Sami Ristimäki

Euroopan unionin kyberturvallisuus:

Kyberturvallisuusstrategioiden vertailu

Tekniikan ja
innovaatiojohtamisen yksikkö
Pro gradu- tutkielma
Tietojärjestelmätiede

Vaasa 2024

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen yksikkö
Tekijä: Sami Ristimäki
Tutkielman nimi: Euroopan unionin kyberturvallisuus : Kyberturvallisuusstrategioiden vertailu
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tietojärjestelmätieteen maisteriohjelma
Työn ohjaaja: Tero Vartiainen
Valmistumisvuosi: 2024 **Sivumäärä:** 47

TIIVISTELMÄ:

Internet on paitsi yhdistänyt ihmisiä, myös helpottanut niin tiedonvälitystä kuin teknologian kehittymistä sen luomisesta lähtien. Vaarana on kuitenkin ollut jo pidempään verkoissa olevan datan turvallisuus. Erinäiset virukset, haittaohjelmat ja tietomurrot ovat olleet osa internetiä jo viime vuosituhannen puolella, eikä unionin jäsenmailla ole ollut yhtenäisiä valmiuksia tai käytäntöjä näiltä uhilta suojautumiseen. Euroopan unioni päätti yhtenäistää jäsenmaiden suojautumista näitä ongelmia vastaan julkistamalla kaksi kyberturvallisuusstrategiaa, joilla se on pyrkinyt suojaamaan sekä ihmisiä että laitteita kyberhyökkäyksiltä ja niiden aiheuttamilta vahingoilta.

Tämän tutkimuksen tarkoituksena on tutkia näitä kahta kyberturvallisuusstrategiaa käyttäen vertailevaa tutkimusta. Tarkoituksena on selvittää mitä eroja näillä kahdella kyberturvallisuusstrategialla on ja miten uusi strategia reagoi ympäristössä ensimmäisen strategian julkistamisen jälkeen tapahtuneisiin muutoksiin. Strategioiden lisäksi tässä tutkimuksessa käsitellään aihetta tukevia materiaaleja kuten World Economic Forumin riskiraportteja kyberturvallisuuden osalta, Enisan ja muiden relevanttien tahojen asiakirjoja. Osana tutkimusta katselmoidaan myös muutamia strategioiden välillä tapahtuneita tunnettuja massiivisia kyberhyökkäyksiä antamaan näkemystä siihen, millaisia uhkia näillä kyberturvallisuusstrategioilla pyritään muun muassa ehkäisemään. Tutkimus rajoittuu Euroopan unionin vaikutusalueelle sekä näiden kahden strategian väliin. Esimerkiksi vuoden 2020 kyberturvallisuusstrategian jälkeen ilmenneitä haavoittuvuuksia ja kyberhyökkäyksiä ei käsitellä. Myöskään helmikuussa 2022 alkaneen Ukrainan sodan aiheuttamaan kybervaikuttamiseen unionin alueella tai Euroopan unionin reagointiin ei ole otettu kantaa.

Tutkimus osoitti, että vuoden 2020 kyberturvallisuusstrategiassa on otettu huomioon yleisen kyberturvallisuustilanteen muutokset ja strategia on päivitetty vastaamaan paremmin erinäisiin uhkiin, joita vuonna 2013 ei joko ollut tai niihin ei vielä ollut osattu kiinnittää vaadittua huomiota. Uusi strategia ottaa uhkien lisäksi huomioon myös uusia teknologioita ja tiedostaa paremmin globaalit muutokset, kuten ilmastonmuutokset. Huomioitavaa on, että teknologiat ovat jatkaneet kehitystään ja uusia teknologioita on noussut pintaan myös tuoreimman strategian luomisen jälkeen. Kyberhyökkäyksiltä suojautuminen ja siten turvallisuusstrategioiden suunnittelu onkin jatkuvaa kilpajuoksua kyberturvallisuusasiantuntijoiden sekä hyökkääjien välillä, joten myös kyberturvallisuustoimet vaativat jatkuvaa kehitystä. Tästä syystä Euroopan unioni on tämän tutkimuksen tekohetkellä suunnittelemassa uutta ’cyber solidarity act’ -nimellä toimivaa säädöstä, jolla se pyrkii parantamaan jäsenmaiden kyberturvallisuutta entisestään kehittämällä jäsenmaiden valmiuksia.

AVAINSANAT: Euroopan unioni, kyberturvallisuus, verkkohyökkäykset, tietoturva

Sisällys

1 Johdanto

Tämä pro gradu -tutkielma käsittelee Euroopan Unionin kyberturvallisuusstrategioita vuosilta 2013 ja 2020. Kyberturvallisuus on noussut yhä tärkeämmäksi aiheeksi tietoverkkorikollisuuden ja kyberhyökkäysten kasvaessa. Euroopan unionin kyberturvallisuusstrategiat ovat vastaus tähän haasteeseen ja niiden tarkoituksena on suojata Euroopan unionin kansalaisia, yrityksiä ja infrastruktuuria kyberuhkilta. Tämän tutkimuksen tavoitteena on analysoida, miten vuoden 2013 strategian keskeiset tavoitteet ovat muuttuneet vuoden 2020 strategiassa, millaisia uusia haasteita on noussut esiin ja millaisia toimenpiteitä strategioissa esitetään näihin haasteisiin vastaamiseksi. Tutkimus perustuu Euroopan komission, Euroopan parlamentin, Euroopan unionin verkko- ja tietoturvaviraston (ENISA) ja muiden relevanttien tahojen julkaisemiin asiakirjoihin sekä akateemiseen kirjallisuuteen kyberturvallisuudesta.

Kyberturvallisuustilanne Euroopassa on muuttunut merkittävästi vuosien 2013 ja 2020 välillä. Vaikkakin kohonneet riskit tiedostettiin jo vuonna 2013, kyberturvallisuutta pidettiin vielä melko uutena ja vähän tunnettuna alana, kun taas vuonna 2020 kyberturvallisuus on noussut yhdeksi tärkeimmistä turvallisuuskysymyksistä Euroopassa. Yksi merkittävä muutos onkin ollut kyberuhkien määrän ja monimuotoisuuden kasvu. Vuonna 2013 tunnistettiin jo useita erilaisia kyberuhkia, mutta vuonna 2020 kyberhyökkäysten määrä on kasvanut ja hyökkäysten monimutkaisuus on lisääntynyt merkittävästi. Kyberrikollisuus on myös kasvanut ja kehittynyt erilaisiin suuntiin, ja se on muuttunut yhä ammattimaisemmaksi ja organisoituneemmaksi.

Toinen merkittävä muutos on ollut kyberturvallisuuden merkityksen kasvu poliittisessa keskustelussa. Vuonna 2013 kyberturvallisuus oli usein tekninen ja vähemmän tunnettu aihe poliittisessa keskustelussa, mutta vuonna 2020 kyberturvallisuus on noussut yhdeksi tärkeimmistä turvallisuuskysymyksistä Euroopassa. Euroopan unioni on lisännyt panostuksiaan kyberturvallisuuteen ja julkaissut uusia strategioita ja aloitteita kyberuhkien torjumiseksi.

Lisäksi vuosien 2013 ja 2020 välillä on tapahtunut teknologinen kehitys, joka on vaikuttanut kyberturvallisuustilanteeseen. Esimerkiksi Internet of Things (IoT) -laitteiden ja teollisen internetin (Industry 4.0) käyttö on kasvanut, mikä on lisännyt kyberturvallisuuden haasteita ja riskejä. Samalla kehitys on luonut uusia mahdollisuuksia kyberturvallisuuden parantamiseksi, kuten tekoälyn ja koneoppimisen hyödyntäminen kyberhyökkäysten tunnistamisessa ja torjumisessa.

Yhteenvetona, kyberturvallisuustilanne Euroopassa on muuttunut merkittävästi vuosien 2013 ja 2020 välillä. Kyberuhkien määrä ja monimuotoisuus ovat kasvaneet, kyberturvallisuuden merkitys on kasvanut poliittisessa keskustelussa ja teknologinen kehitys on vaikuttanut kyberturvallisuuden haasteisiin ja mahdollisuuksiin.

1.1 Yleinen kyberturvallisuustilanne Euroopan unionissa

Vuonna 2013 suurimpia kyberturvallisuusuhat olivat erilaiset tietomurrot ja verkkohyökkäykset, kuten haittaohjelmat, tietojenkalastelu ja tietomurrot. Erityisesti huomiota kiinnitettiin kansallisten infrastruktuurien, kuten energiaverkkojen, televerkkojen ja vesihuollon, kyberturvallisuuteen. Lisäksi teollisuusvakoilu, tietojen urkinta ja muut valtioiden väliset kybersodankäynnin muodot olivat nousseet esille. Sosiaalisen median ja mobiililaitteiden käytön yleistyminen toi myös uusia haasteita, kuten tietojenkalastelun ja haittaohjelmien leviämisen kasvun. Esimerkiksi CNBC listasi vuoden 2013 suurimpiin kyberturvallisuuteen liittyviin uutisiinsa luottokorttitietojen leviämisen, Syyrialaisen hakkeriryhmän hyökkäyksen Twitteriä (nykyinen X) ja uutissivustoja vastaan sekä kasvavan uhan Kiinan valtiojohtoisille verkkohyökkäyksille. (CNBC, 2013)

Saman vuoden aikana Yhdysvalloissa puhuttiin kyberturvallisuuteen liittyvästä epävarmuudesta. Kyberhyökkäykset ja tietomurrot ymmärrettävästi vaikuttivat ihmisten elämään myös Euroopan ulkopuolella. Pidemmän aikavälin tavoitteena pidettiin sitä, ettei kyberosaamisen tasapaino järkkyisi ja vuonna 2030 yksikään valtio ei olisi

hallitsevassa asemassa kyberosaamisessa. Yhdysvaltojen tavoitteena olikin lisätä ymmärrystä kyberympäristöistä, jotta diplomatialla ja yhteistyöllä kansainvälisten kumppanien kanssa saataisiin kehitettyä muun muassa Yhdysvaltojen ja Euroopan kyberturvallisuutta. (Neutze & Nicholas, 2013)

Vuosien 2015 ja 2017 välillä Euroopan ulkoasianneuvostolla oli the Europe's Digital Power -niminen projekti, jonka tavoitteena oli selvittää jäsenvaltioiden näkemyksiä ja valmiuksia kyberturvallisuuden osalta. Projektin aikana kävi ilmi, että vaikka tietoturva on jäsenmaille tärkeä, valmiudet sen ylläpitämiseen on eritasoisia. Johtavien tietoturva-asiantuntijoiden, ”digital championien”, nostaminen jalustalle ja heidän hyödystään koko unionin turvallisuudelle aiheutti epäilyksiä. Monet työpajoihin osallistuneet myös pitivät huolestuttavana mahdollisuutta, että digitaalinen maailma alettaisiin näkemään kilpa-areenana, jossa kunnianhimoisimmat jäsenet kamppailisivat vallasta yhteisen hyvän sijaan. (Soesanto, 2017)

Vuonna 2020 suurimpia kyberturvallisuusuhat ovat edelleen samantyyppisiä kuin vuonna 2013, mutta niiden laajuus ja monimutkaisuus ovat kasvaneet huomattavasti. Esimerkiksi kiristyshaittaohjelmilla tehdyt hyökkäykset, joissa hyökkääjät kryptaavat uhrin tiedostot ja vaativat maksua tiedostojen vapauttamiseksi, ovat lisääntyneet merkittävästi. Lisäksi kasvava riippuvuus digitaalisista palveluista ja teknologioista on lisännyt haavoittuvuuksia kyberturvallisuudessa. Erityisesti tekoälyn ja esineiden internetin (IoT) kehityksen myötä on syntynyt uusia haasteita, kuten tekoälyn käyttö hyökkäysten tehostamisessa ja heikon suojaustason omaavien IoT-laitteiden käyttö bottiverkkohyökkäysten osana.

Kiristyshaittaohjelmilla tehdyt hyökkäykset ovat kasvava huolenaihe kyberturvallisuudessa, ja ne ovat todellinen uhka Euroopan unionin alueella. Kiristyshaittaohjelmat ovat erityisen haitallisia, koska ne saattavat lukita käyttäjän tiedot tai koko järjestelmän käyttäjän ulottumattomiin ja vaatia lunnaita tiedon palauttamiseksi.

