Merja Pohjankoski

KYBERHYÖKKÄYKSISTÄ UKRAINASSA 2022

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Pohjankoski, Merja
Kyberhyökkäyksistä Ukrainassa 2022
Jyväskylä: Jyväskylän yliopisto, 2023, 67 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tutkimustyön tarkoitus oli tutkia pääasiassa Ukrainaan vuoden 2022 aikana kohdistuneita kyberhyökkäyksiä, sekä valaista hiukan myös Venäjän muihin läntisiin naapureihin (Suomi, Viro, Latvia, Liettua ja Puola) kohdistuneita kyberhyökkäyksiä. Työ toteutettiin laadullisena sisältöanalyysinä, jossa tiedonkeruumenetelmänä oli julkaistu tietoaineisto. Asia kiinnosti tutkijaa ajankohtaisuutensa vuoksi. Päätutkimuskysymyksenä oli ”Mitä voimme päätellä vuoden 2022 kyberhyökkäyksistä Ukrainaan”. Tälle päätutkimuskysymykselle on laadittu kolme alatutkimuskysymystä:

1. Millaisia Ukrainaan kohdistuneita, vuoden 2022 aikana tehtyjä kyberhyökkäyksiä on löydetty? Millaisia hyökkäyksiä Suomeen (sekä Baltian maihin ja Puolaan) on tehty vuonna 2022?
2. Miten hyökkäysten määrä, hyökkäystyypit ja hyökkäysten kohteet ovat muuttuneet vuoden aikana?
3. Onko havaittavissa mitään trendiä, ja voidaanko tuloksista päätellä tai ennakoida tulevaa?

Työssä taustoitettiin kybermaailman lainalaisuuksia ja terminologiaa sekä kuvattiin lyhyesti vuoden 2022 Venäjän Ukrainan vastaisen sotilaallisen suurhyökkäyksen tärkeimmät tapahtumat. Selkeyden vuoksi kuvattiin lyhyesti tärkeimmät tapahtumat ja merkittävimmät kyberhyökkäykset myös Krimin valtauksesta (2014) Venäjän tekemään sotilaallisen hyökkäyksen alkamiseen (helmikuu 2022). Tämä nähtiin tarpeelliseksi, jotta voitiin tutkia myös kybertapahtumien muuttumista sotilaallisen suurhyökkäyksen lähestyessä ja sen alettua. Työn ja tutkimuskysymysten rajaus muuttui vielä työn edetessä. Työn tuloksena selvisi, että kyberhyökkäysten määrä lisääntyi voimakkaasti sekä Ukrainassa että muissa Venäjän läntisissä naapurimaissa, mutta hiukan eri tahdissa. Suurhyökkäyksen jälkeen Ukrainaa vastaan kohdistetut hyökkäykset muuttuivat aggressiivisimmiksi. Hyökkäystyypit vaihtelivat kohteen mukaan: Ukrainaa vastaan vuonna 2022 käytettiin pääasiassa erityisen haitallisia, tietoa tuhoavia niin kutsuttuja wiperhyökkäyksiä, kun taas Ukrainaa tukeviin, Venäjän muihin läntisiin naapurimaihin iskettiin erityisesti palvelunestohyökkäyksillä. Ukrainan nopea vastatoiminta ja kansainvälisen yhteisön tuki yllättivät hyökkääjäksi ilmenneen Venäjän, eivätkä hyökkäykset lopulta tuottaneet toivottua tulosta. On kyetty osoittamaan, että Ukrainassa kyberhyökkäyksillä ja kineettisillä sotatoimilla on selkeä korrelaatio.

Asiasanat: kybertoimintaympäristö, kyberturvallisuus, kyberuhka, kyberrikollisuus, kyberhyökkäys, kyberoperaatio, kybersodankäynti, attribuutio

ABSTRACT

Pohjankoski, Merja
On cyber-attacks in Ukraine 2022
Jyväskylä: University of Jyväskylä, 2023, 67 pp.
Cyber Security, Master's Thesis
Supervisor: Lehto, Martti

The aim of this master's thesis work was to study cyber-attacks made during 2022 against Ukraine, and also take a quick look on attacks made against other western neighbor countries of Russia (Finland, Estonia, Latvia, Lithuania and Poland). The study was implemented as a qualitative content analysis, with the data collection method being public published information. The topic of the study was chosen because the phenomena to be studied were very topical in this particular point of time. The main research question was "What conclusions can be made concerning cyber-attacks towards Ukraine in 2022". To support this main question three other sub questions were drafted:

1. What kind of cyber-attacks against Ukraine were found, made during 2022? What kind of attacks against Finland, the Baltic states and Poland were found?
2. How have the amounts, types, and targets of changed during 2022?
3. Can any trends be seen? Is it possible to forecast anything for the future based on the results?

The basic principles and terminology of the cyber world were first introduced. Also, the most significant happenings of Russia's major military invasion (February 2022) were briefly described. For clarity also the main happenings and the most remarkable cyber-attacks between the illegal annexation of Crimea (2014) and the Russian military attack were described. This was seen important to be able to compare the attacks before and after the major military attack. The definitions and delimitations of the main research questions of the study changed as the work advanced. As a result of the study, it was found out that the amount of cyber-attacks increased remarkably both in Ukraine and Russia's other western neighbours, but in a different pace. Also, after the major military attack the cyber-attacks against Ukraine started to be more aggressive. The attack types varied depending on the target countries: the attacks against Ukraine were made using disastrous malware (so called wipers), as the other countries were attacked mainly with denial-of-service attacks. Ukraine's fast counter activities and the wide international support surprised Russia, who was found to be behind the cyber-attacks. The attacks did not bring the success the attacker had wished. Evidence has been found to prove the correlation between physical military operations and cyber-attacks in Ukraine.

Keywords: cyber environment, cyber security, cyber threat, cyber-crime, cyber-attack, cyber operation, cyber warfare, attribution

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tämä tutkimus on Jyväskylän yliopiston Kyberturvallisuuden maisteriohjelman pro gradu -työ. Tarkoituksena oli tutkia yllä mainittuna ajankohtana, vuonna 2022, tapahtuneita Ukrainaan ja muihin Venäjän läntisiin naapurimaihin kohdistuneita kyberhyökkäyksiä tarkastelemalla niiden määrää, laatua, hyökkäysvektoreita eli hyökkäystapoja ja -kohteita sekä näiden muutosta.

1.1 Tutkimuksen tausta, motiivit ja tavoitteet

Työn aihe katsottiin informaatioteknologian tiedekuntaan sopivaksi pro gradu -työksi, koska aihepiiri sisältyy tutkijan kyberturvallisuuden opintojen ja opetussuunnitelman piiriin. Kyberturvallisuuden maisteriohjelmakoulutuksessa tarkastellaan kybermaailmaa ja sen turvallisuutta hallinnollisesta ja teknologisesta näkökulmasta (Jyväskylän Yliopisto, 2023). Lisäksi tutkijan opintosuunta, kokonaisturvallisuus ja strateginen tiedustelu, valmentaa ymmärtämään ja analysoimaan turvallisuuteen vaikuttavia tekijöitä laaja-alaisesti.

Asia kiinnosti tutkijaa ajankohtaisuutensa vuoksi, sekä sen vuoksi, ettei siitä vielä todennäköisesti oltu tehty -juuri asian tuoreuden vuoksi- liian monia tutkimuksia tai opinnäyte- ja gradutöitä, ainakaan tästä näkökulmasta, jossa tutkitaan myös ajallista kehitystä Krimin valtauksesta vuonna 2014 tutkittavaan vuoteen 2022 asti. Työstä sai mielenkiintoista näkymää siihen, olivatko hyökkäykset lisääntyneet vai vähentyneet tarkasteltavan ajanjakson aikana ja etenkin Venäjän helmikuisen sotilaallisen suurhyökkäyksen lähestyessä, ja miten hyökkäykset ovat mahdollisesti muuttuneet. Vaikutti siltä, että esimerkiksi Venäjän kykyä kyberhäirikkönä aikanaan pelättiin ja yliarvioitiin. Myös suojaus- ja puolustautumistoimenpiteet lännessä ovat parantuneet.

Tutkimus voi mahdollisesti myös lisätä yritys- ja organisaatiomaailmassa tietoisuutta ja ymmärrystä kyberkyvykkyyden kasvattamiseen, sekä kasvattaa suojautumisen tahtotilaa, kun nähdään, kuinka myös siviiliorganisaatioihin kohdistetaan kyberhyökkäyksiä, vaikka nämä kohteet eivät olekaan osapuolina

kansainvälisissä sotatoimissa tai muissa konflikteissa. Lisäksi voidaan todeta kyberoperaatioiden ja hyökkäysten selvä lisääntyminen juuri Venäjän tekemää sotilaallista suurhyökkäystä helmikuun lopussa 2022.

1.2 Tutkimusongelma ja tutkimuskysymykset

Tutkimusta aloitettaessa on tärkeää määritellä tutkimuskysymys tai -kysymykset oikein. Tämä on usein tutkijoille haastavaa. Hirsjärven ym. (2015) mukaan tämä haaste tulee useammin vastaan laadullista eli kvalitatiivista tutkimusta tehtäessä, muun muassa siksi, että määrällinen eli kvantitatiivinen tutkimus jakautuu selvemmin erottuviin vaiheisiin. Hirsjärvi ym. (2015) toteavat myös, että kvalitatiivisessa tutkimuksessa varaudutaan siihen, että tutkimusongelma saattaa muuttua tutkimuksen edetessä. Tämä konkretisoitui myös tämän pro gradu -työn yhteydessä. Työn edetessä ja lähdemateriaaleihin tutustuessa työn laajuus ja rajaus kaventuivat ja tutkimuskysymykset täsmentyivät ja muuttuivat hiukan. Myös lähdemateriaalin määrä kasvoi, kun aiheesta julkaistiin uusia raportteja alkuvuoden 2023 aikana.

Tämän tutkimuksen päätutkimuskysymys on muotoiltu seuraavasti:

"Mitä voimme päätellä vuoden 2022 kyberhyökkäyksistä Ukrainaan."

Tälle päätutkimuskysymykselle on laadittu kolme alatutkimuskysymystä:

1. Millaisia Ukrainaan kohdistuneita, vuoden 2022 aikana tehtyjä kyberhyökkäyksiä on löydetty? Millaisia hyökkäyksiä Suomeen, Baltian maihin ja Puolaan on tehty vuonna 2022?
2. Miten hyökkäysten määrä, hyökkäystyypit ja hyökkäysten kohteet ovat muuttuneet vuoden aikana?
3. Onko havaittavissa mitään trendiä, ja voidaanko tuloksista päätellä tai ennakoida tulevaa?

Työssä selvitettiin ensin, millaisia kyberhyökkäyksiä mainitulla aikavälillä on tehty ylipäätään. Tutkimuksen tuloksena selvitettiin, ovatko hyökkäykset mainitulla aikavälillä ja Venäjän Ukrainaan tekemän sotilaallisen suurhyökkäyksen lähestyessä lisääntyneet tai vähentyneet, sekä miten hyökkäykset (lukumäärä, tavat, vektorit, kohteet) ovat mahdollisesti muuttuneet. Työssä tarkasteltiin myös Ukrainan lisäksi Venäjän muihin läntisiin naapurivaltioihin kohdistuneita kyberhyökkäyksiä vertailun ja yleisen tilannekuvan saamiseksi, mutta kevyemmin kuin Ukrainaan kohdistuneita hyökkäyksiä.

1.3 Rajaukset ja tarkenne

Työssä ei käsitelty sotaa, kybersotaa, eikä otettu kantaa kyberhyökkäyksistä osana sotatoimia, vaikka tarkastelun ajallinen aikaikkuna osuikin Venäjän Ukrainassa suorittamien sotilaallisten toimien ajankohtaan, ja vaikka hyökkäävänä osapuolena olikin Venäjä. Sotatoimien yhteydessä tehtyjä kyberoperaatiota sekä niiden kohteita ja tekijöitä olisi vaikea todentaa pelkästään julkisiin lähteisiin perustuen. Lisäksi kybersodan käsite on ristiriitainen myös alalla pitkään toimineiden tutkijoiden ja sotatieteilijöiden mielestä.

Työ rajattiin käsittelemään vain sellaisia kyberhyökkäyksiä, joista on aiheutunut konkreettista haittaa sen kohteelle; ja joissa tapauksissa on jouduttu tekemään korjaavia toimenpiteitä. Konkreettinen haitta voi olla esimerkiksi katkos sen tarjoamissa ulkoisissa palveluissa, oman toiminnan keskeytymisiä, tietovuotoja. Työ rajattiin koskemaan ainoastaan Ukrainaan sekä Venäjän läntisiin naapurimaihin (Suomi, Viro, Latvia, Liettua, Puola) kohdistuneita kyberhyökkäyksiä. Rajausta ei tehty sen perusteella, oliko hyökkäyksen kohde yksityinen vai julkinen taho. Tarkasteluun otettiin sekä yksityisiin yrityksiin että valtiollisiin tai muihin julkishallinnollisiin tahoihin kohdistuneet kyberhyökkäykset, mutta yllä mainituista syistä ei tarkasteltu sotilaallisiin kohteisiin tehtyjä kyberhyökkäyksiä. Työ rajattiin myös koskemaan sellaisia kohteita, joista on saatavilla tietoa julkisista lähteistä ja/tai joista on uutisoitu.

Työssä tarkasteltiin myös sitä, mitä tai keitä ovat olleet hyökkäävät tahot. Niin kutsuttu attribuutio-ongelma (eli mahdottomuus nimetä varmuudella hyökkääviä tahoja) on kuitenkin tunnistettu. On huomioitava, että työn tuloksena ei ole ollut tarkoitus syntyä absoluuttista täydellistä selvitystä kaikista mahdollisista kyseisellä tarkasteluvälillä tehdyistä kyberhyökkäyksistä. Kaikkia tehtyjä kyberhyökkäyksiä ei välttämättä ole ilmoitettu ja tilastoitu. Tämä työ perustuu avoimista lähteistä saatavilla olleisiin, julkaistuihin tietoaineistoihin ja -lähteisiin. Eri julkaisuissa ja raporteissa mittaus-, raportointi- ja luokittelutavat poikkesivat toisistaan. Useat valtiolliset lähteet ilmoittivat tietoturvayhtiöiden raporteista poikkeavia lukumääriä.

1.4 Keskeiset käsitteet

Työn keskeisiä käsitteitä ovat kybertoimintaympäristö, kyberturvallisuus, kyberuhka, kyberrikollisuus, kyberhyökkäys, kyberoperaatio, kybersodankäynti ja attribuutio. Etuliitteenä ja määreenä käytettävän kyber-sanan määrittely ja sen historian tunteminen auttaa ymmärtämään sanasta juontuvia käsitteitä. Kyberkäsitteelle ei ole olemassa yhtä vakiintunutta yleisesti hyväksyttyä määritelmää. Termin on sanottu useissa eri läheteissä saaneen alkunsa kreikan kielen sanasta kybereo, mikä tarkoittaa ohjaamista, opastamista ja hallitsemista. Termin uskotaan tulleen ensimmäisen kerran laajempaan käyttöön vuonna 1948 yhdysvaltalaisen matemaatikon Norbert Wienerin luomassa teoriassa kommunikoinnista ja

sen kontrolloimisesta, josta hän käytti termiä cybernetics (Etymnonline.com). Maanpuolustuskorkeakoulun laatiman oppaan (Kyberkäsikirja Puolustusvoimien henkilöstölle) mukaan kyber-sanan merkitys liittyy yleensä digitaalisessa muodossa olevan informaation käsittelyyn: tietotekniikkaan, digitaaliseen viestintään, tiedonsiirtoon, tietojärjestelmiin tai tietokonejärjestelmiin. Oppaan määritelmän mukaan vasta koko yhdyssanalla voidaan ajatella olevan oma merkityksensä, ja kyber-etuliitteen avulla mikä tahansa fyysisen maailman toiminto voidaan liittää ihmisen luomaan digitaaliseen toimintaympäristöön (Laari ym., 2019).

Kybertoimintaympäristö tarkoittaa yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaa toimintaympäristöä (Turvallisuuskomitea, 2018). Suomen Ulkoministeriö määrittelee kybertoimintaympäristön seuraavasti: ”Kybertoimintaympäristöllä tarkoitetaan ihmisten luomaa digitaalista rinnakkaistodellisuutta, joka maailmanlaajuisesti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta toisiinsa ihmisiä ja laitteita valtioiden rajojen yli” (Ulkoministeriö).

Kyberturvallisuudesta ei ilmeisesti ole yhtä vakiintunutta käsitettä. Turvallisuuskomitean Kyberturvallisuuden sanaston määrittelyn mukaan se on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. (Turvallisuuskomitea, 2018). Euroopan parlamentin mukaan se tarkoitta tieto- ja viestintäjärjestelmien suojaamista, tuotannon tietoturvaa ja digitaalisten järjestelmien suojaamiseen tarvittavia alustoja (Euroopan Parlamentti, 2022). Sisäministeriö määrittelee kyberturvallisuuden yhdeksi kansallisen turvallisuuden tavoitetiloista, tarkoituksenaan suojata digitalisoituvaa yhteiskuntaa ja sen toimintakykyä vihamieliseltä kybervaikuttamiselta ja tietoverkkotiedustelulta.

Kyberuhalla tarkoitetaan Turvallisuuskomitean yllä mainitun Kyberturvallisuuden sanaston määritelmän mukaan mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon. Yhdysvaltalaisen tietoturva-alalla maailmanlaajuisesti tunnistetun ja arvostetun NIST-organisaation (National Institute of Standards and Technology) määritelmän mukaan kyberuhka on mikä tahansa olosuhde tai tapahtuma, joka voi mahdollisesti vaikuttaa haitallisesti organisaation toimintoihin, maineeseen, suojattavaan omaisuuteen tai sen henkilöstöön, ja joka aiheutuu luvattomasta sisäänpääsystä tietojärjestelmiin, tiedon tuhoamisesta, luvattomasta jakamisesta, muokkaamisesta tai palvelun estämisestä (NIST).

Kyberrikollisuus eli tietotekniikkarikollisuus tarkoittaa tietotekniikkaan tai tietoverkkoihin kohdistuvia rikoksia tai tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtäviä rikoksia (Sisäministeriö). Rikollista toimintaa tietoverkoissa on esimerkiksi haittaohjelmien tartuttaminen, hakkerointi ja palvelunestohyökkäykset. Sisäministeriön mukaan tyypillisimpiä rikoksia ovat omaisuusrikokset, joissa eri tavoin huijaamalla pyritään tavoittelemaan taloudellista hyötyä. Kyberrikollisuus on kansainvälinen ongelma ja usein kyberrikollista toimintaa tehdään yli rajojen (Sisäministeriö).

Kyberhyökkäyksiksi kutsutaan suomalaisen tietoturvayrityksen mukaan laajaa kirjoa erilaisia tapoja, joilla pyritään muun muassa lamauttamaan tietojärjestelmiä, varastamaan tietoja tai muuten vain tekemään haittaa (F-Secure). Aiemmin mainittu yhdysvaltalainen tietoturvaorganisaatio NIST määrittelee kyberhyökkäykset haitalliseksi toiminnaksi, jossa yritetään kerätä, häiritä, tuhota, muokata tai vuotaa tietojärjestelmäresursseja tai tietoa itseään (NIST).

Kyberoperaatioksi kutsutaan kybertoimintaympäristössä tai sen avulla tapahtuvaa suunnitelmallista toimintojen kokonaisuutta, jossa pyritään vaikuttamaan kohteen toimintaan (Laari, 2019). Yhdysvaltalainen The National Initiative for Cybersecurity Careers and Studies (NICCS) määrittelee kyberoperaatiot puolustukselliseksi toiminnaksi, jonka avulla kerätään todisteita rikollisesta toiminnasta tai muiden valtioiden tekemästä tiedostelutoiminnasta tarkoituksena suojautua joko reaaliaikaiselta tai mahdollisesti tulevalta uhkalta kuten vakoilulta, sisäpiiriuhkilta, ja kansainvälisiltä terroriteoilta (NICCS).

Kybersodankäynti on tietoverkkoja ja niiden haavoittuvuuksia hyödyntävä, valtioiden välinen vihamielinen toiminta (Turvallisuuskomitea, 2018). Turvallisuuskomitean julkaisema sanasto tunnistaa ja mainitsee termin määrittelyn ongelmallisuuden, koska sotaa ei voi rajata vain yhteen toimintaympäristöön. Rand-ajatushautomo kuvaa kybersodankäynnin joko valtioiden tai kansainvälisten järjestöjen toiminnaksi, jossa on tarkoituksena vahingoittaa toisen valtion tietoverkkoja tai päätelaitteita virusten tai palvelunestohyökkäysten avulla. (RAND, 2022). Tietoturva-asiantuntijan ja alan tunnetun vaikuttajan ja puhujan Mikko Hyppösen mukaan kybersodan määritelmästä tullaan kinastelemaan vielä pitkään akateemisissa konferensseissa. Hän sanoo, että kyberaseen määritteleminen on helpompaa; se on valtiollisen tahon kehittämä ja hyökkäyskäyttöön tarkoitettu haitallinen ohjelma. Kyberaseita voidaan käyttää sodankäynnissä, kuten Venäjän ja Ukrainan konfliktissa vuodesta 2014 eteenpäin, mutta kyberaseen käyttö ei vaadi varsinaista sotaa. Niitä voidaan käyttää myös vakoilussa tai sabotaasissa (Mikko Hyppönen, 2021).

Attribuutio eli vastuullistaminen tai syyksi lukeminen on moniulotteinen käsite, jolla valtiollisesta vihamielisestä kybertoiminnasta (kybervakoilu ja -vaikuttaminen) puhuttaessa tarkoitetaan yhtäältä vastuussa olevan valtiollisen tahon tunnistamista koskevaa prosessia ja toisaalta sen pohjalta vastatoimena tehtyä julkista attribuutiota (Valtioneuvosto, 2023). Kyberhyökkäysten yhteydessä puhutaan usein attribuutio-ongelmasta. Attribuutiota ja siihen liittyviä ongelmia käsitellään luvussa 4.6.

2 TUTKIMUSMENETELMÄT, TUTKIMUKSEN RAKENNE JA SISÄLTÖ

Tämä pro gradu -työ on kvalitatiivinen eli laadullinen sisältöanalyysi, jossa tiedonkeruumenetelmänä on julkaistu tietoaineisto. Aineiston analyysimenetelmänä on sisältöanalyysi. Tutkimuksen rakenne koostuu johdanto-osuudesta, kirjallisuuskatsauksesta, analyysiosuudesta ja yhteenveto-osuudesta.

2.1 Aineistonkeruumenetelmänä julkaistu tietoaineisto

Laadullisessa tutkimuksessa aineistonkeruusuunnitelman tekeminen ei ole välttämätöntä. Tätäkään työtä varten ei tehty erillistä aineistonkeruusuunnitelmaa. Aineistoa lähdettiin koostamaan pääosin sähköisistä lähteistä, sekä hakukonetoimintoja kuten Google ja Google Scholar käyttämällä oman tiedon lisäksi kyberturvallisuusalan tehtävissä toimivilta kollegoilta ja tuttavilta kysymällä. Ensin kerättiin laaja määrä erilaisia lähteitä ja talletettiin linkit kirjanmerkeiksi selaimeen sekä Elsevier-yhtiön Mendeley-viitteidenhallintatyökaluun. Raakadataa, tiedonkeruuta, ideoita ja taulukointia varten luotiin erillinen Word-tiedosto, josta olennainen tieto siirretään pro gradu -työn loppuraporttiin.

