VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Teemu Joensuu

UKRAINAN SODAN VAIKUTUKSET ORGANISAATIOIDEN KYBERTURVALLISUU-TEEN SUOMESSA

Tekniikka
2023

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Teemu Joensuu
Opinnäytetyön nimi	Ukrainan sodan vaikutukset organisaatioiden kyberturvallisuuteen Suomessa
Vuosi	2023
Kieli	suomi
Sivumäärä	33
Ohjaaja	Harri Lehtinen

Opinnäytetyön tarkoituksena oli selvittää, miten Ukrainan sota on vaikuttanut organisaatioiden kyberturvallisuuteen Suomessa. Opinnäytetyön tavoitteena oli tuottaa tietoa siitä, minkälaisia uhkia sota Ukrainassa on tuonut ilmi kyberturvallisuuden näkökulmasta yrityksille ja erilaisille organisaatioille.

Kirjallisuuskatsauksen tavoin tässä opinnäytetyössä hyödynnetään artikkeleista, verkkojulkaisuista, raporteista ja uutisista löydettyä tietoa. Opinnäytetyön tarkoituksena oli selvittää, minkälaisia uhkia sotatilanne oli lisännyt kyberturvallisuudelle ja mitä mahdollisia kyberturvallisuusriskejä organisaatiot saattavat kohdata kyseisen maailmantilanteen seurauksena.

Voidaan todeta, että kiristynyt maailmantilanne on lisännyt kyberturvallisuusriskejä ja Venäjän Suomeen kohdistamaa kybertoimintaa on havaittu aiempaa enemmän. Hyökkäysten kohteena ovat mm. suomalaiset yritykset, huoltovarmuuskriittiset toimijat ja valtionhallinto. Kiristyshaittaohjelmat ja palvelunestohyökkäykset ovat lisääntyneet ja ne ovat entistä kohdennetumpia.

Avainsanat kyberturvallisuus, tietoturva, organisaatio, Ukrainan sota

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Teemu Joensuu
Title	The Impact of the Ukraine War on Organizations Cybersecurity in Finland
Year	2023
Language	Finnish
Pages	33
Name of Supervisor	Harri Lehtinen

The purpose of the thesis was to find out how the war in Ukraine has affected the cyber security of organizations in Finland. The aim of the thesis was to provide information on the threats that the war in Ukraine has brought to companies and organizations from a cyber security perspective.

Like the literature review, this thesis uses information found in articles, online publications, reports, and news. The aim of the thesis was to find out what kind of threats the war situation had added to cybersecurity and what cybersecurity risks organizations might face as a result, of this world situation.

In conclusions it could be stated that the tightened world situation has increased cyber security risks, and more cyber activity directed at Finland by Russia has been observed than before. The targets of the attacks are e.g., Finnish companies, operators critical to security of supply and the state administration. Ransomware and denial-of-service attacks have increased and are more targeted.

Keywords cyber security, information security, organizations, Ukrainian war

SISÄLLYS

KUVALUETTELO

1 JOHDANTO

Venäjän aloittamat sotatoimet Ukrainassa alkoivat helmikuussa 2022, sotatilanne jatkuu edelleen, eikä loppua vielä näy. Kansainvälinen tilanne on muuttunut paljon viime vuosien aikana. 24.2.2022 Venäjä hyökkäsi Ukrainaan ja 18.5.2022 Suomi jätti yhdessä Ruotsin kanssa liittymishakemuksen Natoon. Nämä tapahtumat ovat osaltaan lisänneet merkittävästi kyberuhkaa sekä todennettuja kyberhyökkäyksiä Euroopassa. Ukrainan ja Venäjän välisellä sodalla on merkittäviä vaikutuksia suorasti ja epäsuorasti myös heitä ympäröiviin naapurimaihin, Euroopan maihin sekä Euroopan ulkopuoliseen maailmaan. Sodan vaikutukset näkyvät jokapäiväisessä elämässämme muun muassa, inflaation ja energia kriisin kautta. (Koistinen & Salonen, 2022)

Sota on vaikuttanut myös tietotekniikan alaan eri tavoin, suorasti ja epäsuorasti. Kiristynyt kyberturvallisuustilanne vaikuttaa myös Suomessa toimiviin yrityksiin ja yhteisöihin. Ukraina on yksi Itä-Euroopan kehittyneimpiä tietotekniikkamaita (Raeste 2022). Tämän takia monessa suomalaisessa IT-yrityksessä on ukrainalaisia asiantuntijatehtävissä. Esimerkiksi ohjelmistoyhtiö Tieto-Evryllä on Ukrainassa hieman yli 2000 tietotekniikka-ammattilaista palveluksessaan (Raeste 2022). Tietotekniikka on kansainvälinen ala ja täten sota on vahvasti vaikuttanut henkilöstö- ja kansainvälisiin suhteisiin organisaatiossa sisäisesti ja ulkoisesti. Yrityksillä ja organisaatioilla on myös alihankittuja ohjelmistoja ja ulkoistettuja osaamiskeskuksia Ukrainassa. (Hyppönen, 2022)

Miten Ukrainan sota vaikuttaa organisaatioiden kyberturvallisuuteen Suomessa? Tässä opinnäytetyössä pyrin avaamaan kyberturvallisuuden keskeisimmät käsitteet ja aihealueet ja esittelemään keskeisimpiä vaikutuksia siitä, miten Ukrainan sotatilanne on vaikuttanut ja vaikuttaa kyberympäristöön. Tulen esittelemään kybersodan tapahtumia. Niiden pohjalta pyrin pohtimaan kuinka ne voivat vaikuttaa organisaatioiden kyberturvallisuuteen nyt ja lähitulevaisuudessa.

Tämä opinnäytetyö on koostettu kirjallisuuskatsauksen keinoin hyödyntämällä monipuolisia lähteitä muun muassa, kirjallisuutta, artikkeleita ja uutisia. Tämä opinnäytetyö tarjoaa ajankohtaista tietoa ja kokoaa keskeisimmät perusasiat siitä, mitä organisaatioiden tulisi tietää kybersodasta ja sen mahdollisista seurauksista kyberturvallisuudelle. Vaikka Ukrainan ja Venäjän välinen sota on hyvin aika sensitiivinen teema, on se opettanut ja näyttänyt meille kyberturvallisuuden ja kybersodankäynnin tulevaisuuden. Tiedon ja erilaisen datan kerääminen tältä ajalta on todella keskeistä ja voi tukea huomisen kyberturvallisuuden kehityksessä.

2 OPINNÄYTETYÖPROSESSI

Ukrainan sota on vaikuttanut laajasti kansainväliseen turvallisuusympäristöön ja kyberturvallisuuteen. Sota on aiheuttanut huolta kyberturvallisuuden haavoittuvuudesta ja merkityksestä organisaatioille. Ukrainan sodan aikana on raportoitu useista kyberhyökkäyksistä, jotka ovat suunnattu Ukrainan sotilaalliseen ja taloudelliseen infrastruktuuriin, mutta joita on myös kohdistettu organisaatioihin muilla alueilla, mukaan lukien Suomessa.

2.1 Tutkimuskysymys

Opinnäytetyöni tavoite on vastata kysymykseen: Miten Ukrainan sota vaikuttaa organisaatioiden kyberturvallisuuteen Suomessa.

Lähestyin tutkimusongelmaa seuraavien kysymysten avulla:

Minkälaisia kyberhyökkäyksiä Ukrainaan on kohdistunut?

Mitkä organisaatiot ovat erityisen alttiissa asemassa ja miksi?

