Interdiscplinary journal of Nonlinear Science 17, issue 2.*

Dorner, M. (2014). Normal Accidents and Computer Systems. *In Proceeding zum Seminar Future Internet (FI) und Innovative Internet Technologien und Mobilkommunikation* (IITM)(Vol. 35).

Dunn, C., Myriam. (2010), *The Reality and Future of Cyberwar*, Parliamentary Brief, 30th March 2010

Dörner, D. (1989). *The logic of failure: Why Things Go Wrong and What We Can Do to Make Them Right*. New York: Metropolitan Books.

Dörner, D., Nixon, P., Rosen, S. D. (1990). The Logic of Failure and discussion. *Philosophical Transactions of the Royal Society of London*. Series B, Biological Sciences, *Vol. 327*, No. 1241, 463-473.

Energy.gov. (2021). *Colonial Pipeline Cyber Incident. Office of Cybersecurity, Energy Security, and Emergency Response*. Haettu 15.3.2022 osoitteesta : https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

EU. (2013). *Euroopan unionin kyberturvallisuusstrategia*. EUR-Lex julkaisuja 52013JC0001

Faloutsos, M. Faloutsos, P. & Faloutsos, C. (1999). On Power-Law Relationships of the Internet Topology. *SIGCOMM Computer Communications 29:4, 251–62.*

F-Secure. (2022a). *Virus*. Haettu 25.3.2022 osoitteesta : https://www.f-secure.com/v-descs/articles/virus.shtml

F-Secure. (2022b). *Trojan*. Haettu 25.3.2022 osoitteesta : https://www.f-secure.com/v-descs/articles/trojan.shtml

Gibson, W. (1984). *Neuromancer*. New York : Ace.

Gupta, S. (2022) *All About Conti*. Haettu 19.3.2022 osoitteesta: https://cybersecurityworks.com/blog/ransomware/all-about-conti.html

Gutenberg, B., Richter, C. (1955). Magnitude and Energy of Earthquakes. *Nature 176, 795.*

Greenberg, A. (2019). *Sandworm*. New York : Doubleday.

HS. (2021). *Näin yksi kaivinkone seisautti koko valtionhallinnon : "kahdennetut kaapelit ehkä samassa kourussa, Telialta ja Tieto-Evryltä vaaditaan selitystä"*. Haettu 20.3.2022 osoitteesta https://www.hs.fi/politiikka/art-2000008131530.html

Hruby, A. (2021). *Africa's digital infrastructure is the next playing field for great-power competition*. Haettu 26.3.2022 osoitteesta: https://www.atlanticcouncil.org/blogs/africasource/africas-digital-infrastructure-is-the-next-playing-field-for-great-power-competition/

Hyppönen, M. (2021). *Internet*. Helsinki: WSOY

IBM. (2022). *X-Force Threat Intelligence Index 2022*. Haettu 15.3.2022 osoitteesta: https://www.ibm.com/downloads/cas/ADLMYLAZ

ISO. (2018). *Risk management – Guidelines*. Haettu 4.3.2021 osoitteesta https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Janardhan, S. (2021). *Update about the October 4th outage.* Haettu 7.3.2021 osoitteesta https://engineering.fb.com/2021/10/04/networking-traffic/outage/

Jenkins, A., M. (1985). *Research methodologies and MIS research.* Indiana University, U.S.A.

Johnson, S. (2001). *Emergence: The Connected Lives of Ants, Brains, Cities*. New York: Scribner.

JYU. (2022). *Kansalaisen kyberturvallisuus*. Jyväskylän yliopiston avoin verkkokurssi osoitteessa : https://onlinecourses.jyu.fi/course/view.php?id=5 Noudettu 20.3.2022.

Järvinen, P & Järvinen, A. (2000). *Tutkimustyön metodeista*. Tampere : Opinpajan kirja.

Järvinen, P. (2004). *Research Questions Guiding Selection of an Appropriate Research method.* Department of Computer Sciences University of Tampere

Kari, M. J. (2019). *Johdanto*. Luento 9.9.2019 Jyväskylän yliopiston Informaation hallinta ja tiedustelu 1 -kurssilla.

Kaspersky. (2022a). *What is WannaCry ransomware?* Haettu 25.3.2022 osoitteesta : https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Kaspersky. (2022b). *What is Rootkit – Definition and Explanation*. Haettu 19.3.2022 osoitteesta : https://www.kaspersky.com/resource-center/definitions/what-is-rootkit

Keshner, M. (1982). 1/f Noise. *Proceedings of the IEEE*, *Vol 70*, No 3, 1982.