2.2 Analyysimenetelmänä sisältöanalyysi

Sisältöanalyysiä voidaan tehdä kolmesta eri näkökulmasta: analyysi voi olla aineistolähtöistä, teorialähtöistä tai teoriaohjaavaa. (Tuomi & Sarajärvi, 2009). Tähän työhän sovelletaan ensin mainittua eli aineistolähteistä sisältöanalyysia. Työssä on käytetty kuitenkin sekä induktiivista (aineistolähtöistä) että deduktiivista (teorialähtöistä) päättelyä, sillä huolimatta siitä, että käsiteltävä aihe on tuore, ja tutkimuskysymykset muokkaantuivat aineistoon tutustumisen perusteella, oli ymmärrettävä laajasti aiheesta sekä tilannekuvaa että jo julkaistua ja

tiedettyä tietoa. Eri tekijöiden tutkimusoppaissa muistutetaankin siitä, että analyysi ei voi koskaan olla täysin puhtaasti pelkästään aineistolähtöistä, sillä tutkimusta ei voi edistää ymmärtämättä sen perusteoriaa.

Käytetyn menetelmän riskejä voivat olla muun muassa aineiston validius ja kuten yleensäkin laadullisessa tutkimuksessa, tutkijan subjektiivinen tulkinta. Nämä riskit on tutkijan toimesta tiedostettu, ja työssä on huomioitu lähdekritiikki ja hyvä tutkimusetiikka. Työssä pyritään arvioimaan myös reliabiliteettia ja validiteettia laadulliseen työhön soveltuvalla tavalla. Laadullisen tutkimuksen luotettavuutta voi pohtia ja arvioida esimerkiksi uskottavuuden, vastaavuuden, siirrettävyyden, varmuuden, riippuvuuden, vahvistettavuuden, vahvistuvuuden ja puolueettomuuden käsitteiden kautta (Tuomi & Sarajärvi, 2011).

2.3 Aiempi tutkimus aiheesta

Täysin vastaavaa tutkimustyötä kyseisellä aikajaksolla tehtyihin kyberhyökkäyksiin liittyen ei ole Suomessa tehty, vaikkakin kyberhyökkäyksiä on tutkittu muutoin eri näkökulmista. Venäjän informaatio-operaatioista ja ns. APT-hyökkäyksistä on jo aiempaa tutkimusta, muun muassa opinnäytetöitä, myös vuoden 2014 Krimin valloituksen ajoilta. Jyväskylän yliopistolle on tehty useita pro gradu -töitä kohdennetuista hyökkäyksistä ja niin kutsutuista APT-hyökkäyksistä: Veikko Siukosen työ vuodelta 2019 tutkii APT-operaation inhimillisiä tekijöitä ja Rasmus Huhdan työ (2021) Venäjän federaation tapoja suorittaa hyökkäyksellisiä kyberoperaatioita vuosien 2007–2020 aikana. Myös käyttörajoitettuja tutkimuksia, joita tätä työtä varten ei ole kyetty tarkastelemaan, löytyy useampia; mm Jari Bundan vuonna 2020 tekemä työ ”APT 28 – tapaustutkimus Venäjään yhdistettyjen kyberoperaatioiden kehittymisestä vuosina 2007–2016” sekä Jyrki Karsikkaan vuonna 2021 valmistunut työ ”Monitapaustutkimus Kiinaan ja Venäjään liitetyistä kyberhyökkäyksistä: kohdennetut haittaohjelmahyökkäykset”. Nella Mäntyniemi on tehnyt joulukuussa 2022 Tampereen Yliopistolle kandidaatintutkielman nimeltä ”Venäjän kyberhyökkäykset Ukrainaa vastaan – Vuodesta 2014 helmikuuhun 2022”. Valtiollisten toimijoiden tekemistä kyberoperaatioita ja niihin liittyviä kyberoperaatiota, erityisesti sotilaallisesta näkökulmasta, on tutkittu useiden Maanpuolustuskorkeakoulun tutkijoiden tai pro gradu -töiden tekijöiden toimesta vuosien varrella.

Kansainvälistä tutkimusta kyberhyökkäyksistä löytyy enemmän; mutta tutkimustyön aineistonkeruuvaiheessa ilmeni, että nämä tutkimukset ovat joko yleisesti ilmiöitä selittäviä tai toisaalta tarkasti tiettyyn näkökulmaan, tapahtumaan tai vuoteen rajattuja. Tässä työssä aiottua aikajaksoa (2022, kevyesti taustoitettuna myös ajanjakso 2014–2022) ja kyberhyökkäysten muuttumista tämän tutkimuksen rajausten mukaisesti ei ilmeisesti ole lainkaan tutkittu. Esimerkkejä laajemmista kyberhyökkäyksiä selvittävistä tutkimuksista on esimerkiksi Kiinassa vuonna 2021 Yuchong Lin ja Qinghui Liun tutkimus ”A comprehensive review study of cyberattacks and cybersecurity; emerging trends and recent

developments", sekä vuonna 2015 Romaniassa Andrei Bendovschin tutkimus "Cyber-attacks – trends, patterns and security countermeasures".

Attribuutiota, etenkin sen vahvistamisen vaikeuden näkökulmasta, on tutkittu jo melko paljonkin maailmalla. Thomas Rid ja Ben Buchanan toivat tämän ilmi vuonna 2014 tutkimuksessa nimeltä Attributing cyber attacks sekä vuonna 2018 tutkimuksessa nimeltä Artificial intelligence tools for cyber attribution (Nunes ym, 2018). Suomessa Eveliina Hannikainen on tehnyt vuonna 2021 Helsingin yliopistolle pro gradu -työn aiheesta nimellä "Kuka nimeää kyberhyökkääjän? Strategiset narratiivit tiedustelupalveluiden julkisissa kyberattribuutioissa".

2.4 Pääasialliset lähteet

Tärkeimpinä lähteinä sekä koottuina resursseina alkuperäislähteisiin käytetään muun muassa seuraavia lähteitä, jotka esitellään lyhyesti alempana:

- CyberPeace Institute
- ENISA (Euroopan Unionin Kyberturvallisuusvirasto)
- World Economic Forum
- CSIS (Center for strategic & international studies)
- CHECKPOINT
- MITRE ATT&CK
- Kyberturvallisuuskeskus
- Uutistoimistojen materiaali
- Viron, Latvian, Liettuan ja Puolan CERT ja muut kansalliset lähteet

CyberPeace Institute -niminen organisaatio kerää ja analysoi Ukrainan sodan aikaisia, pääasiassa siviilikohteisiin tehtyjä kyberhyökkäyksiä ja niiden haitallisia vaikutuksia, alkaen tammikuusta 2022. Organisaatio on perustettu Genevessä Sveitsissä 2019 tarkoituksenaan rajoittaa kyberhyökkäysten haittoja ja avustaa haavoittuvia yhteisöjä ja edistää vastuullista toimintaa. Se keskittyy seuraamaan kyberhyökkäysten haitallisia vaikutuksia siviileille pyrkiäkseen « kyberrauhaan » (CyberPeace Institute, 2022). Sen seurantaportaalista voi seurata muun muassa hyökkäysten lukumäärää, esiintymisajankohtaa ja tyyppiä. Hakuja voi tehdä keskittymällä kohdeorganisaaton toimintasektoriin, tiettyihin valtioihin tai maanosaan, hyökkäyksen vaikutukseen, hyökkäystyyppeihin tai hyökkäävään tahoon, mikäli tämä on tiedossa. CyberPeace Institute kerää tietonsa koosteitaan ja seurantaansa varten muun muassa uutistoimistoilta, hallituksilta, CERT-toimijoilta, kyberturvallisuuden parissa toimivien yritysten ja julkisten organisaatioiden raporteista, blogeista ja tiedotteista sekä myös sosiaalisen median sisällöistä (CyberPeace Institute, 2022).

ENISA on Euroopan Unionin Kyberturvallisuusvirasto, jonka tavoitteena on saavuttaa korkea yhteinen kyberturvallisuuden taso koko Euroopassa. ENISA edistää EU:n kyberpolitiikkaa ja laatii kyberturvallisuuden sertifiointijärjestelmiä.

Virasto tekee yhteistyötä EU-maiden ja -elinten kanssa ja auttaa valmistautumaan tuleviin kyberhaasteisiin (ENISA, 2021).

World Economic Forum eli Maailman talousfoorumi kokoaa vuosittain Davosiin korkean tason päätöksentekijöitä sekä julkiselta että yksityissektorilta ympäri maailmaa. Tätä työtä varten on tutustuttu foorumin internetsivuston kyberturvallisuusosioon ja foorumin julkaisemiin Global Risk Report -raportteihin.

CSIS (Center for Strategic & International Studies) on puolueeton voittoa tavoittelematon järjestö, jonka pääkonttori sijaitsee Washingtonissa (CSIS, 2022). Se tutkii ja julkaisee analyysejä liittyen muun muassa talouden ja kansainvälisen kaupan, teknologian, politiikan ja turvallisuuden aihepiireihin.

MITRE ATT&CK on maailmanlaajuisesti vapaasti saatavilla oleva tietokanta, jota voidaan käyttää muun muassa luokittelemaan ja tunnistamaan kyberhyökkääjien tekniikoita ja taktiikoita. Tietokannan tiedot perustuvat tosielämän havaintoihin (MITRE ATT&CK®). Tietokanta on kyberturvallisuuden ammattilaisten laajalti tuntema ja käyttämä.

CHECKPOINT on johtava kyberturvallisuusratkaisujen, muun muassa palomuurituotteiden toimittaja. Yritys julkaisee Cyber Attack Trends Mid-Year Report -nimisiä raportteja

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta ja tuottaa tietoturvallisuuden tilannekuvaa (Kyberturvallisuuskeskus).

RIA (Riigi Infosüsteemi Amet) on Viron tietojärjestelmäviranomainen, jonka alaisuudessa toimii myös Viron tietoliikenneverkoissa tapahtuvien kyberturvallisuustapahtumien käsittelystä vastaava organisaatio nimeltä CERT-EE (RIA).

3 KYBERUHAT

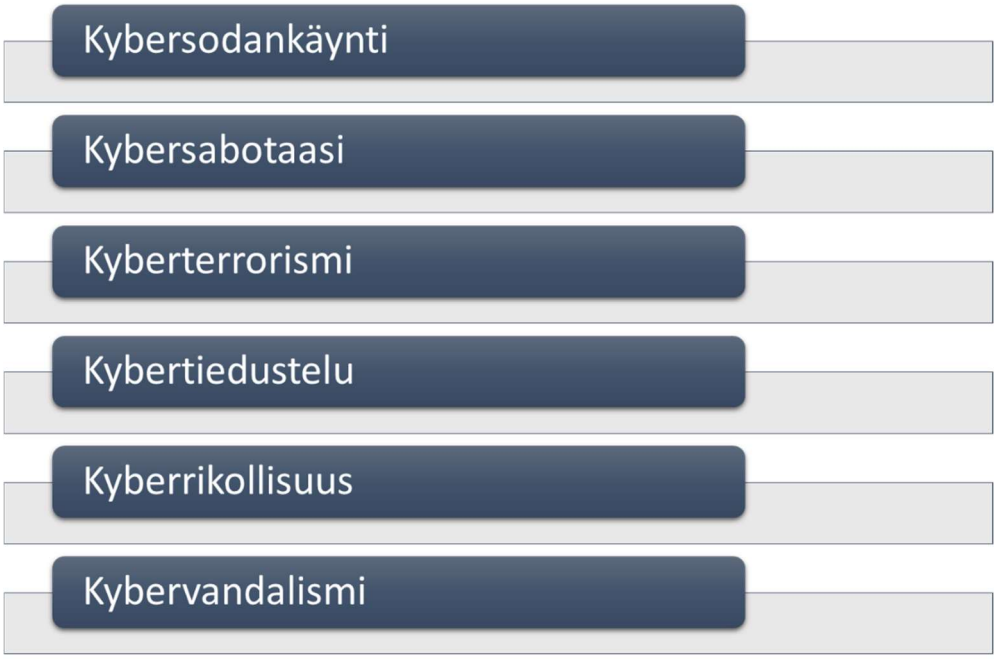
Kybertoimintaympäristössä toimimiseen liittyy erilaisia uhkia, joista kyberuhat ovat kenties merkittävimpiä maailman digitalisoitumisen myötä. Kyberuhalla tarkoitetaan mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon (Turvallisuuskomitea, 2018). Kyberuhkat voivat kohdistua yhteiskunnan elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria tai kansalaisia vastaan joko suoraan tai välillisesti (Lehto, 2021).

3.1 Kyberuhkien luokittelua

Yhdysvaltalainen tietoturvatuotteita valmistava ja markkinoiva, globaalisti tunnettu yhtiö Checkpoint luokittelee modernissa maailmassa yrityksiä ja organisaatioita uhkaaviksi tärkeimmiksi kyberuhkiksi haittaohjelmat, perinteisen niin kutsutun social engineering -manipuloinnin, internetsovellusten haavoittuvuuksien hyväksikäytön, alihankintaketjuihin kohdistuvat hyökkäykset, palvelunestohyökkäykset ja man-in-the-middle – eli väliintulohyökkäykset (Check Point Software).

Jyväskylän yliopiston Informaatioteknologian tiedekunnan ”Johdatus kyberturvallisuuteen” -kurssimateriaalin mukaan kybermaailman uhat voidaan jaotella kolmeen pääalueeseen: fyysisiin, taloudellisiin ja kyberuhkiin eli digitaalisen maailman uhkiin. Mainitut uhat voivat myös esiintyä kaikissa ulottuvuuksissa samanaikaisesti. Kyberuhat voidaan jakaa viiteen luokkaan tai tasoon: kybervandalismi, kyberrikollisuus, kybervakoilu, kyberterrorismi ja taktinen kybersota. Tämä malli pohjautuu sveitsiläisen turvallisuuteen ja riskienhallintaan keskittyvän tutkimuslaitoksen johtajan Myriam Dunn Caveltyn rakennemalliin. Jyväskylän yliopiston professori Martti Lehto on laajentanut luokittelua siten, että alla mainitut neljä luokkaa ovat samat, mutta viidenneksi luokaksi on lisätty kybersabotaasi ja kuudentena luokkana on kybersodankäynti (Lehto, 2021). Alla

olevan kuvion 1 jälkeen kuvataan kunkin kyberuhkatyypin ominaispiirteitä tarkemmin.



KUVIO 1 Kyberuhkien rakennemalli (Lehto, 2020)

Kybervandalismi tarkoittaa CyberWire-nimisen internet-julkaisun sanaston mukaan kyberhyökkäyksiä, joilla ei ole selkeää rationaalista rikollista, poliittista tai ideologista motiivia. Määrittelyn mukaan tällainen vandalismi on usein haavoittuvuuksia sisältävän internet-sivuston pilaavaa, sotkevaa tai tuhoavaa muokkaamista. Motiivina voi myös olla hyökkääjän omien taitojen esittely (CyberWire, 2019). Jyväskylän Yliopiston määritelmän mukaan kybervandalismiin kuuluu hakkerointi, haktivismi ja kyberparveilu. Kyberparveilu on toimintaa, joissa internetin ja matkapuhelinten avulla kootaan ja johdetaan usein väkivaltaisia mielenosoituksia (Jyväskylän Yliopisto, 2021).

Kyberrikollisuus eli tietotekniikkarikollisuus tarkoittaa tietotekniikkaan tai tietoverkkoihin kohdistuvia rikoksia tai tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtäviä rikoksia (Sisäministeriö). Tietoverkkorikosten yhteydessä käytetäänkin usein jakoa tietoverkkosidonnaisiin ja tietoverkkoavusteisiin rikoksiin (Poliisi). Keskusrikospoliisin määrittelyn mukaan tietoverkkosidonnaiset rikokset kohdistuvat tietoverkkoihin ja tietojärjestelmiin. Esimerkkinä näistä ovat palvelunestohyökkäykset, tietomurrot ja datavahingonteko. Tietoverkkoavusteiset rikokset ovat sellaisia rikoksia, joissa hyödynnetään tietoverkkoja tai -järjestelmiä rikoksen tekemisessä. Esimerkkejä näistä ovat petokset, huumausainerikollisuus ja rahanpesu.

Kybervakoilun avulla hankitaan ei-julkisia ja salaisia tietoja yksityistahoilta, kilpailijoilta, ryhmiltä, hallituksilta ja vastustajilta poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen laillisia tai laittomia menetelmiä

internetissä, verkoissa, ohjelmistoissa, sosiaalisessa mediassa tai laitteissa (Cyberwatch Finland & Elinkeinoelämän Keskusliitto, 2018). Kyberterrorismi on terroristista toimintaa, jossa hyökätään tietojärjestelmien kautta kansalaisia, liikeelämää, yhteiskunnan elintärkeitä toimintoja tai kriittistä infrastruktuuria tai muuta kohdetta vastaan(Turvallisuuskomitea, 2018).

Kybersabotaasi on toimintaa, jossa hyökkääjä (valtiollinen toimija tai sen tukema ryhmittymä) operoi sotaa alemmalla tasolla. Tavoitteina voivat olla epävakauden aiheuttaminen kohdemaassa, offensiivisten kyberhyökkäyskykyjen testaaminen, hybridioperaatioiden valmistelu tai sodan valmistelu (Lehto, 2021).

Kybersodankäynnille ei ole ollut täysin vakiintunutta ja yksiselitteistä määritelmää. Turvallisuuskomitean (2018) määrittelyn mukaan kybersota on tietoverkkoja ja niiden haavoittuvuuksia hyödyntävää, valtioiden välistä vihamielistä toimintaa. Martti Lehdon ja Jarno Limnellin mukaan tutkijat toivovat kybersodankäynnin määrittelyn perustuvan sodan tavoitteisiin ja motiiveihin, ei niinkään kyberoperaatioiden muotoihin (Lehto & Limnell, 2017) . Tunnettu puhuja ja tietoturva-asiantuntija Mikko Hyppönen (2022) toteaa, että kybersotaa helpompaa on määritellä kyberase, joka on valtiollisen tahon kehittämä hyökkäyskäyttöön tarkoitettu haitallinen ohjelma. Näitä aseita voidaan käyttää sodankäynnissä, mutta niiden käyttö ei vaadi varsinaista sotatilaa, vaan niitä voidaan käyttää myös vakoilun ja sabotaasin keinoina.

3.2 Ajankohtaisia kyberuhkia

Vaikka tässä tutkimuksessa perehdytäänkin rajatun ajanjakson, vuoden 2022, kyberhyökkäyksiin rajatulla maantieteellisellä alueella, on aiheen ymmärtämisen kannalta hyvä ymmärtää, minkälaisia kyberuhkia tutkimusta kirjoitettaessa globaalissa kybertoimintaympäristössä on. Euroopan parlamentti kuvaa kyberuhkia internetsivuillaan seuraavasti: ”Digitaalisten palveluiden käyttö on kasvanut jo pitkään, ja pandemian myötä etätyöskentely, verkko-ostokset ja yhteydenpito läheisiin verkon välityksellä lisääntyivät huomattavasti. Näistä palveluista voi olla hyötyä kuluttajille ja taloudelle koronapandemian jälkeisessä elpymisessä. Kuitenkin myös verkkorikollisuuden määrä on vastaavasti kasvanut. Hyökkääjät voivat käyttää urkintaan verkkosivuja tai sähköposteja, joissa on haitallisia linkkejä tai liitteitä. Tavoitteena on varastaa esimerkiksi pankkitietoja tai kiristää yhteisöitä niiden tietojärjestelmien ja datan estämisen avulla.” (Euroopan Parlamentti, 2021).

Euroopan Unionin Verkko- ja tietoturvavirasto ENISA:n tuoreen raportin mukaan suurimmat kyberuhat raportin julkaisuhetkellä ovat kiristyshaittaohjelmat, muut haittaohjelmat, ns. social engineering -uhat, tietoon kohdistuvat uhat, saatavuuteen kohdistuvat uhat (palvelunestohyökkäykset, internet-uhat), dis- ja misinformaatio ja toimitusketjuun kohdistuvat uhat (ENISA, 2022).

Euroopan parlamentti on määritellyt kahdeksan yleisintä kyberturvallisuusuhkaa vuoden 2022 aikana ja sen jälkeen. Ensimmäisenä mainitaan kiristyshaittaohjelmat, jotka ovat muuttumassa monimutkaisemmiksi. Myös vaaditut

lunnasrahasummat ovat kasvaneet. Vuonna 2021 maailmassa kiristyshaittaohjelmista aiheutui 18 miljardin euron menetykset, mikä merkitsi 57 kertaa suurempia menetyksiä kuin vuonna 2015. Toisena mainitaan muut haittaohjelmat yleisesti. Näihin kuuluvat muun muassa troijalaiset ja erilaiset vakoiluohjelmat. Kolmantena on mainittu käyttäjien manipulointi ja tietojen hankkiminen inhimillisiä virheitä hyödyntämällä, mikä käytännössä tarkoittaa useimmiten erilaisia tietojenkalastelukampanjoita muun muassa sähköpostin ja tekstiviestien välityksellä. Neljältä uhkana Euroopan parlamentti listasi erilaiset dataan liittyvät uhat, joiden tarkoituksena on tietojen luvaton käyttö ja/tai paljastaminen tai julkaiseminen. Tällaisia uhkia ovat esimerkiksi tietoturvaloukkaukset, joita rikolliset tahot toteuttavat muun muassa kyberhyökkäysten muodossa, sekä tietovuodot, joissa luottamuksellinen tieto leviää tahattomasti. Viidentenä listalla ovat palvelunestohyökkäykset ja muut tiedon tai palvelujen saatavuuteen ja käytettävyyteen liittyvät uhkat. Kuudentena mainitaan saatavuuteen liittyvät sellaiset uhat, joissa haittaa aiheuttavalla taholla on tarkoituksena internet-infrastruktuurin tuhoaminen ja fyysinen haltuunotto. Seitsemänneksi uhkaksi mainitaan dis- ja misinformaatio, eli harhaanjohtavan tiedon levittäminen. Tällaista tietoa levitetään erityisesti sosiaalisen median palveluiden välityksellä. Viimeisenä mainitaan niin kutsutut toimitusketjuhyökkäykset, mikä tarkoittaa sitä, että hyökkäyksen kohteena olevan organisaation itsensä lisäksi kohteena on myös sen asiakas- tai yhteistyö- ja toimittajakumppaneita. Hyökkäyksissä käytetään hyväksi esimerkiksi useiden toimittajien alihankintaketjuja, joissa päävastuussa olevan organisaation on hankalampi kontrolloida kaikkea ketjuissa tapahtuvaa toimintaa ja tietoliikennettä (Euroopan parlamentti, 2022).

4 KYBERHYÖKKÄYKSET

Kyberhyökkäykset ovat haitallista toimintaa, jossa yritetään kerätä, häiritä, tuhota, muokata tai vuotaa tietojärjestelmäresursseja tai tietoa itseään (NIST). Kyberhyökkäyksiksi kutsutaan Suomalaisen tietoturvayrityksen F-Securen mukaan laajaa kirjoa erilaisia tapoja, joilla pyritään muun muassa lamauttamaan tietojärjestelmiä, varastamaan tietoja tai muuten vain tekemään haittaa. Hyökkääjät käyttävät hyväkseen organisaatioiden hyökkäyspinta-alaa ja toteuttavat hyökkäyksiä hyökkäysvektoreiksi kutsuttujen ”reittien” avulla. Alla kuvataan lyhyesti näiden käsitteiden merkitys.