2.2 Tavoite ja tutkimusmenetelmä

Tutkimuskysymykseen pyrin vastaamaan analysoimalla ja kokoamalla tietoa jo tapahtuneista kyberhyökkäyksistä ja tapahtumista kirjallisuuskatsauksen keinoin. Lähdekriittisyys on aiheessani erityisen tärkeää, koska näkökulmia sotaan on useita. Kerätyn tiedon pohjalta pyrin tunnistamaan, millaisia riskejä ja haasteita organisaatiot voivat kohdata tulevaisuudessa. Analysoimalla jo tapahtuneita hyökkäyksiä ja tapahtumia voidaan kehittää parempia strategioita ja toimenpiteitä suomalaisen organisaatioiden kyberturvallisuuden vahvistamiseksi.

Organisaatiot voivat myös oppia hyökkäysten yleisistä kaavoista ja tunnistaa kyberhyökkäyksissä käytettyjä taktiikoita ja menetelmiä, jolloin niiden on helpompi havaita mahdollisia hyökkäyksiä.

3 TEOREETTINEN VIITEKEHYS

Työssäni teoreettisena viitekehyksenä tarkastellaan kyberturvallisuuskäsitteitä ja Ukrainan kybersodan vaiheita, valtiohallinnon kyberturvallisuuden kehittämisohjelmia ja lainsäädäntöä sekä kyberturvallisuuden uhkia ja tilannetta Suomessa.

3.1 Käsitteitä

Kyberturvallisuuteen liittyy paljon erilaisia käsitteitä. Koen käsitteiden auki määrittämisen olennaiseksi, sillä käsitteet saattavat olla valtaväestölle vieraita. Alle olen koonnut tämän opinnäytetyön kannalta keskeisimmät käsitteet ja niiden määritelmät. Käsitteet on otettu kyberturvallisuuden sanastosta, jonka on tuottanut Sanastokeskus TSK ry, 2018 toimeksiantajana on toiminut Turvallisuuskomitea.

Tietoturva; tietoturvallisuus: Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa.

Kyberturvallisuus: Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva

on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.

Haavoittuvuus: Alttius tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa. Nollapäivähaavoittuvuus on tietojärjestelmässä oleva haavoittuvuus, jolle on hyväksikäyttömenetelmä, mutta siihen ei ole saatavilla korjausta.

Tietoturvaloukkaus: Oikeudeton puuttuminen tietoon tai tietojärjestelmään. Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.

Tietoturvauhka: Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen.

Kyberuhka: Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku. Kyberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös digitaalisessa viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista. Kyberuhkat voivat kohdistua yhteiskunnan elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria tai kansalaisia vastaan joko suoraan tai välillisesti. Ne voivat olla peräisin maan rajojen sisältä tai niiden ulkopuolelta. Esimerkkejä kybertoimintaympäristöistä riippuvaisista toiminnoista ovat ydinvoimalan ohjaus, elintarvikkeiden kuljetus ja logistiikka sekä liikenteen ohjaus.

Kyberase: Kyberase on valtiollisen tahon kehittämä ja hyökkäyskäyttöön tarkoitettu haittaohjelma. Kyberaseita voidaan käyttää sodankäynnissä, mutta kyberaseiden käyttö ei vaadi varsinaista sotaa, sillä niitä voidaan käyttää myös vakoilussa tai sabotaasissa (Hyppönen, 2021).

3.2 Kyberturvallisuus

Kyberturvallisuus on yksi turvallisuuden osa-alue. Kyberturvallisuus kattaa kaiken ohjelmistoista toimiin, joilla pyritään turvaamaan esimerkiksi laitteita ja tietoa hyökkäyksiltä, häiriöiltä ja muilta vaaroilta (F-Secure, Mitä on kyberturvallisuus?). Kyberturvallisuudesta puhutaan nykyään paljon, kyberturvallisuuden parissa ei ole ainoastaan IT-alalla toimivat vaan lähes jokainen ihminen on päivittäin tavalla tai toisella tekemisissä kyberturvallisuuden kanssa. Puhelimet, tietokoneet, kodin älylaitteet ja erilaiset sähköiset asiointipalvelut ovat erottamaton osa arkeamme, jonka kautta myös kyberturvallisuus on iso osa arkeamme. (Traficom, Tietoturvailmiöt, jotka muuttivat maailmaa)

Kyberturvallisuus nousee otsikoihin ja kansan tietoisuuteen usein isojen häiriöiden myötä, joiden seuraukset ovat usein isoja ja näkyviä. Haavoittuvuuksista, haittaohjelmista ja muista kybermaailman uhkista päästään tuskin kokonaan eroon. (Traficom, Tietoturvailmiöt, jotka muuttivat maailmaa)

Kyberturvallisuus on myös keskeinen osa valtioiden puolustusta sekä sodankäyntiä. Vaikka isot yritykset ja organisaatiot voivat olla houkuttelevia kohteita verkkorikollisille, riittämättömät toimet omasta kyberturvallisuudesta huolehtimiseen voivat aiheuttaa monenlaista haittaa. Näihin kuuluvat: rahan menetys, identiteettivarkaus, tilien kaappaaminen, henkilökohtaisten tiedostojen lukitseminen, datan katoaminen sekä yksityisyyden menetys (F-secure, Mitä on kyberturvallisuus?)

3.3 Kybertoimintaympäristöt

Kun puhutaan kyberturvallisuudesta, puhutaan usein myös kybertoimintaympäristöistä. Kybertoimintaympäristö koostuu toisiinsa yhdistyneistä tietoverkoista, joissa tietoa siirretään digitaalisessa muodossa käyttäjältä ja koneelta toiselle, tietoliikennetekniikasta, tietokoneista sekä eri tehtäviä hoitavista datasäilöistä, reitittimistä ja palvelimista. (Jansson & Sihvonen, 2018)

Useat yhteiskunnan kriittiset toiminnot ovat riippuvaisia tietojärjestelmien ja verkkojen toimivuudesta. Kyberympäristöt liittyvät yhteiskuntamme jokapäiväisiin elintärkeisiin toimintoihin, kuten teollisuuteen, vesi- ja energiahuoltoon, pankkijärjestelmiin sekä terveydenhuoltoon, muun muassa nämä ovat riippuvaisia digitaalisista verkoista. Kyberturvallisuuden keskeinen tehtävä on turvata nämä kriittiset kybertoimintaympäristöön kuuluvat toiminnat. (Jansson & Sihvonen, 2018)

Kybertoimintaympäristöjä uhkaa esimerkiksi kyberrikollisuus, kybervakoilu sekä erilaiset kyberhyökkäykset. Jotta valtiot, yritykset ja yksityiset kansalaiset voivat hyödyntää kybertoimintaympäristön tuomat mahdollisuudet, on tärkeä varmistaa, että nämä verkot toimivat mahdollisimman luotettavasti ja turvallisesti.

