Opinnäytetyö (AMK)

Tietojenkäsittely

2023

Jesse Rautakoura

Venäjän hyökkäys Ukrainaan ja sen vaikutus Suomen kyberturvallisuuteen

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tietojenkäsittely

2023 | 39 sivua

Jesse Rautakoura

Venäjän hyökkäys Ukrainaan ja sen vaikutus Suomen kyberturvallisuuteen

Opinnäytetyön tarkoituksena oli selvittää, miten helmikuussa 2022 alkanut Venäjän sotilaallinen hyökkäys Ukrainaa kohtaan on vaikuttanut Suomen kyberturvallisuuden tilaan. Opinnäytetyö rajattiin tuottamaan tietoa siitä, minkälaisia uhkia ja toimia hyökkäys on tuonut ilmi kyberturvallisuuden näkökulmasta Suomen valtiota, organisaatioita ja yksittäisiä ihmisiä kohtaan sekä onko mahdollisiin uhkiin reagoitu. Aiheen valintaan vaikutti kirjoittajan oma mielenkiinto sekä aiheen ajankohtaisuus ja merkityksellisyys.

Tutkimusmenetelmäksi valittiin empiirinen tutkimus. Aineistolähteinä hyödynnettiin kyberturvallisuutta koskevaa kirjallisuutta, alalla toimivien yritysten ja yhdistysten julkaisemia artikkeleita sekä viranomaisten raportteja ja verkkosivuja. Tarkoitus oli käyttää mahdollisimman ajantasaisia lähteitä. Teoriaosassa käsiteltiin kyberturvallisuuden peruskäsitteitä, osa-alueita, kyberhyökkäysten tekijöitä ja heidän motivaatioitaan tehdä hyökkäyksiä. Teoriaosuus on kirjoitettu siten, että kyberturvallisuudesta ennalta tietämätön henkilö saa käsityksen kyberturvallisuudesta ja sen tärkeydestä nyky-yhteiskunnan toimivuuden kannalta.

Tutkimustulosten perustella voitiin todeta, että Venäjän hyökkäys Ukrainaan on heijastunut myös Suomen kyberturvallisuuden kokonaiskuvaan. Suomen valtion organisaatioita kohtaan on kohdistettu venäläisten hakkeriryhmien toimesta hyökkäyksiä. Suomalaisia on joutunut väärennettyjen avustuskeräysten kohteiksi sekä Suomen tasavalta on joutunut lisäämään valmiuslakiin hybridipykälän, joka käsittelee kyberturvallisuusuhkia.

Asiasanat:

kyberturvallisuus, kyberuhka, kyberriski, palvelunestohyökkäys, Venäjän-Ukrainan sota

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Business Information Technology

2023 | 39 pages

Jesse Rautakoura

Russia's attack on Ukraine and its impact on Finland's cyber security

The purpose of the thesis was to find out how the Russian military aggression against Ukraine, which began in February 2022, has affected the state of cybersecurity in Finland. The thesis was limited to producing information about the types of cyber threats that have emerged as a result of the Russian attack on Ukraine and their effect on the Finnish state, organizations, and individuals from a cyber security perspective. The thesis also aimed to discover whether any possible threats been made and what has been the reaction to them. The choice of topic was influenced by the author's own interest and the topicality and relevance of the topic.

Empirical research was chosen as the research method of the thesis. The material sources used were included literature on cybersecurity, articles published by companies and associations active in the field together with official reports and websites of public authorities. The information presented was based on as recent sources as possible. The theoretical part covered the basic concepts of cyber security, its components, the perpetrators of cyberattacks and their motivations for committing attacks. The theoretical part is written in such a way that a person with no prior knowledge of cybersecurity can get an understanding of cybersecurity and its importance for the functioning of modern society.

Based on the research results, it could be stated that Russia's attack on Ukraine has also been reflected in the overall picture of Finnish cyber security. There have been attacks from Russian hacker groups. Specially Finns have been victims of fake Ukraine relief fundraisers, and the Republic of Finland has had to add to its Emergency Powers Act a new section, which deals with cybersecurity threats.

Keywords:

cyber security, cyber threat, cyber risk, denial of service attack, Russian-Ukrainian war

Sisältö

Kuvat

Taulukot

Käytetyt lyhenteet ja sanasto

EU	Euroopan unioni. Taloudellinen ja poliittinen liitto, johon kuuluu 27 eurooppalaista jäsenvaltiota.
Hybridipykälä	Suomen valmiuslakiin lisätty uusi pykälä, jonka tarkoituksena on suojata Suomen yhteiskunnan toimintakykyä ja väestön elinmahdollisuuksia poikkeusoloissa.
Hybridiuhka	Yhdistelmäuhka, jossa tarkoituksenmukaisesti hyökätään haluttuun kohteeseen monella eri tavalla. Tavat voivat olla esimerkiksi sotilaallisia, taloudellisia, poliittisia, tai kyberympäristössä tapahtuvia.
Informaatiovaikuttaminen	Tiedon levittämistä, jolla pyritään järjestelmällisesti vaikuttamaan ihmisten yleiseen mielipiteeseen, käyttäytymiseen sekä päätöksentekoon ja sitä kautta yhteiskunnan toimintakykyyn.
Jatkuvuudenhallinta	Organisaation luoma toimintatapa vakavia häiriötekijöitä varten.
Kansallinen turvallisuus	Yhteiskunnan yhteinen turvallisuus ja koskemattomuus.
Kyberturvallisuuskeskus	Liikenne- ja viestintävirasto Traficomin alainen viranomainen, joka kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä tuottaa tietoturvallisuuden tilannekuvaa.
Nato	North Atlantic Treaty Organization eli Pohjois-Atlantin puolustusliitto. Kolmenkymmenen valtion poliittinen ja sotilaallinen liittoutuma. Jäsenvaltiot ovat eurooppalaisia ja pohjoisamerikkalaisia valtioita.

Palvelunestohyökkäys	Verkkohyökkäys, jossa pyritään estämään tietyn verkkopalvelunkäyttö. Hyökkäys toteutetaan kohdistamalla palveluun niin paljon verkkoliikennettä, että palvelu ei enää suoriudu tehtävistään.
Tietoliikenne	Tiedonsiirtoa lähettäjän ja vastaanottajan välillä eli tiedon siirtämistä paikasta toiseen.
Tietojärjestelmä	Sisältää joukon tietoja, tietoja käsitteleviä ihmisiä, tietojenkäsittelylaitteita sekä ohjelmia. Näistä koostuva järjestelmä, jonka tarkoituksena on tietojenkäsittelyn avulla parantaa tai helpottaa jotain tiettyä toimintaa.
Tietoturvallisuus	Tiedon luottamuksellisuuden, saatavuuden ja eheyden ylläpitämistä. Tietoturvallisuuden tarkoitus on suojata tietojärjestelmiä ja -aineistoja.
Toimitusketju	Esineiden valmistajien, jakelijoiden, toimittajien sekä kuluttajien muodostama verkosto, jonka kautta esineet kulkevat valmistajien raaka-ainevaiheesta aina loppukäyttäjien valmiiksi tuotteiksi.

1 Johdanto

Venäjän hyökkäys Ukrainaan helmikuussa 2022 on vaikuttanut monella tapaa koko maailman, Euroopan ja myös Suomen kansalliseen turvallisuuteen. Suojelupoliisi (2022a) on kertonut Suomen infrastruktuuriin kohdistuvan tiedustelun ja vaikuttamisen uhkatason suurentuneen sekä fyysisessä että kyberympäristössä. Suurin syy tähän on Venäjän hyökkäyssodan lisäksi Suomen Nato-jäsenyysprosessi.

Hyökkäyksen toimesta Euroopan unioni on asettanut Venäjää kohtaan pakotteita sekä vienti- ja tuontirajoituksia. Tästä on koitunut seurauksia Venäjän valtiota kohtaan mutta myös Euroopan unionin jäsenmaita kohtaan mukaan lukien Suomi. Seurauksia on ollut talouskasvun heikentyminen, hintojen nousu sekä energiavaje. (Kostiainen 2022.) Näillä seurauksilla varisinkin energiavajeella on myös mahdollisia vaikutuksia, sillä energiankulutusta ja sähköä voidaan joutua tulevaisuudessa säännöstelemään (Eskonen 2022). Tästä saattaa olla vaikutuksia Suomen kyberturvallisuuden tilaan. Sillä suurin osa Suomen Infrastruktuurista pyörii sähköjärjestelmien avulla (Horelli 2020).

Venäjän hyökkäyssota on tuonut myös mukanaan kyberrikollisuutta. Suomen valtion organisaatiot ovat joutuneet palvelunestohyökkäysten kohteiksi venäläisten toimijoiden taholta. (Bogdanov & Tolkki 2022a.) Ukrainan kriisiä on myös käytetty hyväksi levittämällä valekeräyksiä tunnettujen hyväntekeväisyystoimijoiden nimissä. Todellisuudessa näissä keräyksissä lahjoitukset menevät kuitenkin suoraan rikollisille.