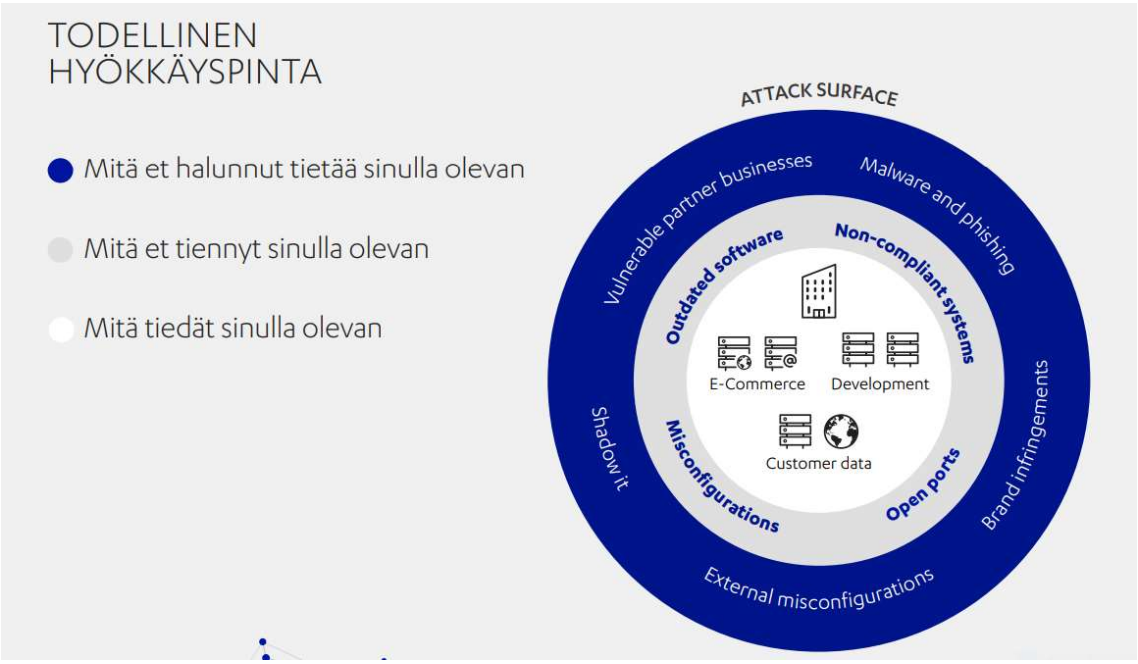
Isossa-Britanniassa toimiva National Cyber Security Center, NCSC.GOV.UK, jakaa kyberhyökkäykset kohdistettuihin ja ei-kohdistettuihin hyökkäyksiin. Ei-kohdistetuilla hyökkäyksillä pyritään tekemään hyökkäyksiä massana mahdollisimman monia, mahdollisia haavoittuvuuksia sisältäviä kohteita (käyttäjät, laitteet, palvelut) vastaan, ja käyttävät hyväkseen internetin avoimuutta. Tällaiset hyökkäykset toteutetaan erimerkiksi tietojenkalastelun avulla ti houkuttelemalla käyttäjä jollekin luotetuksi tunnetulle verkkosivulle, jonne on sijoitettu haitallista sisältöä (niin kutsuttu watering hole -taktiikka). Kohdistetut hyökkäykset kohdistetaan tiettyihin ennalta määriteltyihin tahoihin, usein siksi, että kyseistä organisaatiota tai yksittäistä tahoa vastaan kohdistuu jokin hyökkäävän tahon oma intressi, tai hyökkääjälle voidaan maksaa kohdistetusta hyökkäyksestä. Kohdistetut hyökkäykset ovat usein ei-kohdistettuja hyökkäyksiä tuhoisampia, sillä ne on suunniteltu juuri kyseistä tahoa vastaan (NCSC.GOV.UK,). Näitä hyökkäyksiä toteutetaan muun muassa kohdennetulla tietojenkalastelulla (englanniksi spear phishing), jossa tietylle yhdelle tai useammalle kohdehenkilölle lähetetään sähköpostiviesti, joka sisältää haitallisen linkin tai liitteen. Usein nämä henkilöt ovat kohdeorganisaatiossa vastuutehtävissä olevia. (F-Secure).

Viime vuosina tietoturva-alalla tiheästi mediassakin esiintynyt käsite ”APT-hyökkäys”, Advanced Persistent Threat, tarkoittaa tiettyyn toimijaan kohdistettua tietoturvaloukkausta, jossa huomioidaan kohteen erityispiirteet ja hyödynnetään tunnettuja haavoittuvuuksia, jonka kautta saadaan asennettua kohdennettu haittaohjelma (Kyberturvallisuuskeskus, 2014). Tällaiset hyökkäykset ovat useimmiten hyvin suunniteltuja, pitkäkestoisia, ja niissä hyökkääjä

pyrkii ”piileksimään” uhriorganisaation tietoverkossa mahdollisimman pitkään jäämättä kiinni ja peittämään jälkensä. Nämä hyökkäykset voivat olla erityisen haitallisia, koska niitä on vaikea nopeasti havaita ja koska ne usein kohdistuvat tärkeisiin yhteiskunnallisiin toimintoihin, kuten valtionhallintoon, viranomaistoimintaan ja terveydenhuoltoon sekä merkittäviin kasvu- ja teollisuusyrityksiin (Blue Team Builders, 2021). Nyt jo tunnettuja esimerkkejä APT-hyökkäyksistä ovat Suomen eduskuntaa vastaan kohdistettu, vuonna 2020 löydetty pitkään kestänyt hyökkäys, ja vuonna 2010 havaittu, alun perin Iranin ydinlaitoksia vastaan kehitetty Stuxnet-nimen saaneen haittaohjelman avulla toteutettu hyökkäys.

4.1 Hyökkäyspinta(-ala) ja hyökkäysvektorit

Tietoturva-alalla puhutaan paljon siitä, että kyberhyökkäysten estämiseksi tulisi rajoittaa hyökkäyspinta-alaa. Hyökkäyspinnaksi tai hyökkäyspinta-alaksi voidaan katsoa kaikki Internetiin näkyvät tietojärjestelmät, niissä avoinna olevat tietoliikenneportit ja tietojärjestelmän tarjoavat palvelut (Nixu OYJ, 2014). F-Securen mukaan organisaation hyökkäyspinta-ala kattaa kaikki sisäisen verkkoinfrastruktuurin laitteet, ohjelmistot ja sovellukset sekä internetiin päin näkyvät järjestelmät. Joissakin organisaatioissa ongelmana on se, ettei tunneta omaa järjestelmä- tai kyberarkkitehtuuria riittävästi; tästä esimerkkinä suomalaisen tietoturvayhtiön F-Securen kuva todellisesta hyökkäyspinta-alasta (Kuvio 2).



KUVIO 2 Todellinen hyökkäyspinta-ala, esimerkki (F-Secure)

Hyökkäysvektori on eräänlainen reitti haavoittuvuuden hyödyntämiseksi; se tekijä, joka mahdollistaa tietojärjestelmässä olevan haavoittuvuuden hyväksikäytön (Nixu OYJ, 2014). Tämä reitti voi olla esimerkiksi sähköposti tai USB-tikku.

Marraskuussa 2022 Microsoft varoitti, että päivittämättömät verkkolaitteet ovat hyökkäysvektori energiasektorin kimppuun (Mikrobitti. 2022).

4.2 Toimijat (tekijät ja kohteet) ja motiivit

Kyberhyökkäysten tekijät luokitellaan usein seuraaviin pääryhmiin: valtiolliset tai valtioiden tukemat toimijat, kyberrikolliset, palkatut ostopalveluina hyökkäyksiä tekevät hakkeritoimijat, niin kutsutut haktivistit sekä yksityiset toimijat. Kyberhyökkäysten tekijöiden tavoitteena voi olla taloudellinen hyöty, jokin poliittinen, sotilaallinen tai yhteiskunnallinen motiivi, maineen tai kunnian hankkiminen ja omien taitojen näyttäminen, tai pelkästään kohteen toiminnan häirintä tai pelottelu.

Kyberhyökkäysten kohteena voivat olla yksityishenkilöt, yritykset, organisaatiot tai jopa kokonaiset valtiot. Hyökkäysten toteuttajina voi olla monenlaisia toimijoita: yksittäinen hakkeri, haktivisti, hakkeri- tai haktivistiryhmä, maksettua palvelua tuottava rikollinen tai jokin valtiollinen taho.

Jyväskylän Yliopiston ja MPK:n (Maanpuolustuskoulutusyhdistys) Kansalaisen Kyberturvallisuuskurssin materiaalissa on kuvattu kyberhyökkääjiä seuraavasti: Yksityiset toimijat ovat henkilöitä tai tahoja, jotka motivoituvat tekemään kyberhyökkäyksiä esimerkiksi kokeilunhalun, koston tai oman edun tavoittelun vuoksi. Haktivistit lähtevät toimimaan yleensä vakaumuksensa pohjalta, joka voi olla aatteellinen tai poliittinen. Kyberterroristit puolestaan pyrkivät edistämään jotakin poliittista, usein ääriajatteluun perustuvaa asiaa levittämällä kauhua ja pelkoa. Kyberrikolliset, jotka voivat olla sekä yksittäisiä henkilöitä että järjestöjä, ryhmiä tai jopa yrityksiä, tavoittelevat erilaisia taloudellisia tai muita hyötyjä rikollisella toiminnallaan. Valtiolliset toimijat useimmiten haluavat vaikuttaa tai sekaantua kohdemaan poliittiseen toimintaan, mutta useimmiten käyttävät välitoimijoita, esimerkiksi hakkeriryhmiä, joille maksetaan työstä. Tarkoituksena valtiollisilla toimijoilla voi myös olla kyberhyökkäysten käyttäminen osana vakoilua tai sotilaallisia toimia (Jyväskylän Yliopisto & MPK, 2023)

Hyökkäävien tahojen motiivit ovat tietotekniikkayhtiö IBM:n jaottelun mukaan usein joko rikollisia, poliittisia, tai henkilökohtaisia. Tämän määrittelyn mukaan rikollisin tarkoituksin motivoituneet hyökkäävät tahot tavoittelevat useimmiten rahallista hyötyä varkauksien, tietovarkauksien tai liiketoiminnan häirinnän keinoin. Henkilökohtaisista motiiveista mainitaan esimerkiksi entiset pettyneet tai mielestään kaltoinkohdellut nykyiset tai entiset työntekijät, jotka voivat tavoitella joko rahallista hyötyä tai useammin pelkästään rangaistusta työnantajalleen. Sosiaalipoliittisesti tai poliittisesti motivoituneita hyökkääjiä voivat olla esimerkiksi haktivistit, jotka haluavat saada ajamilleen asioille julkista näkyvyyttä. Teollisuusvakoilu, etu saada epäreilua etua kilpailijoihin nähden, sekä pelkkä älyllinen haaste voivat myös toimia motivaattorina kyberhyökkääjälle (IBM).

4.3 Tunnistettuja kyberhyökkäyksiä tekeviä tahoja

MITRE ATT&CK® on Mitre Corporationin luoma, maailmanlaajuisesti tunnettu tietokanta, johon kerätään jatkuvasti päivittyen ajantasaista tietoa kyberhyökkäyksistä, hyökkäysten toteuttajista ja hyökkäystaktiikoista sekä -tekniikoista. Tietokannan tiedot perustuvat tosielämän havaintoihin. Tietokanta jakautuu kahteen osaan, joista toinen (Enterprise) keskittyy organisaatioiden tietoverkkoja ja pilviä vastaan kohdistuvaan toimintaan, ja toinen (Mobile) keskittyy mobiililaitteita vastaan tehtäviin hyökkäyksiin (MITRE ATT&CK®).

Mitre kerää tietoja merkittävistä, tunnistetuista kyberhyökkäyksiä tekevistä ryhmittymistä. Tällä hetkellä tietokannassa on tietoa 138 ryhmittymästä. Tietokannasta löytyi tutkijan yllätykseksi eniten kiinalaisia toimijoita (32 kpl), seuraavaksi eniten iranilaisia (14 kpl) ja vasta kolmanneksi eniten venäläisiä toimijoita (13 kpl.). On kuitenkin huomattava, että mukana oli useita toimijoita, joita ei oltu attribuoitu, mutta joiden sanottiin toimivan esimerkiksi ”Kiinan ulkopuolella” tai ”toimijat käyttävät kielenään Venäjää” tai että iskut kohdistuvat tiettyihin tahoihin tai tietyllä maantieteellisellä alueella. Myös näiden joukossa voi olla esimerkiksi venäläisiä ja kiinalaisia toimijaryhmiä. Muita aktiivisia valtioita, joista käsin toimii kyberhyökkäyksiä tekeviä ryhmittymiä, oli löydösten mukaan Pohjois-Korea ja Libanon. Lisäksi löytyi useita ryhmiä, joiden tiedettiin toimivan esimerkiksi Etelä-Aasiassa tai Lähi-Idässä. Yksittäisiä ryhmiä löytyi myös muutamia; muun muassa espanjankielisiin maihin ja tahoihin kohdistuva ryhmä, yksi portugalinkielinen ryhmä, yksi vietnamilainen ryhmä, yksi eteläamerikkalainen ryhmä, yksi eteläkorealainen ryhmä, yksi intialainen ryhmä ja muutama pakistanilainen tai pakistanilaiseksi epäilty ryhmä.

Merkittävimpiä edellä mainituista tämän tutkimuksen ja Ukraina-Venäjä-aspektin näkökannalta ovat venäläiset toimijat. Kuten nyttemmin tiedetään, Venäjällä on lukuisia aktiivisia valtiollisesti johdettuja kybertoimijoita, jotka tehtailevat kyberhyökkäyksiä. Mitre Attack- tietokanta nimeää venäläisiksi toimijoiksi seuraavanlaisia ryhmittymiä: Venäjän lukuun toimivia valtiollisia tahoja ovat sotilastiedustelupalvelu GRU:n alaisuudessa toimivat APT28 ja Sandworm, Venäjän ulkomaantiedustelupalvelu SVR:n alaisuudessa toimiva APT29 sekä Venäjän turvallisuuspalvelu FSB:n alaisuudessa toimivat ryhmät Dragonfly ja Gamaredon. Muita venäläisiä toimijoita ovat ryhmä nimeltä Ember Bear, joka todennäköisesti on alkuvuonna 2022 Ukrainaa vastaan tehtyjen tuhoisien Whisper Gate – nimellä kulkeneiden wiper-iskujen takana, venäläinen kyberrikollisryhmittymä Indrik Spider, kriittistä infrastruktuuria vastaan hyökkäyksiä tekevä TEMP.Veles, nyt jo hiukan epäaktiivisempi Turla sekä taloudellista hyötyä tavoitteleva Wizard spider.

Ryhmä nimeltä APT28 on ollut aktiivinen vuodesta 2004. Se on Venäjän sotilastiedustelun GRU:n ylimmän johdon alainen joukko; tarkemmin 85. Erikoispalvelukeskus GTsS:n sotilasyksikkö nro 26165. Ryhmä tai sen osia tunnetaan myös nimillä IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat

Group-4127 ja TG-4127. Ryhmittymä on toteuttanut vuosina 2014–2018 kyberoperaatioita useita eri yhdysvaltalaisia organisaatioita ja maailman anti-doping -toimisto WADA:a vastaan, sekä pyrki vaikuttamaan USA:n vaaleihin vuonna 2016 häiriten muun muassa Hillary Clintonin vaalikampanjaa (MITRE ATT&CK®, 2023). Ryhmittymä on ollut useiden lähteiden, muun muassa CyberPeace Instituten tietokannan perusteella, eräs aktiivisimmista kybertoimijatahoista Venäjän-Ukrainan sodassa.

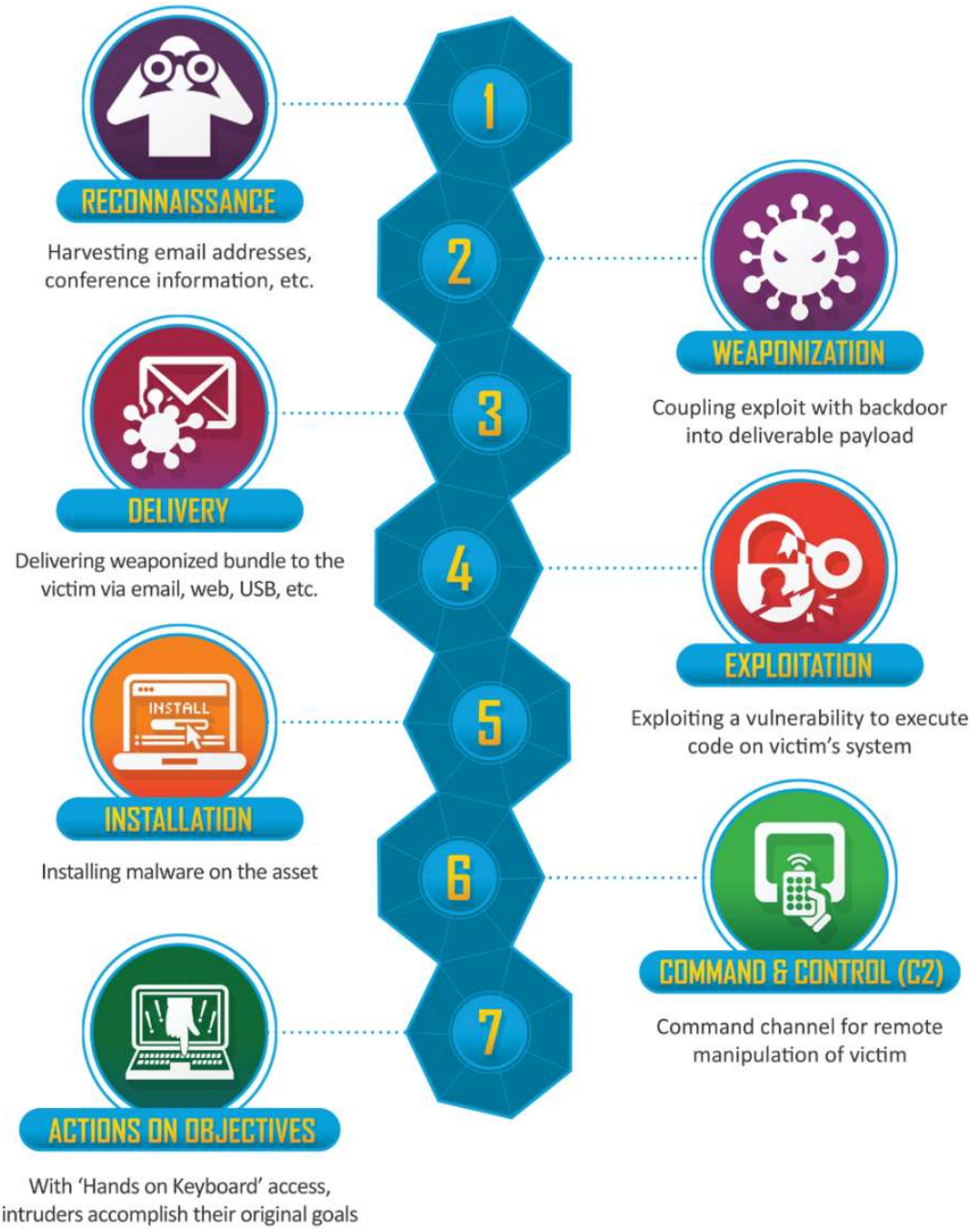
4.4 Hyökkäystavat (taktiikat)

Yllä luvussa 4.2 esitelty MITRE ATT&CK®-portaali tunnistaa ja luokittelee 14 erilaista hyökkäystaktiikkaa. Hyökkäystaktiikka käytännössä kertoo syyn, mitä hyökkääjä tavoittelee, ja minkä vuoksi toimensa suorittaa. Jokainen taktiikka voi sisältää yhden tai useampia tekniikoita, joilla teko toteutetaan. Mitren mukaan nämä 14 taktiikkaa (kuvio 3) ovat seuraavat:

1. Tiedustelu: Pyritään hankkimaan tietoa tulevaa tai tulevia operaatioita varten.
2. Resurssien valmistelu: Hankitaan ja kehitetään operaatiota varten tarvittavat resurssit.
3. Sisäänpääsy: Pyritään pääsemään kohteen tietoverkkoon sisälle.
4. Toteutus: Ajetaan tai yritetään ajaa valittu haittaohjelma kohteen tietoverkossa.
5. Sinnikkyys: Pyritään saamaan jalansijaa uhriorganisaation järjestelmissä.
6. Oikeuksien korottaminen: Pyritään saamaan korkeampia käyttäjäoikeuksia ja mahdollisesti admin- eli ylläpito-oikeuksia.
7. Puolustuksen väistö/välttely: Pyritään välttämään havaituksi ja tunnistetuksi tulemista sekä kiinni jäämistä.
8. Käyttäjätunnusten haltuun saaminen: Pyritään saamaan haltuun kohdejärjestelmän käyttäjien käyttäjätunnuksia ja salasanoja.
9. Havaitseminen: Pyritään tutustumaan tietoympäristöön, johon on päästy sisään jatkotoimien ja -päätösten vahvistamiseksi.
10. Sivuttaisliikkuminen: Pyritään liikkumaan kohdejärjestelmän sisällä. Usein pyritään myös etäohjaamaan järjestelmää.
11. Tiedonkeruu: Pyritään keräämään haluttu tieto.
12. Kaappaaminen ja haltuunotto: Pyritään hallitsemaan tietojärjestelmää ja imitoimaan sen normaalia toimintaa.
13. Tiedon varastaminen: Pyritään siirtämään tietoa järjestelmästä ulospäin hyökkääjälle itselleen.
14. Vaikuttaminen: Pyritään manipuloimaan, häiritsemään tai tuhoamaan kohteen tietoja

KUVIO 3 Mitren määrittelemät hyökkäystaktiikat (Mitre Att&ck)

Mitre ATT&CK® keskittyy toiminnassaan hyökkäystekniikoihin ja -taktiikoihin. Kyberturvallisuusmaailmassa käytetään myös termiä ”kill chain”, mikä tarkoittaa käytännössä kyberuhkien tunnistamiseen ja niiden ehkäisemiseen tarkoitettuja malleja, joiden rakenne muistuttaa Mitre Attack:n taktiikoiden kuvausta. Kill chain -termi on saanut nimensä alun perin Yhdysvaltojen asevoimien kehittämästä kill chain -mallista. Ensimmäisen virallisen mallin kehittivät yhdysvaltalainen ase-, lentokone- ja avaruusteknologiayritys Lockheed Martinin tutkijat havaitessaan kyberhyökkäysten kulun noudattavan tiettyä ”kaavaa” (IEEE Computer Society). Tämä malli on kuvattu alla kuviossa 4.



KUVIO 4 Kill chain -malli (Lockheed Martin)

4.5 Hyökkäystyypit

Erilaisia kyberhyökkäystyyppejä ovat muun muassa kiristyshaittaohjelmat, man-in-the-middle -hyökkäykset, nollapäivähaavoittuvuudet, vakoiluohjelmat, troijalaiset, tietojenkalastelu, tekstiviestihuijaukset ja huijauspuhelut ja palvelunestohyökkäykset sekä niin kutsutut wiper-haittaohjelmat (F-Secure). Alla kuvataan tarkemmin näitä hyökkäystyyppejä.

Kiristyshaittaohjelmat ovat haittaohjelmia, jotka salaavat tai manipuloivat laitteella olevia tietoja ja tyypillisesti vaativat käyttäjältä lunnaita salauksen purkamisesta(Turvallisuuskomitea, 2018). Tällainen ohjelma voi tulla käyttäjän tietokoneelle esimerkiksi sähköpostiviestin saastuneen liitetiedoston välityksellä. Mikäli viestin saaja avaa liitetiedoston, sen sisältämä haittaohjelma aktivoituu ja lataa itsensä käyttäjän tietokoneelle, jonka jälkeen se kykenee kryptaamaan eli salaamaan koneella olevia tiedostoja. Näitä salattuja tiedostoja ei saa avattua ilman hyökkääjältä pyydettävää salausavainta. Usein hyökkääjä vaatii salausavaimen antamisesta ”maksuksi” lunnaita, usein suuri summia rahaa, ja saattaa uhata julkistaa uhrin tai uhriorganisaation luottamuksellisia tietoja, mikäli lunnaita ei makseta. Lunnaiden maksaminenkaan ei kuitenkaan takaa sitä, että hyökännyt taho aikoisi purkaa salauksen ja pitää lupauksensa olla julkistamatta tietoja.

Man-in-the-middle -hyökkäykset eli väliintulohyökkäykset tai kolmas mies -hyökkäykset ovat tilanteita, joissa hyökkääjä kaappaa kahden osapuolen välisen viestinnän verkossa ja esiintyy keskustelun yhtenä osapuolena, pyrkien esimerkiksi urkkimaan salasanoja tai saamaan uhrin asentamaan haittaohjelman laitteelleen (F-Secure).