Koch, S. (2004). Profiling an open source project ecology and its programmers. *Electronic Markets, 14(2):77–88*.

Krebs, B. (2022). *Conti Ransomware Group Diaries, part 1: Evasion*. haettu 19.3.2022 osoitteesta: https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/

KvantiMOTV. (2013). *Kvantitatiivisten menetelmien tietovaranto*. Noudettu 4.3.2022 osoitteesta :
https://www.fsd.tuni.fi/menetelmaopetus/otos/otantamenetelmat.html

Laari, M. (toim.), Flyktman, J., Härmä, K., Timonen, J. & Tuovinen, J. (2019). #kyberpuolustus, kyberkäsikirja Puolustusvoimien henkilöstölle. *Julkaisusarja 3 : työpapereita nro 12, Maanpuolustuskorkeakoulu*.

Lehman, M. M. (1997). Laws of software evolution revisited. *Lecture Notes in Computer Science, 1149:108–124*.

Lehto, M. (2019a). *Kybermaailman ilmiöitä ja määrittelyjä.* Jyväskylän yliopisto.

Lehto, M. (2019b). *Kybermaailman määrittelyä.* Esitys Jyväskylän yliopiston Kybermaailma ja turvallisuus luennolla 6-7.9.2019.

Leigh, D. (2010). *How 250,000 US embassy cables were leaked*. The Guardian, 28.

Li, W. C., Nirei, M., & Yamana, K. (2018). Value of Data: There's No Such Thing as a Free Lunch in the Digital Economy. *Discussion papers 19022, Research Institute of Economy, Trade and Industry* (RIETI).

Liikenne- ja viestintäministeriö. (2001). Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. *Liikenne- ja viestintäministeriön julkaisuja 2021 :1.*

Madey, G., Freeh, V. ja Tynan, R. (2002). The open source software development phenomenon: An analysis based on social network theory. *In Proceedings of Americas Conference on Information Systems, pages 1806–1813*, Dallas, TX.

Malamud, B. & Turcotte, D. (2006). The applicability of power-law frequency statistics to floods. *Journal of Hydrology. 322. 168-180.*

Mandelbrot, B. (1982). *The Fractal Geometry of Nature*. Times Books.

Markopoulou, D., Papakonstantinou, V. ja De Hert, P. (2019). The new EU cybersecurity framework : The NIS Directive, ENISA's role and the General Data protection Regulation. *Computer Law & Security Review 35.*

Martínez, M.J., Eng, M., & Kim, C. (2012). Quantification of Complexity and Coupling Indices to Validate Normal Accident Theory in

Telecommunication Network Accidents. *30th International Conference on System Safety*, August 6-10, 2012. Atlanta, GA.

Mauro, J. C., Diehl, B., Marcellin Jr, R. F., & Vaughn, D. J. (2018). Workplace accidents and self-organized criticality. *Physica A: Statistical Mechanics and its Applications, 506, 284-289.*

Microsoft. (2021a). *Digital Defense report, October 2021*. Haettu 15.3.2022 osoitteesta : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Microsoft. (2022a). *Destructive malware targeting Ukrainian organizations*. Haettu 25.3.2022 osoitteesta : https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Mohurle, S. & Patil, M. (2017) A Brief study of Wannacry Threat : Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*

Morales-Esteban, A., Martínez-Álvarez, F., Troncoso, A., Justo, J. L. & Rubio-Escudero, C. (2010). Pattern recognition to forecast seismic time series. *Expert Systems with Applications*, *37*, 8333–8342.

Murray, P. J. (2003). So What´s New About Complexity. *System Research and Behavioral Science, 20, 409-417.*

Nakazato, K. & Arita, T. (2004). Evolution of complex food web structure based on mass extinction. *In Proc. of the 5th International Conference on Simulated Evolution and Learning*.

NIST. (2018). *Framework for Improving Critical infrastructure Cybersecurity*. National Insitute of Standards and Technology. Haettu 25.2.2022 osoitteesta https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Norton. (2022). *What is a rootkit ? And how to stop them*. Haettu 25.3.2022 osoitteesta : https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html

Nunan, D., Di Domenico, M. (2017). Big Data: A Normal Accident Waiting to Happen?. *J Bus Ethics 145*, 481–491

Park, J. (2021). The Lazarus group: The Cybercrime Syndicate Financing the north Korea State. *Harvard International Review. Cambridge Vol 42, Iss 2, 34-39*

Penttilä, L. (2019). *Kyberpelotteen rakentuminen*. Pro Gradu -tutkielma, yhteiskuntatieteiden ja filosofia laitos, Jyväskylän yliopisto.