Opinnäytetyön tarkoitus on tutkia, miten Venäjän hyökkäyssota Ukrainaa kohtaan on vaikuttanut Suomen valtion ja suomalaisten kyberturvallisuus tilanteeseen ja onko Suomen valtio reagoinut millään tavalla mahdolliseen muuttuneeseen kyberturvallisuus tilanteeseen. Aihe on ajankohtainen ja merkityksellinen suomalaisille, sillä jaamme Venäjän kanssa yhteistä rajaa yli 1300 kilometriä (Lukkari 2016).

2 Kyberturvallisuus

Kyberturvallisuuskeskus määrittelee kyberturvallisuuden yhteiskunnan ja organisaatioiden digitalisoitumisen myötä tulleiksi uudenlaisiksi turvallisuushaasteiksi. Käytännössä tämä tarkoittaa laitteiden, ohjelmistojen, tietojärjestelmien ja tietoliikenneyhteyksien suojaamista erilaisilta kyberuhkilta. Kyberuhkat ovat haitallisia tapahtumia tai kehityskulkuja, joita esiintyy kyberympäristössä. (Traficom 2020.)

Horelli (2020) pohtii artikkelissaan, että nykypäivän yhteiskunnassa suurin osa toiminnoista on riippuvaisia sähköisistä verkoista ja tiedonsiirrosta verkon avulla. Esimerkiksi sähkö, vesi, liikenteen ohjaus, terveydenhuolto, kauppa- ja logistiikka-ala ovat riippuvaisia verkoista ja tietokoneista ja ovat sen myötä alttiita erilaisille kyberuhkille ja häirinnälle (Järvinen 2022, 16).

2.1 Kyberturvallisuuden osa-alueet

Kaspersky (2022) lajittelee kyberturvallisuuden seuraavasti kuuteen eri sektoriin:

- Verkkoturvallisuus on käytäntö, jossa suojataan tietokoneverkkoa tunkeilijoilta.
- Sovellusturvallisuus syventyy laitteiden ja ohjelmistojen turvaamiseen.
- Tietoturvallisuus suojaa tietojen eheyttä ja yksityisyyttä tietojen varastoinnin ja -siirron aikana.
- Toimintaturvallisuus sisältää tietovarallisuuden käsittelyyn ja suojaamiseen liittyvät prosessit ja päätökset. Tällä tarkoitetaan käyttäjien käyttöoikeuksia ja menettelyjä siitä mitä tiedolla saa tehdä.
- Katastrofin palautuksesta ja liiketoiminnan jatkuvuudesta puhutaan, kun mitataan organisaation reagointi kykyä kyberturvallisuushäiriöihin tai tiedon menetyksiin. Poikkeaman sattuessa katastrofin palautus käytännöt sanelevat kuinka organisaatio elvyttää toimintansa takaisin samaan toimintakykyyn kuin ennen poikkeamaa.

- Loppukäyttäjien koulutus käsittelee kaikkein ennalta-arvaamattomimman kyberturvallisuustekijän eli ihmiset. Loppukäyttäjien opastus on merkittävää jokaisen organisaation turvallisuudelle, sillä kuka tahansa voi tietämättään viedä viruksen tietokonejärjestelmään, mikäli käyttäjä ei noudata hyviä turvallisuuskäytäntöjä.

2.2 Haavoittuvuus

National Institute of Standards and Technology (2022) mukaan tietotekniikassa haavoittuvuudella viitataan mihin tahansa heikkouteen tietojärjestelmässä, järjestelmän turvamenettelyissä, sisäisessä valvonnassa tai toteutuksessa, jota verkkorikolliset voivat hyödyntää. Haavoittuvuus voi olla esimerkiksi puuttuva ohjelmistopäivitys tai virhe tietokoneohjelmistossa.

Järjestelmän omistaja pystyy haavoittuvuuksien hallinnan, eli niiden systemaattisen tunnistamisen, luokittelemisen, korjaamisen ja lieventämisen avulla vähentämään haavoittuvuuksia (Limnéll, Majewski ja Salminen 2014, 110).

2.3 Kyberriski

Kyberriskillä tarkoitetaan yleisesti mitä tahansa riskiä, joka johtuu jonkinlaisesta digitaalisen palvelun häiriöstä ja aiheuttaa yritykselle taloudellista vahinkoa, mainehaittaa tai vaikeuttaa yrityksen normaalia toimintaa. (Insta 2020).

Toisin kuin uhkaa, riskiä ei voida torjua vaan se on olemassa kaikessa toiminnassa. Torjumisen sijaan riskeihin pitää suhtautua eri tavalla, kuten omaksua niiden olemassaolo sekä oppia välttämään ja rajaamaan niitä. (Limnéll, Majewski ja Salminen 2014, 108.)

2.4 Kyberuhka

Kyberuhka tarkoittaa digitaalisin keinoin toteutettua uhkaa, joka kohdistuu digitaaliseen omaisuuteen, järjestelmään tai palveluun. Kyberuhkaan kuuluu elementtejä, jotka vaarantavat kohteen luotettavuuden tai toimivuuden. (STEK ry 2022.)

Kun puhutaan kyberuhkasta pitää muistaa, että kyse ei ole vielä vahingoittavasta toiminnasta vaan sillä uhkaamisesta. Parhaiten uhkia vastaan pystytään varautumaan laittamalla organisaation kyberturvallisuuden perusasiat kuntoon eli lisäämällä ihmisten tietoisuutta, toimintakykyä ja pitämällä tietoturva ajan tasalla. (Limnéll, Majewski ja Salminen 2014, 106–107.)

2.5 Kyberrikollisuuden osa-alueet

Kyberuhkien aiheuttajia ovat kaikki ne toimijat, jotka voivat toimillaan saada aikaan riskin arjen toimintojen ja palveluiden käytettävyydelle, toimivuudelle, eheydelle, luotettavuudelle, tunnistettavuudelle sekä varmennettavuudelle. Kyberuhkien aiheuttajat jaotellaan usein motivaatioidensa mukaisesti. (Peda.net 2022.) Yleisimpiä kyberuhkien aiheuttajia ovat valtiot, terroristit, yritykset, rikolliset ja tavalliset ihmiset (Limnéll, Majewski ja Salminen 2014, 113).

Taulukossa 1 on havainnollistettu kyberuhkien aiheuttajia ja syitä miksi hyökkäyksiä tehdään. Lisäksi taulukosta voi nähdä mitkä toimijat toteuttavat hyökkäyksiä ja mitkä ovat yleisempiä kohteita sekä motivaatioita kullekin toimijalle.

Taulukko 1. Kyberuhkien rakenne (Limnéll, Majewski ja Salminen 2014, 113).

	Motivaatio	Toimijat	Kohde
Kybersota	Poliittinen/ Sotilaallinen hallinta	Valtiot	Kriittinen infra
Kyberterrorismi	Poliittinen muutos, pelko	Terroristit	Infra, voimavarat ja julkiset kohteet
Kybervakoilu	Tiedon varastaminen	Valtiot ja yritykset	Hallitukset, yritykset, yksilöt
Kyberrikollisuus	Taloudellinen hyötyminen	Rikolliset	Yritykset, yksilöt
Haktivismi	Poliittinen muutos, egoismi	Aktivistit, haktivistit ja yksilöt	Hallitukset, yritykset, yksilöt

2.5.1 Kybersota

Kybersodankäynnillä tarkoitetaan valtion tai kansainvälisen järjestön toimia, joiden tarkoituksena on hyökätä ja yrittää vahingoittaa toisen maan tietokoneita tai tietoverkkoja esimerkiksi palvelunestohyökkäysten tai tietokonevirusten avulla (Rand corporation 2022). Lisäksi hyökkäyksen kohteina voivat olla muut tietotekniset laitteet, tietoliikenneprotokollat, tietojärjestelmät ja sovellukset. Keskeisempiä tavoitteita kybersodankäynnissä on vaikuttaa vastustajan kriittisen infrastruktuurin toimivuuteen ja heikentää yhteiskunnan elintärkeitä toimintoja sekä asevoimien suorituskykyä. Kybersota ei siis rajoitu vain asevoimia vastaan, vaan kohteena on koko yhteiskunta. (Räty 2022.) Kybersotaan varaudutaan samalla tavalla kuin fyysiseenkin sotaan. Suomessa esimerkiksi varusmiespalveluksen voi suorittaa kybervarusmiehenä perinteisemmän varusmiespalveluksen sijaan. Suomessa kyberturvallisuuden ylläpito ja vastuu on jaettu puolustusvoimien, poliisin, liikenne- ja viestintäministeriön sekä ulkoministeriön kesken. (Haapavuori 2022.)

2.5.2 Kyberterrorismi

Kyberterrorismista puhutaan, kun väkivaltaiseen ääriliikkeeseen kytkeytyneet henkilöt levittävät kyberympäristön avulla propagandaa tai terroristien materiaaleja värvätäkseen uusia jäseniä järjestöihinsä tai aiheuttaakseen vihamielistä radikalisoitumista. Lisäksi internettiä voidaan käyttää terroristisen toimijoiden väliseen kommunikaatioon tai terroriteon suunnitteluun. (Sisäministeriö 2022b.)