Nollapäivähaavoittuvuus on ohjelmiston haavoittuvuus, jonka hakkerit löytävät ennen kuin tuotteen toimittaja on siitä tietoinen. Koska toimittaja ei tiedä haavoittuvuudesta, siihen ei ole olemassa korjaustiedostoa, joten hyökkäykset onnistuvat todennäköisemmin. Termi "nollapäivä" viittaa siihen, että toimittaja tai kehittäjä on aivan juuri huomannut vian, eli hänellä on "nolla päivää" korjata se. Nollapäivähyökkäyksissä hyödynnetään tätä nollapäivän aukkoa vahingon tuottamiseksi tai datan varastamiseksi järjestelmästä, jossa haavoittuvuus on (Kaspersky).

Vakoiluohjelmat kykenevät seuraamaan käyttäjän toimia esimerkiksi tallentamalla tämän näppäimistön painalluksia. Tällä tavoin vakoiluohjelman avulla voidaan muun muassa varastaa tunnuksia ja salasanoja eri palveluihin ja verkkopankkiin (F-Secure).

Troijalaiset ovat haittaohjelma, jotka voivat naamioitua esimerkiksi ohjelmapäivityksiksi tai asialliselta vaikuttaviksi liitetiedostoiksi. Kun käyttäjä on huijattu lataamaan troijalaisen, se voi saastuttaa tietokoneen haittaohjelmalla, joka varastaa tietoja (Kotimikro, 2021).

Tietoturvayhtiö F-Securen (2018) mukaan tietojenkalastelu on toimintaa, jonka avulla pyritään huijaamaan hyökkäyksen uhria ja varastamaan esimerkiksi tämän käyttäjätunnukset. Kalasteluviestejä lähetetään uhreille usein sähköpostilla jonkin luotettavan ja tunnetun tahon nimissä. Esimerkiksi pankkien nimissä lähetetään tekaistuja verkkopankin salasanan vaihtopyyntöjä ja posti- ja kuriiripalvelujen nimissä tekaistuja ilmoituksia saapuvista lähetyksistä. Käyttäjän kirjoittaessa tunnukset sähköpostiviestin sisältämään kenttään tunnukset menevät rikollisen haltuun. Tietojenkalasteluhuijauksia tehdään myös tekstiviestien ja pikaviestipalveluiden avulla puhelimitse. Soittaja voi esiintyä esimerkiksi kohdeorganisaation it-tuen edustajana ja pyytää saada tutkia etäyhteyden avulla tietokoneen tekaistuja ongelmia.

Palvelunestohyökkäykset eli DoS (Denial of Service) -hyökkäykset ovat tietoverkkohyökkäyksiä, jolla estetään verkkopalvelun normaali käyttö kohdistamalla verkkopalveluun niin paljon liikennettä, ettei se kykene palvelemaan asiakkaitaan. Hyökkäykset voivat olla hajautettuja tai kohdennettuja. Hajautetut hyökkäykset (niin kutsutut DDoS- eli Distributed Denial of Service -hyökkäykset) voivat perustua useisiin hyökkääjän hallitsemiin laitteisiin eli ”botteihin”, jotka lähettävät uhripalveluun tietoliikennetulvan. Kohdennettu hyökkäys perustuu uhripalvelussa olevan haavoittuvuuden hyödyntämiseen. Uhrin palveluun lähetetään tietoliikennepaketti, jolla aiheutetaan toiminnan lamauttava häiriötila. Palvelunestohyökkäykset eivät poista tai tuhoa tietoa, niillä pyritään lähinnä häiritsemään ja lamauttamaan normaaleja verkkopalvelutoimintoja tilapäisesti. (Poliisi)

Wiper-haittaohjelmat nimensä mukaisesti pyyhkivät eli poistavat lopullisesti tiedostoja ja ovat sen vuoksi erityisen haitallisia. Kyberturvapalveluja tarjoavan Fortinet-yhtiön määrittelyn mukaan wiper-haittaohjelman nimen mukaisesti sen päätoiminto on pyyhkiä eli poistaa uhrin tietokoneen kovalevy, eli haittaohjelman tarkoituksena on tuhota tietoa (Fortinet, 2022). Wiper-haittaohjelmia käyttävät hyökkäykset ovat yleistyneet Venäjän-Ukrainan sodan aikana merkittävästi. Aikaisemminkin, 2010-luvulla, niitä on jonkin verran käytetty, mutta harvemmin. Iranissa laajalti tunnettua Stuxnet-tapausta tutkittaessa havaittiin, että Iranin öljyteollisuussektoria vastaan hyökättiin huhtikuussa 2012 ennestään melko tuntemattomalla wiper-tyypin haittaohjelmalla (Wired, 2012). Maailmanlaajuisesti tunnetuksi tullut NotPetya-haittaohjelma on ollut tähän mennessä tuhoisin wiper-haittaohjelma. Sillä hyökättiin alun perin vuonna 2017 ukrainalaisia tahoja vastaan.

4.6 Attribuutioon liittyvät ongelmakohdat

Kyberhyökkäyksen tai hyökkäyksellisen kyberoperaation tekijän tunnistaminen ja sitä kautta vastuuseen saattaminen eli attribuutio on usein vaikeaa. Tätä ongelmaa kutsutaan attribuutio-ongelmaksi. Terminä attribuutio tässä kontekstissa tarkoittaa Turvallisuuskomitean Kyberturvallisuussanaston määritelmän mukaan attribuutio on hyökkäyksellisen kyberoperaation toteuttajan tunnistamista, paikantamista ja tarvittaessa oikeudelliseen vastuuseen saattamista (Turvallisuuskomitea, 2018). Käytännössä tämä tarkoittaa yksinkertaistettuna useimmiten hyökkääjän julkista nimeämistä.

Kaspersky-tietoturvayhtiö Kwiatkovskin ja kumppaneiden (2021) mukaan kyberhyökkäysten attribuonnissa on kolme aspektia: tekninen, juridinen ja poliittinen. Teknisellä attribuoinnilla viitataan sen tutkimiseen, kuka tai mikä taho on ollut hyökkäyksen tekijä teknisen analyysin perusteella, juridinen attribuointi selvittää muun muassa, onko rikottu kansainvälisiä lakeja tarkoituksenaan saada tekijä vastuuseen, ja poliittinen attribuointi tarkoittaa sitä, että edellä mainitut arvioinnin tulokset ilmoitetaan joko julkisesti tai yksityisesti ja ne kytketään tiettyyn valtioon tai yksityiseen toimijaan (Kwiatkovski ym, 2021).

CyberPeace Institute käyttää seurannassaan nelijakoista attribuutiota. Teknisen, juridisen ja poliittisen attribuution lisäksi mainitaan neljäntenä luokkana itseattribuutio, jossa termin mukaisesti hyökkäyksen tehnyt taho itse ilmoittautuu vastuulliseksi hyökkäyksestä.

Attribuutio-ongelma johtuu muun muassa siitä, että usein hyökkäävä taho käyttää kaapattuja tietokoneita, palvelimia ja muita verkkoon kytkettyjä laitteita ja pyrkii myös hävittämään eri keinoin digitaaliset jälkensä mahdollisimman tehokkaasti (Lehto, 2021). Hyökkääjän tunnistaminen ja osoittaminen on luonnollisesti tärkeää tapauksista oppimisen ja varautumisen kehittämisen vuoksi, mutta myös laajempien yhteiskunnallisten vaikutusten valossa. Läntisten tiedusteluorganisaatioiden tekemää attribuutiota Helsingin yliopiston valtiotieteellisen tiedekunnan pro gradu -työssään tutkinut Eveliina Hannikainen toteaa, että kun hyökkääjä tunnistetaan ja nimetään julkisesti, tukee tämä valtioiden omaa narratiivia kyberkyvykkyydestään ja toisaalta myös vastaa nykypäivän mediaympäristön avoimuuden vaatimuksiin. (Hannikainen, 2021)

5 TURVALLISUUSTILANTEEN MUUTTUMINEN 2014-2022

Vaikka tutkittava aikaikkuna rajautuu vuoteen 2022, on tärkeää taustoittaa turvallisuuspoliittisen tasapainon muutosta ja tärkeimpiä kybertoimintaympäristön tapahtumia Euroopassa vuodesta 2014 lähtien, jolloin Venäjä laittomasti valtasi Ukrainalta Krimin niemimaan. Tämä taustoitus auttaa ymmärtämään vuoden 2022 kyberhyökkäyksiä sekä niiden määrän kasvua ja muutosta.

Tässä työssä ei käsitellä sotaa tai kybersotaa, eikä oteta kantaa kyberhyökkäyksiin mahdollisena osana sotatoimia, vaikka tarkastelun ajallinen aikaikkuna osuukin Venäjän Ukrainassa suorittamien sotilaallisten toimien ajankohtaan. Työssä kuitenkin kuvataan tänä ajanjaksona tapahtuneet tapahtumat perustasolla, koska ne ovat kiinnostavia, ja ovat mahdollisesti vaikuttaneet myös sotatoimiin liittymättömien kyberhyökkäysten kohdistamiseen tai niiden frekvenssiin tai muihin seikkoihin.

5.1 Krimin valtaus 2014

Ukraina halusi lähentyä Eurooppaa ja solmia vapaakauppasopimuksen Euroopan Unionin kanssa vuoden 2013 lopulla. Venäjä provosoitui tästä aikeesta ja tarjosi tilalle omia sopimuksiaan, muun muassa yhteistä tulliliittoa. Ukraina vetäytyi vapaakauppasopimuksesta EU:n kanssa viime metreillä, todennäköisesti Venäjän painostamana. Ukrainan kansalle oli luvattu lähentymistä Eurooppaan, ja tilanne johti lopulta mielenosoituksiin Maidan-aukiolla Ukrainan pääkaupungin Kiovan keskustassa (YLE Ulkolinja, 2022).

Mielenosoitukset alkoivat muuttua väkivaltaisiksi katutaisteluiksi helmikuun 20. päivänä, jolloin 39 rauhanomaista mielenosoittajaa ja 17 poliisia ammuttiin tuntemattomien tarkk'ampujien toimesta. Pian, helmikuussa 2014, Ukrainalle kuuluvalle Krimin niemimaalle, mm. Simferopolin kaupungin hallintorakennusten ja lentokentän alueille, ilmaantui tunnuksettomia sotilaita. (Sakwa, 2015).

Sotilaita epäiltiin venäläisiksi. Venäjän presidentti Vladimir Putinin hallinto kuitenkin kielsi asian, vaikka myöhemmin kyettiin todistamaan sotilaiden olleen Venäjän erikoisjoukkoja. Tämän jälkeen, maaliskuun 16. päivänä samana vuonna, Venäjä järjesti näytösluontoisen kansanäänestyksen Krimin liittämisestä Venäjän federaatioon. Venäjä liitti tämän jälkeen Krimin niemimaan itseensä laittomasti; Ukrainan hallitus ja länsimaat tuomitsivat kansanäänestyksen perustuslain vastaisena. Länsimaat rankaisivat talouspakotteilla Venäjää Krimin valtauksen vuoksi, mutta Krimin miehitys jatkui (YLE, 2022).

5.2 Venäjän sotatoimet Ukrainassa 2014-2022

Venäjä on jatkanut sotatoimia Ukrainassa vuodesta 2014 lähtien Krimin laittoman valtauksen jälkeen. Ukrainaa tunteva ja useasti Ukrainassa vieraillut Nina Järvenkylä kuvaa kootusti vuoden 2014 tärkeimpiä tapahtumia Iltalehden artikkelissaan: Maalis-huhtikuussa 2014 aseistautuneet joukot valtasivat hallintorakennuksia ja ryöstivät asevarastoja Itä-Ukrainassa erityisesti Donetskin ja Luhanskin alueilla. (Iltalehti, 2022). Toukokuussa 2014 tehdyn mielipidekyselyn perusteella 70 % itäukrainalaisista, mukaan lukien 58 % venäjänkielisistä, halusi pitää Ukrainan koskemattomana. Samanaikaisesti puolet Donbasin ja Luhanskin asukkaista pelkäsi Kiovan hallintoa ja jopa 60–70 % piti Kiovan mellakoita ukrainalaisen opposition ja lännen organisoimina aseellisina vallankaappausyrityksinä (Sakwa, 2015). Toukokuussa itäukrainalaiset separatistit valtasivat Donetskin lentokentän ja samoihin aikoihin Itä-Ukrainassa järjestettiin laittomat vaalit, joiden jälkeen perustettiin niin sanotut Donetskin ja Luhanskin kansantasavallat. Saman vuoden heinäkuussa venäläiset ampuivat alas Amsterdamista Kuala Lumpuriin matkalla olleen siviililentokoneen (Iltalehti, 2022).

Vuoden 2014 lopulla ja 2015 aikana yritettiin sopia tulitauoista, mutta näinäkin aikoina Venäjä muu muassa toimitti sotakalustoa Ukrainaan. Sotatoimet jatkuivat aaltomaisesti, mutta katkeamatta. YLE muistutti 30.1.2017 sotatoimien jatkumisesta ja kapinallisten vuosina 2016 ja 2017 tekemistä Avdivkan ja Mariupolin alueiden valtaamisista. Marraskuussa 2017 Venäjä valtasi 25. marraskuuta kolme ukrainalaista sotalaivaa, jotka kulkivat Krimin sillan ali. Venäjä pyrki näin myös rajoittamaan Ukrainan satamista käytävää merikauppaa (Verkkouutiset, 2018).

Sotatoimet jatkuivat Itä-Ukrainassa ja alkoivat kärjistyä vuonna 2021 Venäjän siirrellessä joukkojaan ja Valko-Venäjän jatkaessa hybridioperaatiotaan, jossa siirrättivät pakolaisia Puolan ja Liettuan rajalle. Helmikuun 21. päivänä vuonna 2021 Venäjän presidentti Vladimir Putin allekirjoitti asetukset Itä-Ukrainan separatistialueiden tunnustamiseksi. Venäjä lähetti myös alueelle sotilaitaan omien sanojensa mukaan rauhaa turvaamaan. Venäjän tekemät joukkojen siirrot ja ryhmien sijoittelut alkoivat indikoida lähestyvää sodanuhkaa (YLE, 2022).

5.3 Venäjän laajamittainen sotilaallinen hyökkäys Ukrainaan

Venäjä aloitti 24.2.2022 YK:n peruskirjaa ja kansainvälistä oikeutta rikkovan sotilaallisen hyökkäyksen Ukrainaan. Venäjän presidentti Vladimir Putin ilmoitti asiasta televisiopuheessaan aikaisin aamulla. Hyökkäys aloitettiin kolmest ilmansuunnasta, kohdistuen muu muassa Harkovan, Odessan, Dnipron, Kramatorskin, Mariupolin ja Kiovan kaupunkeihin. Mariupol on tärkeä satamakaupunki, ja sen valtaaminen mahdollistaisi Venäjälle helpomman yhteyden vuonna 2014 valtaamalleen Krimin niemimaalle (Iltalehti, 2022). Eurooppa-Neuvosto tuomitsi kokouksessaan toukokuussa 2022 jyrkästi Venäjän hyökkäyksen, ja EU-maiden johtajat vaativat Venäjää lopettamaan välittömästi siviileihin kohdistuvat hyökkäykset, mahdollistamaan humanitaarisen avun perille pääsyn ja vetämään kaikki joukkonsa pois Ukrainasta (Eurooppatiedotus, 2022). Venäjän aloittama sota Ukrainaa vastaan on jatkunut kaikesta huolimatta tämän työn valmistumiseen asti.

6 UKRAINAAN KOHDISTUNEET KYBERHYÖKKÄYKSET

Tätä tutkimusta varten rajattiin tutkittavaksi ajankohdaksi hyökkäykset, jotka on tehty vuoden 2022 aikana. Taustatilanteen ymmärtämiseksi on myös tutkittu yleisellä tasolla kyberhyökkäysten määrää hyökkäystä edeltävinä vuosina Krimin valtauksesta 2014 lähtien.

Uutistoimisto Reutersin mukaan Ukrainan Kyberturvallisuusviraston johtaja Yuriy Schygol ilmoitti tammikuussa 2023, että vuonna 2022 Ukrainaa kohtaan tehtiin 2194 kyberhyökkäystä, joista 1655 Venäjän sotilaallisen suurhyökkäyksen (24.2.) jälkeen (Reuters, 2022). Ukrainan Kyberturvallisuusviraston mukaan vuonna 2002 Ukrainassa havaittiin 58 miljardia kybertapahtumaa, joista 181 miljoonaa epäilyttävää tietoturvatapahtumaa, 179 000 kriittistä tietoturvatapahtumaa ja 415 rekisteröityä varsinaista kyberpoikkeamaa (SCPC, 2023). CyberPeace Instituten mukaan Ukrainan siviilikohteisiin tehtiin 220 hyökkäystä. CyberPeace Institute kerää tietoa vain siviilikohteisiin kohdistuneista hyökkäyksistä, ei sotilaskohteisiin kohdistuneista.

6.1 Merkittävät kyberhyökkäykset 2014-2021

Euroopan Parlamentin Tutkimuspalvelun EPRS:n tutkimusraportin mukaan Venäjä iski maaliskuun 13. päivänä 2014, vain kolmea päivää ennen Krimillä järjestettyä « kansanäänestystä », kahdeksan minuuttia kestävällä DDoS-hyökkäyksellä eli hajautetulla palvelunestohyökkäyksellä ukrainalaisia tietoverkkoja vastaan hankaloittaakseen tietoliikennettä ja viestintää Ukrainassa. Hyökkäyksen tarkoituksena on arvioitu olevan huomion vetäminen pois venäläisten joukkojen olemassaolosta Krimillä. (European Parliamentary Research Service EPRS, 2022). Toukokuussa ennen Ukrainan presidentinvaaleja Venäjä-mielinen haktivistiryhmä CyberBerkut yritti manipuloida äänestyksen tulosta. Tämä hyökkäys kuitenkin epäonnistui, ja haktivistien haittaohjelma saatiin poistettua 40 minuuttia

ennen vaaleja. Hakkerit kuitenkin onnistuivat viivästyttämään vaalituloksen laskentaa (European Parliamentary Research Service EPRS, 2022).

Joulukuun 23. päivänä vuonna 2015 tehtiin Ukrainaan kohdistunut DDoS-hyökkäys, tällä kertaa kolmen energiayhtiön verkkoon ja asiakaspalvelukeskukseen. Hyökkäys vaikutti yli 230 000 asukkaan sähkönsaantiin. Lisäksi Venäjän valtion tukemaksi väitetty ryhmittymä nimeltä Sandwork Team hankaloitti 16 pienemmän verkostoon kuuluvan sähkölaitoksen toimintoja (European Parliamentary Research Service EPRS, 2022).

EPRS:n mukaan vuosien 2016 ja 2021 välisenä aikana Ukrainaa vastaan kohdistettujen kyberhyökkäysten määrä oli kasvussa. Merkittävin iskuista oli Not-Petya -haittaohjelman levittäminen, joka heinäkuussa 2017 levisi kirjanpito-ohjelman välityksellä ja iski Chernobylin ydinvoimalaan ja lähes 13 000 julkisten palvelujen tuottajien käyttämään päätelaitteeseen. Joukossa oli muun muassa pankkeja, postipalveluyrityksiä, sanomalehtitaloja ja kuljetusalan yrityksiä. Lopulta haittaohjelma levisi maailmanlaajuisesti ja vaikutti 65 valtion ja noin 50 000 tietojärjestelmän toimintaan. Iskusta kärsineiden yritysten joukossa oli muun muassa FedEx, Maersk ja Merck. (European Parliamentary Research Service EPRS, 2022).

Kaksi merkittävää kyberhyökkäyksen yritystä ukrainalaisia tahoja vastaa tapahtui vuosina 2018 ja 2021. Vuoden 2018 tapauksessa iskua yritettiin Aulyn kloorinsuodatuslaitokseen, ja vuonna 2021 yritettiin iskeä ukrainalaisten turvallisuuspalveluiden internetsivustoihin. Nämä iskut epäonnistuivat tavoitteiltaan, mutta onnistuivat aiheuttamaan jonkinasteista haittaa järjestelmille (European Parliamentary Research Service EPRS, 2022).

6.2 Kyberhyökkäykset vuonna 2022, ennen suurhyökkäystä

EPRS:n edellä mainitun raportin mukaan vuoden 2022 alusta alkaen Ukrainaan kohdistuvien kyberhyökkäysten määrä kasvoi merkittävästi. Microsoft raportoi 13.1.2022 Ukrainan hallitusta sekä useita voittoa tavoittelemattomia organisaatioita ja tietotekniikkayrityksiä vastaan tehdystä haittaohjelmasta. Seuraavana päivänä, 14.1.2022, 70 Ukrainan hallinnon internet-sivustoa päätyi tilapäisesti hakkerien kontrolliin. Ukrainan Digitaalisen transformaation ministeriö piti Venäjää vastuullisena hyökkäyksistä. Nämä Whispergate-hyökkäyksiksi nimetyt hyökkäykset olivat analyysien mukaan suunniteltu näyttämään kiristyshaittaohjelmilta, mutta niistä puuttui lunnaiden jälkeinen palautusmekanismi, ja ne oli tarkoitettu saamaan kohteena oleva päätelaite toimimattomaksi tai vajaatoimintaiseksi, eikä niillä tavoitella lunnaita (CyberPeace Institute, 2022).

Microsoftin tuoreen raportin « A year of hybrid warfare in Ukraine » mukaan näiden Whispergate-hyökkäysten takana on venäläinen, nimeä DEV-0586 -nimeä käyttävä sotilaallinen toimija. Venäläiset toimijat tehtailivat vielä tämän jälkeenkin useita wiper-hyökkäyksiä ukrainalaisia valtiollisia kohteita, kriittisen infrastruktuurin, median ja kaupallisenkin sektorin kohteita vastaan. Wiper-hyökkäykset pyrkivät nimensä mukaisesti pysyvästi pyyhkimään pois eli

poistamaan tiedostoja ja/tai saamaan päätelaitteita toimintakyvyttömiksi (Microsoft, 2023).

Tammikuun puolenvälin paikkeilla Ukrainan valtionhallintoa kohtaan tehtiin massiivinen kyberhyökkäys, jonka yhteydessä oletetut venäläiset hyökkääjätahot jättivät uhkaus- ja pelotteluviestejä ukrainalaisille. Viesteissä kehotettiin pelkäämään ja varautumaan pahimpaan (The Independent, 2022).

KUVIO 5 Uhkausviesti ukrainalaisille (Reuters)

Helmikuun puolivälissä DDoS-hyökkäys kaatoi useita Ukrainan valtionhallinnon alaisia internetsivustoja sekä pankkien ja radioasemien internet-sivustoja useiksi tunneiksi. Samoja sivustoja kohtaan hyökättiin uudelleen 23.2.2022, ja lisäksi levitettiin uutta varianttia tietoja pyyhkivästä ja tuhoavasta haittaohjelmasta (engl. hermetic wiper) sataan talous-, tietotekniikka- ja ilmailualan organisaation (European Parliamentary Research Service EPRS, 2022). Viimeksi mainittu haittaohjelma havaittiin onneksi Microsoftin analytiikkakeskuksessa USA:ssa Seattlen lähellä, ja haittaohjelma tutkittiin pikaisesti. Asiasta informoitiin Ukrainan kyberpuolustusta, ja virustunnistusjärjestelmät päivitettiin muutamassa tunnissa estämään tämä uusi haittaohjelma. Haittaohjelma nimettiin FoxBladeksi. Sen levittäjä oli sama taho kuin 2017 NotPetya-haittaohjelmaa Ukrainaa vastaan levittänyt venäläinen valtiollinen taho, joka on tunnettu Sandworm- tai Iridium-nimisenä toimijana (Microsoft, 2022).