Perrow, C. (1984). *Normal Accidents: Living With High-Risk Technologies*. New York: Basic Books.

Phelan, S. E. (1999). A Note on the Correspondence Between Complexity and Systems Theory. *Systemic Practice and Action Research, Vol 12, No. 3, 1999*

Poliisi. (2022a). *Kyberrikokset*. Haettu 20.3.2022 osoitteesta: https://poliisi.fi/kyberrikokset

Poliisi. (2022b). *Petosrikokset*. Haettu 21.3.2022 osoitteesta: https://poliisi.fi/petosrikokset

Pulsifier, E. (2021). *What happende with Microsoft Azure's Active Directory and DNS outages?* Haettu 15.3.2022 osoitteesta: https://acloudguru.com/blog/engineering/what-happened-with-microsoft-azures-active-directory-and-dns-outages

Rajamäki, J., Nevmerzhitskaya, J. & Virág, C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework. *IEEE Global Engineering Education Conference, 2042-2046*

Raggad, B. G. (2010). *Information Security Management*. CRC-Press.

Ralston, W. (2020). *A Dying man, a therapist and the ransom raid that shook the world.* Haettu 7.3.20222 osoitteesta https://www.wired.co.uk/article/finland-mental-health-data-breach-vastaamo

Raymond, E. S. (1999). *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol: O'Reilly and Associates.

Reuters. (2022). *Ukraina launches 'IT army,' takes aim at Russian cyberspace.* Haettu 15.3.2022 osoitteesta : https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

Rijpma, J. (1997). Complexity, tight–coupling and reliability: Connecting normal accidents theory and high reliability theory. *Journal of Contingencies and Crisis Management, 5(1), 15–23*.

Robertson, J. & Riley, M. (2018). *The Big Hack : How China used a Tiny Chip to Infiltrate U.S. Companies*. Haettu 21.3.2022 osoitteesta : https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Routio, P. (2004). *Hermeneuttinen tulkinta.* Tuotetiede. Taideteollisen korkeakoulun virtuaaliyliopisto. Aineisto haettu 25.2.2022 osoitteesta: http://www2.uiah.fi/virtu/materiaalit/tuotetiede/html_files/120_kirjallisuus.html#herm

Sagan, S. (1993). *The limits of safety: Organizations, accidents, and nuclear weapons.* Princeton, NJ: Princeton University Press.

Sanastokeskus STK ry. (2018). *Kyberturvallisuuden sanasto*. Helsinki: Huoltovarmuuskeskus

Saylors, E. (2015). *Cyber Gravity : The inevitable Collapse of Our Technology*. Haettu 26.1.2022 osoitteesta https://towardsdatascience.com/cyber-gravity-the-inevitable-colaspe-of-technology-260610b0abc7

ScienceDirect. (2013). *Power Law*. Haettu 9.2.2022 osoitteesta https://www.sciencedirect.com/topics/social-sciences/power-law

Scholz, C. H. (1990). *The Mechanics of Earthquakes and Faulting*. Cambridge University Press

Sheng, S., Yingkun, W., Yuyi, L., Yong, L. & Yu, J. (2011). Cyber attack impact on power system blackout. *IET Conference Publications*. 2011. 1-5.

Shrivastava, S. Sonpar, K. & Pazzaglia, F. (2009) Normal Accident Theory versus High Reliability Theory: A resolution and call for an open systems view of accidents. *Human Relations*. *62*, 1357-1390.

Siponen, M. (2002). *Designing secure information systems and software: Critical evaluation of the existing approaches and a new paradigm*. Academic Dissertation to be presented with the assent of the Faculty of Science, University of Oulu.

Siponen, M. (2005). Analysis of modern IS security development approaches : towards the next generation of social and adaptable ISS methods. *Information and Organization 15 339-375.*

Siponen, M. & Klaavuniemi, T. (2021). Demystifying beliefs about the natural sciences in information system. *Journal of Information Technology, 36*, 56-68

Sole, R. V., Manrubia, S. V., Benton, M. & Bak, P. (1997). Self- similarity of extinction statistics in the fossil record. *Nature, 388(21):764–767*, August 1997.

Soliman, W. (2019). *Information Security Management*. Esitys Jyväskylän yliopiston Information Security Management kurssin luennolla lokakuussa 2019.