3.4 Kybersota

Kybersota on todella vaikeasti määriteltävä termi ja sen rajat ovat paljon hämärämmät kuin perinteisen sodan. Jos valtioiden harjoittama verkkotiedustelu on kybersotaa, on globaalia kybersotaa käyty jo vuosikymmenten ajan. (Hallamaa, 2022) Kybersota-käsitettä käytetään hyvinkin laajasti kuvaamaan tapahtumia ja toimia digitaalisessa kybermaailmassa. Toisille kybersota on sotaa virtuaalimaailmassa, toisille se on vastakohta tavanomaiselle sodankäynnille. Tutkijoiden mukaan kybersodankäynnin määrittelyn tulisi perustua sodan tavoitteisiin ja motiiveihin, ei niinkään kyberoperaatioiden muotoihin. Kaikki aktivistien suorittamat

isotkin palvelunestohyökkäykset tai verkkovakoilu eivät ole kybersotaa vaan muuta rikollista toimintaa. (Peltomäki & Norppa 2015)

On tärkeää, että organisaatiot ymmärtävät kybersodan vaikutukset ja varautuvat kyberuhkiin silloin, kun tilanne on edelleen hallinnassa, koska erilaiset kybersodan, sodan tai maailmantilanteiden mukana tuomat ilmiöt voivat näkyä nopeina ja ennakoimattomina muutoksina kyberturvallisuudessa. On myös ymmärrettävä kybersodan vaikutukset laajempana kokonaisuutena, kun vain valtioiden välisinä tapahtumina. (Hallamaa, 2022)

4 KYBERTURVALLISUUS SUOMESSA

Kyberturvallisuuskeskuksen kuukausittain julkaisema kybersääkooste kertoo menneen kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Se on erityisesti suunnattu tietoturvasta vastaaville henkilöille, mutta arjen kyberturvallisuus -osiossa on hyviä neuvoja myös aivan tavalliselle kansalaiselle, jota kiinnostaa yleinen Suomen kyberturvallisuustilanne. Kybersääkoosteesta saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. (Traficom 2022, Kybersää) Kybersään tilanne tiivistetään sivulla kolmella tavalla; Sää on poutainen, jolloin tilanne on rauhallinen, sää on pilvinen, jolloin tilanne on huolestuttava ja jos sää on myrskyisä, niin tilanne on vakava.

Tarkastelin tammikuussa 2023 Traficomin julkaisemaa kybersäätä, tarkastelu ajankohtana viimeisin julkaistu raportti on vuoden 2022 marraskuulta, raportti toteaa kyberturvallisuuden tilan Suomessa huolestuttavaksi. Raportissa Traficom nostaa esille heidän ennustamansa viisi kyberuhkaa lähitulevaisuudessa (6kk- 2 v). Ensimmäisenä listalla on talouden ja politiikan ilmiöiden voimakas vaikutus kyberturvallisuuteen. Erityisesti esille nostetaan Venäjän hyökkäys Ukrainaan ja sen heijastuminen kyberturvallisuuteen. Traficom nostaa esille seuraavat esimerkit sodan ja talouden vaikutuksista. (Traficom, Kybersää marraskuu 2022)

- Sodan aiheuttamat muutokset etenkin talouteen, energian hinnan nopea nousu ja informaatioympäristön. Nämä näkyvät vaikeasti ennakoitavina kehityskulkuina kyberturvallisuuden osalta. Energiamarkkinoiden vaihteleva ja ennakoimaton tilanne voi vaikuttaa myös kyberturvallisuuteen.
- Kriittiseen infrastruktuuriin vaikuttaminen saattaa näkyä kyberympäristön häiriöinä ympäri Euroopassa.
- Sähkön sääntely voi aiheuttaa vaikutuksia myös kyberturvallisuuteen ja ICT-palveluiden toimivuuteen.

- Epävarmuustekijöillä voi olla isoja vaikutuksia organisaatioiden päivittäiseen toimintaan. Organisaatioiden on tärkeä huomioida maailmantilanne ja sen vaikutukset omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan. Etenkin huomioon tulee ottaa toimintaympäristön muutokset ja sen aiheuttamat uhkat kriittisille prosesseille.

Suomen NATO-jäsenyysprosessi on riskialtista aikaa kyberturvallisuuden osalta. Suomen NATO-jäsenyysprosessin aikana Suomea kohtaan voidaan kohdista erilaisia toimia esimerkiksi, kybervaikuttamista sekä verkossa tapahtuvaa informaatiovaikuttamista. Vaikuttaminen voi näkyä esimerkiksi palvelunestohyökkäyksinä. Palvelunestohyökkäyksillä saadaan hetkellisesti näkyvyyttä, mutta Traficom arvelee niiden vaikutusten olevan useimmiten lyhytaikaisia. (Traficom, Kybersää marraskuu 2022)

4.1 Valtion kyberturvallisuus

Kyberturvallisuus on yksi kansallisen turvallisuuden tavoitetiloista. Tarkoituksena on suojata kiihtyvällä vauhdilla digitalisoituvaa yhteiskunta ja yhteiskunnan toimintakykyä vihamieliseltä kybervaikuttamiselta ja tietoverkkotiedustelulta (Sisäministeriö, Kyberturvallisuus osana kansallista turvallisuutta.)

Valtioon kohdistuvat kyberiskut voivat olla tapahtuessaan koko maan lamauttavaa ja sen jäljet voivat olla pitkäkestoisia sekä tuhoisia. Kansallisen turvallisuuden kyberuhat ovat leimallisesti valtiollisia kyberuhkia, joissa hyödynnetään esimerkiksi, tietoverkkoja ja jotka kohdistuvat esimerkiksi kriittisen infrastruktuuriin eli valtion päätöksentekoon ja johtamiseen tai maanpuolustukseen (Sisäministeriö, Kyberturvallisuus osana kansallista turvallisuutta.)

4.2 Kyberturvallisuuden mittaaminen

Mittaaminen on oleellinen työkalu, jonka avulla voidaan tehdä johtopäätöksiä kyberturvallisuuden saralla. Mittausten avulla voidaan testata ja testien perusteella voidaan tehdä ennusteita tulevaisuudesta. Mittaamisen perusteella halutaan

saada tehtyä ja kehitettyä omia toimintoja. Mittaamisen ja arvioinnin tavoitteena on kehittää kyberuhkien aiempaa parempaan hallintaa. Kybermittausta voidaan tehdä laajasti erilaisin menetelmin. Kyberturvallisuuskeskus on kehittänyt tavan auttaa parantamaan yritysten, organisaatioiden ja samalla koko yhteiskunnan kykyä torjua kyberuhkia. Mittauksen nimi on kybermittari. (Traficom, Kybermittari)

Kybermittarin avulla johto saa näkymän toiminnalle tärkeiden kyberkyvykkyyksien kypsyystasoon osa-alueittain ja tavoitteittain. Mittari näyttää, millä tasolla kyberriskien tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen ovat organisaatiossa. Mittari tuo näkymän myös toimitusketjun ja ulkoisten riippuvuuksien hallintaan liittyvään kypsyystasoon. Lisäksi yritysjohto saa arvokasta tietoa siitä, miten oma kyberriskeihin varautuminen vertautuu toimialan keskiarvoon. (Traficom, Kybermittari)

Kybermittari on räätälöity etenkin Suomessa toimivien yritysten ja organisaatioiden tarpeisiin ja se pohjautuu kansainvälisiin kyberkyvykkyyksien mittausmalleihin. (Traficom, Kybermittari)

4.3 Kyberturvallisuuskeskus

Liikenne- ja viestintävirasto Traficomin alaisuudessa toimiva kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Kyberturvallisuuskeskus tuottaa monipuolisesti palveluita ja tietoa. Se muun muassa auttaa organisaatioita havaitsemaan sekä selvittämään niihin kohdistuvia tietoturvaloukkauksia. Kyberturvallisuuskeskuksen NCSA (National Communications Security Authority) -toiminnan lakisääteisenä tehtävänä on myös tarjota arviointi- ja hyväksyntäpalveluita sekä tietoturvaneuvontaa valtionhallinnolle sekä huoltovarmuuskriittisille toimijoille. (Kyberturvallisuuskeskus)

Kyberrikollisryhmät kohdistavat kasvavassa määrin kiristyshaittaohjelmahyökkäyksiä esimerkiksi terveydenhuolto- ja energiasektoreiden toimijoihin. Lisäksi valtiolliset toimijat hyödyntävät kyberrikollisryhmiä alihankkijoinaan salatakseen

oman osallisuutensa (Sisäministeriö, Kyberturvallisuus osana kansallista turvallisuutta.).