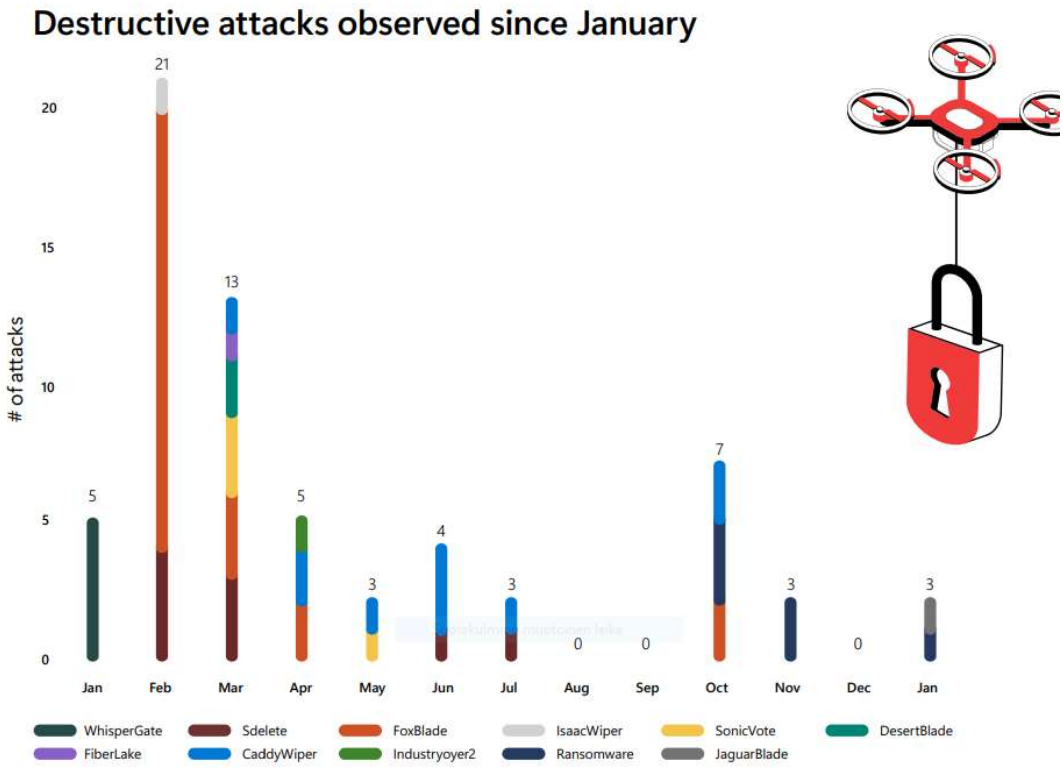
Helmikuun 15. päivänä erään valtio-omisteisen pankin asiakkaat alkoivat saada tekstiviestejä pankkiautomaattien teknisistä toimintahäiriöistä. Ukrainan kyberpoliisiorganisaatio vahvisti tietojen olevan paikkansa pitämättömiä. Hyökkäyksen tarkoituksena oli levittää disinformaatiota Ukrainan väestön keskuudessa. Tekoa ei ole virallisesti attribuoitu. (CyberPeace Institute, 2023).

Vain tuntia ennen Venäjän sotilaallista suurhyökkäystä helmikuun 24. päivänä venäläiset tahot iskivät kyberhyökkäyksellä Viasat-yhtiön omistamaa KA-SAT -satelliittiverkkoa vastaan. Hyökkäys katkaisi ukrainalaisten ja osin muiden eurooppalaisten verkon käyttäjien internet-yhteydet tekemällä modeemit toimintakyvyttömäksi. Hyökkäyksestä aiheutui satunnaisia, umpimähkäisiä viestintäkatkoksia ja toimintahäiriöitä useille viranomaisille, yrityksille ja yksityisille käyttäjille Ukrainassa ja vaikutti myös useisiin EU-maihin (Euroopan Parlamentti, 2022). SentinelLabs:n tutkijoiden mukaan hyökkäys oli toteutettu uudenlaista, AcidRain-nimistä wiper-haittaohjelmaversiota käyttämällä. Tämä haittaohjelma oli erityisesti suunniteltu tyhjentämään haavoittuvia modeemeja ja reitittimiä etäkäytön avulla. Viasat vahvisti myöhemmin, että hyökkäyksen tarkoituksena oli ollut pääasiassa häiritä ja kaataa palveluita, eikä päästä tietoon tai järjestelmiin käsiksi. Yhdysvallat on lausunut, että Venäjän tarkoituksena oli häiritä Ukrainan päätöksentekoa, johtamista ja reagointia sotilaallisen hyökkäyksen aikana (CyberPeace Instutute, 2022).

6.3 Kyberhyökkäykset Venäjän hyökkäyksen jälkeen 2022

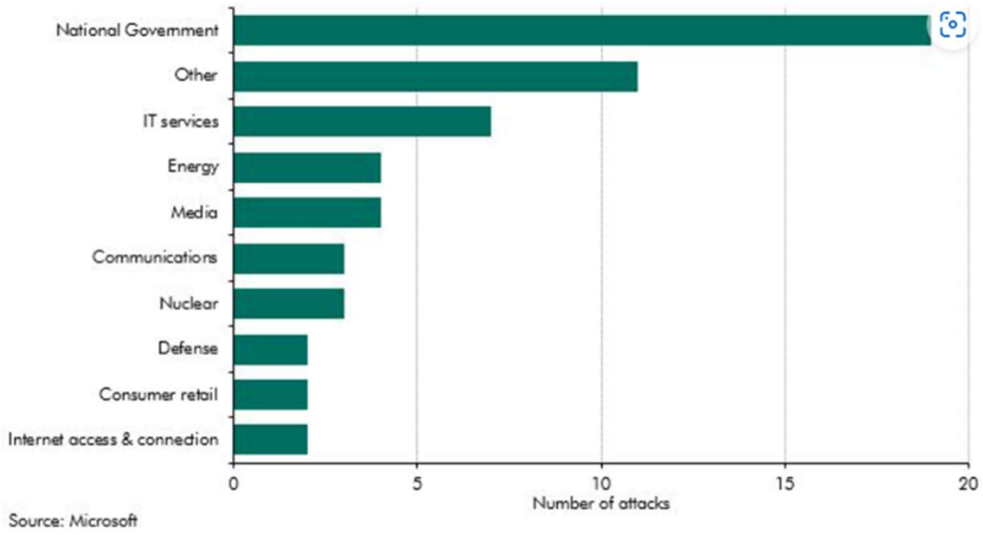
Microsoftin yllä mainitussa tuoreessa raportissa « A year of hybrid warfare in Ukraine » (2023) tutkijat jakavat Ukrainan sodan kolmeen vaiheeseen. Vaihe 1 ulottuu tammikuusta 2022 maaliskuun 2022 loppupuolelle ja käsittää Venäjän sotilaallisen hyökkäyksen alkuvaiheet. Vaihe 2 sisältää ajanjakson maaliskuun 2022 loppupuolelta syyskuuhun 2002, jolloin Venäjän vetäytyi Kiovan valtaamisen yrittämisestä ja keskittyi toimimaan Donbasin alueella. Vaihe 3 ulottuu syyskuusta 2022 raportin julkaisuhetkeen (15.3.2023) ja Venäjän reaktioihin Ukrainan vastaiskuihin itäisessä ja eteläisessä Ukrainassa.

Kuviossa 6 on kuvattu venäläisten toimijoiden tekemät onnistuneet ja tuhoa aikaansaaneet kyberhyökkäykset aikavälillä tammikuu 2022 – tammikuu 2023. Yllä mainitun Microsoftin raportin mukaan vaiheen 1 aikana Venäjä panosti voimakkaasti propagandaan ja informaatiovaikuttamiseen etenkin juuri ennen sotilaallista hyökkäystä ja välittömästi sen alettua. Venäjä ei todennäköisesti ollut varautunut Ukrainan nopeisiin reaktioihin, voimakkaaseen kyberpuolustukseen ja vastatoimintaan ja länsimaisen yhteisön tukeen, sekä ukrainalaisten kykyyn suojautua venäläiseltä propagandalta, josta syystä Venäjä ei kyennyt saavuttamaan tavoitteitaan. Alla olevasta kuvasta ilmenee, että vuoden 2022 aikana Venäjä onnistui saamaan läpi vain muutamia kymmeniä tuhovoimaltaan merkittäviä kyberhyökkäyksiä.



KUVIO 6 Venäjän tuhoisat hyökkäykset 2022 (Microsoft)

Vaiheessa 2 venäläiset siirsivät fokustaan Donbassin alueelle, sekä kyberoperaatioissaan pyrkivät nyt vaikuttamaan haitallisesti Ukrainan sekä kotimaasta että ulkomailta saamaan poliittiseen ja materiaaliseen tukeen. Microsoftin analyytikot havaitsivat kesäkuussa 2022 keväällä tehdyn tuhoisan wiper-hyökkäyksen, jonka oli laskenut liikkeelle Venäjän sotilastiedustelu GRU:n linkittyvä IRIDIUM-nimeä käyttävä hyökkäävä taho. Tämä hyökkäys kohdistui Ukrainan kuljetus- ja logistiikkainfrastruktuuria vastaan.



KUVIO 7 Venäjän tekemät kyberhyökkäykset sektoreittain (Microsoft)

Microsoftin lähteiden mukaan heti Venäjän sotilaallisen suurhyökkäyksen jälkeen helmikuun lopulla 2022 venäläinen Sandworm-nimeä käyttävä valtiollinen toimijaryhmittymä iski Ukrainaa vastaan muun muassa FoxBlade-nimisellä wiper-haittaohjelmalla. Muita, venäläisten tahojen tekemiksi epäiltyjä, mutta ei virallisesti attribuoituja samanaikaisia hyökkäyksiä olivat ainakin DesertBlade- ja IsacWiper -nimisillä wiper-haittaohjelmilla tehdyt hyökkäykset. Sandworm-ryhmä iski Ukrainaa vastaa uudelleen FoxBlade-haittaohjelmaa käyttäen maaliskuun alkupuoliskolla.

Microsoftin raporttien mukaan maaliskuun puolivälin paikkeilla venäläisiksi epäillyt, mutta ei virallisesti attribuoidut tahot, tekivät lisää kyberhyökkäyksiä Ukrainaa vastaan. Tällä kertaa käytössä oli muun muassa DesertBlade-niminen wiper-haittaohjelma, FiberLake-niminen uhrikoneita DDoS-hyökkäyksiin käyttävä troijalainen, tiedostoja kryptaava haittaohjelma nimeltä SonicVote sekä .NET-toiminnallisuuden käyttäminen. Maaliskuun lopulla venäläinen valtiollinen Sandworm-ryhmä iski jälleen FoxBladea käyttäen ja samanaikaisesti toinen, todennäköisesti venäläinen ryhmä, edellä mainittua SonicVote-haittaohjelmaa käyttäen. Vielä maaliskuun lopussa ja huhtikuun alussa venäläiset iskivät CaddyWiper- ja Industroyer 2 -wiper-haittaohjelmilla. Näissä iskuissa takana oli jälleen valtiollinen Sandworm-ryhmä.

CyberPeace Instituten seurannan mukaan Ukrainan siviilikohteita vastaan tehtiin hiukan yli 200 hyökkäystä vuoden 2022 aikana. CyberPeace Institute kerää tietoa vain siviilikohteisiin kohdistuneista hyökkäyksistä, ei sotilaskohteisiin kohdistuneista. CyberPeace Instituten lähteistä selviää, että heti Venäjän sotilaallisen suurhyökkäyksen jälkeen, helmikuun 25. päivänä, ilmeni, että Venäjältä ja Ukrainasta käsin toimiva verkosto ylläpiti internet-sivustoja, jotka olivat olevinaan itsenäisiä uutislähteitä, sekä loivat valehenkilöllisyyksiä sosiaalisen median alustoille Facebookiin, Instagramiin, Twitteriin, YouTubeen, Telegramiin, Odnoklassnikiin ja Vkontakteen. Tutkittaessa asiaa löydettiin mahdollisia linkkejä vuoden 2020 operaatioon, jossa tekijöinä oli yksittäisiä

henkilöitä Venäjältä, Donbassin alueelta Ukrainasta sekä kaksi media-alan yritystä Krimiltä. Tämän kyberoperaation tarkoituksena oli levittää disinformaatiota ukrainalaisten keskuudessa ja heikentää kansalaisten luottamusta hallintoaan kohtaan. Lisäksi tehtailtiin valheellisia tekstiviestejä, joissa ilmoitettiin pankkiautomaattien toimintahäiriöistä. Helmikuun lopussa hakkeroitiin korkean profiilin kansalaisten (sotilashenkilöt, julkisuuden henkilöt) sosiaalisen median tilejä, ja tämän jälkeen pyrittiin tekemään ulostuloja ja julkaisuja näiden nimissä. Tässä taustalla oli venäläinen UNC-1151 -niminen ryhmittymä.

Maaliskuussakin tapahtui paljon Ukrainan kyberrintamalla: ukrainalaiseen tutkimuslaitokseen hyökättiin ja häirittiin sen toimintaa väitetyn Venäjän-vastaisen aseisiin liittyvän salaliittoteorian takia. TV-kanava nimeltä Ukraine 24 hakkeroitiin lähettämään muka Ukrainan presidentiltä tulevaa antautumiskäskyä. Kybervakoilua tehtiin muun muassa erästä energiayhtiötä vastaan lähettämällä sen työntekijälle haitallinen liitetiedosto, joka sisälsi tietoja varastavan haittaohjelman. Vakoilua tehtiin myös muiden tietojenkalastelukampanjoiden muodossa, muun muassa luomalla haitallisilla komponenteilla varustettuja internet-sivustoja, jonne houkuteltiin ukrainalaisen ukr.net -sivuston käyttäjiä.

Huhtikuun alussa venäläinen valtiollinen toimija nimeltä APT28, joka tunnetaan myös nimillä FancyBear ja Strontium, iski ukrainalaista media-alaa vastaan saaden tietokoneita ja -järjestelmiä pitkäksi aikaa pois toiminnasta. Tätä seuranneena päivänä jo aiemmin mainittu venäläinen Sandworm-ryhmä iski energiasektoria vastaan. Huhtikuun puolivälissä venäläiseksi epäilty mutta ei virallisesti attribuoitu ryhmittymä nimeltä UAC-009 hyökkäsi käyttäen työkalunaan levittämäänsä haitallista Excel-liitettä, jossa oli käyttäjätunnuksia kalasteleva troijalainen. Huhtikuussa tehtiin myös ukrainalaista siviiliväestöä vastaan kyberhyökkäys, jossa väärennettyä ”Ukraine 24” -Facebook-sivua imitoivalla sivulla houkuteltiin kansalaisia osallistumaan kyselyyn ”taloudellista apua EU-maista” tarjoavan linkin kautta. Linkin kautta syötetyt henkilötiedot ja maksupyynnöt aiheuttivat maksukorttitietojen päätymisen rikollisten käsiin. Tuntematon taho hyökkäsi kohdennetulla palvelunestohyökkäyksellä (DDoS) Ukrainan postilaitosta vastaan heti sen jälkeen, kun se oli julkaissut sota-aiheisia postimerkkejä. Hyökkäys kaatoi joksikin aikaa postilaitoksen verkkopalvelut. Edelleen huhtikuussa Ukrainaa vastaan tehtiin Venäjän valtiollisen DEV-0586 -ryhmittymän toimesta tietojenkalastelukampanja, jossa GraphSteel- ja GrimPlant -nimiset haittaohjelmat ujutettiin julkishallintoon valtionhallinnon edustajan laittomasti haltuun saatua käyttäjätiliä käyttäen. Toinen julkishallintoa vastaan tehty hyökkäys toteutettiin venäläisen UAC-0098 -ryhmän toimesta levittämällä Meterpreter-nimisellä haittaohjelmalla saastutettua ISO-kuvatiedostoa.

Toukokuussa, heti kuun ensimmäisenä päivänä, Ukrainan rautateitä vastaan tehtiin tuntemattoman tekijän toimesta DDoS-hyökkäys. Noin viikko sen jälkeen venäläinen valtiollinen APT28-ryhmä lähetti tuntemattomalle vastaanottajaryhmälle Ukrainassa massasähköpostiviestin, jonka liite sisälsi "CredoMap_v2" -nimisen tiedon varastamiseen tarkoitetun haittaohjelman.

Seuraavana päivänä tuntematon taho levitti ”Jester Stealer” -nimistä haittaohjelmaa tietojenkalastelusähköpostiviestien välityksellä välittäen tietoa keksitystä ”kemiallisesta hyökkäyksestä”. Hyökkäykset jatkuivat toukokuun edetessä: seuraavaksi CyberPeace Instituten seurannan mukaan hyökättiin tietoliikenne- ja puhelinyhtiöitä ja valtionhallintoa vastaan DDoS-hyökkäyksin ja tietojenkalasteluyrityksin. Myös erään ukrainalaisen kaupungin kaupunginvaltuuston tiedostoja varastettiin erään kyberhyökkäyksen yhteydessä, ja tiedot julkaistiin pian venäläisen Telegram-viestisovelluksen kanavilla. Kansalaisia vastaan tehtiin huijausyrityksiä huhtikuista valekyselyä vastaavalla tekniikalla, tällä kertaa huijaten ihmisiä vastaamaan muka ”YK:n sosiaalisen ohjelman alaiseen talousapuun” liittyvään kyselyyn.

Kesäkuun toisena päivänä Ukrainan valtionhallinnon organisaatioihin iskettiin jakelemalla Cobalt Strike Beacon -nimistä saastunutta liitetiedostoa. Muutamaa päivää myöhemmin jalkapallon maailmancupin osakilpailun Walesin ja Ukrainan välisen ottelun aikana kyberhyökkäys katkaisi ottelun online-lähetyksen. Tietoliikenne uudelleen reititettiin lähettämään ulos venäläisen propagandakanava Izvestian lähetystä jalkapallo-ottelun sijaan. Tarkoituksena oli informaatiovaikuttaminen levittämällä virheellistä tietoa Ukrainan kansalaisille. Kumpaakaan hyökkäystä ei ole CyberPeace Instituten tietojen mukaan attribuoitu virallisesti. Kesäkuussa useat muutkin ryhmittymät, mukaan lukien nyttemmin hyvin tunnetut venäläiset ryhmittymät APT28 ja Sandworm, jatkoivat hyökkäyksiä ukrainalaisia tahoja vastaan. Kohteena oli erityisesti ukrainalainen media. Heinäkuussa kyberhyökkäyksiä ukrainalaisiin tahoihin tekivät muun muassa venäläisryhmittymät DEV-0586, Darya ja Xaknet. Hyökkäystapoina oli muun muassa erilaisten huijaussähköpostien ja kalastelulinkkien jakaminen erilaisille tahoille organisaatioista ja yrityksistä kansalaisiin. Heinäkuussa myös Ukrainan turvallisuuspalvelun SBU:n verkkosivuja vastaan tehtiin DDoS-hyökkäys. Muina kohteina olivat muun muassa Ukrainan terästeollisuus, eräs ohjelmistotalo, internet-palveluntarjoaja sekä julkishallinto. Venäläisryhmittymä Turla hyökkäsi ukrainalaisia aktivistisiteiksi mieltämiään tahoja vastaan käyttämällä StopWar Android App:n -sovelluksen avulla itse kehittämäänsä ja harhaanjohtavasti nimeämäänsä DDoS-sovellusta nimeltä CyberAzov, ja ylläpitivät tätä verkkotunnuksella, joka oli olevinaan Ukrainan Azovin rykmentin verkkotunnus. Ukrainan kansalaisia kiusattiin ja johdettiin harhaan lisäksi muun muassa lähettämällä Ukrainan kansallisen turvallisuusakatemian nimissä väärennettyjä, haitallisia liitteitä sisältäviä viestejä, sekä tehtailemalla ukrainalaisille pakolaisille muka apua tarjoavia huijausviestejä.

Ylläkuvatun kaltaiset kyberhyökkäykset jatkuivat tiiviisti koko loppuvuoden, mutta tähän tutkimustyön loppuraporttiin ei ollut tarkoituksenmukaista avata verbaalisesti jokaista hyökkäystä, sillä niitä on pelkästään ukrainalaisiin siviilikohteisiin tehty ja tunnistettu eri lähteitten mukaan reilusta kahdestasadasta reiluun neljäänsataan ja jopa yli kahteen tuhanteen. Tutkimusta varten kuitenkin käytiin hyvän yleiskuvan ja taustatiedon saamiseksi läpi jokainen CyberPeace Instituten raportoima kyberhyökkäys,

mutta yllä kuvattiin alkuvuoden (helmikuun loppu-toukokuu) tyypillisiä kyberhyökkäyksiä esimerkinomaisesti.

6.4 Vuonna 2022 tehtyjen hyökkäysten kohteet ja tyypit

Eri tietokantoja, koonteja, raportteja ja lähteitä tutkimalla voi todeta, että kyberhyökkäyksiä tehtiin Ukrainassa hyvin laajasti erilaisia toimialueita vastaan. Jopa eräs ravintola ukrainalaisessa Lvivin kaupungissa sai osansa syyskuun alussa. Venäläinen ryhmittymä nimeltä People's CyberArmy teki ravintolaa vastaan DDoS-hyökkäyksen. CyberPeace Instituten keräämien tietojen perusteella Ukrainan siviilikohteisiin vuonna 2022 tehtyjä kyberhyökkäyksiä tehtiin seuraavia toimialoja vastaan: majoitus- ja ravintolatoiminta, hallinto, maatalous, taiteet, kansalaiset, yksityishenkilöt ja kotitaloudet, rakennusala, koulutus, energiasektori, talous- ja rahoitusala, tietojenkäsittely ja tietohallinto, eri tuotteita valmistava teollisuus, media, kaivosala, ei-kaupalliset järjestöt, tiedemaailma, julkishallinto, kaupan ala ja kuljetusala.

CyberPeace Institute jaottelee vuoden 2022 Ukrainan siviilikohteita vastaan tehdyt kyberhyökkäykset seuraaviin kategorioihin: koordinoitu valheellinen toiminta, kybertoiminnan keinoin toteutettu informaatio-operaatio, kybervakoilu, haittaohjelmaa hyödyntävä kybervakoilu, palvelunesto- eli DDoS-hyökkäykset, verkkosivuston turmeleva muokkaaminen, taloudellinen huijaus, hakkerointi ja tietojen vuotaminen, haittaohjelma, tietojenkalastelu, kiristyshaittaohjelma, tietoja tuhoava wiper-haittaohjelma, ja muu/luokittelematon tapa. Seuraavassa taulukossa kuvataan Venäjän Ukrainaa vastaan tekemiä kyberhyökkäyksiä aikajanalla tyypeittäin sodan ensimmäisten kuukausien aikana.

TAULUKKO 1 Alkuvuoden kyberhyökkäyksiä tyypeittäin (Microsoft)

Ajankohta	Hyökkäystyyppi	Käytetty haitatohjelma	Hyökkäysten lukumäärä	Attribuutio
Viikko 1 (23.2-2.3)	Wiper (tietoja pysyvästi pois pyyhkivä haittaohjelma)	FoxBlade, Lasainraw (Isac wiper), DesertBlade, SecureDelete-toiminnallisuuden haitallinen käyttö	22	Foxblade: Sandworm (venäläinen valtiollinen toimija) Isac wiper ja DesertBlade: ei vahvistettu, epäilty venäläinen taho
Viikko 2 (3.-9.3)	-	-	-	-
Viiko 3 (10.-16.3)	Wiper (tietoja pysyvästi pois pyyhkivä haittaohjelma)	FoxBlade, SecureDelete-toiminnallisuuden haitallinen käyttö	4	FoxBlade: Sandworm (venäläinen valtiollinen toimija)
Viikko 4 (17.-23.3)	DesertBlade; Wiper (tietoja pysyvästi pois pyyhkivä haittaohjelma), uhrikoneita DDoS-hyökkäyksiin käyttävä troijalainen FiberLake; uhrikoneita DDoS-hyökkäyksiin käyttävä troijalainen, .NET-toiminnallisuus SonicVote: tiedostojen kryptausohjelma	DesertBlade, FiberLake, SonicVote, SecureDelete-toiminnallisuuden haitallinen käyttö	6	Ei vahvistettu, epäilty venäläinen taho jokaisen takana
Viikko 5 (24.-30.3)	Wiper (tietoja pysyvästi pois pyyhkivä haittaohjelma)	FoxBlade, Sonic Vote, SecureDelete-toiminnallisuuden haitallinen käyttö	3	FoxBlade: Sandworm (venäläinen valtiollinen toimija) SonicVote: Ei vahvistettu, epäilty venäläinen taho
Viikko 6 (31.3.-8.4)	Wiper (tietoja pysyvästi pois pyyhkivä haittaohjelma)	CaddyWiper, Industroyer2.0	2	Sandworm (venäläinen valtiollinen toimija)

7 HYÖKKÄÄJÄT JA KÄYTETYT TYÖKALUT

CyberPeace Instituten portaalista etsittyjen ja yhdisteltyjen tietojen mukaan Venäjän-Ukrainan sodassa on toiminut ainakin 17 erilaista kansallisvaltiotoimijaa, 42 kollektiivia ja neljä kyberrikollisryhmää. Toimijoita on jaoteltu yksityistoimijoihin, kyberrikollisiin, kollektiiveihin ja kansallisvaltiotoimijoihin. Alla kuvataan sellaisia tiedossa olevia kyberhyökkääjätahoja, joiden tiedetään tehneen vuonna 2022 kyberhyökkäyksiä Ukrainaa vastaan.