2.5.3 Kyberrikollisuus

Kyberrikollisuudella tarkoitetaan tietotekniikkaan tai tietoverkkoihin kohdistuvia rikoksia tai näitä hyväksi käyttäen tehtyjä rikoksia. Tietoverkkorikoksia ovat esimerkiksi hakkerointi, jonka avulla tunkeudutaan luvatta uhrin tietoverkkoon tai tietojärjestelmään ja näin voidaan tuhota tietojärjestelmässä olevaa tietoa tai käyttää järjestelmää omiin tarkoituksiin. Tietokoneeseen voidaan myös tartuttaa haittaohjelmia, joiden avulla voidaan vakoilla uhria tai käyttää sitä osana palvelunestohyökkäyksiä, jolla taas pyritään hidastamaan tai estämään kohteen tietojärjestelmän toimintaa. Yksi yleisempiä kyberrikollisuuden motivaatioita ovat omaisuusrikokset eli taloudellinen hyöty, johon kuuluu petokset, maksuvälinepetokset, rahanpesu ja kiristykset. (Sisäministeriö 2022b.)

2.5.4 Haktivismi

Haktivismi on tietokonejärjestelmän tai verkon väärinkäyttöä sosiaalisesti tai poliittisesti motivoiduista syistä. Haktivismia harjoittavia henkilöitä kutsutaan haktivisteiksi. Haktivismin tarkoituksena on kiinnittää yleisön huomio johonkin, jonka haktivisti uskoo olevan tärkeä asia tai syy, kuten tiedonvälityksen vapaus, ihmisoikeudet tai uskonnollinen näkökulma. (Techtarget 2021.)

2.5.5 Motivaatio

Kyberrikollisuudella on paljon eri motiiveja. Niitä ovat esimerkiksi taloudellinen hyöty, vakoilu, tiedon kerääminen tai sen tuhoaminen sekä terrorismi. Lisäksi kyberrikollisuutta pystyy harjoittamaan kansainvälisesti. Kyberympäristössä tapahtuvat rikokset ovat monesti kansalliset rajat ylittäviä. Suurin osa kyberrikollisuudesta ei saavu poliisin tietoon ja rikokset, joista poliisi aloittaa esitutkinnan, jäävät usein selvittämättä tai selviävät vain osittain. (Sisäministeriö 2022b.)

3 Venäjän hyökkäys Ukrainaan 2022

Venäjä aloitti vuonna 2021 laajan sotilasjoukkojen keskityksen Ukrainan itäosien rajan läheisyyteen. Tilanteen jatkuttua useita viikkoja päätti Venäjän presidentti Vladimir Putin tunnustaa Ukrainalle kuuluvien Donetskin ja Luhanskin alueiden muut kuin Ukrainan hallituksen valvomat osat itsenäisiksi ja lähettää alueille venäläisiä joukkoja. Venäjä käynnisti hyökkäyksen Ukrainaa kohtaan 24. helmikuuta 2022. (Eurooppa-neuvosto 2022a.)

3.1 EU:n reaktio

EU on jyrkästi tuominnut Vladimir Putinin päätöksen tunnustaa Ukrainan itäosien alueet itsenäiseksi sekä perusteettoman sotilaallisen hyökkäyksen Ukrainaa kohtaan. EU-johtajat ovat vaatineet useasti Venäjää lopettamaan kaikki sotilaallinen toiminta Ukrainassa ja vetämään venäläiset sotilaat ja sotakaluston pois Ukrainasta. EU myös ”kunnioittaa täysimääräisesti Ukrainan alueellista koskemattomuutta, suvereniteettia ja itsenäisyyttä” ja painottaa Ukrainan oikeutta päättää kohtalostaan. (Eurooppa-neuvosto 2022a.)

EU on reagoinut sotilaalliseen hyökkäykseen laajentamalla huomattavasti Venäjän vastaisia pakotteita lisäämällä yhteisöjä ja henkilöitä pakoteluetteloon. Tämän lisäksi EU on antanut Ukrainalle humanitaarista, poliittista, taloudellista sekä sotilaallista tukea. (Eurooppa-neuvosto 2022a.)

3.2 Venäjään kohdistuvat pakotteet

Venäjän hyökättyä Ukrainaan, EU on asettanut yhteensä kahdeksan pakotepakettia Venäjää kohtaan. Viimeinen pakotepaketti on asetettu 6.10.2022. Pakotteisiin sisältyy rajoittavia toimenpiteitä, kuten henkilö- ja talouspakotteita sekä diplomaattisia toimenpiteitä. (Eurooppa-neuvosto 2022a.)

Talouspakotteiden tarkoitus on tuottaa Venäjälle suurta taloudellista haittaa ja vaikeuttaa Venäjää jatkamasta sotatoimia Ukrainassa. Henkilöpakotteet on

suunnattu henkilöihin ja yhteisöihin, ”jotka ovat vastuussa Ukrainan alueellista koskemattomuutta, suvereniteettia ja itsenäisyyttä heikentävien toimien tukemisesta, rahoittamisesta tai täytäntöönpanosta tai hyötyvät niistä.”. (Eurooppa-neuvosto 2022b.)

3.3 Vienti- ja tuontirajoitteet

EU:n vienti- ja tuontirajoitukset Venäjää kohtaan ovat todella laajat. Rajoituksiin kuuluu suuria määriä eri raakamateriaaleja, komponentteja puolustustarvikkeita, setelirahat, yleistuotteita sekä laajasti eri palveluita. (Elinkeinoelämän keskusliitto 2022.)

Vaikka vaikutukset Venäjän valtiota kohtaan ovat suuria, vaikuttavat pakotteet ja vientirajoitukset myös Euroopan Unionin jäsenmaihin. Suomeen ei esimerkiksi tule Venäjältä enää maakaasua tai sähköä. Tämä tarkoittaa sitä, että todennäköisesti myös suomalaiset joutuvat tulevana talvena vähentämään energiankulutusta. Lisäksi on mahdollista, että energiateollisuus voi joutua säännöstelemään sähkönjakelua Suomessa tulevana talvena. (Eskonen 2022.)

4 Suomen kyberturvallisuustilanne

Venäjän hyökkäys Ukrainaan ja siitä johtuva kansainvälinen turvallisuustilanne koskettaa väistämättömästi myös digitaalista maailmaa sekä aiheuttavat tarvetta varautua uusiin kyberuhkiin. Organisaatioiden on tärkeää tarkastella tämänhetkistä maailmantilannetta ja muokata kyberturvallisuuden suojauskäytäntöjään sen mukaisesti. (Traficom 2022c.)

Epävarmuustekijät vaikuttavat myös organisaatioiden riskienhallintaan. Organisaatioiden tulee ottaa huomioon omassa riskienhallinnassa entistä tarkemmin esille toimintaympäristön aiheuttamat uhkat. (Traficom 2022c.) Kyberturvallisuuskeskus on kesällä 2022 julkaissut ohjeet, joiden avulla organisaatiot voivat parantaa kyberturvallisuuttaan sekä pienentää riskiä hyökkäyksen joutumisen kohteeksi. (Traficom 2022f.)

4.1 Kyberympäristön uhkataso

Kyberhyökkäysten määrät ovat kasvaneet maailmanlaajuisesti vuoden 2022 aikana. Hyökkäyksiä kohdistuu myös kasvavassa määrin Suomeen. Suomalaisiin organisaatioihin suuntautuvissa kyberhyökkäyksissä etenkin haittaohjelmien, tietojenkalastelun ja palvelunestohyökkäysten lukumäärät ovat nousseet. (Traficom 2022f.)

Hyökkääjien motivaatiota on vaikea päätellä, mutta Kyberturvallisuuskeskus arvioi, että valtioiden tekemät poliittiset päätökset sekä turvallisuusympäristössä tapahtuvat käänteet voivat houkutella rikollisia kohdistamaan hyökkäyksiä suomalaisia organisaatioita kohtaan. Kyberturvallisuuskeskus on näiden tapahtumien vuoksi arvioinut kyberturvallisuuden uhkatason nousseen Suomessa. (Traficom 2022f.)

Kuva 1. Suomeen kohdistuu vuosittain yhä enemmän kyberhyökkäyksiä (Traficom 2022f).

Kuvassa 1 on kuvattu statistiikkaa kyberympäristön uhkatason noususta. Merkittävin uhka eri organisaatioille on kiristyshaittaohjelmat. Kesän 2022 aikana useat organisaatiot ovat joutuneet kiristyshaittaohjelmien uhriksi. Kiristyshaittaohjelmien määrät ovat kasvaneet vuodessa noin 30 % vuoteen 2021 verrattuna. Suomalaisiin organisaatioihin kohdistetut kyberhyökkäykset ovat entistä kohdennetumpia ja suunnattu tiettyihin yksittäisiin organisaatioihin aikaisemman hakuammunnan sijaan. (Traficom 2022f.)