Tämä voi johtaa merkittäviin taloudellisiin menetyksiin ja maineen vahingoittumiseen, erityisesti yritysten ja organisaatioiden kohdalla.

Vuonna 2020 Euroopan kyberturvallisuusvirasto (ENISA) julkaisi raportin, joka käsittelee kiristyshaittaohjelmilla tehtyjä hyökkäyksiä Euroopassa. Raportin mukaan kiristyshaittaohjelmat ovat kasvava ongelma Euroopassa, ja ne kohdistuvat erityisesti julkisiin sektoreihin, kuten terveydenhuoltoon ja koulutukseen. Raportin mukaan myös pk-yritykset ovat erityisen haavoittuvia kiristyshaittaohjelmien aiheuttamille vahingoille, ja niiden on syytä kiinnittää erityistä huomiota kyberturvallisuuteensa. (Enisa 2020)

1.2 Esimerkkejä kyberturvallisuusuhista viime vuosina

Yksi merkittävä haaste on ollut verkkorikollisuuden lisääntyminen, johon liittyy usein tietomurtoja, identiteettivarkauksia ja petoksia. Esimerkiksi vuonna 2020 tietomurtoja ilmoitettiin useissa EU-maissa ja muun muassa kyberturvallisuuskeskukset varoittivat yleisöä huijausviesteistä, jotka liittyivät koronavirukseen. (Booz Allen, 2020)

Toinen merkittävä haaste on ollut valtiolliset kyberuhat, jotka ovat johtaneet moniin vakaviin kyberhyökkäyksiin. Esimerkiksi vuonna 2017 Venäjän epäiltiin olevan vastuussa WannaCry-kiristyshaittaohjelmasta, joka vaikutti useisiin EU-maihin. Samana vuonna Venäjän epäiltiin myös yrittäneen sekaantua Ranskan vaaleihin (Euractiv, 2017).

Lisäksi EU on kärsinyt muista kyberhyökkäyksistä, kuten tietovuodoista ja tietojen varastamisesta. Esimerkiksi vuonna 2018 selvisi, että Facebookin käyttäjätietoja oli varastettu ja käytetty väärin. Syyskuussa 2018 paljastui yli vuoden jatkunut haavoittuvuuden hyväksikäyttö Facebookissa, joka vaikutti yli 50 miljoonaan käyttäjään eri puolilla maailmaa. Hyökkääjät pystyivät hyödyntämään heikkouksia Facebookin tietoturvan ja saivat haltuunsa käyttäjien kirjautumistietoja. Tämä mahdollisti hakkereille pääsyn miljooniin käyttäjäprofiileihin ja heidän henkilökohtaisiin tietoihinsa.

Erityisen huolestuttavaa oli, että hakkereilla oli pääsy käyttäjien henkilökohtaisiin viesteihin ja tietoihin, jotka olivat aiemmin pidetty luottamuksellisina. (The Guardian, 2018)

Aiemmin samana vuonna ilmi tulleen Cambridge Analyticaan liittyvän skandaalin kanssa tietomurto sai laajaa mediahuomiota ja käyttäjät vaativatkin emoyhtiötä, nykyiseltä nimeltään Metaa, korjaamaan tietoturvaan liittyvät ongelmansa. (New York Times, 2018). Ikhlaq Rehman (2019) kertoo artikkelissaan datan keräyksen olleen tietomurron sijaan tietovuoto. Cambridge Analytica keräsi tietoja Facebookin käyttäjistä ja saikin haltuunsa noin 87 miljoonan käyttäjän tietoja käyttäjien annettua oikeudet profiilinsa tietoihin päästäkseen Qualtricsin luomaan verkkokyselyyn. Oikeudet saatuaan ja tiedot kerättyään Campbridge Analytica myi haltuunsa saamaa dataa eteenpäin. Muun muassa yhdysvaltain entinen presidentti Donald Trump käytti käyttäjätietoja hyväkseen kohdistamalla Facebook-markkinointiaan henkilöille, joiden äänestyskäyttäytymiseen oli datan mukaan parhaat mahdollisuudet vaikuttaa.

1.3 Tutkimuskysymys ja tutkimusmenetelmä

Kyberturvallisuus on tärkeä aihe, joka on herättänyt paljon huomiota viime vuosina. Teknologian kehittyessä kyberturvallisuusuhkien määrä on kasvanut, mikä on johtanut siihen, että unionin jäsenvaltiot ovat kehittäneet erilaisia strategioita torjuakseen näitä uhkia. Tässä tutkielmassa tarkastellaan Euroopan unionin kyberturvallisuusstrategioita vuosilta 2013 ja 2020. Tutkimuskysymyksenä on, miten nämä kaksi strategiaa eroavat toisistaan ja miten kyberturvallisuustilanne on muuttunut Euroopassa näiden strategioiden välissä.

Tutkimusmenetelmäksi tämän tutkimuksen tekemiseen on valikoitunut vertaileva tutkimus. Charles Ragin ja David Zaret avasivat kahta käytettyä strategiaa vertailevan tutkimuksen tekemiseen artikkelissaan ”Theory and method in comparative research: Two strategies” (1983) Heidän vertailemissa strategioissa yhteneväistä oli se, miten

molemmat tutkimusstrategiat keskittyivät eri kohteiden tai ryhmien vertailuun ja analysointiin. Vertailevassa tutkimuksessa pyritään tunnistamaan yhtäläisyyksiä, eroja ja suhteita eri ilmiöiden tai ryhmien välillä.

Tässä tutkimuksessa käytetään pohjana edellä mainittuja vuosien 2013 ja 2020 kyberturvallisuusstrategioita havainnollistamaan miten kyberturvallisuusympäristö on muuttunut Euroopan unionin alueella näiden seitsemän vuoden aikana ja mitkä piirteet näissä muutoksissa ovat ajaneet uuden kyberturvallisuusstrategian luontiin. Tutkimuksessa vertaillaan kyberturvallisuusstrategioita keskenään keskeisten eroavaisuuksien löytämiseksi strategioiden väliltä huomioiden myös yhteneväisyydet, joihin ei ole ollut tarvetta puuttua ensimmäisen strategian luonnin jälkeen. Kyberturvallisuusstrategioiden lisäksi tutkimuksessa esitellään esimerkinomaisesti muutamia näiden välillä Euroopan unioniin tai sen jäsenvaltioihin kohdistuneita kyberturvallisuusuhkia tarkoituksena selvittää onko vuoden 2013 kyberturvallisuusstrategia valmistautunut näihin, tai vaihtoehtoisesti onko uudistettu vuoden 2020 strategia ottanut esiin tulleet uhat selkeämmin huomioon ja valmistautunut vastaavien hyökkäysten ehkäisemiseen.

1.4 Tutkimuksen rajoitukset

Tässä tutkimuksessa vertaillaan Euroopan unionin ensimmäistä ja toista kyberturvallisuusstrategiaa keskenään. Itse strategioiden ymmärryksen tueksi tässä tullaan perehtymään pinnallisesti World Economic Forumin raportteihin, sekä esimerkiksi tunnettuihin verkkohyökkäyksiin. Vaikka jokaisella jäsenmaalla, sekä useimmilla organisaatioilla on tämän lisäksi omia strategioitaan tietoturvan parantamiseksi, näihin ei tulla kiinnittämään erityistä huomiota.

1.5 Tutkimuksen rakenne

Tutkielma alkaa yleiskatsauksella strategioihin ja miten ne mukautuvat toimintaympäristöihinsä. Tällä rakennetaan pohjaa sille, mitä voidaan odottaa vertailun kohteina olevien kyberturvallisuusstrategioiden pitävän sisällään ja ottavan kantaa.

Seuraavaksi käsitellään Euroopan unionin ensimmäistä, vuoden 2013, kyberturvallisuusstrategiaa, otetaan selvää mihin riskeihin se ottaa kantaa ja mitä turvaavia toimenpiteitä siinä tuodaan esille. Samassa kappaleessa katsotaan myös World Economic Forumin samaisen vuoden riskiraporttia kyberturvallisuuden osalta.

Ensimmäisen strategian läpikäynnin jälkeen käydään läpi muutamia esimerkkejä tunnetummista verkkohyökkäyksistä, jotka aikanaan olivat suurina puheenaiheina sekä mediassa että organisaatioissa.

Esimerkkitapausten annettua osviittaa kyberriskeistä, käydään läpi päivitetty, vuoden 2020, kyberturvallisuusstrategia. Käydään läpi vuoden 2013 strategian tapaan mihin riskeihin uudistettu strategia keskittyy ja millaisia toimenpiteitä siinä suositellaan jäsenistön -jäsenvaltioiden sekä organisaatioiden- tehtäväksi. Vastaavasti myös vuodelta 2020 katselmoidaan World Economic Forumin riskiraporttia.

Molempien kyberturvallisuusstrategioiden tutkimisen jälkeen, näitä vertaillaan keskenään ja avataan enemmän mitä eroja näiden välillä on. Lopuksi vielä otetaan katsaus kyberturvallisuustilanteeseen Euroopan unionin alueella tuoreemman kyberturvallisuusstrategian julkaisun jälkeen sekä kerrotaan mitä muita toimia näiden strategioiden lisäksi on tehty kyberturvallisuuden kehittämiseksi Euroopan unionissa.

2 Strategiat ja niiden mukautuminen ympäristöön

Strategioiden kehittäminen organisaatioissa on monivaiheinen prosessi, joka edellyttää huolellista harkintaa ja suunnittelua. On kyse sitten yksittäisestä yrityksestä tai Euroopan unionin kokoisesta organisaatiosta, kehitysprosessit käynnistyvät yleensä tilanneanalyysillä. Tilanneanalyysi sisältää organisaation nykytilan ja ympäristön arvioinnin.

2.1 Strategia organisaatioissa ja valtiollisella tasolla

Loizos Heracleous määrittelee strategian osana organisaatioiden toimintaa ja onnistuneen stragien hyötyjä kirjassaan Strategy and Organization - Realizing Strategic Management (2003) muun muassa seuraavilla tavoilla:
Strategian rooli organisaatiossa on moniulotteinen ja vaikuttaa monin eri tavoin organisaation toimintaan. Yhtenä perinteisempänä määritelmänä strategia toimii organisaation kompassina. Se määrittelee organisaation pitkän aikavälin visiot ja tavoitteet, antaen suunnan ja merkityksen kaikelle toiminnalle. Strategia toimii aktiivisena suunnannäyttäjänä sen sijaan että organisaatio vain reagoisi ympäröivän maailman tapahtumiin. Strategia tosin myös auttaa organisaatiota sopeutumaan muuttuviin olosuhteisiin tarjoamalla joustavan kehyksen, jonka avulla organisaatio voi reagoida muutoksiin ja uusiin haasteisiin.

Näiden lisäksi strategialla on useita muita hyötyjä. Strategia auttaa organisaatiota keskittymään olennaiseen. Se asettaa selkeät tavoitteet ja auttaa organisaatiota valitsemaan ne toimenpiteet ja resurssit, jotka tukevat parhaiten näiden tavoitteiden saavuttamista. Tämä resurssien kohdentaminen on olennaista tehokkuuden ja tuloksellisuuden kannalta.

Strategia tukee päätöksentekoa. Se tarjoaa viitekehyksen päätösten arviointiin ja auttaa organisaatiota tekemään johdonmukaisia ja yhtenäisiä päätöksiä. Näin varmistetaan,

että päätökset tukevat organisaation pitkän aikavälin tavoitteita. Samalla päätöksenteko strategian mukaisesti edesauttaa organisaation kilpailuedun rakentamista. Hyvin laadittu strategia auttaa organisaatiota erottumaan kilpailijoistaan tarjoamalla ainutlaatuisia arvoa tuottavia tekijöitä asiakkailleen.

Strategia luo yhteisen näkemyksen organisaation sisällä ja nivoo organisaatiota yhteen. Se auttaa jäseniä ymmärtämään organisaation tavoitteet ja sitoutumaan niiden saavuttamiseen. Tämä luo yhtenäisyyttä ja tukee tiimityötä. Strategialla on mahdollisuus myös tarjota mittareita ja puitteet organisaation suorituksen arviointiin. Se auttaa organisaatiota oppimaan omista toimintatavoistaan ja parantamaan niitä tarvittaessa.