Instituutin mukaan Venäjälle uskollisia tai Venäjän lukuun toimivaksi tunnistettuja venäläisiä kollektiiveja ovat ainakin NoName057(16), Anonymous Russia, People's Cyber Army, KillNet, Mirai, XakNet, BearIT Army, KillNet Collective, ICC_H@ckTeam, UAC-0041, Zarya, RaHDit ja FRwL. Venäjän lukuun toimii CyberPeace Instituten lähteiden perusteella myös muunmaalaisia kollektiiveja: ukrainalaiset Phoenix ja Vermin, brasilialainen theMx0nday, iranilainen AlTahrea sekä joukko kollektiivitoimijoita, joiden kansalaisuus ei ole tiedossa. Näitä viimeksi mainittuja ovat Russian Hackers Team, Anonymous Sudan, Legion Cyber Spetsnaz, RADIS, Red Haclers Alliance, Clowns, Genesis Day ja AnonymousX777Z.

Lisäksi on tunnistettu Venäjän lukuun toimivia venäläisiä muita tahoja, joista ei tiedetä varmuudella toimijatyyppiä, kuten esimerkiksi nimeä UAC-0098 käyttävä taho. Venäjän lukuun toimivia muita tahoja, joiden toimijatyyppiä eikä kansallisuutta tiedetä, ovat ainakin National Hackers of Russia (HXP), Netside Group, Russian Hackers Community, Cyber Cat, TA499, UAC-0050, Russian Clay, Winter Vivern, UAC-0088, Furious Russian Hackers, UAC-0132, UAC-0094 ja UNC4166.

Venäjän valtiollisiksi toimijoiksi on pystytty nimeämään toimijat nimeltä Sandworm, DEV-0586, Gamaredon, Cold River, Turla ja Dragonfly InvisiMole. Valko-Venäjän nimiin vuonna 2022 Ukrainaan vastaan toimivat ainakin UNC1151 ja FancyBear. Muista valtiollisista toimijoista listoilta löytyy Kiinan Scarab.

Yksittäisistä kyberrikollisista listoilla on venäläinen toimija nimeltä Wizard Spider sekä kaksi kyberrikollista tahoa, joiden kansallisuutta ei tiedetä: Black

Basta ja @Conti. Muista yksittäisistä toimijoista on listattu venäläinen taho, joka käyttää nimeä KillMilk.

Mitre Attack- tietokanta nimeää venäläisiksi toimijoiksi seuraavanlaisia ryhmittymiä: venäläiseksi epäilty kybervakoilua suorittava ryhmittymä ALLANITE, Venäjän sotilastiedustelupalvelu GRU:n alaisuudessa toimivat APT28 ja Sandworm, Venäjän ulkomaantiedustelupalvelu SVR:n alaisuudessa toimiva APT29, ja Venäjän turvallisuuspalvelu FSB:n alaisuudessa toimivat ryhmät Dragonfly ja Gamaredon.

Muita venäläisiä kyberhyökkääjätahoja Mitren mukaan ovat ainakin Ember Bear -niminen ryhmittymä, joka on todennäköisesti ollut alkuvuonna 2022 Ukrainaa vastaan tehtyjen tuhoisien Whisper Gate – iskujen takana, sekä Indrik Spider -niminen kyberrikollisryhmittymä, kriittistä infrastruktuuria vastaan hyökkäyksiä tekevä TEMP.Veles, jo aiemmilta vuosilta tuttuTurla, sekä taloudellisesti motivoitunut Wizard spider -ryhmittymä.

Microsoftin raportin « A year of hybrid warfare in Ukraine » mukaan Ukrainaan kohdistetut, onnistuneet haitallisimmat hyökkäykset oli toteutettu suurimmaksi osaksi tietoja lopullisesti poispyyhkivien wiper-haittaohjelmien avulla. Vuonna 2022 tunnistetut, tuhoisimmat haittaohjelmat olivat nimeltään WhisperGate, Sdelete, Foxblade, IsaacWiper, SonicVote, DesertBlade, FiberLake, CaddyWiper, Industryoyer2, Ransomware ja JaguarBlade.

8 MUIHIN VENÄJÄN NAAPURIMAIHIN KOHDISTUNEET HYÖKKÄYKSET

Kokonaisuuden ymmärtämäisen ja tilannekuvan luomisen tukemiseksi tutkittiin myös Venäjän muihin naapurivaltioihin kohdistuneita kyberhyökkäyksiä. Suomi ei ollut vielä vuonna 2022 puolustusliitto Naton jäsenmaa. Tilastojen mukaan näyttää siltä, että Suomea kohtaan tehtyjen kyberhyökkäysten lukumäärä jäi Venäjän Natoon kuuluviin naapurimaihin kohdistuneita hyökkäyksiä selvästi alhaisemmaksi. Tilastoja tutkittaessa ja verrattaessa on huomioita myös, että kaikki lähteet, kuten esimerkiksi CyberPeace Institute, ei seuraa ja raportoi sotilaallisiin kohteisiin kohdistuneita kyberhyökkäyksiä.

Thales DIS Finlandin maaliskuun 2023 lopulla julkaiseman raportin mukaan Ukrainan tapahtumiin liittyvissä kyberhyökkäyksissä tapahtui merkittävä käänne vuoden 2022 loppupuolella. Raportin mukaan kyberhyökkäyksiä alettiin kohdistaa erityisesti Puolan, Baltian maiden ja Pohjoismaiden kriittistä infrastruktuuria vastaan. Venäjän ja Ukrainan välinen kybersodankäynti muuttui Euroopan laajuiseen korkean intensiteetin hybridi-kybersotaan. Myös EU-kandidaattivaltiot kuten Montenegro ja Moldova ovat joutuneet myös yhä useammin kyberhyökkäysten kohteeksi (Thales DIS Finland Oy, 2023).

8.1 Suomi hyökkäysten kohteena

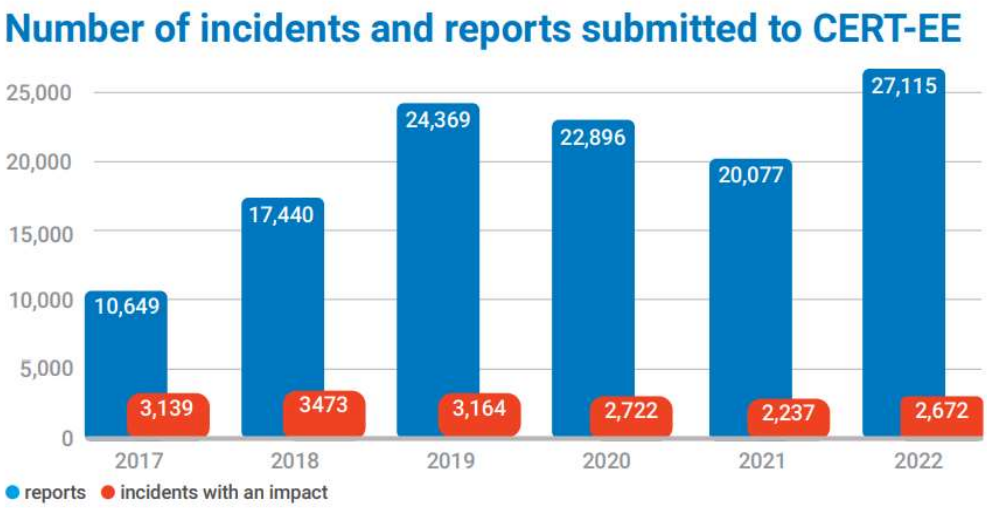
Suomeen kohdistuu Kyberturvallisuuskeskuksen (KTK) mukaan kymmeniä tuhansia palvelunestohyökkäystä vuosittain. KTK:n vuoden 2022 viimeisen viikkokatsauksen mukaan Venäjän Ukrainassa käymän hyökkäyssodan odotettiin aiheuttavan enemmän kyberhyökkäyksiä sekä Euroopan-laajuisesti että Suomeen kohdistuen, mutta Suomessa alkuvuonna 2022 laaja-alaisten kyberhyökkäysten määrä pysyi maltillisena. Hyökkäysten määrä lähti nousuun vuoden toisella puoliskolla. Erityisesti nousivat haittaohjelmien, tietojenkalastelun ja palvelunestohyökkäysten (DoS- ja DDoS-hyökkäykset)

määrät. Raportin mukaan aktiivisimmat ajat tässä mielessä vuonna 2022 olivat loka-, marras- ja joulukuu. Hyökkäysten kohteena oli sote-, finanssi-, liikenne-, logistiikka- ja media-alan organisaatiot. Nousevana ilmiönä vuonna 2022 KTK kuvaa venäjämielisten, vapaaehtoisten sosiaalisessa mediassa organisoituvien haktivistien aktivoitumisen. Näkyvin ja aktiivisin näistä ryhmistä on ollut Killnet-niminen ryhmä. KTK raportoi myös kiristyshaittaohjelmien lisääntymisestä vuonna 2022 erityispiirteenään se, että kiristyshaittaohjelmien avulla tehtyjen hyökkäysten kohteena eivät enää olleet vain isot organisaatiot, vaan myös pienempiin organisaatioihin tehtiin hyökkäyksiä (Kyberturvallisuuskeskus, 2022).

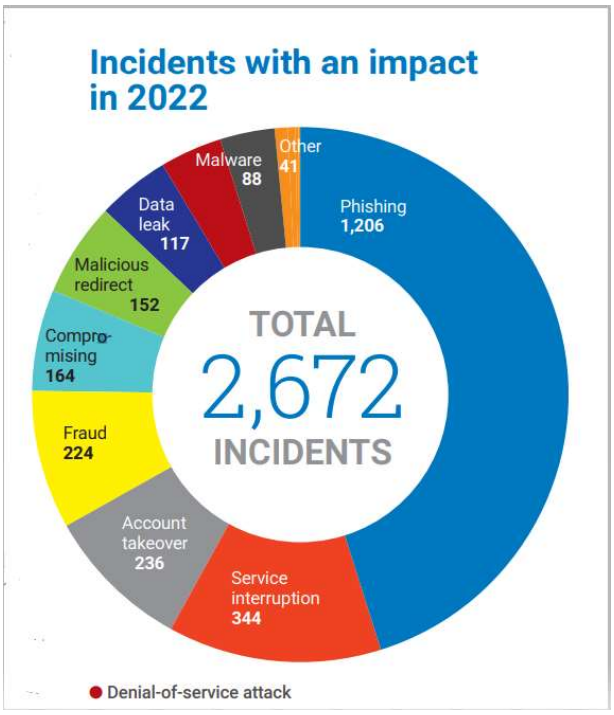
CyberPeace Instituten mukaan muita, vakavampia kyberhyökkäyksiä kohdistui Suomeen vuoden 2022 aikana kahdeksan kappaletta, ja ne alkoivat huhtikuun alussa. Huhtikuun 8. päivänä Ukrainan presidentin Volodymyr Zelenskyin puhuessa Suomen eduskunnalle videoyhteyden kautta, Suomen Puolustus- ja Ulkoministeriöihin kohdistettiin palvelunestohyökkäykset. Aikaisemmin samana päivänä raportoitiin venäläisen valtiollisen ilma-aluksen tekemästä ilmatilanloukkauksesta. Elokuun 10. päivänä venäläinen taho nimeltä NoName057(16) ilmoitti tehneensä hajautetun palvelunestohyökkäyksen (DDoS) Suomen eduskunnan internetsivustoja vastaan. Marraskuun alussa, 4.-5.11.2022, samainen taho (NoName057(16)) iski useaan valtiolliseen kohteeseen Suomessa DDoS-hyökkäyksellä. Yksi kohteista oli ministeriö, toinen valtion omista ympäristöpalveluita tuottava organisaatio ja kolmas ”itsenäisen ja demilitarisoidun suomalaisalueen hallinnon internetsivusto”. Joulukuun 12. päivänä venäläinen kybertoimija nimeltä Anonymous Russia kertoi tehneensä DDoS-hyökkäykset kuuden suomalaisen pankin internetsivustoja kohtaan, suomalaista rakennusyhtiötä kohtaan sekä suomalaista, Suomesta kertovaa tietosivustoa kohtaan.

8.2 Viroon kohdistuneista hyökkäyksistä

Viron tietojärjestelmäviranomaisen RIA:n mukaan vuonna 2022 Viron kyberympäristössä rekisteröitiin 2672 virolaisiin ihmisiin, liiketoimintaan ja palveluihin vaikuttanutta kybertapahtumaa. Palvelunestohyökkäyksien määrä kasvoi eniten, ja niitä käytettiin erityisesti ulkopolitiikan työkaluna. Venäjän hyökkäys Ukrainaan laajeni myös kyberympäristöön aiheuttaen ennennäkemättömän määrän Viroa vastaan kohdistettuja palvelunestohyökkäyksiä (RIA). Kuvio 8 kuvaa Viron kyberturvallisuusviranomaiselle, CERT-EE:lle raportoitujen kyberhyökkäysten vuotuista kasvua. Kuvio 9 kuvaa Viroon kohdistuneiden kyberhyökkäysten jaottelun hyökkäystyypeittäin. CERT-EE:n mukaan valtaosa vuoden 2022 kyberhyökkäyksistä toteutettiin tietojenkalastelun keinoin (1206 kpl), ja seuraavaksi eniten tehtiin palvelunesto- tai häirintähyökkäyksiä (344 kpl), käyttäjätilien laittomia haltuunottoja (236 kpl) ja erilaisia petoksia (224 kpl).



KUVIO 8 Viroon kohdistuneiden hyökkäysten määrä (CERT-EE)



KUVIO 9 Viroon kohdistuneiden hyökkäysten jaottelu (CERT-EE)

CyberPeace Institute on raportoinut Viroon kohdistuneen 27 kyberhyökkäystä vuoden 2022 aikana. Hyökkäykset alkoivat maaliskuun lopulla. Ajanjaksolla 28.3–3.4 Naton Osaamiskeskukseen kohdistui työntekijöiden käyttäjätunnusten ja salasanojen kalastelukampanja. Huhtikuussa, 18.-24.4, Viron valtionhallinnon sivustoja kohtaan hyökättiin DDoS-hyökkäyskampanjan keinoin. Heinäkuun alussa raportoitiin Viron presidentinkanslian internet-sivustoon kohdistetusta DDoS-hyökkäyskampanjasta, joka oli ollut aktiivinen edelliset kolme viikkoa.

Hyökkäysten huippu oli 2.7, jolloin tunnissa rekisteröitiin jopa 40 miljoonaa palvelupyyntöä tunnissa. Sivujen kaatumisen lisäksi muuta haitallista vaikutusta ei tapahtunut.

CyberPeace Instituten tilastoista ilmenee, että elokuun 17. päivänä Viroon kohdistui maan kybertuvallisuusjohdon mukaan laajin kyberhyökkäys vuoden 2007 jälkeen. Kymmenestä eri hyökkäyksestä koostuvalla DDoS-hyökkäyksellä pyrittiin vaikuttamaan sekä julkiseen että yksityiseen sektoriin hyökkäysten kohdistuessa muun muassa finanssisalaan, asumispalveluja tarjoavaan alaan, terveydenhuoltoon, vakuutus- ja eläketoimialaan, koulutustoimialaan, valtiollisiin palveluihin, taiteen ja viihteen toimialaan, SAAS-palveluja ja ohjelmistoja toimittaviin yrityksiin ja muihin kaupallisiin aloihin. Hyökkäyksen tekijäksi ilmoittautui venäläinen Killnet-taho.

Syksyllä muidenkin venäläisten kyberhyökkääjien toiminta jatkui aktiivisena. Elokuun lopulla vielä kohdistettiin palvelunestohyökkäyksiä virolaiseen uutistoimistoon, syyskuussa valtionhallintoon, lokakuussa media-, kuljetus- ja finanssisektorille. Näiden hyökkäysten takana oli aina venäläinen taho; joko NoName057(16) tai Anonymous Russia.

8.3 Latvia, Liettua ja Puola hyökkäysten kohteena

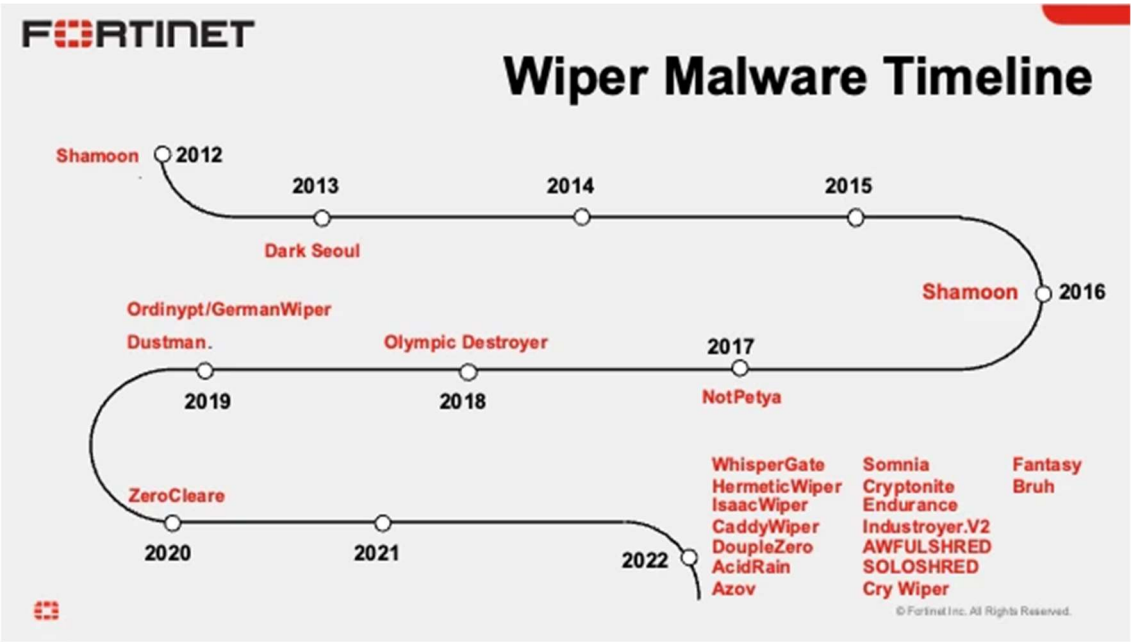
Latviaan kohdistui vuoden 2022 aikana 67 kyberhyökkäystä CyberPeace Instituten lähteiden mukaan. Latviaan kohdistuneet hyökkäykset alkoivat vasta toukokuun alussa, 2.5.2022. Liettuaa kohtaan tehtiin vuoden 2022 aikana 49 kyberhyökkäystä. Nämä hyökkäykset aloitettiin kesäkuun lopulla, 29.6. Puolaa vastaan tehtiin huhtikuussa yksi kyberhyökkäys, mutta vasta heinäkuussa, 4.7.2022, alkoi kyberhyökkäysten suma. Puolaa vastaan tehtyjä hyökkäyksiä CyberPeace Institute raportoi 99 kappaletta.

Bleeping Computer -julkaisu raportoi CyberPeace Instituten mukaan 23.2.2022 eli päivää ennen Venäjän sotilaallista suurhyökkäystä Ukrainaan, että samoja kyberhyökkäyksiä, joita tehtiin Ukrainaa vastaan, havaittiin tehdyn myös Latviaa ja Liettuaa vastaan samanaikaisesti. CyberPeace Instituten mukaan Security Affairs -sivusto uutisoi kesäkuussa 2022, että Liettuaa kohtaan tehtiin bottiverkkoja hyväksi käyttäen kyberhyökkäyksiä logistiikka, liikenne- ja energiayhtiöitä sekä pankkeja, teleoperaattoreita, lentokenttiä ja mediaa vastaan. Iskujen kohteeksi joutuivat myös ministeriöt, poliisi ja presidentinkanslia. Nämä iskut olivat DDoS-hyökkäyksiä eli hajautettuja palvelunestohyökkäyksiä, jotka ”vain” kaatoivat sähköiset palvelut, mutta eivät tuhonneet tietoa.

9 ANALYYSI, LÖYDÖKSET JA TULOKSET

Tutkimusta tehdessä selvisi, että Ukrainaan alkoi kohdistua kyberhyökkäyksiä jo hiukan ennen Krimin valtausta ja sen jälkeen, mutta aika Krimin valtauksesta Venäjän sotilaalliseen suurhyökkäykseen alkuvuodesta 2022 oli melko hiljaista kyberhyökkäysten suhteen. Selvisi lisäksi, että Ukrainaan kohdistuneiden kyberhyökkäysten määrä nousi selkeästi helmikuussa juuri ennen Venäjän sotilaallista suurhyökkäystä Ukrainaan. Löydöksenä oli myös se ero, että hyökkäykset Ukrainaa vastaan alkoivat jo ennen sotilaallista suurhyökkäystä, mutta muihin mainittuihin Venäjän naapurimaihin kohdistuneet hyökkäykset alkoivat myöhemmin eri kuukausien aikana porrastetun oloisesti. Tämä herättää kysymyksen, onko pääasiallinen hyökkääjätaho eli Venäjän valtio halunnut laajentaa kyberhyökkäyksiään naapurivaltioihin osoittaakseen Ukrainaa tukeville valtiolle, etteivät hekään ole suojassa. Kyberhyökkäysten alkamisaika eri valtiossa voisi mahdollisesti kertoa myös siitä, että kyberhyökkäyksiä on mahdollisesti suunniteltu ja ikään kuin porrastettu.

Hyökkäystyyppien muuttuminen oli myös selkeä löydös. Hyökkäykset ovat muuttuneet siten, että aikaisempina vuosina myös Ukrainaa vastaan tehtiin paljon palvelunestohyökkäyksiä, mutta Venäjän sotilaallisen suurhyökkäyksen lähestyessä ja sen alettua Ukrainaan iskettiin voimallisesti erityisesti hyvin haitallisilla wiper-haittaohjelmilla. Näyttäisikin löydösten valossa siltä, että wiper-haittaohjelmat ovat tulleet kyber- ja hybridisodankäynnin merkittävimmäksi välineeksi vuoden 2022 aikana. Tätä ilmentää myös globaalin kyberturvapalveluja tuottavan Fortinet-yhtiön koostama aikajana (kuvio 11). Tutkimuksessa havaittiin myös, että muihin kuin Ukrainaan kohdistuneista kyberhyökkäyksistä valtaosa oli palvelunestohyökkäyksiä, usein hajautettuja eli DDoS-hyökkäyksiä. Vaikuttaisi, että niillä pyrittiin lähinnä haittamaan tilapäisesti muun muassa julkisten verkkopalvelujen saatavuutta ja kiusantekomielessä osoittamaan mieltä Ukrainaa tukevia läntisiä valtioita vastaan, sekä mahdollisesti pelottelemaan muita Venäjän naapurimaita.