5 KYBERSODAN KESKEISIMPIÄ VAIHEITA

Ukraina on ollut venäläisten verkkohyökkäysten pysyvä kohde ainakin vuodesta 2014 lähtien. Helmikuun 24. päivän 2022 jälkeen hyökkäykset ovat olleet suhteellisen vähäisiä mutta sitäkin odotetumpia. Ukrainan sota on kyberaikakauden suurin sotilaallinen konflikti, ja se on ensimmäinen, jossa kyberoperaatiot ovat olleet näin merkittäviä kaikilla osapuolilla. (Przetacznik J. & Simona T., 2022)

Kyberhyökkäykset ovat olleet kaiken kaikkiaan epäonnistuneita yrityksiä helmikuussa alkaneen sodan jälkeen. Asiantuntijat ovat spekuloineet syitä, miksi kyberhyökkäykset ovat olleet niin vähäisiä. Kyberhyökkäysten rajallisuuteen saattaa vaikuttaa Ukrainan tietotekniikkaverkon suojelun korkea taso, Ukraina on joutunut hallitsemaan kyberuhkia ja kehittämään kyberpuolustustaan jo vuosia, ennen sodan syttymistä. Toiset asiantuntijat taas spekuloivat, että Venäjä saattaa vain odottaa sopivaa hetkeä käynnistää laajoja kyberhyökkäyksiä. Laajamittainen verkkohyökkäys voisi levitä nopeasti myös muihin maihin. (Przetacznik J. & Simona T., 2022)

Käsittelen seuraavaksi tämän opinnäytetyön kannalta keskeisimmät Venäjän suorittamat kyberhyökkäykset Ukrainaan.

5.1 Palvelunestohyökkäys vuonna 2014

13. maaliskuuta 2014, kolme päivää ennen Krimin aseman kansanäänestystä, Venäjä käynnisti kahdeksan minuutin mittaisen palvelunestohyökkäyksen horjuttaakseen Ukrainan tietoverkkoja ja viestintää. Tavoitteena uskotaan olleen Venäjän fyysisen hyökkäyksen edistäminen katkaisemalla yhteydenpito Ukrainan joukkojen ja valtionjohdon välillä, siirtämällä huomio pois Venäjän joukkojen läsnäolosta Krimillä. (Przetacznik & Tarpova, 2022).

Palvelunestohyökkäyksellä pyritään estämään verkkoresurssin tai palvelun käytön häiritsemällä sen toimintaa. Hyökkäys voidaan toteuttaa esimerkiksi kuormittamalla kohdepalvelu tai verkkoliikenne ylimääräisellä liikenteellä tai hyödyntämällä

palvelussa tai verkkolaitteessa olevaa haavoittuvuutta. Nykyään suurin osa palvelunestohyökkäyksistä on hajautettuja, eli liikenne lähetetään kohteeseen useasta lähteestä samanaikaisesti. Hajautettujen hyökkäysten taustalla on usein hyökkääjän hallitsema bottiverkko, joka koostuu useista internetiin kytketyistä laitteista, jotka ovat kaapattu hyökkäyskäyttöön laitteiden omistajien tietämättä. (Traficom, Toimintaohje – Palvelunestohyökkäys)

5.2 Hyökkäys Ukrainan sähkönjakelujärjestelmää vastaan vuonna 2015

Ukrainassa 23. joulukuuta 2015 tapahtumat alkoivat kolmen työntekijän havaitsemista hyökkäyksistä, jotka tapahtuivat 30 minuutin välein toisistaan, mikä pakotti heidät vaihtamaan toimintonsa manuaalisiksi. Tämä johti sähkökatkoihin, jonka seurauksena tuhannet ihmiset jäivät ilman sähköä useiden tuntien ajaksi. Sähkön katkettua, hyökkääjät pyyhkivät Master Boot Recordin (MBR) estääkseen koneiden uudelleen käynnistyksen, ja poistivat keskeytymättömän virransyötön (UPS). Samanaikaisesti tehtiin palvelunestohyökkäys, joka esti puhelinyhteydet työntekijöiden välillä. (Maynard, McLaughlin & Sezer)

5.3 Hyökkäys Ukrainan sähkönjakelujärjestelmää vastaan vuonna 2016

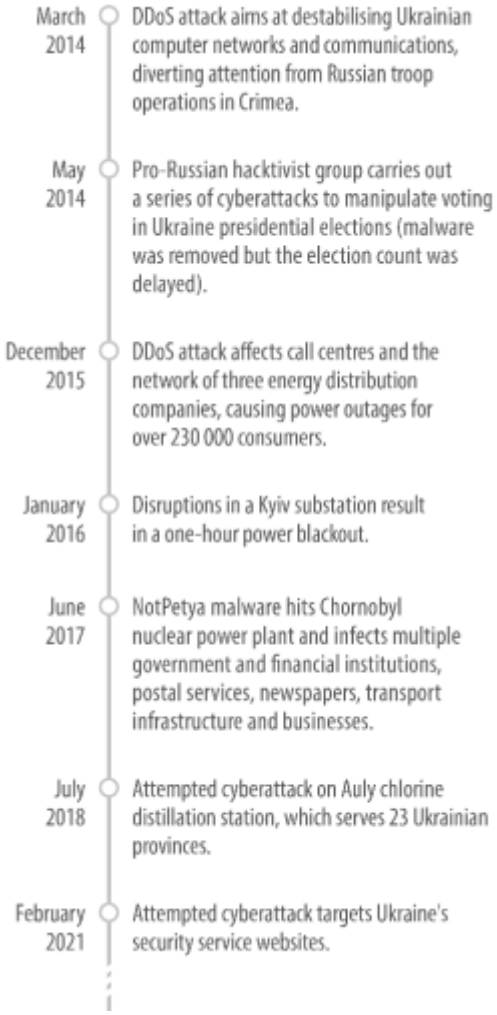
Vuonna 2016 Ukrainan sähkönjakelujärjestelmät joutuivat uudelleenhyökkäyksen kohteeksi. Hyökkäys oli samanlainen kuin edellinen mutta sen kohteeksi joutuivat myös palvelut, kuten rautatiet, Ukrainan eläkerahastot, Ukrainan valtionkassa, valtiovarainministeriö ja infrastruktuuriministeriö. Sähkökatkoksen syynä oli kyberhyökkäys, joka oli jälleen kohdistettu Ukrainan sähkönjakelujärjestelmää vastaan (Maynard et al., 2020).

5.4 Hyökkäys Ukrainan taloussektoria vastaan vuonna 2017

Vuoden 2017 kesäkuussa venäläisten toimijoiden uskottiin tehneen laajan kyberhyökkäyksen Ukrainan taloussektoria vastaan (Huhta, 2021). Hyökkäyksen kohteisiin kuuluivat Ukrainan kansallispankki, valtionjohto, energiayhtiöitä, mediaa sekä Boryspilin lentokenttä. Hyökkäyksen tarkoituksena oli siis maan kriittisen

infrastruktuurin lamauttaminen (Guchua et al., 2022). Hyökkäys toteutettiin käyttämällä NotPetya nimistä haittaohjelmaa. NotPetya loi mielikuvan, että kyseessä olisi jokin rikollisten yleisesti käyttämä kiristyshaittaohjelma. Todellisuudessa haittaohjelmalla pyrittiin aiheuttamaan pysyviä tuhoja tietojärjestelmiin.