Kaiken kaikkiaan onnistunut ja huolellisesti laadittu strategia on organisaation menestyksen perusta. Se toimii suunnannäyttäjänä, joka auttaa organisaatiota saavuttamaan tavoitteensa, hallitsemaan resurssejaan tehokkaasti ja sopeutumaan muuttuviin olosuhteisiin. (Loizos Heracleous, 2003)

Kyberturvallisuus muodostaa keskeisen osan kokonaisturvallisuutta ja on tullut yhä tärkeämmäksi osaksi yhteiskunnallista turvallisuutta nykyaikaisessa digitaalisessa maailmassa. Kyseessä on laaja ja monimutkainen käsite, joka ulottuu yli fyysisen turvallisuuden ja koskettaa taloudellisia, poliittisia ja yhteiskunnallisia ulottuvuuksia.

Puolustusministeriön turvallisuuskomitea otti vuonna 2021 kantaa pandemian tuomiin ongelmiin ja painotti miten kriittinen osa kokonaisturvallisuutta esimerkiksi viestintäverkkojen turvallisuuden ja toimintavarmuuden varmistaminen on (Turvallisuuskomitea 2021). Kyberiskuilla ja esimerkiksi palvelunestohyökkäyksillä olisi mahdollista pyrkiä häiritsemään tele- ja verkkoliikennettä ja näin lamauttaa tai ainakin häiritä iskun kohteen toimintaa, oli se sitten yksittäinen yritys tai laajempi organisaatiokokonaisuus.

Kriittinen infrastruktuuri ja resilienssi: Kyberturvallisuuden näkökulmasta tärkeä näkökohta on kriittisen infrastruktuurin, kuten sähköverkkojen, vesihuollon ja liikenteen, suojeleminen. Yhteiskunnan toimivuus riippuu suuresti näiden infrastruktuurijärjestelmien häiriöttömästä toiminnasta, ja kyberhyökkäykset voivat heikentää niiden resilienssiä.

Kansallinen puolustus ja kyberhyökkäykset: Kyberulottuvuus on nykyään kiinteä osa kansallista puolustusta monissa maissa. Kyberhyökkäykset voivat kohdistua valtion tietojärjestelmiin, asevoimiin tai jopa ydinasejärjestelmiin. Kyberturvallisuuden strategiat ovat siten keskeisiä kansallisen turvallisuuden ylläpitämisessä.

Talous ja teollisuusvakoilu: Kyberturvallisuus liittyy myös taloudelliseen turvallisuuteen. Yritykset joutuvat usein kohteeksi teollisuusvakoilulle ja tietomurroille, jotka voivat vaarantaa niiden liiketoiminnan ja kilpailuedun.

Kansalaisten yksityisyys ja tietosuoja: Yksityisyydensuoja ja henkilötietojen turvallisuus ovat olennainen osa kokonaisturvallisuutta. Kyberhyökkäykset voivat vaarantaa kansalaisten yksityisyyden ja altistaa heidät tietoturvariskeille.

Kansallinen turvallisuus ja ulkoinen uhka: Kyberhyökkäykset voivat olla myös osa valtioiden välistä konfliktia ja hybridisotaa. Ne voivat kohdistua poliittisiin instituutioihin, vaikuttaa vaaleihin ja heikentää hallituksen toimintakykyä.

Yllä olevat näkökulmat korostavat, että kyberturvallisuus on laaja-alainen ja moniulotteinen käsite, joka vaikuttaa moniin eri osa-alueisiin kokonaisturvallisuuden puitteissa. Sen huomioiminen on välttämätöntä yhteiskunnan haavoittuvuuden vähentämiseksi ja sen toimivuuden säilyttämiseksi digitaalisen aikakauden haasteissa.

2.2 Yksityisten ja julkisten yhteisöjen erot

Strategian sisältö on muun muassa kyberturvallisuuden osalta vahvasti riippuvainen siitä onko kyseessä yksityinen yritys vai julkinen yhteisö. Valtiotasolla kyberturvallisuuden ylläpitämisessä ja kehittämissä tuleekin ottaa huomioon, että huomattava osa esimerkiksi kriittisestä infrastruktuurista on yksityisessä omistuksessa valtion sijaan. Jason Healey (2017) arvioi jopa 85 prosenttia Yhdysvaltojen kriittisestä infrastruktuurista olevan yksityisen sektorin hallinnassa.

Artikkelissaan Healey erottelee lähestymistavat valtiojohtoiseen, yksityiseen ja nämä yhdistävään kumppanuuteen. Valtiojohtoisessa lähestymistavassa vahvuutena on skaalaus ja kontrolli. Mikäli valtio hallitsisi eri osa-alueita, esimerkiksi verkon suojausta, resursseja pystyttäisiin keskittämään nopeasti tarpeen mukaan. Kyberturvallisuuden päällimmäisenä organisoijana valtio taas pystyisi antamaan yhteneväisiä ohjeistuksia organisaatioille ja pyrkisi ohjaamaan niitä samaan suuntaan uhkien torjumiseksi. Kumppanuuslähtöisesti valtio ja yksityiset toimijat olisivat lähtökohtaisesti tasa-arvoisessa asemassa. Tällöin valtiolla ei olisi monopolia kybersuojauksessa, vaan yksityisillä omistajilla olisi myös mahdollisuus vaikuttaa omaan tekemiseensä. Yksityisen sektorin johtamassa lähestymistavassa turvallisuudesta ja infrastruktuurista vastaavat tahot olisivat pääosin itsenäisiä valtion ohjauksesta. Kyberhyökkäykset kohdistuvat usein yksittäisiin yrityksiin ja yritykset suojautuvat sekä korjaavat haavoittuvuuksia ilman valtion väliintuloa. Yksityisen sektorin ollessa vastuussa infrastruktuurista, valtio on kuitenkin taustalla tukemassa. (Healey, 2017)

Euroopassa esimerkiksi Ranska on osoittanut julkisia investointeja yksityiseen sektoriin ja ottanut tällä osan kontrollista kybertuvallisuuden osalta. Ranskan hallituksella on läheisiä välejä yksityiseen sektoriin, ja suhteet vaikuttavat myös muun muassa edellä mainitun kriittisen infrastruktuurin hallintaan ja ylläpitoon. Isossa Britanniassa taas valtion ja yritysten raja on selkeämpi ja kyberturvallisuus on enemmän yksityisten toimijoiden varassa. Ilman Ranskan tyyppisiä keskitettyjä toimintoja, valtiolla ei ole samanlaista vaikutusvaltaa toimintaan. (Calcara & Marchetti, 2021)

Yritysmaailman roolia osana kansallista kyberturvallisuutta on tutkittu ja strategioita on luotu näiden yhteistoiminnan vahvistamiseksi. James Farwell (2012) antaa sekä positiivisia sekä negatiivisia huomioita eri tavoista, joilla yhteistyötä yritysten ja valtion välillä olisi mahdollista kehittää. Lainsäädännön muuttaminen on yleisesti kankeaa ja hidastempoista, eikä lainsäädännöllä muutettavat määräykset esimerkiksi hyväksyttyjen turvallisuusstandardien käytöstä pysy kyberrikollisuuden perästä. Julkisten toimialojen, kuten sairaanhoidon ja armeijan, omistama data myös eroaa merkittävästi esimerkiksi kaupallisen alan yritysten datasta. Valtion tulee ottaa huomioon, että lainsäädännöllä otetaan huomioon molempien ääripäiden tarpeet, ilman että joko jätetään isoja määriä kriittistä dataa ilman lain määräämää suojaa tai pienet yritykset, joiden data ei ole relevanttia ulkopuolisille joutuvat kärsimään liian tiukoista rajoituksista.

Farwellin mukaan yhteistyö on tärkeää yksityisen ja julkisen sektorin välillä tällaisten ongelmien minimoimiseksi. Yhteistyö ja tietojen jakaminen kuitenkin luo omia haasteitaan. Kumppanuuslähtöisessä kyberturvallisuusstrategiassa tulee huolehtia siitä, että informaatio kulkee kumpaankin suuntaan tasapainoisesti, ilman että mahdollisia sensitiivisiä tietoja päätyy ulkopuolisten käsiin. Kumppanuudet ja yhteiset kuitenkin nopeuttavat suojautumista, tiedonvälitystä ja mukautumista muuttuviin riskeihin. Internetin peruskäyttäjällä on artikkelin mukaan teknologiaa joka 15 vuotta aiemmin oli käytössä vain asevoimilla. Tämä teknologian kehitys on kasvattanut myös kyberhyökkäysten määrää, joten reagoinnin täytyy olla yhtä nopeaa ja tehokasta. (Farwell, 2012)

3 Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö

Vuoden 2013 Euroopan unionin kyberturvallisuusstrategia oli ensimmäinen laatuaan ja sen tarkoituksena oli varmistaa Euroopan unionin ja sen jäsenvaltioiden toimintaedellytykset ja kilpailukyky digitaalisessa maailmassa. Euroopan komissio julkisti strategian yhteisenä tiedonantona Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle 7. helmikuuta 2013. (Eur-Lex, 2013) Strategian keskeiset tavoitteet olivat kyberturvallisuuskulttuurin kehittäminen, tietoisuuden lisääminen, valmiuksien parantaminen, yhteistyön vahvistaminen ja kansainvälisten kumppanuuksien edistäminen. Strategiassa tunnistettiin myös keskeisiä kyberuhkia, kuten tietojen varastaminen ja väärentäminen, verkkoiskut ja kyberterrorismi. Tärkeimmät toimenpiteet liittyivät unionin yhteisen kyberturvallisuusstrategian laatimiseen, kansallisten valmiuksien kehittämiseen, yhteistyön edistämiseen, koulutukseen ja tietoisuuden lisäämiseen. Strategiaan sisältyi myös kyberturvallisuutta koskevien standardien kehittäminen ja kyberturvallisuuden yhteisten standardien edistäminen Euroopan unionin jäsenvaltioiden välillä.

Vuoden 2013 kyberturvallisuusstrategiassa keskityttiin kolmeen pääkohtaan: suojaamiseen, valvontaan ja valveuttamiseen. Strategian tavoitteena oli suojata kansallisia tieto- ja viestintäjärjestelmiä, varmistaa tietojen luottamuksellisuus ja saatavuus, sekä torjua kyberuhkia. Strategiassa korostettiin myös tarvetta kehittää kansainvälistä yhteistyötä ja jakaa tietoa kyberuhkista eri maiden välillä. Lisäksi strategiassa painotettiin julkisen ja yksityisen sektorin yhteistyön tärkeyttä, jotta kyberturvallisuutta voitaisiin parantaa koko yhteiskunnan tasolla.

Kyberturvallisuuskyvykkyyksien vahvistaminen osalta strategiassa korostettiin tarvetta kehittää jäsenvaltioiden kyberturvallisuuskyvykkyyksiä, kuten tietoturva-alan ammattilaisten koulutusta, tietojen jakamista ja yhteistyötä eri sidosryhmien välillä. Strategiassa korostettiin tarvetta myös kansainväliseen yhteistyöhön

kyberturvallisuusasioissa, erityisesti yhteistyöhön unionin kumppanimaiden kanssa ja kansainvälisten tietoturvaorganisaatioiden kanssa.

Valvonnan osalta strategiassa käsiteltiin enimmäkseen kyberrikollisuuden torjuntaa ja tarvetta yhteistyöhön lainvalvontaviranomaisten kanssa, jotta kyberrikolliset saataisiin vastuuseen teoistaan. Torjunnan lisäksi strategiassa korostettiin tarvetta suojata henkilötietoja ja muita arkaluonteisia tietoja digitaalisessa ympäristössä kyberhyökkäysten varalta.

Valveuttamiseen liittyen strategiassa korostettiin koulutuksen, tietoisuuden ja ymmärryksen lisäämisen merkitystä kyberturvallisuudesta, jotta kansalaiset ja organisaatiot olisivat paremmin valmistautuneita kyberuhkiin ja osaisivat suojata itseään paremmin. Strategiassa esitettiin myös konkreettisia toimenpiteitä, kuten kansallisen kyberharjoituksen järjestämistä ja kyberturvallisuusalan yhteistyön tiivistämistä.

Vuoden 2013 kyberturvallisuusstrategiassa tunnistettiin myös useita haasteita, jotka vaikuttavat kyberturvallisuuden parantamiseen. Yksi keskeinen haaste oli nopeasti kehittyvä teknologia, joka johti uusien kyberuhkien syntyyn ja edellytti jatkuvaa kehittämistä ja päivittämistä kyberturvallisuuskyvykkyyksien ylläpitämiseksi. Toinen haaste oli kyberhyökkäysten monimuotoisuus ja monimutkaisuus, jotka edellyttivät laajaa yhteistyötä eri organisaatioiden välillä kyberuhkien torjumiseksi.