Kyberturvallisuuteen kuuluu oikeanlaiset suojaustoimet, valmistautuminen ja hyvä jatkuvuudenhallinta. Ne vähentävät hyökkäyksien vaikutuksia ja riskiä joutua hyökkäysten uhreiksi. Nämä helpottavat organisaatioita palautumaan takaisin normaaleihin olosuhteisiin. (Traficom 2022f.)

4.2 Energiavaje

On hyvin mahdollista, että sota Ukrainassa tulee vaikuttamaan digitaalisen maailman toimivuuteen. Taloudessa tapahtuvat voimakkaat muutokset ja energian nopea hinnannousu ovat yhteydessä myös digitaaliseen maailmaan. Tätä voidaan pitää kyberuhkana. (Traficom 2022a.) Sodasta johtuvat pakotteet ovat johtaneet siihen, että Venäjältä ei tule enää sähköä Suomeen. Hanhinen (2022) kirjoittaa artikkelissaan, että Venäjältä tuodun sähkön osuus Suomeen on ollut viime vuosina noin kymmenen prosenttia koko Suomen kokonaiskulutuksesta. Tämä sähkön osuus on kuitenkin tarkoitus korvata tuulivoimalatuotannon lisääntymisellä sekä ydinvoimalla. Suomen on tarkoitus tuottaa kaikki sähkö omavaraisesti jo vuonna 2023.

Energiamarkkinoilla on suuri yhteys kybertoimintaympäristöön, sillä ympäristö tarvitsee toimiakseen jatkuvasti sähköä. Energiamarkkinoiden epävakaat ja arvaamattomat olosuhteet voivat heijastua kyberturvallisuuteen sekä niillä voi olla vaikutuksia ICT-palveluiden toimivuuteen (Traficom 2022a.)

Taulukossa 2 puolustusministeriö (2019) on kuvannut sähkökatkojen vaikutuksia Suomessa. Vaikka taulukon tapahtumat koskevatkin kokonaisvaltaista sähkökatkoa Suomessa, antaa se silti hyvän havainnekuvan digitaalisen ympäristön tärkeydestä.

Taulukko 2. Sähkökatkon vaikutus Suomen infrastruktuuriin (Puolustusministeriö 2019).

Näin Sähkökatko vaikuttaa	
0 sekuntia	• Raitiovaunut, metro, lähi- ja kaukojunat pysähtyvät • Pankkiautomaatit ja pankkien konttorit menevät kiinni, maksukortit eivät toimi • Vedentulo lakkaa osalla ihmisistä, • Vessan voi vetää vain kerran • Huoltoasemalta tai jakelupisteestä ei saa polttoainetta • Hissit pysähtyvät • Lämmitys katkeaa lukuun ottamatta puu-uuneja • Valot sammuvat, kodinkoneet eivät toimi • Katuvalot ja liikennevalot sammuvat • Jääkaapit ja pakastimet alkavat lämmetä
15 minuuttia	• Useimmat ruokakaupat ja muut pienet liikkeet sulkevat ovensa
2 tuntia	• Ensimmäiset tietoliikenteen tukiasemat mykistyvät – sen jälkeen ei voi soittaa eikä pääse nettiin • Isot ruokamarketit ja kauppakeskukset alkavat sulkeutua
6 tuntia	• Suurimmalta osalta suomalaisia puhelin- ja nettiyhteydet ovat poikki • Henkilöautoista, takseista ja linja-autoista loppuu vähitellen polttoaine
18 tuntia ja siitä eteenpäin	• Talojen sisäilma lämpötilat alkavat laskea alle +10 asteen. • Alle +10 asteen lämpötilassa ihminen tarvitsee lihasten tuottamaa lämpöä, jotta kehon lämpötila ei laske. Huonosti liikkuvat ihmiset, kuten pikkulapset, vanhukset ja sairaat eivät voi oleskella näin viileässä tilassa enää pitkään.

4.3 Toimitusketjut

Toimitusketjut häiriintyivät koronapandemian alkaessa vakavasti. Autoliiton jäsenlehden mukaan sirupula sai alkunsa vuonna 2020 äkillisesti alkaneesta puolijohdetuotteiden kysynnän kasvusta varsinkin kulutuselektroniikan, tietokoneiden ja tiedontallennuksen saralla (Autoliitto 2022).

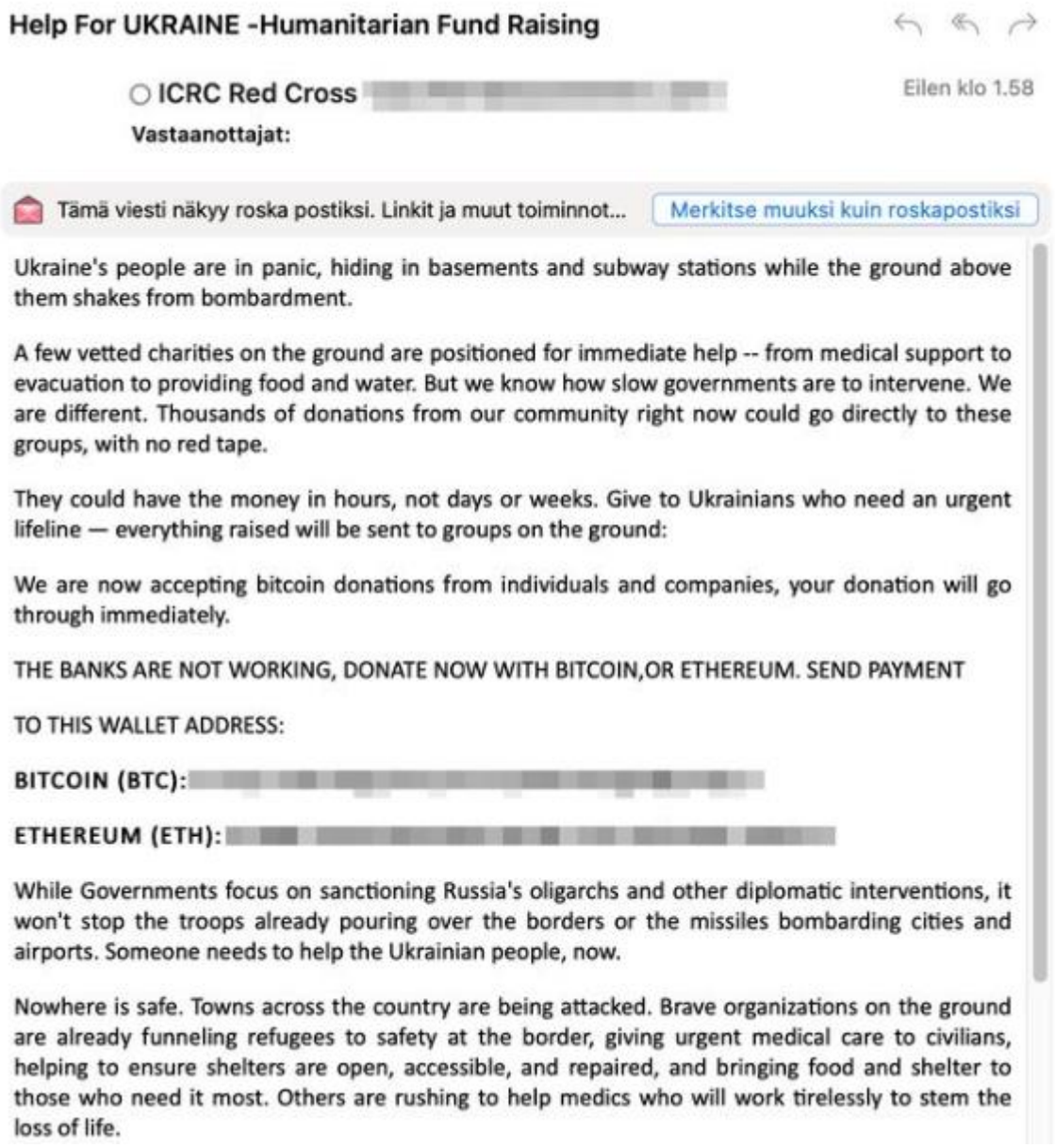
Näistä syistä organisaatiot voivat joutua odottamaan uusia laitteitaan useita kuukausia. Tämä johtaa siihen, että organisaatiot joutuvat pitkittämään elinkaaren lopussa olevien laitteiden käyttöä ja uusien suojaratkaisuiden rakentamisessa tulee kestämään tarkoitettua pidempään. (Traficom 2022b.)

Laitteiden saatavuushäiriöt ja hintojen nousu ovat tuoneet myös lisää huijareita mukaan elektroniikka markkinoille. Kyberturvallisuuskeskus varoittaakin huijareista, jotka kaupittelevat halpoja kopioita laitteista. Harkintakykyä tarvitsee käyttää yhä enemmän myös laitekaupoilla. (Traficom 2022b.)