NotPetya tarttui ukrainalaisen verotietojen käsittelyyn käytetyn kirjanpito-ohjelmiston ohjelmistopäivityksen avulla. Pääasiassa uhrit olivat Ukrainassa, mutta osumia saivat myös muut maassa liiketoimintaa harjoittavat yritykset. Tunnetuin Ukrainan ulkopuolinen NotPetya-uhri lienee logistiikkayhtiö A.P. Moller–Maersk, jonka oma arvio tappioista oli 200–300 miljoonaa dollaria. Suomalaisissa organisaatioissa vaikutukset jäivät muutamiin tartuntoihin. Kyberturvallisuuskeskuksen tiedossa olevissa tapauksissa yhtiöillä oli toimintaa Ukrainassa, ja NotPetya oli tarttunut Suomeen yhtiön sisäverkon kautta. (Kyberturvallisuuskeskus, Tietoturvan vuosi 2017)



Kuva 1. Kyberhyökkäysten aikajana 2014–2021 (EPRS | European Parliamentary Research Service)

6 KYBERHYÖKKÄYKSET 2022-2023

Venäjä on käyttänyt laajasti kyberhyökkäyksiä osana sotilaallista toimintaansa Ukrainassa. Venäjä on käyttänyt erilaisia taktiikoita, kuten haittaohjelmia, tietomurtoja sekä palvelunestohyökkäyksiä. CERT EU:n Russia's war on Ukraine: One year of Cyber Operations (2023) raportti jakaa kyberoperaatiot kolmeen eri vaiheeseen, jotka ovat vapaasti suomennettuna valmistelu-, nopea ja raivoisa- sekä pysyvä vaihe.

6.1 Valmisteluvaihe

Valmisteluvaiheessa (preparation phase) 13.1.2022 – 22.2.2022, havaittiin pyyhkijähyökkäyksiä, palvelunestohyökkäyksiä, sivustojen kaappaamisia sekä informaatio-operaatioita. Ilmoitetut hyökkäykset kohdistuivat lähes yksinomaan Ukrainaan (Cert-Eu, Russia's War on Ukraine: One year of Cyber Operations). Tammikuussa 2022 Microsoft raportoi tuhoisasta haittaohjelma operaatiosta, joka kohdistui useisiin eri ukrainalaisiin organisaatioihin. Microsoft on havainnut tämän operaatiossa käytettävän haittaohjelman WhisperGateksi, joka on pyyhkijä -tyyppinen haittaohjelma. Pyyhkijän (wiper) tarkoituksena on pyyhkiä käyttäjän tiedot palautuskyvyttömäksi (Crowstrike, The Anatomy of Wiper Malware, Part 1: Common Techniques). Sivustojen kaappaamiset kohdistuivat Ukrainan ulkoministeriön ja useiden muiden valtion virastojen nettisivuihin. (Microsoft, Destructive malware targeting Ukrainian organizations).

6.2 Nopea ja raivoisa vaihe

Nopean ja raivoisan vaiheen (Fast and furious phase) alussa 23.2.2022, Viasat KA-SAT-satelliittiverkkoon suunnattiin kyberhyökkäys, jossa käytettiin haittaohjelmaa nimeltä AcidRain, hyökkäys kohdistui Ukrainan organisaation viestintäinfrastruktuuriin. Hyökkäyksellä oli rajat ylittävä vaikutus ja se vaikutti noin 30 000 satelliittiterminaaliin, joita käytetään eri yrityksissä ja teollisuudenaloilla ympäri Euroop-

paa. Satelliittiverkon katkeaminen häiritsi myös noin 3 000 saksalaisen tuuliturbiinipalveluntarjoajan tuulivoimalan etäviestintää. (Cert-Eu, Russia's war on Ukraine: One year of cyber operations)

On todennäköistä, että tämä katkos oli sivuvaikutus eikä tarkoituksellinen osa hyökkäystä. European Union Agency for Cybersecurity (2023) Raportti korostaa, että joissakin tapauksissa kyberhyökkäykset kohdistuvat tai vaikuttavat organisaatioihin useammassa kuin yhdessä maassa samanaikaisesti, mikä voi johtaa merkittäviin rajat ylittäviin vaikutuksiin.

Satelliittiverkkoon suunnatun hyökkäyksen lisäksi havaittiin useita pyyhkijähyökkäyksiä, joissa käytettiin haittaohjelmia kuten HermeticWiper, IsaacWiper ja CaddyWiper. Vaiheen aikana suoritettiin myös paljon muuta häirintää, kuten palvelunestohyökkäyksiä ja verkkosivujen muokkaamista. Ukraina kokosi oman IT-armeijan 25.2.2022. Maaliskuu 2022 oli kuukausi, jolloin raportointiin korkein määrä hyökkäyksiä. Tämän piikin syynä oli jatkuvat, lievästi lisääntyneet hyökkäykset Ukrainaa vastaan sekä Venäjää vastaan suunnattujen hyökkäysten voimakas kasvu. (Cert-Eu, Russia's war on Ukraine: One year of cyber operations)

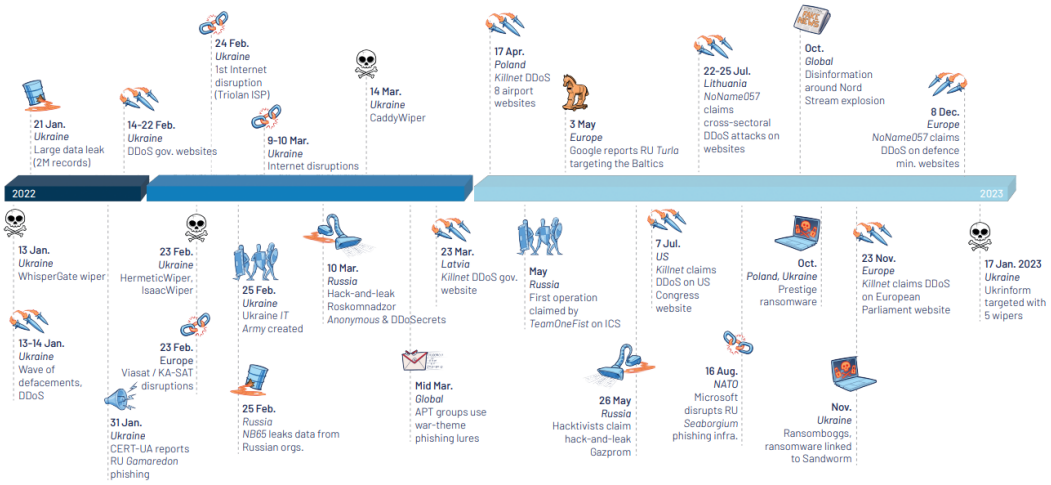
6.3 Pysyvä vaihe

Huhti- ja toukokuussa ei havaittu uusia pyyhkijähyökkäyksiä, lisäksi häiritseviä hyökkäyksiä havaittiin Ukrainassa aiempaa vähemmän. Venäjällä havaittiin suuria määriä tietovuotoja, mutta vähemmän palvelunestohyökkäyksiä. Toukokuussa alkoi hyökkäykset, jotka kohdistettiin teollisuuden hallintajärjestelmiin (ICS). EU-maissa oli palvelunestohyökkäysten aalto. (Cert-Eu, Russia's war on Ukraine: One year of cyber operations)