Lisäksi strategiassa tunnistettiin haasteita liittyen yhteistyöhön ja tiedonvaihtoon. Kyberhyökkäykset eivät tunnista kansallisia rajoja, mikä edellyttää kansainvälistä yhteistyötä ja koordinaatiota kyberuhkien torjumiseksi. Yhteistyö ja tiedonvaihto eri organisaatioiden välillä nähtiin mahdollisuuden lisäksi myös haasteena, sillä eri organisaatiot käyttävät erilaisia teknologioita ja järjestelmiä, mikä vaikeuttaa tietojen yhdistämistä ja analysointia.

Lisäksi strategiassa korostettiin henkilöstön osaamisen ja resurssien riittävyyden merkitystä kyberturvallisuuden parantamisessa. Henkilöstön koulutus ja tietoisuuden lisääminen kyberuhkista ovat avainasemassa, jotta organisaatiot pystyvät tunnistamaan ja torjumaan kyberuhkia tehokkaasti.

3.1 Strategian tavoitteet

Vuoden 2013 kyberturvallisuusstrategiassa (Eur-Lex, 2013) oli useita tavoitteita edellä mainittuihin suojaamiseen, valvontaan ja valveuttamiseen liittyen. Kyberturvallisuuden perusperiaatteina pidettiin muun muassa perusoikeuksien, ilmaisunvapauden, henkilötietojen ja yksityisyyden suojaamista sekä avointa pääsyä jokaiselle Euroopan unionin alueella olevalle. Strategiassa haluttiin painottaa yhteistä vastuuta kyberturvallisuuden ylläpidosta sekä kommentoitiin samaan aikaan julkaistua lainsäädäntöehdotusta, jolla varmistetaan tiedonsiirto eri toimijoiden välillä. Yksityisillä toimijoilla ei ollut kannustimia auttaa heidän kilpailijoitaan varoittamalla heitä huomatuista haavoittuvuuksista tai uhista, joten lainsäädäntöä vaadittiin apuun. Lakiuudistuksella pyrittiin varmistamaan, että kriittisten alojen, kuten pankkitoiminnan, energian ja julkishallinnon toimijat pitävät tietoturvansa vaaditulla tasolla ja jakavat tietonsa verkko- ja tietoturvasta toimivaltaisten viranomaisten kanssa.

3.2 Strategiset toimenpiteet

Vuoden 2013 Euroopan unionin kyberturvallisuusstrategiassa (Eur-Lex, 2013) strategiset painopisteet oli jaettu viiteen osioon: Verkon vakauteen, verkkorikollisuuden huomattavaan vähentämiseen, yhteisen verkkopuolustuspolitiikan ja valmiuksien kehittämiseen, kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittämiseen sekä johdonmukaisen verkkotoimintapolitiikan luomiseen Euroopan unionille.

Strategiassa pyrittiin parantamaan kyberturvallisuutta tehokkaasti torjumalla kyberrikollisuutta, vahvistamalla kriittisten verkkoinfrastruktuurien suojelua ja

edistämällä kansainvälistä yhteistyötä kyberuhkien torjumiseksi. Lisäksi strategiassa korostettiin tarvetta lisätä tietoisuutta kyberuhkista kaikilla yhteiskunnan tasoilla ja edistää teknologista kehitystä kyberturvallisuuden alalla vastataksemme jatkuvasti muuttuviin kyberuhkiin. Strategian keskeisenä tavoitteena oli luoda vahvempi ja turvallisempi digitaalinen ympäristö Euroopassa.

3.3 World Economic Forum 2013

World Economic Forumin 8. maailmanlaajuisia riskejä kuvaavassa julkaisussa internettiä ja kyberturvallisuutta käsittelevä osio ” Digital Wildfires in a Hyperconnected World” käsittelee oleellisimpana uhkakuvana massiivista digitaalista disinformaatioaaltoa, jonka lisäksi se ottaa kantaa, miten verkkojen laajentuminen muodostaa uusia uhkakuvia kyberhyökkäysten ja jopa digitaaliseen terrorismiin liittyen. Raportti sisältää kaavion sivulla neljä, josta ilmenee, että vuonna 2013 sekä kyberhyökkäyksiä että tietomurtoja pidettiin lievästi todennäköisempänä verrattuna edeltävään vuoteen. Vuodessa muutos ei ole iso, mutta pienikin muutos kertoo, että ensimmäistä kyberturvallisuusstrategiaa valmistellessa, uhkien trendi ei ole ollut ainakaan aleneva. Kyberhyökkäyksiä pidettiin sekä todennäköisempänä, että suurempaa vahinkoa aiheuttavana tietomurtoihin nähden.

4 Tunnetut ja laajat verkkohyökkäykset

Tässä luvussa tullaan käymään läpi vuosien 2013 ja 2020 välillä Euroopan Unionin alueella tapahtuneita laajoja tai kriittisiä verkkohyökkäyksiä.

World Economic Forumin vuoden 2020 riskiraportissa on heti ensimmäisellä sivulla nähtävillä taulukot todennäköisimmistä ja vakavimmista maailmanlaajuisista riskeistä vuosien 2007 ja 2020 välillä. Riskiluokitukset on annettu jokaisesta foorumin osa-alueesta, joten teknologiset riskit (kuten kyberhyökkäykset) on vain yhtenä osa-alueena. Kuvasta pystyy silti näkemään, että ensimmäisen strategian luontiaikana kyberhyökkäykset ovat olleet todennäköisimpien riskien listalla neljäntenä. Muutaman välivuoden jälkeen kyberhyökkäykset palasivat listalle 2018 ja 2019 sekä niihin liittyvänä riskinä nousi tietomurrot ja -huijaukset.
Yhteensä kyberhyökkäykset ovat olleet vertailun kohteena olevien ensimmäisen ja toisen kyberturvallisuusstrategian välisenä aikana kolmesti, vuosina 2014, 2018 ja 2019. Tietomurrot ja -huijaukset nousivat samaiselle listalle niin ikään kolmesti, 2017, 2018 ja 2019. Vaikka esimerkiksi vuonna 2020 viisi todennäköisintä riskiä liittyivät kaikki ympäristöön, sisältäen muun muassa äärimmäiset sääolosuhteet ja biodiversiteetin menettämisen, se ei suoranaisesti tarkoita kybertilanteen parantumista.

4.1 WannaCry

WannaCry-hyökkäys tapahtui toukokuussa 2017, kun haittaohjelma levisi nopeasti eri puolille maailmaa, aiheuttaen merkittäviä häiriöitä lukuisille yrityksille, organisaatioille ja julkishallinnolle. Hyökkäys hyödynsi EternalBlue-nimistä haavoittuvuutta, joka oli peräisin Yhdysvaltain kansallisen turvallisuusviraston (NSA) varastetuista hakkerointityökaluista. Haavoittuvuus koski Microsoftin Windows-käyttöjärjestelmiä, joihin ei ollut asennettu uusimpia päivityksiä. Haavoittuvuus itsessään ja WannaCryn vaarallisuus olivat niin vakavia, että Microsoft päätyi tekemään korjaavan päivityksen

paitsi tuetuille järjestelmilleen, myös vielä 2017 yleisesti käytössä olleille Windows XP ja Windows 2003 -järjestelmille, joille Microsoft ei ollut antanut tukea vuosiin. (Harkins & Freed, 2018)

Euroopan alueella WannaCry-virus aiheutti laajaa tuhoa. Etenkin Isossa Britanniassa NHS (National Health Service) -terveydenhuoltojärjestelmään kohdistui merkittäviä vaikutuksia. Useat sairaalat ja terveyskeskukset joutuivat sulkemaan toimintojaan ja perumaan hoitojaan, kun tietojärjestelmiä ei voitu käyttää. Tämä vaikutti vakavasti potilasturvallisuuteen ja terveydenhuollon palveluiden saatavuuteen. (NHS, 2023)

WannaCry-hyökkäys osoitti selkeästi, kuinka haavoittuvainen Euroopan alueen tietoinfrastruktuuri voi olla kyberuhkien edessä. Monet organisaatiot eivät olleet tehneet riittäviä tietoturvatoimia, kuten päivittäneet järjestelmiään tai varmistaneet tietojensa asianmukaista varmuuskopiointia. Tämä antoi WannaCry-virukselle mahdollisuuden levitä nopeasti ja aiheuttaa suurta vahinkoa.

Euroopan unionin reaktio WannaCry-hyökkäykseen oli nopea ja päättäväinen. Euroopan komissio ja kyberturvallisuusvirasto ENISA koordinoivat toimia jäsenvaltioiden kanssa. Komissio julkaisi tiedotteen, jossa kehotettiin jäsenvaltioita tiivistämään yhteistyötään ja parantamaan kyberturvallisuuttaan. ENISA tarjosi teknistä tukea jäsenvaltioille ja auttoi levittämään tietoa haavoittuvuudesta ja suojaustoimenpiteistä. (ENISA, 2017)

WannaCry-hyökkäys toimi herätyskellona Euroopan unionille kyberuhkien vakavuudesta. Tämä tapaus korosti tarvetta vahvistaa unionin kyberpuolustuskykyä ja lisätä yhteistyötä jäsenvaltioiden välillä. Euroopan unioni on ottanut käyttöön useita toimenpiteitä kyberturvallisuuden parantamiseksi, kuten kyberturvallisuusdirektiivin ja Euroopan kyberturvallisuusviraston vahvistamisen. Lisäksi Euroopan unioni on aktiivisesti mukana kansainvälisessä yhteistyössä kyberturvallisuuden edistämiseksi.

WannaCry-hyökkäys myös paljasti Euroopan alueen haavoittuvuudet kyberhyökkäyksille ja korosti tarvetta jatkuvasti kehittää ja päivittää tietoturvatoimia. Kyberuhkien kasvaessa Euroopan unionin on keskityttävä entistä enemmän kyberresilienssin ja valmiuden vahvistamiseen. Yhteistyön lisääminen, tiedonjakaminen ja kyberturvallisuuskoulutuksen parantaminen ovat avainasemassa, jotta Euroopan unioni voi tehokkaasti torjua tulevia kyberuhkia.

4.2 Petya & NotPetya

Petya-nimellä tunnettu haittaohjelma ilmestyi ensimmäisen kerran vuonna 2016. Se levisi laajalti ympäri maailmaa ja vaikutti moniin suuriin yrityksiin ja organisaatioihin. Petya hyödynsi EternalBlue-haavoittuvuutta, joka oli WannaCry-viruksen tavoin peräisin Yhdysvaltain kansallisen turvallisuusviraston (NSA) varastetuista hakkerointityökaluista. Petya hyökkäsi järjestelmiin, kryptasi käyttäjän tiedostot ja vaati lunnaita salauksen purkamiseksi. (Pandasecurity, 2017)

NotPetya-hyökkäys tapahtui vuonna 2017 ja oli edistyneempi versio Petya-haittaohjelmasta. Se levisi pääasiassa Ukrainassa, mutta vaikutti myös muihin maihin. NotPetya hyödynsi saman EternalBlue-haavoittuvuuden lisäksi muita keinoja levitä ja aiheuttaa vahinkoa. Hyökkäyksen tavoitteena oli tuhota ja häiritä järjestelmiä, eikä se ollut ensisijaisesti taloudellisesti motivoitu, vaikka se vaati myös lunnaita. (BBC 2017)

Petya- ja NotPetya-hyökkäyksillä oli laajat vaikutukset sekä taloudellisesti että operatiivisesti. Ne aiheuttivat suuria häiriöitä eri teollisuudenaloille, kuten logistiikkaan, energiantuotantoon, pankkialalle ja terveydenhuoltoon. Monet yritykset joutuivat sulkemaan toimintojaan ja kärsivät suuria taloudellisia menetyksiä. Esimerkiksi Capanon (2023) artikkelissa keskitytään Maersk-nimiseen yritykseen, joka on yksi maailman suurimmista merenkulun yrityksistä. Yksin Maersk kärsi arvioiden mukaan 250–300 miljoonan dollarin menetykset NotPetya-hyökkäyksen seurauksena.