KUVIO 10 Wiper-hyökkäykset 2012–2022 (Fortinet)

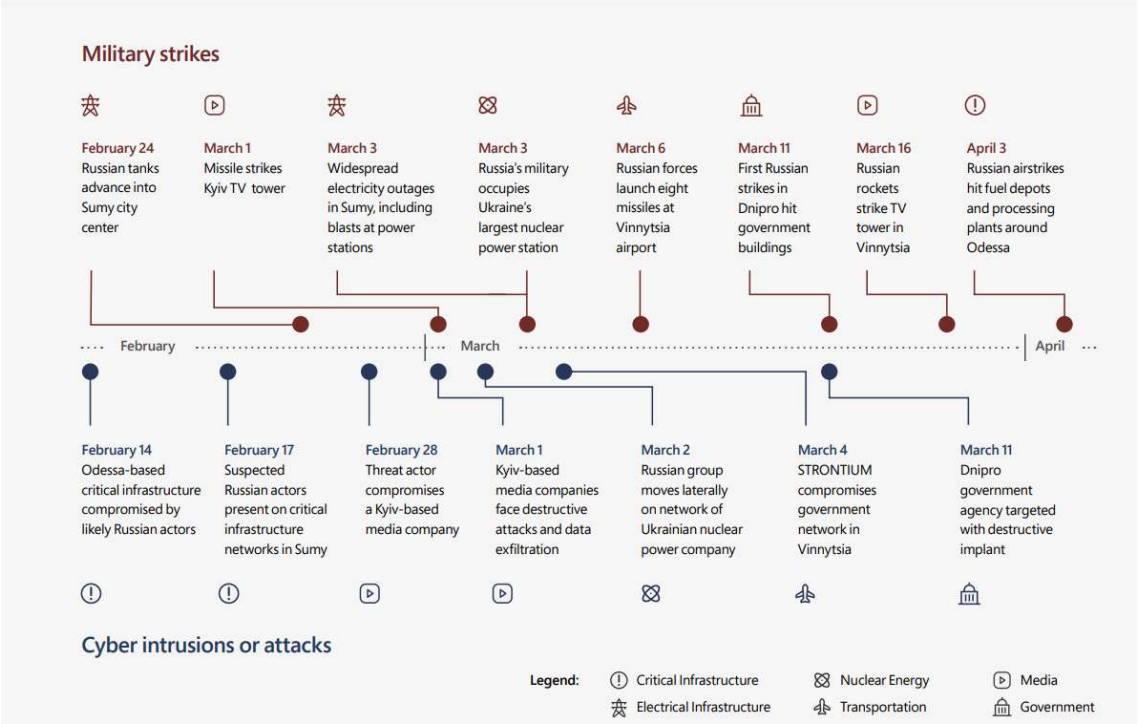
Eräs löydös oli se havainto, että Venäjä alkoi pidättäytymään laajamittaisista tuhoisista kyberhyökkäyksistä Ukrainaan kineettisen sodankäynnin alettua vuoden 2022 aikana. Eräs syy tähän on joidenkin lähteiden mukaan se, että Venäjä pyrki samanaikaisesti käyttämään Ukrainan infrastruktuuria hyväkseen (Office for Budget Responsibility). Näistä spekuloinneista huolimatta kyberhyökkäyksillä on eri analyytikkojen mukaan ollut kuitenkin merkittävä rooli Venäjän sodankäynnin työkaluna Ukrainaa vastaan. Muun muassa Microsoftin myöhemmät analyysit osoittavat, että sotilaallisten edistymisten ja kybertoiminnan aktiviteetin välillä on ollut selkeä korrelaatio. Varsinaisten kyberhyökkäysten lisäksi Venäjä on käyttänyt kybertoimintaympäristöä hyväkseen informaatiovaikuttamisessa tukemaan sotilaallisia toimiaan, muun muassa levittämällä valheellisia narratiiveja. Myös oma tutkimustyö toi esille sen, että Venäjä hyökkäsi häikäilemättömästi ja organisoitusti siviilikohteita, kansalaisia ja julkishallintoa vastaan ja pyrki monin eri keinoin saamaan aikaan epästabiiliutta ja kaaosta Ukrainassa ja kylvämään epäluottamusta maan hallintoa kohtaan kansalaisten keskuudessa samaan aikaan kun toisaalla edistettiin sotilaallisia toimia. Vaikka hyökkäystoiminta oli laajaa ja kohdistui lähes kaikkiin toimialoihin, oli se silti valtaosaltaan häirintää ja kaaoksen aiheuttamiseen pyrkivää kiusaamista, ja pienempi osa hyökkäyksistä oli vakavaa tai pysyvää haittaa aiheuttavaa.

Attribuutiosta voidaan lähdeaineiston perusteella löydöksenä todeta, että valtaosa Venäjän sotilaallisen hyökkäyksen jälkeen toteutetuista, attribuoiduista kyberhyökkäyksistä on ollut sellaisia, joissa tekijätaho on itse ilmoittautunut vastuulliseksi hyökkäyksestä, ja se seikka, että Ukrainaa vastaan tehtyjen hyökkäysten takana on ollut lähes kaikissa tapauksissa takana jokin venäläinen, usein valtiollinen tai valtion tukema taho.

Microsoftin raportin « A year of hybrid warfare in Ukraine » (2013) mukaan Venäjä on onnistunut kylvämään fyysistä tuhoa Ukrainassa, mutta ei ole saavuttanut tavoitteitaan osittain siitä syystä, että samanaikaiset kyber- ja informaatiovaikuttamisoperaatiot ovat epäonnistuneet. Raportin mukaan vaikuttaa siltä, että Venäjä keskitti myös kyberhyökkäysvoimansa sotilaallisen hyökkäyksen alkuvaiheeseen olettaen saavansa nopeaa vaikutusta ja ylipäätään nopean voiton Ukrainasta. Ukrainan nopea vastatoiminta ja kansainvälisen yhteisön tuki yllättivät Venäjän, eivätkä kyberhyökkäykset tuottaneet toivottua tulosta. Vaikuttaa myös siltä, että Ukrainan kansan taistelutahto ja yksimielisyys puolustaa maataan aggressiivista hyökkääjää vastaan, sekä maassa Venäjää vapaammin saatavilla oleva tieto ja kansalaisten asenne ja suhtautuminen ovat aiheuttaneet sen, ettei venäläinen propaganda pure toivotusti.

Tutkimalla venäläisiin toimijoihin liitettyjä kyberhyökkäyksiä voidaan ennakoida myös tulevia hyökkäyksiä ja hyökkäyksien kohteita. Hyökkäyksien rakenteen perusteella voidaan varautua ja suojautua tuleviin hyökkäyksiin (Mäntyniemi, 2023). Microsoftin analyytikkojen mukaan venäläiset toimijat saattavat pyrkiä laajentamaan sotilaallisiin ja humanitaarisiin toimitusketjuihin kohdistuvia hyökkäyksiään Ukrainan ja Puolan ulkopuolellekin, mikäli Venäjä jatkossa kärsii yhä enemmän tappioita taistelukentällä. Mikäli venäläiset jatkavat samanlaisella toimintasuunnitelmalla kuin vuonna 2022, tulevat he kehittämään vieläkin uudempia tuhoisia haittaohjelmavariantteja (Microsoft, 2023).

Useiden tahojen tutkijat ovat havainneet, että kineettiset sotilaalliset operaatiot ja kyberympäristössä tapahtuvat operaatiot ovat koordinoituja. Esimerkkinä tästä maaliskuun 1. päivän hyökkäys vuonna 2022, jossa Venäjä iski Kiovan TV-torniin ohjuksilla jäädyttäen joksikin aikaa TV-lähetykset. Samaan aikaan tehtiin kyberhyökkäys, jolla oli sama tarkoitus (Check Point, 2022.). Kuvio 13 kuvaa hyvin sotilaallisten iskujen ja kyberhyökkäysten korrelaatiota.



KUVIO 11 Sotilaallisten iskujen ja kyberhyökkäysten korrelaatio (Microsoft)

10 YHTEENVETO JA POHDINTA

Tutkimus oli dokumentteihin perustuva laadullinen sisällön analyysi, jonka tarkoituksena ei ollut luoda uutta teoriaa tai tiedettä, vaan kvalitatiivisen tutkimuksen luonteelle ominaisesti pyrkiä ymmärtämään tarkasteluta ilmiötä ja sen lainalaisuuksia.

10.1 Tutkimukset odotukset ja saavutetut tulokset

Tutkimuksessa selvitettiin ensin, minkä verran ja millaisia kyberhyökkäyksiä mainitulla aikavälillä on tehty Venäjään ja sen läntisiin naapurimaihin kohdistuen, sekä miten eri tekijät (määrä, laatu, frekvenssi) ovat muuttuneet vuoden 2022 aikana. Tutkimuksen tarkoituksena ei ollut saada tuloksena täydellistä kattavaa luetteloa tai tutkimusta kaikista vuoden aikana tehdyistä kyberhyökkäyksistä mainittuihin valtioihin. Käytännössä tämä olisi lähes mahdotontakin, koska ei ole olemassa aukottomia tilastoja jokaiseen valtioon kohdistetuista kyberhyökkäyksistä. Lisäksi sotilaallisista hyökkäyksistä etenkin sotilaskohteisiin on vaikea saada tietoa julkisista lähteistä. Nämä näkökohdat huomioon ottaen tutkimus oli onnistunut ja saavutti sille suunnitellut tarkoitukset. Pääasiallisiin tutkimuskysymyksiin saatiin vastaukset. Pääasiallisten tutkimuskysymysten vastausten lisäksi tutkimus toi useita muitakin mielenkiintoisia löydöksiä. Nämä löydökset kuvataan luvussa 9.

10.2 Tutkimuksen reliabiliteetti ja validiteetti sekä tutkimusetiikka

Usein kvalitatiivisissa tutkimuksissa pyritään välttämään reliabiliteetin ja validiteetin termejä, sillä niitä saatetaan kytkeä kvantitatiiviseen tutkimukseen. Kuitenkin myös kvalitatiivisen tutkimuksen luotettavuutta ja pätevyyttä tulisi arvioida jollakin tavoin. (Hirsjärvi ym. 1997, 217). Kvalitatiivisessa tutkimuksessa riskinä voi olla tutkijan subjektiivinen tulkinta. Kvantitatiivisessa tutkimuksessa objektiivisuus saavutetaan sillä, että tutkija pysyy erillään haastateltavasta kohteesta ja mittarit perustellaan teoriasta. Kvalitatiivisessa tutkimuksessa sen sijaan objektiivisuus lähtee siitä, ettei tutkija sekoita omia arvojaan, uskomuksiaan tai asenteitaan tutkimukseen. Täydellinen objektiivisuus ei kuitenkaan ole mahdollista - eihän kenenkään ole mahdollista irrottautua itsestään ja sulkea pois täysin omaa ajatteluaan. Riittääkin, että tutkija pyrkii aktiivisesti tiedostamaan omat asenteensa ja uskomuksensa, ja koettaa parhaansa mukaan toimia siten, etteivät ne vaikuttaisi tutkimukseen liiaksi (Saaranen-Kauppinen ja Puusniekka, 2006).

Tutkimusprojektissa huomioitiin myös etiikka ja hyvä tieteellinen käytäntö ja toimittiin näiden periaatteiden mukaisesti. Hyvän tieteellisen käytännön perusperiaatteita ovat eurooppalaisen tutkimuseettisen ohjeistuksen mukaan luotettavuus, rehellisyys, arvostus ja vastuunkanto. Hyvä tieteellinen käytäntö koostuu menettelytavoista, joilla huolehditaan hyvän tieteellisen käytännön toteutumisesta tieteellisen toiminnan koko elinkaaren ajan. Tutkimuseettisen neuvottelukunnan ohjeistuksen mukaan hyvät tieteelliset menettelytavat liittyvät kahdeksaan eri toiminnan alueeseen, jotka ovat toimintaympäristö, koulutus, ohjaus ja mentorointi, tieteellisen työn tekeminen, eettisyys ja ennakointi, tutkimusaineistojen käsittely ja hallinta, yhteistyö, tekijyys, julkaiseminen ja viestintä sekä asiantuntija- ja arviointitehtävät (Tutkimuseettinen neuvottelukunta, 2023).

10.3 « Lessons learned » –retrospektiivi itsearviona

Alkuun oli vaikea päättää rajauksesta, ja työn edistyessä vahvistui todeksi se ohjaajan, opponentin ja muiden opiskelijakollegoiden vihje siitä, että työn fokus ja tutkimuskysymys saattavat vielä hiukan muovautua kirjallisuuskatsauksen jälkeen varsinaiseen tutkimusvaiheeseen päästäessä.

Tutkimustyön edetessä, jo melko alkuvaiheessa lähdemateriaaliin tutustuttaessa, ilmeni, että työn tuloksena saadaan kuvaa myös siitä, miten siviilikohteisiin tehtyjä kyberhyökkäyksiä on mahdollisesti käytetty sotilaallisten operaatioiden tukena tai mahdollisesti myös osana. Materiaalia, erityisesti englanninkielistä, alkoi löytymään varsin laajasti, ja työn edetessä päätettiin rajata tutkimus koskemaan sellaisia kyberhyökkäyksiä, joissa kohteena on

pääasiassa Ukraina ja kevyemmällä painotuksella vertailun ja yleiskuvan saamiseksi Venäjän läntiset naapurimaat (Baltian maat eli Viro, Latvia ja Liettua sekä Suomi ja Puola).

Haasteena työssä oli se, että eri lähteiden taulukot, yhteenvedot, raportit ja taustamateriaalit erosivat toisistaan paljon ja antoivat erilaista tietoa ja erilaisia lukumääriä kyberhyökkäyksistä Ukrainaa kohtaan vuoden 2022 aikana. Syynä tähän on osaltaan se, että osa lähteistä oli keskittynyt siviilikohteisiin, osassa lähteitä oli keskitytty erityisen haitallisiin kyberhyökkäyksiin ja osa lähteistä oli julkaissut taulukko- tai muuta tietoa kaikista havaituista kybertapahtumista tai mikäli vain kyberhyökkäyksistä, mukana olivat myös lievempää haittaa aiheuttaneet kyberhyökkäykset. Lisäksi sotilaallisiin kohteisiin tehtyjä kyberhyökkäyksiä ei ole aina julkisuudessa avoimesti raportoitu. Lisähaasteen, tosin mielenkiintoisen sellaisen, toi uuden lähdemateriaalin ja tutkimusraporttien ilmestyminen työn edistymisen aikana.

10.4 Tutkimuksen hyödyntäminen ja jatkotutkimuksen aiheet

Tutkimus toi ymmärrystä kybermaailman uhkakuviin ja niiden toteutumiseen informaatiovaikuttamisen jatkeena ja hybridivaikuttamisen osana sekä ennakoivana vaiheena ennen Venäjän sotilaallista suurhyökkäystä. Tutkimus avasi myös hiukan lisää hyökkääjän, joka useimmissa tapauksissa oli Venäjä, tapaa toimia kybermaailmassa.

Jälkikäteen ajateltuna olisi ollut mielenkiintoista ottaa tarkasteltavien kohdevaltioiden joukkoon vielä Ruotsi, joka ei ole Venäjän naapurimaa, mutta on osoittanut kiinnostuksensa ja aikeensa Suomen ohella Natoon liittymisestä. Eräs jatkotutkimuksen aihe voisikin olla tutkia nimenomaan Ruotsiin kohdistuneita kyberhyökkäyksiä, ja selvittää muun muassa sitä, minkälaisia kyberhäirintäkampanjoita Ruotsia kohtaan ilmenee sen tiellä Natoon. Toinen kiinnostava tarkasteltava valtio kyberhyökkäysten kohteena voisi olla Moldova, jolla on yhteistä rajaa Ukrainan kanssa, ja jonka aluetta (Transnistria) Venäjä yhä miehittää.

Tutkimuksellisesti kiinnostavaa olisi myös selvittää maailmalla toimivien kyberhyökkäyksiä tekevien ryhmittymien kartoittaminen – millaisia tiedettyjä ryhmittymiä on olemassa, mitä tekniikoita ja taktiikoita nämä ryhmittymät käyttävät, kenen lukuun he toimivat ja millaisiin kohteisiin he iskujaan kohdentavat. Eri valtioiden turvallisuusorganisaatiot työkseen tosin jo todennäköisesti seuraavat näiden toimijoiden aktiviteettia, ja pystyvät tuottamaan tiedustelutietoa, joka auttaa varautumaan myös mahdollisiin kineettisiin sotilaallisiin iskuihin tai terrori-iskuihin.

Tutkimustyö vahvisti osaltaan sitä tietoa, että kyberiskuilla ja kineettisillä iskuilla on usein keskinäinen korrelaatio, ja kyberiskut voivat edeltää muita sotilaallisia tai terroristisia toimia, josta syystä kybertoimintaympäristöä on maanpuolustuksellisesti ja yhteiskuntarauhan vuoksi erittäin tärkeää aktiivisesti seurata. Kyberuhkat ja kyberhyökkäykset tulisikin ottaa vakavasti huomioon

mahdollisen laajemmankin yhteiskunnallisen, poliittisen ja sotilaallisen merkityksen vuoksi. Vesa Kanniainen toteaa Maanpuolustuskorkeakoulun Sotatekniikan laitokselle laatimassaan julkaisussa ”Polttopisteenä Suomen turvallisuus”, että sellainen valtio, joka onnistuu kehittämään kyberteknologiaansa ja siihen perustuvaa iskukykyä, omaa myös mahdollisuuden sotilaalliseen ensi-iskuun kyberteknologian keinoin. Kyberisku jo sinänsä saattaa tuhota osan vihollisen taistelukyvystä ja kyberiskun jälkeen hyökkääjä saattaa edetä perinteisin sotatoimin (Kanniainen, 2021).

Maailman silmät -syystäkin- ovat olleet viime ajat Ukrainassa ja Venäjän toimissa siellä. Ymmärrämme, että siellä taistellaan koko Euroopan ja eurooppalaisten arvojen ja itsemääräämisoikeuden puolesta. Tutkijoiden ja turvallisuusviranomaisten olisi jatkossa kuitenkin tärkeää tutkia myös muita kuin venäläisiä ryhmittymiä. Kuten tämän tutkimuksen löydöksiä kuvatessa mainittiin, kiinalaisia kyberhyökkäyksiä tehtailevia ryhmittymiä on huomattavasti enemmän -ainakin tunnistettu- kuin venäläisiä. Myös Lähi-Idässä toimii aktiivisia ryhmittymiä, erityisesti Iranissa ja Pakistanissa. Olisi kenties hyödyllistä informaatioteknologian ja kyberturvallisuuden tutkimuksen tarpeiden lisäksi, myös yhteiskunnan turvallisuuden ja terrorismintorjunnan edistämiseksi, tutkia esimerkiksi Kiinan ja Iranin kyberryhmittymien toimintaa ja toiminnan muuttumista sekä käytettyjä keinoja ja yhtäläisyksiä maailman tapahtumiin.

Ihmisoikeuksien ja kansainvälisen oikeuden kannalta voisi olla kiinnostavaa tutkia myös sitä, miten kybertoimijat käyttävät taitojaan ja verkostojaan myös omien maiden kansalaisia vastaan. Kiinalaiset toimijat keskittyvät maan ulkopuolisten tahojen lisäksi hyökkäämään oman maan vähemmistökansallisuuksia vastaan. Myös muiden Aasian maiden sekä Lähi-Idän alueilla toimivien ryhmittymien motiiveista löytyi tiettyjä etnisiä tai kielellisiä kansanryhmiä vastaan toimiminen. Tällaisten tutkimusten tuloksia voitaisiin hyödyntää kenties kansainvälisesti, yhteiskunnallisesti ja poikkitieteellisesti. Myös kyberpuolustuksen saralta tässä mainittuihin jatkotutkimuksen aiheisiin liittyen löytyisi varmasti mielenkiintoista tutkittavaa.

LÄHTEET

Blue Team Builders. (2021). *APT-hyökkäykset*. Noudettu 29. huhtikuuta 2023 osoitteesta https://www.linkedin.com/pulse/blue-team-builders-raportti-apt-hy%C3%B6kk%C3%A4ykset-marcus-s%C3%B6derblom/

Check Point. (2022). *Introduction to the check point 2022 security report*. Noudettu 27. marraskuuta 2022 osoitteesta https://go.checkpoint.com/security-report/page-introduction.php

Check Point. *Top 6 Cybersecurity Threats.* Noudettu 24. toukokuuta 2023 osoitteesta https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

CSIS, Center for Strategic and International Studies. (2022). *About CSIS* Noudettu 7. toukokuuta 2023, osoitteesta https://www.csis.org/about

CSRC. *Cyber Attack – Glossary*. Noudettu 7. toukokuuta 2023 osoitteesta https://csrc.nist.gov/glossary/term/cyber_attack

CyberPeaceInstitute. (2022). *Cyber Attacks in Times of Conflict.* Noudettu 23. marraskuuta 2022 osoitteesta https://cyberconflicts.cyberpeaceinstitute.org/

CyberPeaceInstitute. (2023). *Home.* Noudettu 7. toukokuuta 2023 osoitteesta https://cyberpeaceinstitute.org/

CyberWire. *Cyber Vandalism Definition - Cybersecurity Terms*. Noudettu 24. toukokuuta 2023 osoitteesta https://thecyberwire.com/glossary/cyber-vandalism

Elinkeinoelämän Keskusliitto ja CyberWatch Finland. (2018). *Kybervakoilu 2018*. Noudettu 7. toukokuuta 2023 osoitteesta https://ek.fi/wp-content/uploads/Kybervakoilu2018.pdf

ENISA. (2022). *ENISA threat landsdcape 2022.* Noudettu osoitteesta https://doi.org/10.2824/764318

Etymonline com. *Etymology, origin and meaning of cyber- by etymonline.* Noudettu 29. toukokuuta 2023 osoitteesta https://www.etymonline.com/word/cyber-

Euroopan komisso. (2021). *Digitaalisen kybermaailman ilmiöitä ja määrittelyjä.* Noudettu 7. toukokuuta 2023 osoitteesta https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fi

European Parliament. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. Noudettu 26. helmikuuta 2022 osoitteesta https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

Euroopan parlamentti. (2022). *Miksi kyberturvallisuus on tärkeää EU:lle?* Noudettu 20. marraskuuta 2022 osoitteesta https://www.europarl.europa.eu/news/fi/headlines/society/20211008STO14521/miksi-kyberturvallisuus-on-tarkeaa-eu-lle

Euroopan parlamentti. (2022). *Kyberturvallisuus: nykyiset ja tulevat uhat.* Noudettu 22. toukokuuta 2023 osoitteesta https://www.europarl.europa.eu/news/fi/headlines/society/20220120STO21428/kyberturvallisuus-nykyiset-ja-tulevat-uhat

Euroopan parlamentti (2022). *Kyberturvallisuus: suurimmat ja kasvavat uhat 2021 (infografiikka).* Noudettu 26. marraskuuta 2022 osoitteesta https://www.europarl.europa.eu/news/fi/headlines/society/20220120STO21428/kyberturvallisuus-suurimmat-ja-kasvavat-uhat-2021-infografiikka

Eurooppatiedotus. (2022). *EU-johtajat sopivat kuudennesta Venäjän vastaisesta pakotepaketista.* Noudettu 10. kesäkuuta 2023 osoitteesta https://eurooppatiedotus.fi/2022/05/31/eu-johtajat-sopivat-kuudennesta-venajan-vastaisesta-pakotepaketista/

Fortinet. (2022). *An Overview of the Increasing Wiper Malware Threat | FortiGuard Labs.* Noudettu 23. huhtikuuta 2023 osoitteesta https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

F-Secure. *Mikä on kyberhyökkäys?* Noudettu 26. marraskuuta 2022 osoitteesta https://www.f-secure.com/fi/home/articles/what-is-a-cyber-attack

Hannikainen, E. (2021). *Kuka nimeää kyberhyökkääjän? Strategiset narratiivit tiedustelupalveluiden julkisissa kyberattribuutioissa.* (Pro-gradu tutkielma). Helsingin yliopisto.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2005). *Tutki ja kirjoita.* 10. uud. painos, Helsinki:Tammi.