4.4 Kriisin hyväksikäyttö

Yleisesti huijarit pyrkivät hyväksikäyttämään kansainvälisiä kriisejä, sekä ihmisten halua auttaa. Tämän kaltaista toimintaa nähtiin myös koronapandemian alkuaikoina. Näin on käynyt myös Venäjä-Ukraina sodassa. Huijarit ovat levitelleet haittaohjelmia ja kalastelleet rahaa sekä tietoja Ukrainan sodan verukkeella. Lisäksi Ukrainan tapahtumat ovat vaikuttaneet väärennettyyn sähköpostiliikenteeseen. Väärennettyä sähköpostiliikennettä on liikkunut sodan alkamisen jälkeen enemmän. (Traficom 2022e.)

Kemppi (2022) kirjoittaa artikkelissaan, että Venäjän hyökättyä Ukrainaan on liikkeellä ollut paljon huijaussivustoja, -julkaisuja ja -sähköpostiviestejä, joiden vakuutetaan liittyvän virallisiin keräyksiin. Huijarit esittävät usein tunnettuja toimijoita, kuten hyväntekeväisyysjärjestöjä. Todellisuudessa valekeräysten kautta tehdyt lahjoitukset menevät suoraan rikollisille. Huijauksia on helppo levittää sosiaalisen median kautta, sillä ihmisten on helppo jakaa eteenpäin valekeräyksiä tietämättä, että kyseessä on valekeräys.



Kuva 2. Kyseinen viesti levisi sähköpostinvälityksellä (Kemppi 2022).

Kuvassa 2 viitataan viestiin, joka on lähetetty Punaisen Ristin nimissä. Viestissä pyydetään vastaanottajaa lahjoittamaan rahaa ukrainalaisille sodan uhreille ja lähettämään kryptovaluuttaa sähköpostissa julkaistuihin kryptolompakoihin, koska pankit eivät Ukrainassa toimi. Keräyksiin lahjoittaessa tulisikin aina varmistaa keräyksen pitäjältä, onko kyseistä keräilykampanjaa sillä hetkellä käynnissä. Erityistä varovaisuutta ja harkintakykyä tarvitsee käyttää silloin, jos

keräysilmoituksessa on suora tilinumero tai kuten yllä olevan kuvan 2 viestissä ilmoitettu kryptolompakko, johon rahoja voi lahjoittaa (Kemppi 2022.)

4.5 Suomen Nato-jäsenyysprosessi

Kybertuvallisuuskeskus varoitti, että Nato-jäsenhakemuksen seurauksena, Suomeen voi kohdistua erilaista kybervaikuttamista ja informaatiovaikuttamista verkossa. Vaikuttaminen voisi olla Kyberturvallisuuskeskuksen mukaan esimerkiksi palvelunestohyökkäyksiä. Palvelunestohyökkäyksillä voidaan saavuttaa helposti näkyvyyttä, mutta niiden vaikutukset jäävät usein suppeiksi ja lyhytaikaisiksi. (Traficom 2022c.)

Suojelupoliisi (2022b) arvioi, että Suomen Nato-jäsenyysprosessin myötä, Suomi on entistä kiinnostavampi kohde tiedustelun ja vaikuttamisen näkökulmasta. Suojelupoliisin mukaan suurimmat tiedustelun ja vaikuttamisen uhkat muodostavatkin Venäjä ja Kiina.

Venäjä yrittää saavuttaa Natoon liittyvää tietoa Suomen kautta. Todennäköistä on myös, että Venäjän harjoittama yritysvakoilu suomalaisia yrityksiä kohtaan on kasvussa, sillä maalla on tarve käynnistää korvaavaa huipputeknologian teollisuutta. Tarve on suuri, sillä EU:n Venäjää kohtaan asetetut vienti- ja tuonti rajoitteet vaikeuttavat maata saamaan haltuunsa heille tärkeitä tuotteita ja komponentteja. (Suojelupoliisi 2022b.)

4.6 Kyberhyökkäykset

Palvelunestohyökkäyksiä, kuten muitakin verkon välityksellä tehtäviä hyökkäyksiä kutsutaan kyberhyökkäyksiksi. Suomea kohtaan tehdään kymmeniätuhansia palvelunestohyökkäyksiä joka vuosi, mutta harvasta niistä on suurempia vaikutuksia, koska Suomen valtio on varautunut niitä kohtaan todella hyvin. (Mtv uutiset 2022.) Kuitenkin ajoittain onnistutaan toteutettaman laajamittaisia palvelunestohyökkäyksiä, joista on vaikutuksia Suomen kyberturvallisuuden tilaan. Näistä hyökkäyksistä usein uutisoidaan myös

mediassa. Hyökkäyksiä kohdistuu Suomea kohtaan myös Venäjältä, ja kohteena ovat olleet Suomen valtion organisaatiot.

4.6.1 Kohteena ministeriöt ja valtioneuvosto

Ministeriöiden ja valtioneuvoston verkkosivuille kohdistettiin palvelunestohyökkäys huhtikuussa 2022. Hyökkäys sulki ainakin hetkellisesti puolustusministeriön ylläpitämiä sivustoja. Hyökkäys vaikutti myös ulkoministeriön sivuille. (Kaleva 2022.)

Hyökkäyksen tekijää ei ole vielä pystytty jäljittämään ja voi olla, että se jääkin selvittämättä. Kuitenkin ulkoministeri Pekka Haavisto arvioi, että samana päivänä tehty venäläisen lentokoneen ilmatilaloukkaus, Ukrainan presidentti Volodymyr Zelenskyin pitämä puhe Suomen eduskunnalle sekä palvelunestohyökkäys olivat yhteydessä toisiinsa. (Kaleva 2022.)

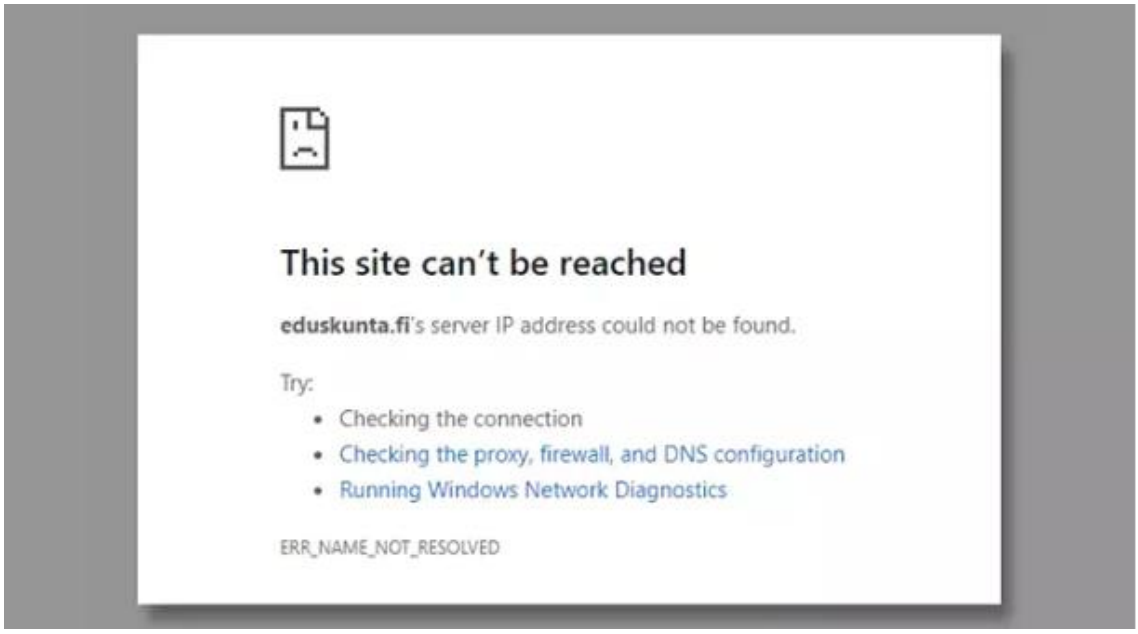
Kyberhyökkäyksen tekijän tunnistaminen on aina haastavaa. Hyökkääjä tai tunkeutuja pyrkii yleisesti peittämään jälkensä esimerkiksi ohjaamalla hyökkäyksensä useiden kaupallisten palvelimien kautta, johdattamalla tahallisesti harhaan tai käyttämällä ulkopuolisia toimijoita hyökkäyksiään varten. (Sisäministeriö 2022c.)

4.6.2 Kohteena Suomen eduskunta

Eduskunnan sivuilla toteutettiin palvelunestohyökkäys elokuussa 2022. Kyberhyökkäyksen toteutti venäläinen hakkeriryhmä nimeltään NoName057(16). Ryhmä kertoi asiasta omalla Telegram viestintäsovellus kanavallaan. Motiivikseen ryhmä kertoi Suomen Nato liittymisaikeet. Ryhmä on myös sanonut hyökänneensä useita muita valtioiden instituutteja kohtaan. Kohteita ovat olleet ryhmän mukaan ainakin Puola, Liettua ja Norja. (Bogdanov & Tolkki 2022a.)