Petya- ja NotPetya-hyökkäykset korostivat kyberuhkien vakavuutta ja kyvykkyyttä aiheuttaa laajoja häiriöitä yhteiskunnalle. Ne osoittivat myös, että hyökkääjät voivat hyödyntää varastettuja hakkerointityökaluja ja haavoittuvuuksia luodakseen tuhoisia haittaohjelmia. Näiden hyökkäysten vaikutukset korostivat tarvetta vahvistaa organisaatioiden ja valtioiden kyberpuolustuskykyä sekä investoida tietoturvatoimenpiteisiin ja valmiussuunnitelmiin. (BBC, 2017b)

Petya- ja NotPetya-hyökkäysten seurauksena on tapahtunut merkittäviä muutoksia kyberturvallisuuden käytännöissä ja politiikoissa. Organisaatiot ja valtiot ovat parantaneet tietoturvatoimiaan, lisänneet tietoisuutta haavoittuvuuksista ja käyttäneet enemmän resursseja kyberturvallisuuden vahvistamiseen. Esimerkiksi Euroopan unioni on ottanut käyttöön kyberresilienssiä koskevia strategioita ja direktiivejä, joilla pyritään parantamaan organisaatioiden ja valtioiden valmiutta vastata kyberhyökkäyksiin.

4.3 Hyökkäyksiä valtiollisiin elimiin

Myöskään valtiolliset elimet ja toimijat eivät ole säästyneet tietomurroilta. Alla on esiteltynä muutamia esimerkkejä ensimmäisen kyberturvallisuusstrategian julkistamisen jälkeen tapahtuneista tietomurroista Euroopan Unionin alueella. Tietomurrot valtiollisiin toimielimiin ovat omiaan aiheuttamaan vakavaa vahinkoa tai vähintäänkin turvallisuusriskejä salatun materiaalin ja kriittisen informaation määrän takia.

Ylen heinäkuussa 2014 julkaiseman uutisartikkelin mukaan ulkoministeriö on joutunut verkkovakoilun kohteeksi, joka tuli viranomaisten tietoon kevättalvella 2013. Ulkoministeri Erkki Tuomiojan mukaan vinkki vakoiluohjelmasta tuli ulkopuolelta, mutta ei tarkentanut mistä tämä vihje on peräisin. Vakoilun kerrottiin jatkuneen vuosia ja suojelupoliisin tutkivan havaittua verkkovakoilua. Samassa artikkelissa kerrottiin, että kaikkein arkaluontoisin tieto ei ole päätynyt verkkovakoilijan haltuun. (Yle, 2014)

Helsingin Sanomien saman vuoden syyskuussa julkaiseman artikkeli antaa tarkempaa tietoa ja kertoo, että ulkoministeriöön tehtiin vuonna 2013 tietomurto Uroboros-haittaohjelmalla, jonka johdosta huomattava määrä luottamuksellista dataa päätyi vakoojien haltuun. Paperille tulostettuna datamäärä olisi artikkelin mukaan mitattu rekkalasteissa. Tämä data oli julkiseen verkkoon kytketystä verkosta kaapattuja alimman turvaluokan viranomaistietoja. Uutisartikkeli tarkensi, että Suomi sai tiedon verkkovakoilusta tammikuussa 2013 Ruotsin puolustusministeriön alaiselta signaalitiedustelulaitokselta. Tutkinta kesti kolme kuukautta, koska Uroboros peitti tehokkaasti jälkensä. Kesän 2013 alussa Suomi oli alkanut jakamaan tunnusmerkkejä haittaohjelman toiminnasta muille valtioille, jolloin paljastui, ettei Suomi ollut vakoilun ainut uhri. Artikkelin mukaan tietoturvayhtiöt ovat löytäneet jälkiä Uroborosista muun muassa useista maista ympäri Eurooppaa sekä Yhdysvalloista. (Helsingin sanomat, 2014) Ilta Sanomat on myös julkaissut artikkelin vuonna 2019 liittyen samaiseen ulkoministeriöön kohdistuneeseen verkkovakoiluun. Tämän mukaan suojelupoliisi on keskeyttänyt verkkovakoiluun liittyvän tutkinnan, koska rikosepäilyä ei ollut kuuden vuoden aikana voitu kohdistaa kehenkään yksittäiseen henkilöön. (Iltasanomat, 2019)

Norjan parlamentti on vastaavasti ollut uutisissa tietomurron vuoksi vuonna 2020. Muun muassa lakiin keskittynyt Courthouse News Service, teknologiauutissivusto ZDNet ja Euronews ovat kirjoittaneet uutisartikkelit Norjan poliisin (Politiets sikkerhetstjeneste, PST) julkaiseman tiedotteen pohjalta joulukuussa 2020. Muun muassa BBC uutisoi jo syyskuun alussa, että Norjan parlamenttiin on hyökätty hakkereiden toimesta. Uutisartikkeli kertoo tiiviisti useampien työväenpuoleen, silloisen pääoppositiopuolueen, edustajien sähköpostien joutuneen hakkeroinnin uhreiksi ja että tilannetta analysoidaan vahinkojen kartoittamiseksi. (BBC, 2020)

Tarkempaa tietoa tapauksesta annettiin joulukuussa Norjan poliisin julkaistua aiemmin mainitun tiedotteen. Tiedotteen mukaan sähköposteihin oli päästy käsiksi väsytyshyökkäyksellä (engl. brute force), jossa salasanoja tuotetaan ja käytetään tileihin odottaen, että oikea salasana avaa tilin. Useampia sähköpostitilejä oli onnistuttu

avaamaan tällä tekniikalla, ja niistä löytynyttä arkaluontoista materiaalia oli päätynyt hakkereiden haltuun. Samat hakkerit olivat yrittäneet päästä syvemmälle kohdejärjestelmiin, mutta analysoidun datan mukaan yritykset eivät olleet onnistuneet. Tiedotteessa huomautetaan, että yleiset turvallisuusmekanismit, kuten käyttäjän kaksivaiheinen todennus kirjautumisen yhteydessä olisi todennäköisesti estänyt tietomurron. (PST 2020)

Jo samana päivänä Euronews (2020) julkaisi artikkelin, jossa epäillään venäläistä hakkeriryhmää parlamentin tietomurron tekijöiksi. Norjan sisäisen turvallisuuden viraston mukaan tutkimukset osoittavat Venäjän sotilasvoimiin kytköksissä olevan APT28-nimisen ryhmän olevan vastuussa tietomurrosta. Viraston mukaan tutkimukset on kuitenkin keskeytetty riittävien todisteiden puuttuessa. Artikkelissa myös muistutetaan miten Norjan ulkoministeri Ine Eriksen Søreide syytti Venäjää tietomurrosta jo lokakuussa mainiten myös, miten Venäjä piti tällaista syytöstä mahdottomana hyväksyä ja valtioiden välistä suhdetta tuhoavana provokaationa.

Viimeisimpänä esimerkkinä Norjan parlamentin tavoin, myös Saksan parlamentti joutui tietomurron kohteeksi vuonna 2016. BBC julkaisi toukokuussa 2016 artikkelin, jossa kerrotaan Venäjälle oletettavasti työskennelleen hakkeriryhmän tehneen useita cyber hyökkäyksiä Saksan tietojärjestelmiä vastaan. (BBC, 2016)

5 EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle

Euroopan Unionin kyberturvallisuusstrategia vuodelta 2020 pyrkii vastaamaan yhä kasvavaan kyberuhkien määrään, monimuotoisuuteen ja vakavuuteen. Euroopan komissio julkisti strategian yhteisenä tiedonantona Euroopan parlamentille ja neuvosotolle 16. joulukuuta 2020. (Eur-Lex, 2020)
Strategian mukaan kyberuhkat ovat yleisempiä, laajemmin levinneitä ja monimutkaisempia kuin koskaan aiemmin. Tästä syystä strategian kolmeksi keskeisimmäksi osaksi on muodostunut turvallisuuden parantaminen, valmiuden lisääminen sekä strategisten kyberturvallisuuskykyjen kehittäminen

Strategiassa mainittu digitaalisten haavoittuvuuksien korjaaminen ja tietoverkkojen turvallisuuden parantaminen tarkoittaa, että Euroopan unionin ja sen jäsenmaiden on parannettava tietoverkkojensa turvallisuutta, suojauduttava tietomurroilta ja estettävä haitallisten toimien leviäminen tietoverkkojen kautta. Unionin on kehitettävä ja ylläpidettävä valmiutta vastata kyberhyökkäyksiin, jotta sen kansalaiset ja yritykset voivat turvallisesti käyttää digitaalisia palveluita. Tämä edellyttää myös yhteistyötä jäsenmaiden kesken sekä yhteistyötä kansainvälisten kumppanien kanssa. Euroopan unionin on myös strategian mukaisesti kehitettävä ja ylläpidettävä tarvittavia teknologisia ja inhimillisiä resursseja vastatakseen nykyisiin ja tuleviin kyberuhkiin. Se sisältää myös investoimisen innovatiivisiin ratkaisuihin ja teknologioihin, jotta Euroopan unioni pysyy ajan tasalla nopeasti kehittyvässä digitaalisessa ympäristössä.

Strategia käsittelee laajasti digitaalisen ympäristön haasteita ja korostaa tarvetta jatkuvasti kehittää ja päivittää kyberturvallisuuskyvykkyyksiä vastaamaan yhä monimutkaisempia ja kehittyneempiä kyberuhkia. Strategia korostaa organisaatioiden, yritysten ja yhteiskuntien kykyä häiriönsietokykyä eli kykyä selviytyä kyberhyökkäyksistä ja vastata niihin nopeasti ja tehokkaasti. Tämä tarkoittaa, että organisaatioiden on varauduttava kyberhyökkäyksiin etukäteen ja laadittava suunnitelmia, joiden avulla ne

voivat minimoida mahdolliset vahingot ja palautua hyökkäysten jälkeen mahdollisimman nopeasti.

Strategia ottaa huomioon tuoreita teknologioita, kuten 5G-verkot, ja ottaa huomioon näihin liittyviä kyberriskejä. Tarvetta teknologian kehittämiseen ja innovaatioihin, joilla voidaan vastata kasvavaan kyberuhkien määrään, huomioidaan myös muilla tavoin. Esimerkiksi tekoälyn ja koneoppimisen hyödyntämistä voidaan käyttää kyberturvallisuuden parantamisessa, uusia tietoturvateknologioita kehitetään tauotta ja sekä uusien liiketoimintamallien luonnilla voidaan vähentää riskejä ja parantaa tietoturvaa.

5.1 Strategian tavoitteet

Vuoden 2020 kyberturvallisuusstrategian päätavoitteena on varmistaa maailmanlaajuinen ja avoin internet, jossa eurooppalaisten turvallisuutta ja perusoikeuksia ja -vapauksia voidaan tehokkaasti suojella niihin kohdistuvilta riskeiltä (Eur-Lex, 2020) Tähän tavoitteeseen pyritään pääsemään usean osatavoitteen voimin.

EU pyrkii parantamaan kyberturvallisuutta yhteistyössä jäsenmaiden, yritysten ja kansalaisyhteiskunnan kanssa. Kyberturvallisuuden parantaminen on olennaisen tärkeää, jotta ihmiset voivat luottaa siihen, että esimerkiksi digitaalisten palveluiden käyttö on turvallista sekä henkilötiedot ovat asianmukaisesti suojattuja. Infrastruktuurin ja kriittisten palveluiden häiriönsietokykyä myös pidetään yllä ja pyritään parantamaan.

Toisena osana strategiassa puhutaan kyberturvallisuusjärjestelmien kehittämisestä. Yhtenä konkreettisena tapana kehittää järjestelmiä, komissio ehdottaa strategiassa, että koko Euroopan unionin alueelle rakennettaisiin tietoturvan valvomopalveluiden verkosto. Tällä pyritään parantamaan viestintää eri viranomaistahojen välillä ja nopeuttamaan informaation kulkua esimerkiksi haavoittuvuuksien tai uhkien ilmestyessä. Samoin strategia pyrkii vahvistamaan tietoturvaa yksityisellä sektorilla ja

valvomopalveluiden piiriin ja niiden osaksi tulisi valtiollisten toimijoiden lisäksi muun muassa pk-yrityksiä.

Digitaalisia taitojen kehityksen jatkamista tulisi strategian mukaan jatkaa samoin kuin uusien innovaatioiden edistämistä. Uudet innovaatiot ovat omiaan parantamaan kyberturvallisuutta Euroopan unionin alueella ja digitaalisten taitojen kehittäminen pienentää muun muassa inhimillisten virheiden riskejä.