Suojelupoliisi. (2021a). *Kansallisen turvallisuuden katsaus : Suomeen kohdistuu jatkuvia kybervakoiluyrityksiä*. Haettu 20.3.2022 osoitteesta : https://supo.fi/-/suomeen-kohdistuu-jatkuvia-kybervakoiluyrityksia

Suojelupoliisi. (2021b). *Suojelupoliisi tunnisti eduskuntaan kohdistuneen kybervakoiluoperaation APT31 :ksi*. haettu 20.3.2022 osoitteesta : https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kybervakoiluoperaation-apt31-ksi

Suojelupoliisi. (2021c). *Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun*. haettu 25.3.2022 osoitteesta : https://supo.fi/-/ulkomaiset-tiedustelupalvelut-kayttavat-yritysten-ja-yksityishenkiloiden-verkkoreitittimia-kybervakoiluun

Suojelupoliisi. (2022d). *APT on kybervakoojan työkalupakki*. haettu 19.3.2022 osoitteesta : https://supo.fi/apt-operaatiot

Sutcliffe, K. (2011). High Reliability Organizations (HROs). *Best Practice & Research Clinical Anaesthesiology*, *25*, 133-144

Taleb, N. N. (2007). *Black Swan - The Impact of Highly Impropable*. Random House.

Trafikom. (2021). *Kybersää*, helmikuu 2021. Haettu 15.3.2022 osoitteesta: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybersää_helmikuu_2021_TLP_WHITE.pdf

Turton, W., Mehtrotra, K. (2021). *Hackers Breached Colonial Pipeline using Compromised password.* Haettu 15.3.2021 osoitteesta : https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?sref=ylv224K8

Turvallisuuskomitea. (2019). *Suomen kyberturvallisuusstrategia*. haettu 25.2.2022 osoitteesta https://vm.fi/kyberturvallisuusstrategia

Tetlock, P. & Gardner, D. (2015). *Superennustajat: ennustamisen taito ja tiede* (suom. K. Pietiläinen, alkuteos Superforecasting. The Art and Science of Prediction, 2015). Helsinki: TerraCognita.

The Guardian. (2018). *The great firewall of Chine : Xi Jinping'd internet shutdown*. haettu 26.3.2022 osoitteesta : https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

The Guardian. (2019). *The Internet, but not as we know it : life online in China, Cuba, India and Russia.* Haettu 15.3.2022 osoitteesta : https://www.theguardian.com/technology/ng-interactive/2019/jan/11/the-internet-but-not-as-we-know-it-life-online-in-china-russia-cuba-and-india

The Intercept. (2019). *Everybody does it : the messy truth about infiltrating computer supply chains*. haettu 1.4.2022 osoitteesta : https://theintercept.com/2019/01/24/computer-supply-chain-attacks/

Ulkoministeriö. (2022). *Ulkoministeriö on saanut selvitettyä siihen kohdistuneen vakoilutapauksen*. Haettu 20.3.2022 osoitteesta : https://um.fi/ajankohtaista/-/asset_publisher/gc654PySnjTX/content/ulkoministerio-on-saanut-selvitettya-siihen-kohdistuneen-vakoilutapauksen

Yle. (2014). *Supo : Vieraat valtiot vakoilleet useita Suomen viranomaisverkkoja.* Haettu 20.3.2022 osoitteesta : https://yle.fi/uutiset/3-7120527.

Yle. (2018). *Katso paljastava piilokameravideo – Ylen toimittaja testasi tärkeiden yritysten ja laitosten tilaturvallisuutta : Lähes kaikilla puutteita kulunvalvonnassa*. Haettu 21.3.2022 osoitteesta : https://yle.fi/uutiset/3-10320853

Yle. (2020). *Tulli takavarikoi Tor-verkossa toimineen huumeiden kauppapaikan Sipulimarketin palvelimen sisällön.* Haettu 18.3.2022 osoitteesta : https://yle.fi/uutiset/3-11692785

Yle. (2021). *Sievissä aloittaa etälääkärin vastaanotto -terveyskeskuslääkärin paikkaan ei ollut hakijoita.* Haettu 15.3.2022 osoitteesta : https://yle.fi/uutiset/3-12080772

Yle. (2022). *Ukrainan puolesta taistelee ennennäkemätön hakkeriarmeija, mukana suomalainen "Jouni" – asiantuntijat varoittavat: "Tämä ei ole leikkisotaa"*. Haettu 15.3.2022 osoitteesta : https://yle.fi/uutiset/3-12338836