Helsingin sanomien (2022) mukaan ryhmän motiivi oli geopoliittinen ja tavoite oli luoda pelkoa ja epävarmuutta Suomen Nato-jäsenyyteen liittyen. Samana päivänä Yhdysvaltain presidentti Joe Biden allekirjoitti Suomen ja Ruotsin Natoa koskevat liittymisasiakirjat Yhdysvalloissa, joka on voinut myös toimia lisä motiivina hyökkäykselle.

NoName057(16) -hakkeriryhmä on erikoistunut nimenomaan palvelunestohyökkäyksiin ja he ovatkin avoimesti kertoneet olevansa länsimaiden Venäjää kohdistettuja toimia vastaan taisteleva ryhmä. Tätä voidaan kutsua haktivismiksi. (Helsingin sanomat 2022.)



Kuva 3. Tältä www.eduskunta.fi näytti hyökkäyksen aikana (Helsingin Sanomat 2022).

Hyökkäyksen takia eduskunnan verkkosivut toimivat normaalia hitaammin. Sivut olivat jopa hetken aikaa kokonaan pois käytöstä, tämä on esitetty kuvassa 3. Tietovuotoja hyökkäyksessä ei kuitenkaan tapahtunut. Palvelunestohyökkäys kesti noin kahdeksan tuntia, joka on pitkä aika palvelunestohyökkäykseksi. (Bogdanov & Tolkki 2022a.) Sillä Traficom (2022d) mukaan noin 79 % Suomessa tapahtuvista palvelunestohyökkäyksistä kestää alle 15 minuuttia.

4.6.3 Kohteena Valtioneuvoston julkaisuarkisto

Venäläinen hakkeriryhmä NoName057(16) ilmoitti toteuttaneensa jo toisen palvelunestohyökkäyksensä Suomen valtiota kohtaan. Hyökkäys tapahtui elokuussa 2022. Hakkeriryhmä on sama, joka päivää aikaisemmin kohdisti palvelunestohyökkäyksen eduskunnan sivuja kohtaan. (Bogdanov & Tolkki 2022b.)

Hyökkäys kohdennettiin kansalliskirjaston ylläpitämään julkaisuarkisto Valtoon. Hyökkäys kohdistettiin todennäköisesti Valtoon, koska valtioneuvoston varsinaisilla verkkosivuilla on tehokkaat suojaukset. Valton sivustojen suojaus on jäänyt heikommalle tasolle ja täten sivuston ruuhkauttamisella saatiin helpommin näkyvyyttä. Hyökkäyksen vuoksi julkaisuarkiston sivut eivät kaatuneet hyökkäyksestä, mutta ruuhkautuivat ja hidastuivat merkittävästi. (Bogdanov & Tolkki 2022b.)

Seuraavaksi kohteeksi hakkeriryhmä on vihjaillut Telegram-kanavallaan Kyberturvallisuuskeskusta (Bogdanov & Tolkki 2022b). Julkisuuteen ei ole tullut tietoa Kyberturvallisuuskeskukseen kohdennetusta onnistuneesta hyökkäyksestä.

4.7 Valmiuslaki

Hallitus esitti eduskunnalle 28.6.2022 valmiuslain (1552/2011) muuttamisesta. Valmiuslain tarkoitus on sota-aikana tai poikkeusoloissa turvata Suomen väestön toimeentulo ja maan talouselämä, ylläpitää oikeusjärjestystä, perusoikeuksia ja ihmisoikeuksia sekä turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys. Nykyinen valmiuslaki on tullut voimaan vuonna 2012 ja sitä on jouduttu soveltamaan ainoastaan koronapandemian vuoksi. (Eduskunta 2022.)

Valmiuslain (1552/2011) kokonaisuudistus oli käynnistymässä oikeusministeriön toimesta jo ennen Venäjän hyökkäystä Ukrainaan. Uudistuksen kestoksi oli arvioitu noin kolme vuotta. Venäjän hyökkäys Ukrainaa kohtaa muutti tilannetta

siten, että lainuudistamiseen oli tarvetta paljon nopeammalla aikataululla. Tästä syystä valmisteluun otettiin mukaan uusi hybridipykälä, jonka avulla on tarkoitus varmistaa, että valmiuslain nykyisiin poikkeusoloihin ei jää sellaisia aukkoja, joita Suomea kohtaan vihamielinen toimija pystyisi käyttämään hyväkseen. (Eduskunta 2022)

Oikeusministeriö (2022) tiedotti verkkosivuillaan, että valmiuslain (1552/2011) poikkeusolomääritelmää on täydennetty 15.7.2022. Lakimuutoksen perustana on laajasti tunnistettavissa oleva tarve kyetä vastaamaan erilaisiin hybridiuhkiin, kuten rajaturvallisuuden vaarantumiseen tai tietoliikenteen ja tietojärjestelmien toimivuuden vakavaan vaarantamiseen. Valmiuslain uudistus sallii toimivaltuuksien käytön erityyppisissä vakavissa hybridivaikuttamistilanteissa.

Hybridivaikuttamisessa tavoite on käyttää hyväkseen kohteeksi valitun valtion haavoittuvuuksia ja tehdä se mahdollisimman peitellysti (Sisäministeriö 2022a).

Valmiuslakia (1552/2011) on muutettu siten, että sen kolmannen pykälän ensimmäiseen momenttiin on lisätty kohta kuusi eli niin sanottu hybridipykälä;

> Poikkeusoloja tämän lain mukaan ovat sellainen
>
> a) julkisen vallan päätöksentekokykyyn;
>
> b) rajaturvallisuuden tai yleisen järjestyksen ja turvallisuuden ylläpitämiseen;
>
> c) välttämättömien sosiaali- ja terveydenhuollon tai pelastustoimen palvelujen saatavuuteen;
>
> d) energian, veden, elintarvikkeiden, lääkkeiden tai muiden välttämättömien hyödykkeiden saatavuuteen;
>
> e) välttämättömien maksu- ja arvopaperipalvelujen saatavuuteen;
>
> f) yhteiskunnallisesti kriittisten liikennejärjestelmien toimivuuteen; tai
>
> g) edellä a–f alakohdassa lueteltuja toimintoja ylläpitävien tieto- ja viestintäteknisten palvelujen tai tietojärjestelmien toimivuuteen
>
> kohdistuva uhka, toiminta, tapahtuma tai näiden yhteisvaikutus, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti ja laajamittaisesti estyvät tai lamaantuvat tai joka muulla näihin vakavuudeltaan rinnastuvalla tavalla erityisen vakavasti ja olennaisesti vaarantaa yhteiskunnan toimintakykyä tai väestön elinmahdollisuuksia.

Valmiuslain tarkoitus on poikkeusoloissa suojata väestöä ja turvata heidän toimeentulonsa sekä talouselämä. Ylläpitää oikeusjärjestystä, perusoikeuksia ja ihmisoikeuksia. Lain tarkoitus on myös turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys. Valmiuslaki voidaan ottaa käyttöön poikkeusolojen aikana. (Valmiuslaki 2011/1552)

5 Tutkimusmenetelmät ja tiedonkeruu

Opinnäytetyön tutkimusmenetelmäksi valikoitui empiirinen eli kokemusperäinen tutkimus. Kyseisessä tutkimusmenetelmässä tutkimustulokset saavutetaan tekemällä konkreettisia havaintoja tutkimuskohteesta ja analysoimalla sekä mittaamalla sitä. Tutkimusmenetelmässä konkreettinen ja koottu tutkimusaineisto on tutkimuksen keskiössä ja tämä toimii tutkimuksen lähtökohtana. (Koppa 2022a.) Tässä opinnäytetyössä mitattiin ja havainnointiin Suomen kyberturvallisuuden tilaa. Työssä tutkittiin myös ilmiöiden välistä yhteyttä tutkimustulokseen, joka lajitellaan empiirisen tutkimuksen piiriin (Koppa 2022b).

Menetelmä valikoitui koska tutkimuksen tarkoituksena oli saada mahdollisimman laaja jakauma helposti analysoitavaa tietoa, josta voidaan tehdä yleispäteviä tulkintoja. Empiirinen osuus koostui hyvin samantapaisista lähteistä kuin teoreettinen osuus.

Tutkimuksessa havainnointiin pääasiassa aiheesta julkaistuja uutisia ja artikkeleita mutta myös Suomen lakia sekä Suomen viranomaisten julkaisemia lausuntoja, artikkeleita, ohjeistuksia ja raportteja. Opinnäytetyötä varten on myös analysoitu Traficomin (2022a) alaisuudessa toimivan kyberturvallisuuskeskuksen julkaisemia kybersää raportteja. Nämä ovat joka kuukausi julkaistavia raportteja kuluneen kuukauden merkittävimmistä tietoturvapoikkeamista ja ilmiöistä. Näitä lähteitä käyttämällä voidaan todeta, että tutkimuksen reliabiliteetti toteutui varsin hyvin.