Strategian tavoitteiden saavuttamiseksi EU suunnittelee useita toimenpiteitä, kuten Euroopan unionin tietoturvaviraston (ENISA) vahvistamista ja yhteistyön parantamista jäsenmaiden välillä. Lisäksi EU pyrkii kehittämään kyberturvallisuusstandardit ja -sertifikaatit, jotka edistävät parempaa tietoverkkojen turvallisuutta. Strategian avulla EU pyrkii takaamaan, että digitaalinen ympäristö on turvallinen, että kansalaisten yksityisyys ja henkilötiedot ovat suojattuja ja että talouskasvu ja innovaatiot voivat jatkua häiriöttä.

5.2 Strategiset toimenpiteet

Vuoden 2020 Euroopan unionin kyberturvallisuusstrategiassa keskeisinä tavoitteina ovat vastustuskyvyn vahvistaminen, kyberrikollisuuden torjunta ja infrastruktuurin suojaaminen. Strategiassa painotettiin unionin kyberturvallisuuden kokonaisvaltaisen vastustuskyvyn parantamista jäsenvaltioiden ja unionin instituutioiden tasolla. Lisäksi tavoitteena oli tehostaa toimia kyberrikollisuuden torjumiseksi ja vahvistaa unionin kykyä havaita, tutkia ja torjua kyberrikoksia. Infrastruktuurin suojaamiseen liittyen pyrittiin vahvistamaan kriittisten infrastruktuurien, kuten sähköverkkojen ja terveydenhuollon järjestelmien, kyberturvallisuutta ja varmistamaan niiden jatkuvuus kyberuhilta. Lisäksi strategiassa korostettiin kansainvälisen yhteistyön tärkeyttä kyberturvallisuuden alalla sekä yksityisen ja julkisen sektorin välisen yhteistyön lisäämistä. Strategian tavoitteena oli luoda turvallisempi ja vastustuskykyisempi digitaalinen ympäristö Euroopassa vastataksemme nykyisiin ja tuleviin kyberuhkiin.

5.3 Kyberturvallisuusraportit ja World Economic Forum 2020

World Economic Forumin 15. maailmanlaajuisia riskejä kuvaavassa julkaisussa internettiä ja kyberturvallisuutta käsittelevä osio ”Wild Wide Web” käsittelee uusia teknologioita ja niihin liittyviä riskejä. Uusista teknologioista, kuten kehittyvästä tekoälystä ja pilvipalveluiden laajenemisesta. koostuu merkittävä osa riskien liikkeistä sivujen kolme ja neljä taulukoissa. Kaikki teknologiaan liitetyt riskit, kyberhyökkäykset, datavarkaudet sekä teknologian kehityksen negatiiviset vaikutukset ovat vaikutuksiltaan suurempia, kun verrataan vuosia 2019 ja 2020 keskenään. Infrastruktuurin hajoaminen on pysynyt melkein samassa tilassa, vaikkakin myös sen vaikutuksia on arvioitu lievästi korkeammiksi. (World Economic Forum, 2020)

Forumin mukaan teknologioiden kehitys on jatkuvaa kilpajuoksua, jolloin uusimman teknologian ensimmäisillä käyttäjillä on selkeä etulyöntiasema muihin nähden. Neljänteen teolliseen vallankumoukseen, eli digitaalisen itsenäisyyden aikaan liittyviä patenttihakemuksia tehdään kasvavissa määrin, joten myös tietoturvan täytyisi kehittyä samassa tahdissa. (World Economic Forum, 2020)

6 Strategioiden vertailu

Tässä kappaleessa vertaillaan edellä mainittuja Euroopan unionin vuosien 2013 ja 2020 kyberturvallisuusstrategioita sekä vastaavien vuosien World Economic Forumin riskiraporttien sisältöjä keskenään. Kappaleessa käsitellyt tiedot pohjautuvat mainittuihin strategioihin ja raportteihin ellei toisin mainita.

6.1 Kyberturvallisuusstrategioiden vertailu

Euroopan unionin ensimmäinen kyberturvallisuusstrategia julkaistiin vuonna 2013 (Eur-Lex, 2013) ja siitä lähtien kyberturvallisuuden haasteet ovat kasvaneet merkittävästi. Tästä syystä EU alkoi valmistelemaan uutta kyberturvallisuusstrategiaansa ja julkaisi päivitetyn strategian vuonna 2020 (Eur-Lex, 2020).

Vuoden 2020 strategia on kattavampi ja kohdistuu laajempiin haasteisiin, kuten tekoälyyn, esineiden internetiin (IoT) ja disinformaatioon. Vuoden 2013 strategiassa näitä kolmea termiä ei käytetä kertaakaan, kun taas vuoden 2020 strategiassa esimerkiksi tekoäly saa huomiota uusien, tehokkaampien puolustautumistoimien mahdollistajana. Vuoden 2020 strategiassa korostaa myös muita uusia kyvykkyyksiä, kuten kehitettävää kvanttiteknologiaa kyberturvallisuuden tukemiseksi.

Vuoden 2020 strategia käsittelee globaaleja haasteita laajemmin kuin vuoden 2013 strategia. Esimerkkeinä tästä ovat kyberturvallisuusdiplomatia, yhteistyö kansainvälisten kumppanien kanssa ja kyberuhkien torjunta kansainvälisellä tasolla. Myös vihreä teknologia ja ympäristöasiat ovat saaneet tilaa vuoden 2020 strategiassa, toisin kuin vanhemmassa strategiassa.

Riskienhallinnassa ei ole määrältään merkittävää eroa eri strategioiden välillä. Molemmat strategiat tosin keskittyvät omien painopisteidensä riskienhallintaan. Vuonna 2013 keskityttiin enemmän tiedonvaihdon mahdollistamaan tehokkaampaan riskienhallintaan, kun taas vuonna 2020 keskityttiin esimerkiksi 5G-teknologian

riskienhallintaan uutena teknologiana. Huomioitavaa on, että erinäiset direktiivit kuten NIS-direktiivi, keskittyvät enemmän riskienhallintaan, joten kyberturvallisuusstrategioissa ei ole niihin erityisesti keskitytty.

Vuoden 2020 strategiassa korostetaan vahvistettua yhteistyötä jäsenmaiden välillä, jotta kyberturvallisuuskyvykkyydet ja parhaat käytännöt voitaisiin jakaa laajemmin. Tällaisesta yhteistyöstä puhuttiin jo vuoden 2013 strategiassa, mutta tarve yhteistyölle on vain lisääntynyt ja strategioiden ulkopuoliset ohjeistukset, säädökset ja direktiivit (kuten NIS-direktiivi) ovat vahvistaneet yhteistyötä ja kommunikaatiota näiden strategioiden välissä. Vuoden 2020 strategiassa korostetaan kriittisten infrastruktuurien, kuten energia- ja vesihuollon, rautatieverkon ja terveydenhuollon, suojaamisen merkitystä ja pyritään varmistamaan niiden jatkuvuus. Vuoden 2013 strategiassa neuvottiin lähinnä kriittisiä toimijoita arvioimaan omat kyberturvallisuusriskinsä, kun taas vuoden 2020 strategiassa kriittinen infrastruktuuri on saanut laajemman osuuden.

6.2 Riskiraporttien vertailu

Vaikka sekä Global Risks 2013 -raportti (World Economic Forum, 2013) että The Global Risks Report 2020 (World Economic Forum, 2020) käsittelevät kyberturvallisuutta ja kyberuhkia, niiden sisällöllä on joitain eroja, jotka heijastavat kyberturvallisuuden kehittymistä ja muuttuvia uhkakuvia ajan kuluessa.

Vuonna 2013 kyberuhkat olivat vielä suhteellisen uusi aihe globaaleissa riskeissä, ja niiden merkitystä ei ehkä ymmärretty täysin. Vuoteen 2020 mennessä kyberuhkat olivat nousseet keskeisiksi huolenaiheiksi, ja niistä oli tullut laajalti tunnettuja ja tunnustettuja uhkia. Kyberhyökkäykset ja niihin liittyvät tapahtumat ovat myös saaneet laajaa mediahuomiota vuosien 2013 ja 2020 välillä. Merkittävät tapaukset, kuten suuret tietomurrot ja verkkohyökkäykset, ovat olleet usein otsikoissa ja herättäneet keskustelua kyberuhkien vakavuudesta ja laajuudesta. Hallitukset ja kyberturvallisuuteen erikoistuneet organisaatiot ovat järjestäneet tiedotuskampanjoita ja valistusohjelmia, jotka pyrkivät lisäämään yleistä tietoisuutta kyberuhkista ja antamaan kansalaisille ja

yrityksille ohjeita turvallisemman verkkokäyttäytymisen edistämiseksi. Yritykset ovat alkaneet ymmärtää aiempaa paremmin kyberuhkien vakavuuden ja niiden potentiaaliset vaikutukset liiketoimintaan. Tämä on johtanut investointeihin kyberturvallisuuden parantamiseksi ja riskienhallinnan strategioiden kehittämiseksi. Kyberturvallisuuskoulutus ja -koulutusohjelmat ovat lisääntyneet eri tasoilla, mukaan lukien koulutuslaitokset, yritykset ja julkiset organisaatiot. Ihmiset ovat alkaneet ymmärtää paremmin kyberuhkien luonteen ja oppia keinoja suojautua niitä vastaan. Kyberhyökkäykset ovat lisääntyneet sekä määrällisesti että laadullisesti, mikä on lisännyt tietoisuutta niiden uhista. Tapausten lisääntyminen on pakottanut organisaatiot ja yksilöt kiinnittämään enemmän huomiota kyberturvallisuuteen ja valmistautumaan paremmin mahdollisiin hyökkäyksiin.

Vuoden 2020 raportti korostaa kyberhyökkäysten kasvavaa monimutkaisuutta ja vakavuutta verrattuna vuoden 2013 raporttiin. Teknologian kehittyminen ja kyberrikollisuuden ammattimaistuminen ovat johtaneet monimutkaisempiin ja laajamittaisempiin hyökkäyksiin. Teknologian jatkuva kehitys on mahdollistanut monimutkaisempien ja tehokkaampien hyökkäysten suunnittelun ja toteuttamisen. Esimerkiksi kehittyneemmät haittaohjelmat ja haitalliset työkalut tarjoavat hyökkääjille enemmän mahdollisuuksia päästä käsiksi järjestelmiin ja tietoihin. Kyberrikollisuus on muuttunut yhä ammattimaisemmaksi, ja hyökkääjät voivat olla osaorganisoituneita rikollisia verkostoja tai jopa valtiollisia toimijoita. Tämä ammattimaisuus tekee hyökkäyksistä monimutkaisempia ja vaikeampia havaita ja torjua. Nykyaikaiset hyökkäykset ovat usein monitasoisia ja monivaiheisia, joissa hyökkääjät käyttävät useita eri tekniikoita ja menetelmiä päästäkseen käsiksi kohdejärjestelmiin. Tällaiset hyökkäykset voivat olla vaikeita havaita ja torjua, koska ne voivat tapahtua useiden eri väylien kautta samanaikaisesti.

Vuoden 2020 raportissa korostetaan enemmän tietosuojan ja henkilökohtaisten tietojen suojan merkitystä, mikä heijastaa kasvavaa huolta yksityisyyden säilyttämisestä digitaalisessa ympäristössä. Henkilökohtaisia tietoja ovat kaikki tiedot, jotka liittyvät

tunnistettuun tai tunnistettavissa olevaan henkilöön. Tähän sisältyvät esimerkiksi nimi, osoite, syntymäaika, sähköpostiosoite, puhelinnumero, sosiaaliturvatunnus ja biometriset tiedot. Monissa maissa ja alueilla on voimassa tietosuojalainsäädäntöä, joka säätelee henkilökohtaisten tietojen käsittelyä ja suojaamista. Esimerkiksi Euroopan unionin yleinen tietosuoja-asetus (GDPR) asettaa tiukat vaatimukset henkilökohtaisten tietojen käsittelylle ja suojaamiselle. Organisaatioiden odotetaan noudattavan yksityisyysperiaatteita ja -käytäntöjä henkilökohtaisten tietojen käsittelyssä. Tämä voi sisältää tietojen keräämisen ja käytön rajoittamisen tarkoituksenmukaisiin tarkoituksiin sekä asianmukaisen tietoturvan ja suojaustoimenpiteiden toteuttamisen. Tietoturva on olennainen osa henkilökohtaisten tietojen suojaa. Organisaatioiden on toteutettava asianmukaisia teknisiä ja organisatorisia toimenpiteitä tietojen suojaamiseksi luvattomalta pääsyltä, tietojen vuotamiselta ja väärinkäytöltä. Tämä voi sisältää tietojen salaamisen, palomuurien käytön, pääsynhallinnan ja tietoturvatarkastusten suorittamisen. Yksilöille on tarjottava läpinäkyvyyttä siitä, miten heidän henkilökohtaisia tietojaan käsitellään, ja heille on annettava mahdollisuus antaa suostumus tietojensa keräämiseen ja käyttöön. Tämä voi sisältää tietojen käsittelyn tarkoituksen ja menetelmien selittämisen sekä mahdollisuuden kieltää tietojen käsittely tai pyytää tietojen poistamista.