Kesä- lokakuussa Ukrainassa jatkui kalasteluhyökkäysten sarja, häiritseviä hyökkäyksiä havaittiin vähemmän ja havaintoja uusista pyyhkijähyökkäyksistä ei ollut. Venäjää vastaan havaittiin rajoitettu määrä jatkuvia palvelunestohyökkäyksiä. Lisäksi ilmoitettiin uusista hyökkäyksistä, jotka kohdistuivat ICS-järjestelmiin. EU-

maissa oli vähemmän palvelunestohyökkäyksiä. (Cert-Eu, Russia's war on Ukraine: One year of cyber operations)

Marras- tammikuussa Ukrainassa havaittiin uusia pyyhkijähyökkäyksiä, lisäksi EU maihin ja Ukrainaa tukeviin maihin kohdistuneiden palvelunestohyökkäysten määrä lisääntyi. (Cert-Eu, Russia's war on Ukraine: One year of cyber operations)



Kuva 2. Kyberhyökkäysten aikajana 2022–2023 (Cert-Eu; Russia's war on Ukraine: One year of Cyber Operations)

7 KYBERUHAT ORGANISAATIOIDEN NÄKÖKULMASTA

Kyberhyökkäykset ovat lisääntyneet maailmanlaajuisesti kuluvan vuoden aikana. Samalla niitä kohdistuu hiljaisemman kevään jälkeen kasvavassa määrin myös Suomeen. Traficomin Kyberturvallisuuskeskuksen saamien ilmoitusten mukaan suomalaisiin organisaatioihin kohdistuvissa kyberhyökkäyksissä, erityisesti haittaohjelmien, tietojenkalastelun ja palvelunestohyökkäysten lukumäärät ovat kasvaneet. (Traficom Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt 2022)

7.1 Erityisessä uhassa olevat toimialat ja alueet

Venäjän tiedustelupalvelut ovat kohdistaneet huomionsa erityisesti diplomaattisiin ja sotilaallisiin organisaatioihin NATO-maissa, Ukrainan naapurimaissa ja yksityisellä sektorilla, joka on suoraan tai epäsuorasti mukana Ukrainan sotilaallisessa toimitusketjussa. Suurimpana kiinnostuksen kohteena on ollut valtionhallinto ja IT-sektorin organisaatiot, näin on ollut myös Ukrainassa. IT-yrityksiin kohdistettujen hyökkäysten tavoitteena on hyödyntää yritysten teknisiä yhteyksiä ja saavuttaa pääsy näiden yritysten hallituksiin, politiikkaan ja muihin herkkiin organisaatioihin kuuluvien asiakkaiden tietoihin. (Microsoft, Destructive malware targeting Ukrainian organizations)

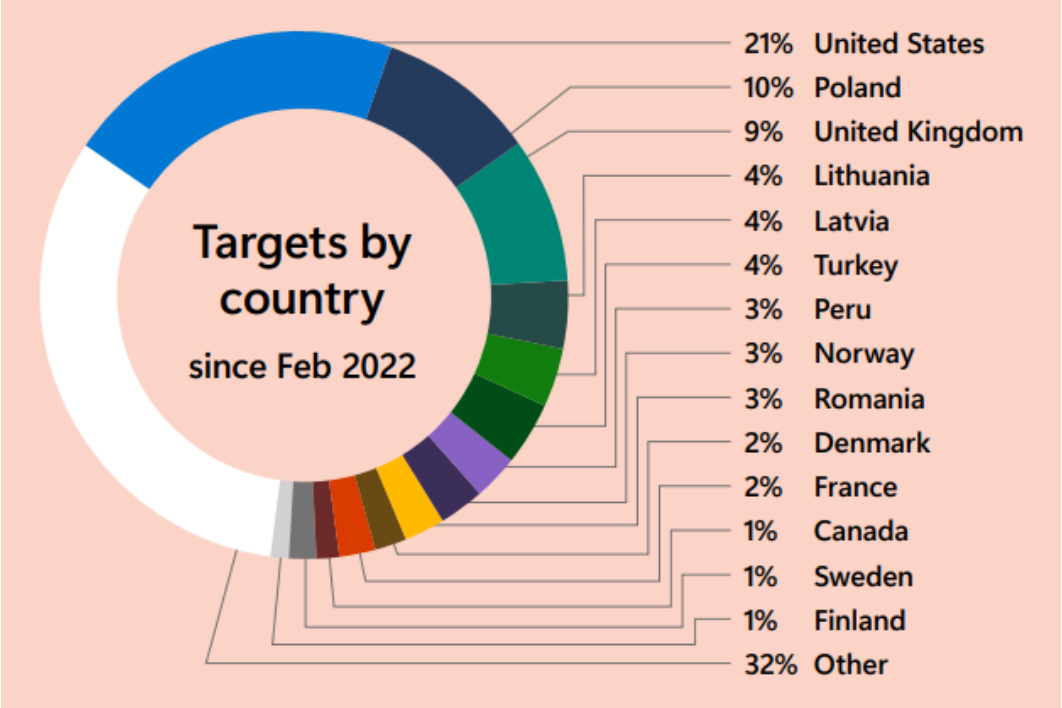
Maihin, joihin on kohdistettu eniten uhkia, Ukrainaa lukuun ottamatta ovat EU:n ja NATOn jäsenmaat, erityisesti Itä-Euroopan maat ovat kymmenen eniten kohdistettujen maiden joukossa. (Microsoft, Destructive malware targeting Ukrainian organizations)

7.2 Venäjää kiinnostava tieto Suomessa

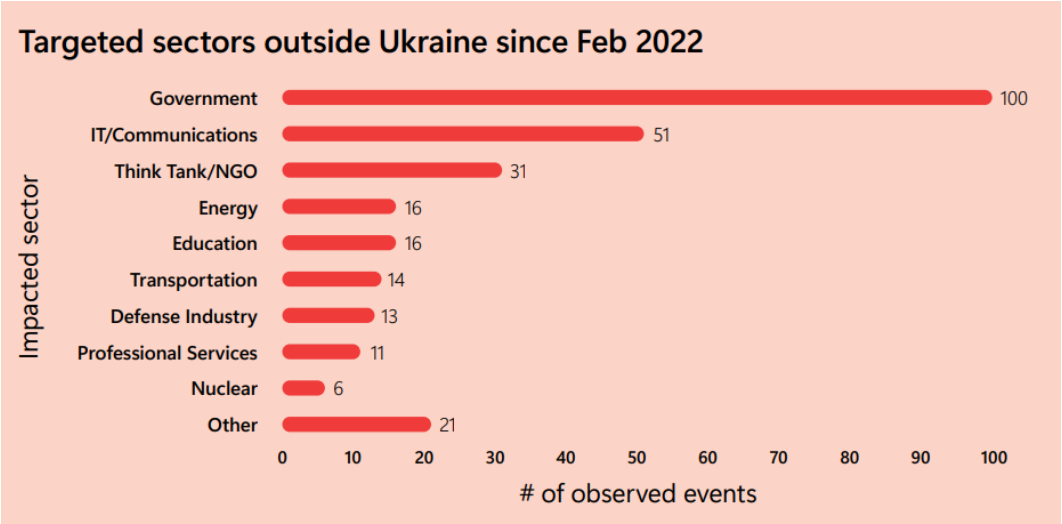
NATO-jäsenyys on tehnyt Suomesta entistä kiinnostavamman tiedustelun kohteen venäjälle, kriittiseen infrastruktuuriin kohdistuvan tiedustelun uhka on kohonnut ja myös yritykset ovat venäjän kybervakoilun kohteena. Venäjä pyrkii todennäköi-