Suurimpia hankaluuksia työssä aiheutti kunnollisten lähteiden löytäminen ja niiden laajuus. Tutkimustyössä kävin vuoden ajalta kyberturvallisuuskeskuksen raportteja Suomen kyberturvallisuuden tilasta. Niissä oli vain siellä täällä mainintoja Venäjään ja sotaan liittyvistä hyökkäyksistä, uhkista ja toimista Suomen kyberturvallisuutta kohtaan. Myös aiheen arkaluontoisuus vaikeuttaa opinnäytetyön tekoa, sillä mahdolliset Suomeen kohdistuvat kyberhyökkäykset eivät ole automaattisesti julkista tietoa ja näistä ei välttämättä julkaista yleiseen tietoon mitään.

Opinnäytetyötä kirjoittaessani opin, kuinka tärkeää on lähdekriittisyys. Aiheita ja tapahtumia opinnäytetyön teemasta löytyi, mutta lähteet, niiden julkaisijat sekä kirjoittajat voivat olla Venäjä myönteisiä tai vastaisia. Lähteinä onkin hyvä käyttää tieteellisiä julkaisuja sekä poliittisesti neutraaleja julkaisualustoja. Tällä välttää mahdollisen harhaanjohtavan disinformaation ja tiedon oikeellisuudesta voi olla entistä varmempi. On myös tärkeää merkata aina kaikki mahdolliset sivustot ja muut lähteet ylös. Useasti opinnäytetyötä korjatessani jouduin tekemään ylimääräistä työtä, kun jokin lähde oli unohtunut merkata. Näin laajan tutkimuksen tekeminen oli kokonaisuudessaan uusi prosessi, ja sen edetessä opin koko ajan uutta. On tärkeää osata hahmotella tutkimus oikeaan muotoon ja rakentaa tutkimuksen rakenne johdonmukaisesti.

Ammatillinen osaaminen kehittyi myös laajasti tutkimustyötä tehdessä. Pystyn nyt ymmärtämään ja tiedostamaan erityyppisiä kyberturvallisuusuhkia. Kykenen antamaan neuvoja ja ehdotuksia organisaatioiden tai yksityisten ihmisten tietoturvallisuus käytäntöihin ja etsimään helposti tietoa muun muassa ajankohtaisista kyberuhkista, hyökkäyksistä ja haittaohjelmista. Kyseistä tietoa on tärkeä jakaa avoimesti organisaation sisällä ja kertoa myös mahdollisista vaikutuksista avoimesti. Ymmärrys kyberturvallisuuden eri toimintatavoista, termeistä ja laajamittaisuudesta karttuivat myös laajasti.

6 Tutkimustulosten analysointi ja yhteenveto

Opinnäytetyön päätavoitteena oli tutkia miten Venäjän hyökkäys Ukrainaan on vaikuttanut Suomen kyberturvallisuuden tilaan. Tutkimuksessa oli tarkoitus selvittää, pystytäänkö löytämään mitään Suomen kyberturvallisuus tilanteeseen vaikuttavaa tekijää, joka johtuisi suoranaisesti Ukrainassa käytävästä sodasta. Opinnäytetyön tavoitteena oli myös selvittää onko Venäjältä kohdistunut suoraa kybervaikuttamista Suomea kohtaan ja onko Suomessa reagoitu mitenkään mahdollisiin tulevaisuuden kyberuhkiin.

Tutkimuksen validiteetti toteutui hyvin, sillä tutkimuksesta voidaan todeta, että Suomen kyberturvallisuuden tila on muuttunut sen jälkeen, kun Venäjä on hyökännyt Ukrainaan. Tutkimuksen tuloksena sain selvitettyä, että Venäjän hyökkäyssodalla Ukrainaa kohtaan on todella ollut myös vaikutusta Suomen kyberturvallisuus tilaan. Kyberturvallisuustilanne on muuttunut Suomen valtion, yritysten sekä kansalaisten näkökulmasta. Suomalaisia organisaatioita on joutunut kyberhyökkäysten kohteiksi ja yksittäiset ihmiset ovat kärsineet enemmän kyberhuijauksista. Suomalaisiin organisaatioihin kohdistuneet kyberhyökkäyksien määrät ovat nousseet, varsinkin haittaohjelmien, tietojenkalastelun ja palvelunestohyökkäysten lukumäärät ovat kasvaneet (Traficom 2022f).

6.1. Toimitusketjujen häiriintyminen

Toimitusketjujen häiriintyminen heijastuu Suomen kyberturvallisuuden tilanteeseen. Autoliiton (2022) julkaisemassa artikkelissa kerrotaan häiriöistä toimitusketjuissa, jotka alkoivat olla havaittavissa jo vuonna 2020, kun elektronistenlaitteiden suuri kysyntä aiheutti maailmanlaajuisen sirupulan. Tämän takia uusia elektronisia laitteita ei voitu toimittaa asiakkaille ajoissa. Tämä vaikuttaa edelleen suomalaisiin organisaatioihin ja yrityksiin, siten että laitteiden elinkaarta joudutaan pitkittämään liian pitkäksi ja uusien

suojaratkaisuiden rakentamisessa tulee kestämään tarkoitettua pidempään. (Traficom 2022e.)

Lisäksi kyberrikolliset ovat nähneet laitteiden saatavuushäiriöissä ja hintojen nousussa tilaisuuden huijata ihmisiä. Traficom (2022e) varoittaakin huijareista, jotka kaupittelevat halpoja kopioita laitteista. Harkintakykyä on käytettävä entistä enemmän ostaessaan uusia laitteita.

6.2. Sodan heijastus Suomen kyberturvallisuuteen

Venäjän hyökättyä Ukrainaan, Euroopan Unioni on asettanut Venäjää kohtaan pakotteita, vienti- ja tuontirajoitteita. Näiden asioiden takia Eurooppa voi mahdollisesti ajautua energiakriisiin. Hanhinen (2022) kirjoitti artikkelissaan Venäjän lopettaneen sähkönsiirtämisen Suomeen toukokuussa 2022, sähkön tuonnin osuus Venäjältä Suomeen oli noin kymmenen prosenttia. Ainakaan toistaiseksi Suomen energiayhtiöt ei ole vielä joutuneet säännöstelemään sähkön käyttöä, mutta talvi kuukausina se voi olla mahdollista. Tutkimuksessa käy ilmi että, tästä voi olla myös vaikutuksia Suomen kyberturvallisuudentilaan sekä ICT-palveluiden toimivuuteen, sillä nämä vaativat toimiakseen jatkuvasti sähköä.

Viranomaiset ovat myös varoittaneet, että Nato-jäsenyyden hakeminen saattaa vaikuttaa Suomen kyberturvallisuustilanteeseen. Suojelupoliisin (2022b) mukaan Suomen Nato-prosessi tekee Suomesta kiinnostavamman vakoilun ja informaatiovaikuttamisen kohteena. Suurimpana uhkana suojelupoliisi pitää Kiinaa ja Venäjää.

Venäjä yrittää saavuttaa Natoon liittyvää tietoa vakoilemalla Suomea. Venäjä yrittää todennäköisesti myös vakoilla suomalaisia yrityksiä sillä maalla on suuri tarve alkaa tuottamaan itse palveluja ja teknologiaa rajoitteiden takia. (Suojelupoliisi 2022b.)

Tutkimuksessa ilmeni myös, että kyberrikolliset käyttävät Ukrainan kriisiä avukseen huijatakseen ihmisiä lahjoittamaan rahaa kriisialueelle vaikka,

todellisuudessa nämä rahat menevät suoraan kyberrikollisille. Tekaistuja rahankeräyksiä on nähty levitettävän ainakin sähköpostien ja sosiaalisenmedian välityksellä. (Kemppi 2022.)

Tutkimustuloksista voidaan todeta että, Venäjän hyökkäys Ukrainaa kohtaan ja siitä seuranneet jatkumot esimerkiksi Suomen Nato-jäsenyyden hakeminen ovat aiheuttaneet kyberhyökkäyksiä Suomea kohtaan Venäjän toimesta. Suomen valtion eri organisaatiot ovat joutuneet palvelunestohyökkäysten kohteeksi. Tekijöiksi on ilmoittautunut venäläiset hakkeriryhmät ja syyksi he ovat sanoneet Suomen nykyisen Nato-myönteisyyden. Palvelunestohyökkäysten kohteeksi ovat joutuneet eri ministeriöiden, eduskunnan sekä valtioneuvoston verkkosivuja.

Suomen kyberturvallisuuden kannalta on myös tapahtunut verrattain suuria muutoksia, kun Suomen valmiuslakia uudistettiin. Suomen nykyistä valmiuslakia on jouduttu uudistamaan vain kerran entuudestaan, joten tapahtuma on sinänsä merkittävä. Valmiuslakiin lisättiin uusi pykälä, jota eduskunta nimitti hybridipykäläksi. Tämän pykälän tarkoitus on suojata Suomea mahdollisilta hybridiuhkilta (Valmiuslaki 2011/1552).