Sosiaalisen median ja verkkofoorumien rooli tapahtumien välittämisessä ja tiedon jakamisessa on lisääntynyt merkittävästi vuosien varrella. Tämä on johtanut siihen, että kyberhyökkäykset saavat nopeasti laajaa näkyvyyttä ja herättävät keskustelua sosiaalisessa mediassa ja muissa verkkoalustoissa. Median kiinnostus kyberhyökkäyksiä kohtaan on kasvanut, ja kyberhyökkäykset saavat enemmän kattavuutta ja raportointia niin perinteisissä medioissa kuin verkossa. Tämä lisää yleistä tietoisuutta kyberuhkista ja voi myös kannustaa muita hyökkääjiä toimimaan. Hallitukset ja viranomaiset ovat kiinnittäneet enemmän huomiota kyberuhkiin ja niiden torjuntaan, mikä on lisännyt myös kyberhyökkäysten tapausten määrää ja näkyvyyttä. Viranomaisten toimet ja reaktiot kyberhyökkäyksiin ovat usein uutisoituja, mikä lisää niiden julkista tietoisuutta.

Yhteenvetona voisi todeta, että vaikka molemmat raportit käsittelevät kyberturvallisuutta ja kyberuhkia, niiden sisällöllä on eroja, jotka heijastavat kyberuhkien kehitystä ja muuttuvia uhkakuvia ajan kuluessa.

7 Uudet kyberturvallisuushaasteet

Nykyään yhä useampi elämämme osa-alue on siirtynyt digitaaliseen ympäristöön, mikä on johtanut myös uusien kyberturvallisuushaasteiden esiin tulemiseen. Yksi suuri haaste on tietojen ja henkilötietojen suojaaminen, sillä nykyään yksityishenkilöiden ja yritysten tiedot ovat alttiina monenlaisille uhkille, kuten tietomurroille, identiteettivarkauksille ja tietojenkalastelulle. Toisaalta myös yritykset ja organisaatiot ovat haavoittuvaisia kyberhyökkäyksille, joihin sisältyy esimerkiksi virusten, troijalaisten ja kiristyshaittaohjelmien leviäminen, tietomurrot sekä verkkosivujen tai palveluiden kaatuminen denial-of-service-hyökkäysten seurauksena. Lisäksi tekoälyyn perustuvat hyökkäykset ovat yleistymässä, mikä lisää entisestään haasteita kyberturvallisuuden varmistamisessa.

Toinen merkittävä haaste on kyberturvallisuustietoisuuden lisääminen. Vaikka monet yksityishenkilöt ja organisaatiot tietävät kyberuhkista, moni ei kuitenkaan osaa suojautua niiltä. Tietoisuuden lisääminen onkin tärkeää, jotta ihmiset ja organisaatiot voivat tunnistaa ja ennaltaehkäistä kyberhyökkäyksiä.

Lopuksi myös kansainväliset kyberturvallisuusongelmat ovat haaste nyky-yhteiskunnassa. Koska tietoja ja palveluita on helppo siirtää yli valtioiden rajojen, on tärkeää, että valtiot ja organisaatiot tekevät yhteistyötä kyberturvallisuuden varmistamiseksi. Ilman kansainvälistä yhteistyötä, kyberturvallisuuden varmistaminen voi olla haastavaa ja hyökkäysten seuraukset voivat olla erittäin vakavia.

8 Kyberturvallisuuden kehitys Euroopan Unionin alueella

Kaiken kaikkiaan vuodesta 2013 vuoteen 2020 Euroopan kyberturvallisuus on siirtynyt monimutkaisesta ja epäselvästä alasta merkittäväksi strategiseksi tavoitteeksi. Euroopan unioni ja sen jäsenvaltiot ovat tunnistaneet kyberuhkien vakavuuden uudella tavalla ja ovat ottaneet käyttöön toimenpiteitä, jotka pyrkivät parantamaan kyberpuolustuskykyä, tiedonjakoa ja yhteistyötä. Kuitenkin kyberturvallisuuden jatkuva kehittyminen edellyttää jatkuvaa tietoisuutta ja sitoutumista, jotta Euroopan alue säilyisi turvallisena digitaalisessa maailmassa.

Kyberuhkien kasvaessa Euroopan unioni ja sen jäsenvaltiot ovat lisänneet tietoisuutta kyberturvallisuuden merkityksestä. Tämä on johtanut myös resurssien kasvuun kyberpuolustuskyvyn parantamiseksi. Näitä resursseja on kohdennettu esimerkiksi haavoittuvuuksien tunnistamiseen ja korjaamiseen tärkeissä järjestelmissä, kuten julkishallinnossa ja terveydenhuollossa. Esimerkkinä resurssien kohdentamisesta sosiaali- ja terveysministeriö on julkaissut erillisen kyberturvallisuusohjeen sosiaali- ja terveydenhuollon toimijoille vuonna 2019. (Sari Vuorinen, 2019)

Myös säädöksillä ja direktiiveillä on ohjattu organisaatioita parantamaan kyberturvallisuuttaan. Jo edellä mainittu yhteistyön ja kommunikaation lisääminen on jatkunut vuoden 2013 kyberturvallisuusstrategiasta lähtien. Tämän lisäksi muun muassa NIS-direktiivi (Network and Information Security) on otettu käyttöön Euroopan unionin toimesta. NIS-direktiiviin perehdytään tarkemmin alla. (Eur-Lex, 2016)

Teknologian kehittyminen on tuonut sekä uusia mahdollisuuksia että haasteita. Kyberuhkien määrä on kasvanut vuosien varrella, ja hyökkäykset ovat muuttuneet monimutkaisemmiksi ja kohdistuneet laajemmin eri toimialoille. Toisaalta monimuotoisempien hyökkäysten mahdollistava teknologian nopea kehitys on samalla myös mahdollistanut uusia innovaatioita ja ratkaisuja kyberuhkien torjumiseksi.

8.1 NIS-direktiivi

Euroopan unionin verkko- ja tietoturvadirektiivi, toiselta nimeltään NIS-direktiivi, on merkittävä säädös, joka on suunniteltu vahvistamaan digitaalisen infrastruktuurin ja tietoverkkojen turvallisuutta Euroopan unionissa. Direktiivi on vastaus kasvavaan uhkaan kyberhyökkäyksistä ja tietoturvauhkista, jotka voivat vaarantaa EU-maiden turvallisuuden, talouden ja kansalaisten hyvinvoinnin. NIS-direktiivi astui voimaan vuonna 2016, ja sen tarkoituksena on edistää yhteistyötä jäsenvaltioiden välillä ja varmistaa, että kaikki EU-maat ottavat käyttöön vähimmäisvaatimukset kriittisen infrastruktuurin turvaamiseksi tietoverkkohyökkäyksiltä. (Eur-Lex, 2016)

NIS-direktiivi kohdistuu erityisesti tiettyihin toimialoihin, jotka ovat kriittisen infrastruktuurin ja digitaalisten palvelujen kannalta elintärkeitä. Tähän sisältyvät esimerkiksi energia, liikenne, terveydenhuolto, rahoitus ja digitaalipalveluntarjoajat. Nämä sektorit muodostavat perustan yhteiskunnan toiminnalle ja ovat alttiita merkittäville tietoturvauhkille ja hyökkäyksille. Tämän vuoksi NIS-direktiivi asettaa velvoitteita näille toimijoille tietoturvatoimenpiteiden toteuttamiseksi ja raportointivelvollisuuden tietoturvapoikkeamista.
Kriittiset infrastruktuurit ja digitaaliset palveluntarjoajat velvoitetaan suorittamaan säännöllisiä riskien arviointeja ja laatimaan riskinhallintasuunnitelmia. Tämän avulla ne voivat tunnistaa ja arvioida mahdolliset tietoturvauhat ja toteuttaa tarvittavat toimenpiteet riskien vähentämiseksi.

Direktiivi edellyttää, että kriittisten toimialojen toimijat ottavat käyttöön asianmukaisia tietoturvatoimenpiteitä ja -käytäntöjä, mukaan lukien tietojärjestelmien suojaus, verkkoturvallisuus, käyttöoikeuksien hallinta ja haavoittuvuuden hallinta. Direktiivillä asetetaan vaatimus ilmoittaa merkittävistä tietoturvapoikkeamista kansallisille viranomaisille. Tämän avulla viranomaiset voivat nopeasti reagoida ja koordinoida toimia vahinkojen minimoimiseksi ja palautumisen helpottamiseksi.

Direktiivi edistää yhteistyötä ja tiedonvaihtoa jäsenvaltioiden välillä sekä unionin tasolla. Oikea-aikainen ja informatiivinen tiedonvälitys mahdollistaa paremman ymmärryksen kyberuhkista ja hyökkäyksistä sekä parhaiden käytäntöjen jakamisen ja oppimisen. Direktiivissä määrätään lisäksi säännöllisestä seurannasta ja arvioinnista sen varmistamiseksi, että jäsenvaltiot noudattavat direktiivin vaatimuksia ja että niiden tietoturvatoimenpiteet ovat tehokkaita ja asianmukaisia. Asianmukaiset tietoturvatoimet sisältävät riskien tunnistamisen, arvioinnin ja hallinnan sekä tarvittavien tietoturvatoimenpiteiden ja -järjestelmien käyttöönoton.

Jäsenvaltioiden odotetaan seuraavan ja arvioivan NIS-direktiivin täytäntöönpanoa kansallisella tasolla varmistaakseen, että direktiivin vaatimukset ja velvoitteet toteutetaan asianmukaisesti. Euroopan unionin komissiolla on rooli direktiivin täytäntöönpanon valvonnassa ja seurannassa. Se voi antaa suosituksia ja ohjeita jäsenvaltioille, jotka eivät täytä direktiivin vaatimuksia asianmukaisesti. Yhtenä vaihtoehtona on myös sanktioiden jakaminen, mikäli direktiivin vaatimuksia ei saada täytettyä kehotuksista huolimatta.

Direktiivi edellyttää jäsenvaltioita varmistamaan, että kyber- ja tietoturvallisuuden alan sääntöjen rikkomisista voidaan määrätä tehokkaita, oikeasuhteisia ja varoittavia hallinnollisia sakkoja ja muita sanktioita. Sanktioiden tulee kattaa mahdolliset rikkomukset, kuten tietoturvaloukkaukset, ilmoitusvelvollisuuden laiminlyönnit ja vaatimusten noudattamatta jättämiset. Ne voivat vaihdella sakosta ja varoituksesta merkittäviin taloudellisiin seuraamuksiin. Sanktioiden on oltava oikeasuhteisia ja asianmukaisia rikkomuksen vakavuuteen nähden. Ne voivat myös kohdistua toistuviin rikkomuksiin, jotka eivät ole parantuneet asianmukaisesti.

NIS-direktiivi edistää myös kansainvälistä yhteistyötä kyberturvallisuuden alalla, mikä on tärkeää ottaen huomioon kyberuhkien rajat ylittävä luonne. Euroopan unionin ulkopuolisten maiden ja organisaatioiden kanssa tehtävän yhteistyön kautta pyritään parantamaan tietojen jakamista, parhaita käytäntöjä ja yhteisiä standardeja. Direktiivi

velvoittaa jäsenvaltiot edistämään tietojen vaihtoa ja yhteistyötä paitsi muiden EU-maiden, myös kolmansien maiden kanssa kyberturvallisuuden alalla. Direktiivi antaa Euroopan unionille valtuudet käydä neuvotteluja ja solmia sopimuksia kolmansien maiden kanssa kyberturvallisuuteen liittyvissä asioissa. Tämä voi sisältää tietojen vaihtoa, yhteistyötä kyberrikollisuuden torjunnassa ja tietoturvan edistämistä kansainvälisellä tasolla. NIS-direktiivi voi edistää myös kyberdiplomatian kehittämistä ja Euroopan unionin roolin vahvistamista kansainvälisenä toimijana kyberasioiden hallinnassa. Direktiivissä voidaan myös kannustaa perustamaan kansainvälisiä foorumeita ja verkostoja, joissa voidaan käydä avointa keskustelua ja yhteistyötä kyberturvallisuuteen liittyvistä asioista.