sesti hankkimaan tietoa, millainen NATO-jäsen suomesta tulee ja mitkä ovat Suomen aikomukset NATO-jäsenyyden suhteen. Toisaalta Venäjä pyrkii myös Suomen kautta hankkimaan tietoa NATOsta, koska nyt Suomella NATO-jäsenenä on kaikki tieto NATOsta myös Suomessa. Venäjä pyrkii hankkimaan tietoa kriittisestä infrastruktuurista, jotta se voisi tilanteen eskaloituessa tarvittaessa vaikuttamaan tämän kriittisen infran toimintaan. Vaikka kriittiseen infraan kohdistuva tiedusteluuhka on kohonnut, suojelupoliisi pitää ainakin lyhyellä aikavälillä epätodennäköisenä toimintaa, jolla pyrittäisiin lamauttamaan Suomen kriittistä infraa, koska tällainen toiminta merkitsisi uudenlaista eskalaatiota, johon Venäjä on tuskin halukas tällä hetkellä. (Karlamaa & Pelttari)

Venäjää kiinnostaa myös yhä enemmän yritysten tuotekehitystieto kasvavassa määrin. Venäjää vastaan kohdistettujen pakotteiden myötä korkean teknologian vienti Venäjälle on vaikeutunut, ja venäjällä on vaikeuksia käynnistää länsimaista teknologiaa korvaavaa tuotantoa. Tämä johtaa siihen, että myös yritykset, ennen kaikkea sellaiset, jotka tekevät sotilasteknologiaa / sotilaallisen varautumisen kannalta merkittäviä asioita ovat Venäjän kybervakoilun kohteena. (Karlamaa & Pelttari)



Kuva 3. Maat, joihin on kohdistettu eniten uhkia (Targets by country, Microsoft Threat Intelligence)



Kuva 4. Hyökkäysten kohteena olevat alat Ukrainan ulkopuolella **(**Targeted sectors outside Ukraine since Feb 2022, Microsoft Threat Intelligence)

7.3 Organisaatioiden varautuminen Suomessa

Tietoturvatyötä on merkittävää tehdä joka päivä, eikä ainoastaan vasta siinä vaiheessa, kun hyökkäys on jo tapahtunut (Karlamaa & Pelttari). Organisaatiot käyttävät yhä enemmän digitaalisia järjestelmiä ja palveluita, mikä tekee niistä alttiimpia kyberhyökkäyksille. Tämä korostaa tarvetta tietoturvallisten käytäntöjen kehittämiselle ja niiden jatkuvuudelle organisaation toiminnassa, esimerkiksi ylläpitämällä kattavia lokitietoja, jotta jos jotain tapahtuu, lokitietojen avulla haitallisen toiminnan selvittäminen on helpompaa. (Karlamaa & Pelttari)

Voidaan todeta, että Suomessa toimivat organisaatiot ovat alttiita samankaltaisille hyökkäyksille, joita on kohdistettu Ukrainaan. Erityisesti energia-alan, finanssialan ja julkisen sektorin organisaatiot ovat alttiita, sillä ne ovat tärkeitä kansalliselle turvallisuudelle. Hyökkäysten kohteeksi ovat joutuneet suomalaisyrityksistä muun muassa Wärtsilä, Uponor ja Suomen Tietotoimisto. Terveydenhuolto ei ole ainakaan toistaiseksi Suomessa ollut erityisen houkutteleva kohde. (Karlamaa & Pelttari)

Organisaatioiden tulisi siis ottaa kyberturvallisuus vakavasti ja kehittää selkeät ja jatkuvat tietoturvallisuuden käytännöt ja toimintasuunnitelmat. Niiden tulee myös kouluttaa henkilöstöään, tarkastella ja päivittää säännöllisesti tietoturvakäytäntöjään sekä tehdä yhteistyötä alan asiantuntijoiden kanssa turvallisuusriskien minimoimiseksi. Olennaista on hyvä yhteistyö kaikkien eri tahojen, niin viranomaisten kuin yksityistenkin tahojen kesken. (Karlamaa & Pelttari)

Valtiollisen tiedustelun uhka kohdistuu pääosin valikoituihin organisaatioihin ja ihmisiin, eli tahoihin, joilla on pääsy tällaiseen vierasta valtiota kiinnostavaan tietoon**.** On kuitenkin hyvä tunnistaa, että tietoturvatyö kannattaa kaikkien näkökulmasta ja olennaista on se, että kaikkien järjestelmien tietoturvapäivitykset ovat ajan tasalla. (Karlamaa & Pelttari)

Vaikka Suomessa eletään talouden kannalta vaikeita aikoja ja monien organisaatioiden taloudellinen tilanne on tiukka, ei kyberturvallisuus ole oikea säästämisen kohde, ei julkisella eikä yksityiselläkään puolella. (Karlamaa & Pelttari)

Organisaatioiden tulee ottaa huomioon omassa riskienhallinnassa entistä tarkemmin esille toimintaympäristön aiheuttamat uhkat sekä tehdä toimenpiteitä kyberturvallisuuden takaamiseksi.

7.4 Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa

Kyberturvallisuuskeskus on elokuussa 2022 julkaissut ohjeet, joiden avulla organisaatiot voivat parantaa kyberturvallisuuttaan sekä pienentää riskiä hyökkäyksen joutumisen kohteeksi. (Traficom, Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt 2022)

Tämä Kyberturvallisuuskeskuksen julkaisema ohje on tarkoitettu kaikille suomalaisille organisaatioille kyberturvallisuuden vahvistamiseen. Ohjeet eivät rajoitu ainoastaan vuoden 2022 alun kansainvälisen tilanteen aiheuttamaan varautumistarpeeseen, vaan niiden avulla on mahdollista kehittää myös yleisemmin organisaatioiden kyberturvallisuutta. (Traficom, Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - ohje johdolle ja asiantuntijoille)

Elokuussa julkaistuissa ohjeissa Kyberturvallisuuskeskus nostaa esille seuraavat teemat:

Kyberturvallisuuden johtaminen

- Huomioikaa muutokset kyberturvallisuuden uhkakuvissa.
- Määritelkää liiketoimintakriittiset ympäristönne.

Kyberturvallisuuden kontrollit

- Suojatkaa liiketoimintakriittiset ympäristönne.
- Ottakaa käyttöön monivaiheinen tunnistautuminen.

- Asentakaa tietoturvapäivitykset viipymättä.
- Varmistakaa tietoliikenteen turvallisuus.
- Suojautukaa haittaohjelmilta.
- Varautukaa palvelunestohyökkäyksiin.
- Suojatkaa myös pilvipalvelut.
- Varmistakaa etäyhteyksien turvallisuus.
- Huolehtikaa varmuuskopioista.
- Tarkastakaa julkiseen verkkoon näkyvät palvelunne.
- Tarkastelkaa langattomien teknologioiden muodostamia riskejä.

Havainnointi, reagointi ja toiminnan jatkuvuus

- Havainnoikaa ja analysoikaa tapahtumia.
- Reagoikaa tapahtumiin ja häiriöihin.
- Varmistakaa toiminnan jatkuvuus.
- Informoikaa henkilöstöä.
- Ilmoittakaa tietoturvaloukkauksista tai niiden epäillyistä.