Lähteet

Autoliitto 2022. Sirupula jatkuu ensi vuoteen – taustalla muun muassa Ukrainan sota. Moottori. Viitattu 11.10.2022 https://moottori.fi/ajoneuvot/jutut/sirupula-jatkuu-ensi-vuoteen-taustalla-muun-muassa-ukrainan-sota/

Bogdanov, J. & Tolkki, K., 2022a. Venäläinen hakkeriryhmä ilmoittautui eduskunnan sivujen kaatajaksi – Mikko Hyppönen: ei ole mitään syytä epäillä ilmoitusta. Yle. Viitattu 7.10.2022 https://yle.fi/uutiset/3-12569629

Bogdanov, J. & Tolkki, K., 2022a. Venäläinen hakkeriryhmä väittää tehneensä jo toisen palvelunestohyökkäyksen – kohteena valtioneuvoston julkaisuarkisto. Yle. Viitattu 7.10.2022 https://yle.fi/uutiset/3-12571164

Eduskunta 2022. Täysistunnon pöytäkirja PTK 81/2022 vp. Viitattu 13.10.2022 https://www.eduskunta.fi/FI/vaski/PoytakirjaAsiakohta/Sivut/PTK_81+2022+7.aspx

Elinkeinoelämän keskusliitto 2022. Venäjä - pakotteet: Päivitetyt QA-vastaukset yritysten kysymyksiin. Viitattu 18.10.2022 https://ek.fi/ajankohtaista/uutiset/venaja-pakotteet-qa-vastaukset-yritysten-kysymyksiin/#_Toc100850930

Eskonen, H., 2022. Suomi pyytää pian kansalaisia vähentämään energian kulutusta: "Suihkussa enintään viisi minuuttia" – viimeksi vastaava kampanja oli 70-luvulla. Yle. Viitattu 18.10.2022 https://yle.fi/uutiset/3-12553330

Eurooppa-neuvosto 2022a. EU:n vastaus Venäjän hyökkäykseen Ukrainaan. Viitattu 18.10.2022 https://www.consilium.europa.eu/fi/policies/eu-response-ukraine-invasion/#how

Eurooppa-neuvosto 2022b. EU:n Venäjä vastaiset pakotteet. Viitattu 18.10.2022 https://www.consilium.europa.eu/fi/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/#sanctions

Haapavuori, K., 2022. Mitä on kybersota?. Micro magic. Viitattu 30.11.2022 https://micromagic.fi/story/mita-on-kybersota/

Hanhinen, H., 2022. Venäjä keskeytti sähkön tuonnin Suomeen lauantaina – ei ole ollut suurta vaikutusta, kertoo Fingrid. Yle. Viitattu 2.11.2022 https://yle.fi/uutiset/3-12447025

Helsingin Sanomat 2022. Palvelunestohyökkäys kaatoi eduskunnan verkkosivut, venäläinen hakkeri-ryhmä kertoo tehneensä hyökkäyksen. Viitattu 10.10.2022 https://www.hs.fi/politiikka/art-2000008994152.html

Horelli, M., 2020. Erillisverkot, Kyberturvallisuudesta tuli loputon kilpajuoksu. Viitattu 28.9.2022 https://www.erillisverkot.fi/kyberturvallisuudesta-tuli-loputon-kilpajuoksu/

Insta 2020, Miksi riskinottajat voittavat (ja miksi kyberriski on otettavissa). Viitattu 28.10.2022 https://www.insta.fi/nakemyksia/tietoturvapalvelut/kyberriski-ja-riskin-ottaminen

Järvinen, P., 2022. Helsingin seudun kauppakamari 2022, Yrityksen tietoturvaopas. Viitattu 28.9.2022 https://kauppakamaritieto-fi.ezproxy.turkuamk.fi/ammattikirjasto/teos/yrityksen-tietoturvaopas-2022#kohta:2.((20)Kyberturvallisuus)

Kaleva 2022. Valtioneuvoston ja ministeriöiden nettisivuille kohdistettu palvelunestohyökkäys tältä erää ohi. Viitattu 12.10.2022 https://www.kaleva.fi/valtioneuvoston-ja-ministerioiden-nettisivuille-ko/4505302

Kaspersky 2022. What is Cyber Security? Viitattu 27.9.2022 https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kemppi, J., 2022. Huijarit jahtaavat suomalaisten Ukraina-lahjoituksia – luotettavalta vaikuttava avustuspyyntö voikin tulla rikollisilta. Iltalehti. Viitattu 12.10.2022 https://www.iltalehti.fi/tietoturva/a/9c306595-f1bf-4ecb-9d2d-b697271978f7

Koppa 2022a. Empiirinen tutkimus. Jyväskylän yliopisto. Viitattu 27.12.2022 https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus

Koppa 2022b. Ilmiöiden välisten yhteyksien kuvaaminen. Jyväskylän yliopisto. Viitattu 27.12.2022 https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/ongelmanasettelu/ilmioiden-valisten-yhteyksien-kuvaaminen

Kyberuhat ja niiden aiheuttajat 2022. Johdatus kyberturvallisuuteen -verkkokurssi. Vastuuopettaja: Juho Kotakallio. Jyväskylän yliopisto. Peda.net. Viitattu 29.9.2022 https://peda.net/id/92d2c36a5ee

Limnéll, J.; Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Lukkari, M., 2016. Turvallisuusjohtaja toppuuttelee Venäjä-pelkoja – "Ei pelätä tarvitse, mutta seurata kyllä". Yle. Viitattu 21.11.2022 https://yle.fi/uutiset/3-9137693

Lutkevich, B., 2021. What is hacktivism?. TechTarget. Viitattu 30.9.2022 https://www.techtarget.com/searchsecurity/definition/hacktivism

Mtv uutiset 2022. EU julisti Venäjän terrorismia tukevaksi valtioksi – näin se vaikuttaa Suomen kyberturvallisuuteen. Viitattu 30.11.2022 https://www.mtvuutiset.fi/artikkeli/eu-julisti-venajan-terrorismia-tukevaksi-valtioksi-nain-se-vaikuttaa-suomen-kyberturvallisuuteen/8579216#gs.jiohnw

National Institute of Standards and Technology 2022. vulnerability. Viitattu 28.9.2022 https://csrc.nist.gov/glossary/term/vulnerability

Oikeusministeriö 2022. Valmiuslain hybridiuhkia koskeva päivitys vahvistettiin. Viitattu 7.10.2022 https://oikeusministeo.fi/-/valmiuslain-hybridiuhkia-koskeva-paivitys-vahvistettiin

Puolustusministeriö 2019. Näin varaudut pitkiin sähkökatkoihin. Viitattu 21.10.2022 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161847/N%c3%a4in_varaudut_pitkiin_s%c3%a4hk%c3%b6katkoihin.pdf?sequence=1&isAllowed=y

Rand corporation 2022. Cyber Warfare. Viitattu 30.11.2022 https://www.rand.org/topics/cyber-warfare.html

Räty, P., 2022. Tällaista on kybersota – vakavia seurauksia myös fyysisessä maailmassa. Tekniikka & Talous. Viitattu 30.9.2022 https://www-tekniikkatalous-fi.ezproxy.turkuamk.fi/uutiset/tallaista-on-kybersota-vakavia-seurauksia-myos-fyysisessa-maailmassa/d575764a-fe62-4f11-a621-5843a868ddb7

Sisäministeriö 2022a. Hybridiuhat ja hybridivaikuttaminen. Viitattu 7.10.2022 https://intermin.fi/kansallinen-turvallisuus/hybridiuhat

Sisäministeriö 2022b. Kyberrikollisuus ylittää rajat tietoverkoissa. Viitattu 29.9.2022 https://intermin.fi/poliisiasiat/kyberrikollisuus

Sisäministeriö 2022c. Kyberturvallisuus osana kansallista turvallisuutta. Viitattu 12.10.2022 https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

STEK 2022. Sähkötekniikan ja energiatehokkuuden edistämiskeskus, Perustietoa sähköstä. Viitattu 28.9.2022 https://stek.fi/perustietoa-sahkosta/termit/'

Suojelupoliisi 2022a. Kansallisen turvallisuuden katsaus 2022. Viitattu 26.10.2022 https://supo.fi/kansallisen-turvallisuuden-katsaus

Suojelupoliisi 2022b. Tiedustelu ja vaikuttaminen. Viitattu 17.10.2022 https://supo.fi/tiedustelu-ja-vaikuttaminen

Traficom 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 28.9.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Traficom 2022a. Kybersää, elokuu 15.9.2022. Viitattu 11.10.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20elokuu%202022.pdf

Traficom 2022b. Kybersää, helmikuu 17.3.2022. Viitattu 11.10.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20helmikuu%202022.pdf

Traficom 2022c. Kybersää, huhtikuu 12.5.2022 Viitattu 6.10.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20huhtikuu%202022.pdf

Traficom 2022d Kybersää, kesäkuu 3.8.2022. Viitattu 7.10.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20kes%C3%A4kuu%202022.pdf

Traficom 2022e. Kybersää, maaliskuu 14.4.2022. Viitattu 6.10.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20maaliskuu%202022_0.pdf

Traficom 2022f. Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt 12.09.2022. Viitattu 17.10.2022 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

Valmiuslaki 2011/1552. Annettu Naantalissa ja Helsingissä 8.7.2022. Saatavilla https://www.finlex.fi/fi/laki/alkup/2022/20220706#Pidm45949345105120