Verkkouutiset. (2021). *kaivinkone hyydytti Suomen valtio it-järjestelmät*. Haettu 9.4.2022 osoitteesta : https://www.verkkouutiset.fi/a/yle-valtion-it-jarjestelmat-hyytyivat-syyna-kaivinkone/#22e5c5d1

Von Solms & Van Niekerk. (2013) From Information Security to Cyber Security. *Computers & Security, 38*, 97-102

Wentian, L. (2002). Zipf's Law Everywhere. *Glottometrics 5*, 14-21

Whittaker, Z. (2022). *Conti ransomware gang's internal chats leaked online after declaring support for Russian invasion*. haettu 19.3.2022 osoitteesta https://techcrunch.com/2022/02/28/conti-ransomware-chats-leaked/

Wikipedia. (2021a). *Self-Organized Criticality*. Haettu 10.2.2022 osoitteesta https://en.wikipedia.org/wiki/Self-organized_criticality

Wired. (2019). *Planting Tiny Spy Chips in Hardware Can Cost as little as $200*. Haettu 1.4.2022 osoitteesta : https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/

Wu, J., Spitzer, C. W., Hassan, A. E. & Holt, R. C. (2004). Evolution spectrographs: Visualizing punctuated change in software evolution. In *Proceedings of the International Workshop on Principles of Software Evolution, pages 57–66,* Ky- oto, Japan.

Wu, J., Holt, R. & Hassan, A. E. (2007). Empirical Evidence for SOC Dynamics in Software Evolution. *IEEE International Conference on Software Maintenance*, ICSM. 244 - 254.

Zetter, K. (2013). *Snowden Smuggled Documents From NSA on a Thumb Drive.* Haettu 7.3.2022 osoitteesta https://www.wired.com/2013/06/snowden-thumb-drive/

Zetter, K. (2014). *Countdown to Zero Day*. New York : Broadway Books.

Zipf, G. K. (1949). *Human behavior and the principle of least effort.* Addison-Wesley Press.

Zwick, M. (1997). *Complexity theory and systems theory*. Paper presented at the International Institute for General Systems Studies, Second Workshop, San Marcos, TX.

LIITE 1 KYBERHYÖKKÄYKSET UKRAINASSA 2013-2022

2013

- Operaatio Snake. Vuosia jatkunut aggressiivinen vakoiluohjelma paljastui.
- Operaatio Armageddon. Ukrainalaisten vaikuttajien vakoilu ja tiedonhankinta, jolla seurataan vakoilevan toimijan näkökulmasta haitallisten suhteiden kehittymistä.

2014

- Massiivisia palvelunestohyökkäyksiä, jotka samalla katkaisevat internetin. **Krimi vallataan samanaikaisesti**.
- Vaalijärjestelmä kaadetaan kyberhyökkäyksellä kolme päivää ennen Ukrainan presidentin vaaleja.

2015

- Kyberhyökkäys, jolla haltuun otetaan ukrainalainen voimalaitos. 235 000 asukasta ilman sähköä.

2016

- Uusi hyökkäys voimalaitokseen, jolla saatettiin osa pääkaupunki Kiovan ja lähialueiden asukkaat sähköttömiksi n. tunnin ajaksi. Käytetty haittaohjelma oli rakennettu juuri tätä hyökkäystä varten ja osasi mm. ohjata fyysistä järjestelmää.

2017

- **NotPetya**. Ukrainaan kohdistettu ja maailman historian toistaiseksi tuhoisin haittaohjelma, joka kryptasi tietoa peruttamattomasti. Haittaohjelma karkasi 65 maahan ja saastutti n. 50 000 tietokonetta useilta toimialoilta mm. ydinvoimalan valvontajärjestelmä, terveydenhuollon järjestelmiä, logistiikkaa (mm. *Maersk*). Tuhojen aineelliset kustannukset arvioidaan olevan n. 10 Miljardia dollaria.

2018

- Epäonnistunut hyökkäys vedenpuhdistusasemaan, jossa pyrittiin lisäämään veden klooripitoisuutta. Onnistuessaan hyökkäys olisi vaikuttanut 23 Ukrainan provinssin lisäksi Moldovan ja Valko-venäjän veden puhtauteen.
- Kolmen Ukrainan laivaston aluksen kaappausta edelsi maan viranomaisia vastaan suunnattu kyberhyökkäys, jolla varastettiin tietoa operaation toteuttamiseksi.