IBM. *What is a cyberattack?* Noudettu 7. toukokuuta 2023 osoitteesta https://www.ibm.com/topics/cyber-attack

IEEE Computer Society. *What is the Cyber Kill Chain.* Noudettu 10. kesäkuuta 2023 osoitteesta https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks

Iltalehti. (2022). *Miksi Ukrainassa soditaan ja mitä tapahtuu seuraavaksi?* Noudettu 7. toukokuuta 2023 osoitteesta https://www.iltalehti.fi/ulkomaat/a/b03a46bf-f630-4cd8-9d9b-b6eb2245490f

The Independent. (2022). *'Prepare for the worst': Ukraine government websites targeted in cyberattack.* Noudettu 26. helmikuuta 2023 osoitteesta

https://www.independent.co.uk/news/world/europe/ukraine-government-website-cyber-attack-b1993135.html

Jyväskylän yliopisto. (2023). *Kyberturvallisuuden maisteriohjelma, filosofian maisteri (2 v), syksy 2023 – Jyväskylän yliopisto*. Noudettu 6. toukokuuta 2023 osoitteesta https://www.jyu.fi/fi/hakijalle/koulutustarjonta/kyberturvallisuuden-maisteriohjelma-filosofian-maisteri-2-v-syksy-2023

Jyväskylän yliopisto. *Kybervandalismi* (Johdatus kyberturvallisuuteen -kurssi). Noudettu 7. toukokuuta 2023 osoitteesta https://peda.net/jyu/it/do/kkv/4kjna/4kj/kvm2/t1k2

Jyväskylän yliopisto ja Maanpuolustuskoulutusyhdistys. (2023). *Kurssi: Kansalaisen kyberturvallisuus kevät 2023*. Noudettu 7. toukokuuta 2023 osoitteesta https://onlinecourses.jyu.fi/course/view.php?id=43

Kanniainen, V. (2021). *Polttopisteessä Suomen turvallisuus*. Maanpuolustuskorkeakoulu, Sotatekniikan laitoksen julkaisuja. Noudettu 24. toukokuuta 2023 osoitteesta http://www.doria.fi/handle/10024/73990

Kaspersky. *Nollapäivän aukkoa hyödyntävä haittakoodi ja nollapäivähyökkäys*. (ei pvm.). Noudettu 27. joulukuuta 2022 osoitteesta https://www.kaspersky.fi/resource-center/definitions/zero-day-exploit

Kotimikro (2021). *Troijalainen hämää ilmoituksilla.* Noudettu 27. joulukuuta 2022 osoitteesta https://kotimikro.fi/tietoturva/virus/troijalainen-hamaa-ilmoituksilla

Kyberturvallisuuskeskus. (2014). *Kohdistetut_haittaohjelmahyökkäykset_uhka_otettava_vakavasti_raportti_28082014.* Noudettu 29. huhtikuuta 2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf

Kyberturvallisuuskeskus. (2022). *Kyberturvallisuuskeskuksen viikkokatsaus - 52/2022.* Noudettu 24. toukokuuta 2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-522022

Kyberturvallisuuskeskus. *Palvelumme.* Noudettu 7. toukokuuta 2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme

Laari, T. (2019). *Maanpuolustuskorkeakoulu Kyberkäsikirja Puolustusvoimien henkilöstölle*. Noudettu 22. toukokuuta 2023 osoitteesta http://www.doria.fi/handle/10024/73990

Lehto, M. (2020). *Digitaalinen maailma ja turvallisuus.* Luento Jyväskylän yliopistossa 24.10.2020.

Lehto, M. (2021). *Digitaalisen kybermaailman ilmiöitä ja määrittelyjä*, V. 12.0. Jyväskylä: Jyväskylän yliopisto

Lehto, M., & Limnéll, J. (2017). *Kybersodankäynnin kehityksestä ja tulevaisuudesta.* Tiede Ja Ase, 75. Noudettu 27. maaliskuuta 2023 osoitteesta https://journal.fi/ta/article/view/67730

Mikrobitti. (2022). *Microsoft varoittaa: päivittämättömät verkkolaitteet ovat hyökkäysvektori energiasektorin kimppuun.* Noudettu 27. marraskuuta 2022 osoitteesta https://www.mikrobitti.fi/uutiset/microsoft-varoittaa-paivittamattomat-verkkolaitteet-ovat-hyokkaysvektori-energiasektorin-kimppuun/5be4b9d0-69d7-42cb-93e1-cfbe5229454e

Microsoft.(2023). *A year of Russian hybrid warfare in Ukraine*. Noudettu 27. maaliskuuta 2023 osoitteesta https://twitter.com/paulaerizanu/status/1562783147397640196

Microsoft. (2022). *Defending Ukraine: Early Lessons from the Cyber War*. Noudettu 1. maaliskuuta 2023 osoitteesta https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Mikko Hyppönen (2022). *Mikko Hyppösen näkemyksiä kybersodasta ja -turvallisuudesta – MySpeaker Oy*. Noudettu 18. toukokuuta 2023 osoitteesta https://www.myspeaker.fi/uutiset/mikko-hypposen-nakemyksia-kybersodasta-ja-turvallisuudesta/

MITRE ATT&CK® Noudettu 27. marraskuuta 2022, osoitteesta https://attack.mitre.org/

Mitre Atta&ck®. *Groups.* Noudettu 20. marraskuuta 2022, osoitteesta https://attack.mitre.org/groups/

Mäntyniemi, N. *2023. Venäjän kyberhyökkäykset Ukrainaa vastaan: Vuodesta 2014 helmikuuhun 2022.* (Kandidaattityö, Tampereen yliopisto). Noudettu 10. kesäkuuta 2023 osoitteesta https://trepo.tuni.fi/handle/10024/144574

NCSC.GOV.UK. (2015). *How cyber attacks work.* Noudettu 20. marraskuuta 2022 osoitteesta https://www.ncsc.gov.uk/information/how-cyber-attacks-work

NICCS. *Cyber Operations*. Noudettu 22. toukokuuta 2023 osoitteesta https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cyber-operations

Nixu OYJ. (2014). *Mitä ovat hyökkäyspinta ja hyökkäysvektori? Nixu Cybersecurity.* Noudettu 25. marraskuuta 2022, osoitteesta https://www.nixu.com/fi/blog/mita-ovat-hyokkayspinta-ja-hyokkaysvektori

Nunes, E., Shakarian, P., Simari, G. I., & Ruef, A. (2018). *Artificial Intelligence Tools for Cyber Attribution. (Springer briefs in Computer Science).* Noudettu 22. marraskuuta 2022 osoitteesta http://www.springer.com/series/10028

Office for Budget Responsibility. (2022). *Cyber-attacks during the Russian invasion of Ukraine* . Noudettu 6. toukokuuta 2023 osoitteesta https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/

Poliisi. *Kyberrikokset -mitä kyber tarkoittaa?* Noudettu 27. marraskuuta 2022 osoitteesta https://poliisi.fi/kyberrikokset

RAND. *Cyber Warfare.* Noudettu 24. toukokuuta 2023 osoitteesta https://www.rand.org/topics/cyber-warfare.html

RIA. (2023). *The number of cyber attacks in 2022 was a hundred times higher than during the April Unrest.* Noudettu 2. maaliskuuta 2023 osoitteesta https://www.ria.ee/en/news/ria-number-cyber-attacks-2022-was-hundred-times-higher-during-april-unrest

RIA. *Home.* Noudettu 7. toukokuuta 2023 osoitteesta https://www.ria.ee/en

Reuters. (2022). *Ukraine blames Russia for most of over 2,000 cyberattacks in 2022.* Noudettu 8. maaliskuuta 2023 osoitteesta https://www.reuters.com/world/europe/ukraine-blames-russia-most-over-2000-cyberattacks-2022-2023-01-17/

Saaranen-Kauppinen A ja Puusniekka A. (2006). *KvaliMOTV - Tutkijan asema. Menetelmäopetuksen tietovaranto.* Tampere: Yhteiskuntatieteellinen tietoarkisto. Noudettu 10. kesäkuuta 2023 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_2.html

Sakwa, R. (2015). *Frontline Ukraine*. Lontoo: I.B.Tauris & Co Ltd. Noudettu 10. kesäkuuta 2023 osoitteesta https://www.researchgate.net/publication/304577389_Frontline_Ukraine

SCPC (Ukrainan Kyberturvallisuusvirasto). Noudettu 8. maaliskuuta 2023 osoitteesta https://scpc.gov.ua/article/233

Securelist. (2022). *'Unpacking' technical attribution and challenges for ensuring stability in cyberspace.* Noudettu 10. kesäkuuta 2023 osoitteesta https://securelist.com/unpacking-technical-attribution/106791/

Sisäministeriö. *Kyberrikollisuus.* Noudettu 26. marraskuuta 2022 osoitteesta https://intermin.fi/poliisiasiat/kyberrikollisuus

Thales DIS Finland Oy. (2023). *Kyberkonfliktissa. käänne Ukrainasta koko Eurooppaan.* Noudettu 17. huhtikuuta 2023 osoitteesta https://www.sttinfo.fi/tiedote/kyberkonfliktissa-kaanne-ukrainasta-koko-eurooppaan?publisherId=2034&releaseId=69971113

Tuomi, Jouni & Sarajärvi, Anneli (2018). Laadullinen tutkimus ja sisältöanalyysi (uud. laitos). Helsinki: Tammi.

Tutkimuseettinen neuvottelukunta. (2023). *Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa*. Noudettu 10. kesäkuuta 2023

osoitteesta https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf

Turvallisuuskomitea. (2018). *Sanasto.* Noudettu 20. marraskuuta 2022 osoitteesta www.huoltovarmuuskeskus.fi

Ulkoministeriö. *Kyberturvallisuus ja kybertoimintaympäristö.* Noudettu 27. marraskuuta 2022 osoitteesta https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

Valtioneuvosto. (2023). *Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa*. Noudettu 1. kesäkuuta 2023 osoitteesta https://julkaisut.valtioneuvosto.fi/handle/10024/164793

Verkkouutiset. (2018). Asovanmeren konflikti - Venäjä ei laskenut leikkiä. Noudettu 26. helmikuuta 2023 osoitteesta https://www.verkkouutiset.fi/a/asovanmeren-konflikti-askel-kohti-avoimempaa-sotaa/#85b32f84

Wired. 2012. *Wiper Malware That Hit Iran Left Possible Clues of Its Origins.* Noudettu 23. huhtikuuta 2023 osoitteesta https://www.wired.com/2012/08/wiper-possible-origins/

YLE. (2022). *Sytytyslanka alkoi palaa Ukrainassa vuonna 2014, kun Venäjä miehitti Ulkolinja, Elävä arkisto – yle.fi*. Noudettu 22. marraskuuta 2022 osoitteesta https://yle.fi/aihe/a/20-10002310

LIITE 1 Ukrainalaisiin siviilikohteisiin vuonna 2022 kohdistuneita kyberhyökkäyksiä

Hyökkäystyyppi ja -tapa (vektori)	Kategoria	Tavoiteltu tai aiheutunut vahinko	Hyök-käysten määrä	Hyökkäysten ajankohta	Hyökkäysten kohderyhmä	Hyökkäysten attribuutio
Koordinoitu valheellinen toiminta			**2**			
Valheelliset tekstiviestit pankkiautomaattien toimintahäiriöistä	Disinformaatio	Valheellisen tiedon levittäminen	1	14.-20.2	Kansalaiset	Ei vahvistettu
Valheellisten henkilöllisyyksien luominen sosiaaliseen mediaan	Disinformaatio	Valheellisen tiedon levittäminen, luottamuksen heikentäminen	1	2 1.-27.2	FB- ja Instagram-käyttäjät	Ei vahvistettu
Kybertoiminnan keinoin toteutettu informaatio-operaato			**4**			
Korkean profiilin kansalaisten (sotilashenkilöt, julkisuuden henkilöt) sosiaalisen median tilien hakkeroiminen, joka jälkeen julkaiseminen näiden nimissä	Disinformaatio	Luottamuksen heikentäminen	1	21.-27.2	Kansalaiset	UNC-1151
Ukrainalaisen tutkimuslaitoksen häirintä (Venäjän vastaista aseisiin liittyvää salaliittoteoriaa)	Disinformaatio	Ei tiedossa	1	7.-13.3	Ei tiedossa	Ei vahvistettu
TV-kanava Ukraine 24 hakkeroitiin lähettämään muka Ukrainan presidentiltä tulevaa antautumiskäskyä	Disinformaatio	Valheellisen tiedon levittäminen kansallisen uutistoimiston nimissä	1	14.-20.3	Media	Ei vahvistettu
Ukrainalainen TV-kanava hakkeroitiin, hyökkääjä lähetti Telegram-kanavallaan TV-yhtiön tilojen valvontakameran live-kuvaa	Data	Psykologinen operaatio ukrainamielistä uutisvälittäjää vastaan	1	27.6–3.7	Media	ICC_H@ckTeam
Kybervakoilu			**11**			
Kalasteluviestejä energiayhtiön työntekijälle; viestissä liitetiedosto joka	Data	Ei tiedossa	1	31.1–6.2	Energiasektori	DEV.0586

sisälsi tietoja varastavan haittaohjelman						
Kalasteluviestejä erityisesti intialaisille yhteisöille	Data	Ei tiedossa	1	28.2–6.3	Kansalaiset	Ei vahvistettu
Kalastelusivujen luonti ja ukr.net -käyttäjien houkuttelu sivuille	Data	Henkilötietojen laiton julkaisu	4	7.-13.3	Media	APT28
Ukrainanaisiin organisaatioihin lähetettiin kalasteluviestiä, joka sisälsi LoadEdge -takaoven	Data	Ei tiedossa	1	18.3	Julkishallinto	InvisiMole
Kansalaisille lähetettiin viestejä, joissa oli useita haittaohjelmia sisältävä XLS-tiedosto.	Data	Käyttäjätunnus-ten kalastelu	1	14.4	Kansalaiset	UAC-009
Common Magic -nimeä kantava operaatio, jolla pyrittiin varastamaan tietoa USB-laitteista Krimin, Donetskin ja Luhanskin alueen käyttäjiltä.	Data	Tiedon varastaminen	3	1.10	Julkishallinto, maanviljelys, kuljetusala	Ei vahvistettu
Kiristyshaittaohjelmat			**1**			
Prestige-kiristyshaittaohjelman avulla uhattiin kuljetus- ja logistiikka-alan organisaatioita	Data	Ei tiedossa		11.10	Kuljetus ja liikenne	Sandworm
Tiedon turmeleminen			**11**			
Ortodoksien uutena vuotena yli 70 Ukrainan hallinnon internet-sivustoa, töhrittiin poliittissisältöisillä kuvilla ja ukrainan-, venäjän- ja puolankielisillä teksteillä.	Häirintä	Yhteiskunnan tasapainon järkyttäminen, kaaoksen aiheuttaminen	2	14.1	ICT-ala, julkishallinto	UNC-1151
Yli 30 yliopistoon tehtiin kyberhyökkäys.	Häirintä		1	25.2	Koulutusala	theMx0nday
Kyberhyökkäys suosittuun ukrainalaiseen mediataloon, jonka internetsivustot sotkettiin Ukrainassa kielletyillä symboleilla.	Disinformaatio	Ei tiedossa	1	17.3	Media	Ei vahvistettu
Kyberhyökkäys mediataloa vastaan Walesin ja Ukrainan välisen ottelun aikana katkaisi ottelun online-lähetyksen. Tietoliikenne	Disinformaatio	Valheellisen tiedon jakaminen	1	5.6	Media	Ei vahvistettu

uudelleen reititettiin lähettämään ulos venäläisen propagandakanava Izvestian lähetystä jalkapallo-ottelun sijaan. Ukrainalaisia tv-livelähetyksiä hakkeroitiin ja häirittiin ja sotkettiin.	Disinformaatio	Psykologinen operaatio Ukrainan kansalaisia vastaan	2	28.6-1.7	Media	ICC_H@ckTeam
Ukrainan arkistolaitos hakkeroitiin ja TV-kanava hakkeroitiin lähettämään muka Ukrainan presidentiltä tulevaa antautumiskäskyä. Ukrainan radioon hyökättiin ja lähetettiin valheellista lähetystä, jossa kerrottiin Ukrainan presidentin olevan tehohoidossa ja Verkhovna Radan puheenjohtajan ottavan hänen tehtävänsä hoitaakseen.	Disinformaatio	Psykologinen operaatio Ukrainan kansalaisia vastaan	1	7.7	Julkishallinto	Zarya
	Disinformaatio	Ei tiedossa	1	1.7	Media	Ei vahvistettu
	Disinformaatio	Ei tiedossa	1	9.9	Julkishallinto	Anonymous Russia
Hyökkääjä väitti iskeneensä Ukrainan presidentin internet-sivustolle ja poistaneensa osan sivustosta. Kyberhyökkäys Kiovassa sijaitseviin yliopistoihin.	Disinformaatio	Yliopistojen internet-sivustojen sotkeminen	1	13.9	Koulutus	NoName057 (16)
Taloudellinen petos tai huijaus Valheellisena toimijana esiintyen saatiin käyttäjiä valheellisen kyselynlinkin taakse käyttämällä houkuttimena keksittyä "YK:n sosiaalisen ohjelman taloudellista tukea "	Data	Luottokorttitietojen kerääminen	**1**	15.4	Kansalaiset	Ei vahvistettu
Hakkerointi ja tiedon vuotaminen Eri julkishallinnon tahoihin hyökättiin ja niiden tietoa julkaistiin mm. venäläisillä Telegram-kanavilla. Kansalaisten henkilötietoa varastettiin.	Data	Kansalaisten henkilötietojen vuotaminen, tietojen varastaminen,	**6**	31.3 13.5 18.7 19.8 21.9 21.11	Julkishallinto Julkishallinto Julkishallinto Teollisuus Julkishallinto	XakNet Ei tiedossa XakNet Zarya XakNet XakNet

Teollisuusyritysten tietoa varastettiin.		julkistamine n ja tuhoaminen			Teollisuus Julkishallint o	
Haittaohjelmat			**20**			
Venäläiseksi epäilty taho hyökkäsi "DesertBlade" -haittaohjelmalla ukrainalaista mediayhtiötä vastaan. Samana päivänä Venäjän armeija ilmoitti aikeistaan tuhota Ukrainan "disinformaatiolähteet" ja teki ohjusiskun TV-torniin Kiovassa.	Häirintä	Häiritä ukrainalaisten pääsyä valtion pääasiallisee n tiedonlähtee seen	1	1.3	Media	Ei vahvistettu
Haittaohjelmia kohdistettiin selkeästi erilaisia ei-kaupallisia organisaatioita vastaan.	Häirintä	Ukrainalaist en lääkkeiden, ruuan ja vaatehuollon toimitusten hankaloittam inen sotatoimien aikana	1	4.3	Ei-kaupalliset organisaatiot	Ei vahvistettu
Julkishallinnon ja sotilastahojen edustajia vastaan hyökättiin mm sähköpostiviestein toimitetuilla Spectr, Grimplant, Graphsteel -haittaohjelmilla.	Data	Ei tiedossa	2	17.-27.3	Julkishallint o	Vermin, DEV-0586
Julkishallinnon edustajia vastaan hyökättiin käyttäen viestejä joissa Cobalt Strike Beacon -haittaohjelman sisältävä liitetiedosto.	Data	Ei tiedossa	1	2.6	Julkishallint o	Ei vahvistettu
Median edustajia vastaan hyökättiin käyttäen viestejä, joissa CrescentImp-haittaohjelman sisältävä docx-liitetiedosto, sekä monille tahoille viestejä, joissa CredoMap-haittaohjelma.	Data	Ei tiedossa	2	10.6	Media	Sandworm, APT28
Teleoperaattoreita vastaan kohdistettiin hyökkäys käyttämällä DarkCrystal -etäkäyttötroijalaista.	Data	Ei tiedossa	1	24.6	ICT-ala	Sandworm
Cobalt Strike Beacon -haittaohjelmia levitettiin mm. valheellisten työpaikkailmoitusten ja humanitaarisesta	Data	Ei tiedossa	2	4.-17.7	Julkishallint o, Kansalaiset	DEV-0586

katastrofista kertovan keksityn raportin välityksellä. Ukrainalaisia aktivisteja vastaan hyökättiin mm valheellisia sovelluksia (mm CyberAzov) luoden ja käyttäjiä näihin houkutellen. Toinen venäläisten rahoittama taho hyökkäsi ohjelmistotaloa vastaan GoMet -nimisellä avoimen lähteen haittaohjelmalla. Andromeda-haittaohjelman uhreille lähetettiin mm Quietcanary-haittaohjelmaa sisältäviä viestejä. Kansalaisille lähetettiin tietoja varastavia haittaohjelmia sisältäviä viestejä. Valtiollisiin kohteisiin hyökättiin valheellisella, Ukrainan asevoimien nimissä lähetetyllä viestillä, joka sisälsi RomCom-haittaohjelman. Muita hyökkäyksiä julkisiin kohteisiin. Julkishallinnon kohteisiin ja useisiin muihin organisaatioihin hyökättiin erilaisin haittaohjelmin	Häirintä Data Mm. Data Data, Häirintä	Ei tiedossa Ei tiedossa Ei tiedossa Ei tiedossa	2 3 3 2	19.7–21.7 6.9–19.9 21.10–11.11 18.11–28.11	ICT-ala Ei tiedossa Kansalaiset Kansalaiset Mm. julkishallinto Julkishallinto, organisaatiot	Turla Turla Gamaredon Sandworm UAC-0132 Gamaredon Sandworm UNC-4166 Sandworm
Roskaposti/spämmäys Tekijä esiintyi piiritetyn Mariupolin ukrainalaisena asukkaana, joka moitti hallintoa hylkäämisestä, sekä yllytti toimimaan Ukrainan hallintoa vastaan.	Disinformaatio	Väärän tiedon levittäminen tarkoituksena saada kansalaiset kääntymään hallintoaan vastaan.	**1**	8.4	Kansalaiset	DEV-0586
Wiper-haittaohjelmat Hyökkäys WhisperGate -haittaohjelmaa käyttäen	Tuhoaminen	Kohteet joutuivat ajamaan järjestelmänsä alas ja rakentamaan ne uudelleen alusta	**15** 3	13.1	ICT-ala, Julkishallinto, Ei-kaupalliset toimijat	DEV-0586

Laajoja kyberhyökkäyksiä Venäjän sotilaallisten hyökkäysten tukena; mm. laajakaistasatelliittiyhteyden katkaiseminen, joka vaikutti myös muissa maissa. Aseena mm IsacWiper, HermeticWiper – haittaohjelmat. Kyberhyökkäyksiä käyttäen DoubleZero- ja wiper-haittaohjelmia.	Tuhoaminen Tuhoaminen	Internetiin pääsy estetty 2 viikon ajan. Useiden organisaatioiden tietojärjestelmät häiriintyivät. Ei tiedossa	8 4	23.2–25.2 14.3–8.4	Rahoitusala, ICT-ala, energiasektori, julkishallinto, maatalous Mm energiasektori	Sandworm, Venäjän valtio Sandworm, UAC-0088
Tietojenkalastelu Mm. saastuneen Word-dokumentin toimittaminen liitetiedostona, valheellisten Telegram-tileihin liittyvän, haitallisen linkin sisältävän turvallisuustiedotteen lähettäminen, Telegram-tilien hakkerointiyritys, väärennettyjen internet-sivujen luominen, tietoja varastavien haitallisten linkkien toimittaminen.	Data	Mm. käyttäjätietojen ja autentikointidatan kerääminen	**16**	1.2–9.11	Julkishallinto	Gamaredon, UAC-0094, DEV-0586, UAC-0098, APT-28 UAC-0041, UAC-0133
Hajautettu palvelunestohyökkäys Laajasti eri tahoihin kohdistuneita palvelunestohyökkäyksiä lähes kaikkiin sektoreihin kohdistuen, painottuen eniten julkishallinnon median ja kriittisen infrastruktuurin kohteisiin.	Häirintä	Mm. julkishallinnon palvelujen ja internet-sivujen tilapäinen toimimattomuus	**128**	7.5-	Julkishallinto, Media ja lähes kaikki sektorit	Mm. RaHDIt, People's CyberArmy, Anonymous Russia, ChaosSec
Yhteensä			**224**			

Koottu CyberPeace Instituten tiedon perusteella.