8 JOHTOPÄÄTÖKSET

Venäjän tekemät kyberhyökkäykset Ukrainaan ovat osoittaneet, että kyberhyökkäykset voivat olla erittäin tuhoisia ja vaikuttaa merkittävästi yhteiskuntien toimintaan. Suomalaisiin organisaatioihin kohdistuu suojelupoliisin ja Traficomin mukaan jatkuvasti kasvavaa kiinnostusta ja kyberhyökkäysten luonne on muuttunut. Tapausmäärän kasvusta huolimatta Traficom ja suojelupoliisi pitävät yhteiskuntaa lamauttavaa kyberhyökkäystä epätodennäköisenä. (Karlamaa & Pelttari)

Ukrainan sota on vaikuttanut merkittävästi organisaatioiden kyberturvallisuuteen Suomessa. Keräämälläni aineistolla pyrin vastaamaan siihen, millaisia kyberhyökkäyksiä Ukrainaan on kohdistunut ja mitkä organisaatiot ovat erityisen alttiissa asemassa ja miksi. Kyberhyökkäykset ovat kehittyneet ja monipuolistuneet huomattavasti viime vuosina, ja Ukrainan sota on ollut yksi tärkeimmistä tapahtumista, joka on vaikuttanut tähän kehitykseen.

Aineiston pohjalta voidaan todeta, että kiristynyt maailmantilanne on lisännyt kyberturvallisuusriskejä ja Venäjän Suomeen kohdistamaa kybertoimintaa on havaittu aiempaa enemmän. Hyökkäysten kohteena ovat mm. Suomalaiset yritykset, huoltovarmuuskriittiset toimijat ja valtionhallinto. Kiristyshaittaohjelmat ja palvelunestohyökkäykset ovat lisääntyneet ja ne ovat entistä kohdennetumpia.

Organisaatioiden on tärkeää panostaa kyberturvallisuuteen ja kehittää strategioita, jotka mahdollistavat nopean reagoinnin kyberhyökkäyksiin. On myös tärkeää, että organisaatiot seuraavat kyberturvallisuuden ajankohtaisia ilmiöitä ja pysyvät ajan tasalla mahdollisista uhkista.

Koska tutkimustyöni perustui runsaaseen ja monipuoliseen lähdemateriaaliin, sekä suomalaisiin että kansainvälisiin lähteisiin, sen voidaan katsoa olevan melko luotettava. Tärkeänä tekijänä tutkimuksessani oli lähdekriittisyys, jota noudatin aineiston keruussa ja opinnäytetyön tekemisessä. Pyrin käyttämään lähdeaineistona laadukkaita ja kattavia lähteitä.

Haastavaa tässä opinnäytetyö prosessissa oli etenkin aiheen arkaluontoisuus ja ajankohtaisuus, sillä mahdolliset Suomeen kohdistuvat kyberhyökkäykset eivät ole automaattisesti julkista tietoa. Ajankohtaisuudella viittaan aihepiirin jatkuvaan muutokseen, uusia kyberturvallisuutta koskevia tapahtumia tapahtuu ja uutta tietoa ja tutkimuksia julkaistaan jatkuvasti. Koin aiheen ajankohtaisuuden ajoittain lannistavana, sillä jatkuva muutos ja uusien tapahtumien sekä tutkimusten tulva saattoivat tuntua ylivoimaisilta pysyäkseen mukana.

Tämän opinnäytetyön kirjoittaminen oli mielenkiintoinen ja laaja prosessi, ja sen edetessä opin koko ajan uutta ja ammatillinen osaamiseni kehittyi. Sain laajasti tietoa ja ymmärrystä kyberturvallisuudesta eri toimintatavoista, termeistä ja sen laajuudesta, mikä edisti kokonaisvaltaista näkemystä aiheesta.

LÄHTEET

CERT-EU. RUSSIA'S WAR ON UKRAINE: ONE YEAR OF CYBER OPERATIONS. 2023. Viitattu 17.4.2023. https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Crowstrike. 2022. The Anatomy of Wiper Malware, Part 1: Common Techniques. Viitattu 22.5.2023. https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/

EPRS. European Parliamentary Research Service. 2022. Viitattu 12.2.2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

F-secure. Mitä on kyberturvallisuus. Viitattu 14.2.2023. https://www.f-secure.com/fi/home/articles/what-is-cyber-security

Guchua, A., Zedelashvili, T., & Giorgadze, G. 2022. Geopolitics of the RussiaUkraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats. Ukrainian Policymaker. Viitattu 11.4.2023. https://doi.org/10.29202/up/10/4

Hallamaa. 2022. Yle uutiset. Verkkoon piirretty viiva. Viitattu 22.5.2023. https://yle.fi/a/3-12370108

Hyppönen, M. 2021. Internet. WSOY.

Jansson, S & Sihvonen, T. 2018. Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhat. Viitattu 12.2.2023. https://journal.fi/mediaviestinta/article/view/69950/31049

Karlamaa, K & Pelttari, A. 2023. Mikä on suomen kyberturvallisuuden taso? Ajankohtaisohjelma. Yle uutiset. Viitattu 11.5.2023. https://areena.yle.fi/1-65667546

Koistinen, P & Salonen, I. 2022. Ukrainan sota ja maailma sen jälkeen. Vastapaino.

Kyberturvallisuuskeskus. Verkkosivu. Viitattu 22.5.2023. https://www.kyberturvallisuuskeskus.fi/fi

Maynard P., McLaughlin K., Sezer S. (2020) Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. Jour-nal of Cybersecurity. Viitattu 5.4.2023. https://academic.oup.com/cybersecurity/article/6/1/tyaa020/6034412

Microsoft. Destructive malware targeting Ukrainian organizations. 2022. Viitattu 17.4.2023. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Peltomäki, J & Norppa, K. 2015. Rikos meni verkkoon. Helsinki: Talentum.

Przetacznik J. & Simona T. 2022. European Parlament. Russia's war on Ukraine: Timeline of cyber-attacks. Viitattu 12.2.2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Przetacznik, J., & Tarpova, S. (2022). Russia’s war on Ukraine: Timeline of cyber-attacks. European Parliamentary Research Service (EPRS). Viitattu 5.4.2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Raeste, J.P. 2022. Helsingin Sanomat. Viitattu 8.12.2022. https://www.hs.fi/talous/art-2000008653639.html

Sitra. 2022. Sitra. Ennakointia Venäjän hyökkäyssodan vaikutuksista. Viitattu 8.12.2022. https://www.sitra.fi/julkaisut/ennakointia-venajan-hyokkayssodan-vaikutuksista/#miksi-juuri-nyt-tarvitaan-tulevaisuusajattelua

Traficom 2022. Kybersää, marraskuu 2022. Viitattu 6.1.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20marraskuu%202022_0.pdf

Traficom. 2023. Kybermittari. Viitattu 22.5.2023. https://www.kyberturvallisuus-keskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

Traficom. 2022. Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - ohje johdolle ja asiantuntijoille. Viitattu 22.5.2023. https://www.kyberturvalli-suuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-vahvistami-nen-suomalaisissa-organisaatiossa-ohje

Traficom. 2022. Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt. Viitattu 9.5.2023. https://www.kyberturvallisuuskes-kus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomea-kin-kohtaan-lisaantynyt

Traficom. 2022. Tietoturvailmiöt, jotka muuttivat maailmaa. Viitattu 8.12.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvailmiot-jotka-muuttivat-maailmaa

Traficom. 2022. Toimintaohje – palvelunestohyökkäys. Viitattu 22.5.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publica-tion/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf

Turvallisuus komitea. 2018. Kyberturvallisuuden sanasto. Viitattu 6.1.2023. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuu-den-sanasto.pdf