2019

- Vaalivaikuttamista Facebookissa. Hyökkäys oli kehittyneempi versio vuoden 2016 Yhdysvaltojen vaalivaikuttamisen keinoista. Uutena elementtinä hyökkääjä pyrki kiertämään Facebookin suojamekanismeja maksamalla Ukrainan kansalaisille pääsystä heidän henkilökohtaisille sivuilleen.
- Garmaredon ryhmän kybervakoiluoperaatio

2020

- Pitkäkestoinen informaatio-operaatio.

2021

- Kohdennettu verkkourkinta.

2022

- 13.1 Tilanne eskaloituu: Ensimmäiset havainnot **WhisperGate**-haittaohjelmasta, joka tuhoaa tietokoneita korjauskelvottomaksi. Hyökkäys kohdentui ukrainalaisiin kriittisen infrastruktuurin organisaatioihin.
- 14.1 Ukrainan hallinnon ja paikallishallinnon verkkosivut joutuivat hyökkäyksen kohteeksi. Verkkosivuille tunkeutunut taho jätti sivulle viestin, jossa käskettiin "*pelkäämään ja odottamaan pahinta*". EU tukee Ukrainaa ja tuomitsee tehdyt kybertoimet.
- 15.1 Ukrainan mukaan hyökkäys kohdistui yhteensä 70 hallituksen verkkosivuun ja kymmeneen kohdistui murto.
- 16.1 Ensimmäiset attribuutiot, jotka osoittavat Venäjän olevan hyökkäyksen takana.
- 21.1 Ukrainan hallitus lähetti EU:lle pyynnön, jossa maa toivoo apua mm. kyberturvallisuuden osalta.
- 22.1 #*StandWithUkraine* aihetunnisteen käyttö alkaa Twitterissä
- 24.1 Yhdysvalloissa DHS varoittaa kriittisen infrastruktuurin toimijoit ja julkista sektoria. EU ja Britannia seuraa omilla suosituksillaan.
- 26.1 Palvelunestohyökkäys Ukrainalaiselle julkishallinnon ylläpitämälle verkkosivulle.
- 28.1 Ukrainassa havaittu lapsiin kohdistuvaa informaatiovaikuttamista. Kampanjassa houkutellaan katsomaan videota, joka osoittautuukin pelottavaksi ja uhkailee sodalla. Vastaavaa kampanjointia havaittiin myös Ruotsissa 17.1
- 15.2 Ukrainan puolustusministeriön ja asevoimien verkkosivut sekä kaksi pankkia joutuivat kyberhyökkäyksen kohteeksi.
- 16.2 Kohdennettu kalastelukampanja puolustushallintoon.
- 18.2 Ukrainalaiset viranomaiset kertoivat että teleoperaattori Vodafonen verkkoihin kohdistui torstaina häirintää Luhanskin ja Donetskin alueella.
- 23.2 **HermeticWiper** haittaohjelma tuhosi satoja tietokoneita kriittisen infrastruktuurin sektorilta. Uusi palvelunestohyökkäys kohdistui pankkeihin ja valtion hallintoon. Tästä oli jo aiemmin viitteitä ja Ukraina antoi toimijoille erillisen varoituksen alkuviikosta.
- 24.2 Venäjä teki kineettisen hyökkäyksen Ukrainaan ja aloitti sodan.
- 25.2 Ukraina on värvännyt tuhansia kyberturvallisuuden ammattilaisia sotaan Venäjää vastaan.
- 6.3 Venäjä lisää siviiliväestöön kohdistuvia kyberhyökkäyksiä. Mm. Phishing-kampanja, jossa jaetaan **MicroBackdoor**-haittaohjelmaa.
- 9.3 Ukrainan teleoperaattoreita kohtaan isketty. Estetään 4,6 miljoonaa kyberhyökkäystä Ukrainalaisten ja Puolalaisten tietokoneita ja puhelimia kohtaan. Tämä on kymmenkertainen määrä euroopan normaaliin keskiarvoon.
- 15.3 Sota jatkuu, mutta tiedon keräys tämän gradun osalta päättyy.

Keskeisimmät lähteet:
https://www.hhs.gov/sites/default/files/russia-ukraine-cyber-conflict-analyst-note-tlpwhite.pdf

https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html
https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/?preview_id=65075
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/
https://en.wikipedia.org/wiki/2022_Ukraine_cyberattacks
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/
https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/
https://www.nytimes.com/2019/03/29/world/europe/ukraine-russia-election-tampering-propaganda.html

LIITE 2 KYBERVYÖRYN LAAJA KÄSITEMALLI