8.2 Enisa

Enisa (European Union Agency for Cybersecurity) on vuonna 2004 perustettu Euroopan unionin virasto, joka keskittyy tietoturvaan ja digitaaliseen turvallisuuteen. Sen tehtävänä on edistää korkeaa tietoturvatasoa sekä luoda yhteinen tietoturvakulttuuri Euroopassa. Enisan toimintaan kuuluu muun muassa riskien arviointi, tietoturvaan liittyvien tietojen ja parhaiden käytäntöjen jakaminen, sekä yhteistyö eri sidosryhmien, kuten julkisen sektorin, teollisuuden ja akateemisen maailman kanssa. Lisäksi Enisa tarjoaa neuvoja ja tukea Euroopan unionin jäsenvaltioille tietoturvaan liittyvissä asioissa. (Enisa 2024)

9 Diskussio

Tämän tutkielman tarkoituksena oli tarkastella Euroopan unionin kyberturvallisuusstrategioiden kehittymistä vuosien 2013 ja 2020 välillä. Tutkimusmenetelmänä oli vertaileva tutkimus ja tutkimusmateriaalina oli Euroopan unionin työstämät ja julkaisemat kyberturvallisuusstrategiat vuosilta 2013 ja 2020 sekä vastaavien vuosien World Economic Forumin riskiraportit kyberturvallisuuden osalta. Tutkimuksessa kävi ilmi, että vuoden 2020 strategia on huomattavasti kattavampi ja monipuolisempi kuin vuoden 2013 strategia. Esimerkkeinä kattavuudesta on tuoreemmat teknologiat kuten tekoälyn kehittyminen sekä 5G-verkot. Myös vihreä siirtymä ja ympäristöhuolet on otettu huomioon vuoden 2020 strategiassa.

Kyberturvallisuustilanne Euroopassa on muuttunut huomattavasti vuodesta 2013. Tietoturvan uhkakuvat ovat moninaistuneet ja monimutkaistuneet, ja haasteet ovat lisääntyneet niin yksityisellä kuin julkisellakin sektorilla. Esimerkiksi verkkorikollisuus ja tietomurrot ovat yleistyneet, ja uudet teknologiat, kuten tekoäly, ovat tuoneet uusia haasteita kyberturvallisuuden alalle. Vuoden 2020 strategia onkin suuntautunut edeltäjäänsä enemmän tulevaisuuteen ja korostaa digitalisaation jatkuvaa kasvua ja sen mukanaan tuomia haasteita.

Strategioiden vertailussa selvisi, että vuoden 2020 strategiassa painotetaan entistä enemmän riskien hallintaa ja ennaltaehkäisyä sekä yhteistyön merkitystä, kun taas vuoden 2013 strategia keskittyi enemmän perinteisempään tietoturvaan ja tekniseen puolustukseen. Strategioiden välillä oli myös muita eroja, kuten uuden strategian painotus resurssien kohdentamisessa sekä kansainvälisessä yhteistyössä.

Johtopäätöksenä voidaan todeta, että kyberturvallisuuden merkitys on kasvanut huomattavasti Euroopassa viime vuosina, ja kyberturvallisuusstrategioiden kehittäminen on välttämätöntä. Strategiat ovat tärkeitä välineitä haasteisiin vastaamisessa ja turvallisuuden parantamisessa, mutta yhteistyö eri toimijoiden välillä ja kansainvälisesti on tärkeä osa kyberturvallisuuden kehittämistä. On tärkeää seurata

kehitystä ja päivittää strategioita tarpeen mukaan, jotta kyberturvallisuustilanne pysyy mahdollisimman hyvänä ja haasteisiin voidaan vastata tehokkaasti.

9.1 Jatkotutkimusmahdollisuudet

Tässä tutkimuksessa vertailtiin vain Euroopan unionin kahta ensimmäistä kyberturvallisuusstrategiaa keskenään. Vaikka Euroopan unioni on luonut kattavan strategian, jäsenmailla on myös omat strategiansa kyberturvallisuuden kehittämiseksi. Euroopan unioni on myös huhtikuussa 2023 julkaissut ehdotuksen uudeksi strategiaksi nimellä ’cyber solidarity act’ (Eur-Lex, 2023). Uusi kyberturvallisuusstrategia tuonee esiin toimenpiteitä ja huomionarvioisia asioita, jotka aiempien strategioiden luontiaikana ovat joko olleet epäolennaisia tai jääneet huomiotta.

9.2 Ohjeita käytäntöön

Jokaisen tätä tutkimusta lukevan kannattaa ottaa huomioon, että kyberturvallisuus on jatkuvaa ”kissa ja hiiri -leikkiä” eri toimijoiden välillä. Esimerkiksi hakkeriryhmät etsivät jatkuvasti uusia keinoja murtautua eri järjestelmiin tai yksityisiin verkkoihin päästäkseen joko käsiksi uhrien dataan tai vaihtoehtoisesti aiheuttaakseen tuhoa. Samaan aikaan eri organisaatiot muiden suojaavien toimenpiteiden ohella esimerkiksi tekevät penetraatiotestausta löytääkseen tietosuojansa heikot kohdat korjatakseen ne ennen vahinkojen tapahtumista. Muun muassa tästä syystä, sekä esimerkiksi uusien teknologioiden yleistyttyä vuoden 2020 kyberturvallisuusstrategiakin alkaa olla jo osiltaan vanhentunut. Seitsemän vuoden aikana tapahtuneiden teknologisten harppausten ymmärtäminen ja jatkuvan kehityksen sisäistäminen antaa kuitenkin hyvää pohjaa sille mitä hyvän kyberturvallisuusstrategian kuuluisi ottaa huomioon. Jo aiemmin tässä kappaleessa mainittu cyber solidarity act:n ehdotus antanee päivitettyä kokonaiskuvaa kyberturvallisuuden ja uhkien tilasta vuonna 2024.

Eri toimijoiden on myös hyvä muistaa, että Euroopan unioni kattaa merkittävän osan koko Euroopasta ja siten myös strategioiden täytyy olla sopivia aina Pohjoismaista Välimerelle saakka. Omaan toimintaan ja omaan toimintaympäristöön keskittyvä, juuri omalle organisaatiolle tuotettu strategia on aina tehokkaampi kuin mahdollisimman geneerinen ja suuren yleisön tarpeita huomioiva paketti. Euroopan unionin kyberturvallisuusstrategia on tästä huolimatta hyödyllinen erityisesti koulutuksien ja kommunikaation osalta.

9.3 Rajoitteet

Tutkimuksessa on vertailtu Euroopan unionin kyberturvallisuusstrategiaa. Tämä strategia ei ole kaikenkattava, vaan jokaisella jäsenmaalla sekä organisaatiolla on myös omia strategioitaan ja toimintatapojaan. Tutkittujen kyberturvallisuusstrategioiden ymmärtäminen antaa pohjan sille, miten Euroopan alueella pääsääntöisesti ehkäistään kyberhyökkäyksiä ja miten niiden vahinkoja minimoidaan, mutta nämä ovat olleet aikaansa sovitettuja ohjeistuksia, joita on hyödynnetty organisaatioiden yksilöllisempien strategioiden kehitykseen. Vuoden 2020 kyberturvallisuusstrategia ei myöskään välttämättä anna enää kattavaa tietoa nykypäivän uhkakartasta tai todennäköisimmistä hyökkäystavoista, sillä teknologia ja siten siihen liittyvät uhat ovat jatkaneet kehittymistään strategian luonnin jälkeen.

Lähteet

BBC (2016) Russia 'was behind German parliament hack' [online] Saatavilla: https://www.bbc.com/news/technology-36284447-

BBC (2017) Global ransomware attack causes turmoil. [online] Saatavilla: https://www.bbc.com/news/technology-40416611

BBC (2020) Hackers attack Norwegian parliament [online] Saatavilla: https://www.bbc.com/news/technology-53985422

Booz Allen (2020) 4 CORONAVIRUS-RELATED CYBER THREATS TO WATCH OUT FOR [online] Saatavilla: https://www.boozallen.com/insights/covid-19/coronavirus-related-cyber-threats.html

Calcara, A., & Marchetti, R. (2021). State-industry relations and cybersecurity governance in Europe. Review of International Political Economy, 29(4), 1237–1262. https://doi.org/10.1080/09692290.2021.1913438

Capano, D. E. (2023). Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk: Do you debate risks vs. cost of cybersecurity technologies, processes and training? Maersk estimated NotPetya costs at $250-300 million. Control Engineering, 70(4), 39+. https://link.gale.com/apps/doc/A762916159/AONE?u=anon~c89e8e21&sid=googleScholar&xid=a41bba5f

CNBC (2013) Top 2013 cybersecurity stories and what to watch for in 2014 [Online] Saatavilla: https://www.cnbc.com/2013/12/27/top-2013-cybersecurity-stories-and-what-to-watch-for-in-2014.html

ENISA (2017) WannaCry Ransomware: First ever case of cyber cooperation at EU level [online] Saatavilla: https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level

ENISA (2020) ENISA Threat Landscape 2020 [online] Saatavilla: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020

ENISA (2024) Tietoa Euroopan unionin kyberturvallisuusvirastosta (ENISA) [online] Saatavilla: https://www.enisa.europa.eu/about-enisa/about/fi

Eur-Lex (2013) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [online] Saatavilla: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

Eur-Lex (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [online] Saatavilla: http://data.europa.eu/eli/dir/2016/1148/oj

Eur-Lex (2020) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade [online] Saatavilla: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

Eur-Lex (2023) The EU Cyber Solidarity Act [online] Saatavilla: https://www.eu-cyber-solidarity-act.com/

Euractiv (2017) How France successfully countered Russian interference during the presidential election [online] Saatavilla: https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/

Euronews (2020) Norway's Intelligence Service says Russian groups 'likely' behind Parliament cyber attack https://www.euronews.com/2020/12/08/norway-s-intelligence-service-says-russian-groups-likely-behind-parliament-cyber-attack

Farwell, J. P. (2012). Industry’s Vital Role in National Cyber Security. Strategic Studies Quarterly, 6(4), 10–41. http://www.jstor.org/stable/26270565

Harkins, M., & Freed, A. M. (2018). The Ransomware Assault on the Healthcare Sector. Journal of Law & Cyber Warfare, 6(2), 148–164. http://www.jstor.org/stable/26441292

Healey, J. (2017). Who’s in Control: Balance in Cyber’s Public-Private Sector Partnerships. Georgetown Journal of International Affairs, 18(3), 120–130. http://www.jstor.org/stable/26395931

Helsingin Sanomat (2014) Ulkoministeriöön vuonna 2013 iskenyt vakoiluohjelma vei tietoja "rekkalasteittain" [online] Saatavilla:https://www.hs.fi/kotimaa/art-2000002764588.html

Heracleous, L. (2003) Strategy and Organization: Realizing Strategic Management. Cambridge: Cambridge University Press. DOI:10.1017/CBO9780511615313

Iltasanomat (2019) Supo: Ulkoministeriöön vuonna 2013 kohdistuneen laajan verkkovakoilun tutkinta on keskeytetty [online] Saatavilla: https://www.is.fi/kotimaa/art-2000006178446.html

Neutze, J., & Nicholas, J. P. (2013). Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms. Georgetown Journal of International Affairs, 3–15. http://www.jstor.org/stable/43134318

New York Times (2018) Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. [online] Saatavilla: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

NHS (2023) NHS England business continuity management toolkit case study: WannaCry attack [online]. Saatavilla: https://www.england.nhs.uk/long-read/case-study-wannacry-attack/

Pandasecurity, (2017) Petya [online] Saatavilla: https://www.pandasecurity.com/en/security-info/petya/

PST (2020) Datainnbruddet mot Stortinget er ferdig etterforsket. [online] Saatavilla: https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

Ragin, C. & Zaret, D. (1983) Theory and Method in Comparative Research: Two Strategies [online] https://doi.org/10.1093/sf/61.3.731

Rehman, Ikhlaq. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. Library Philosophy and Practice. https://core.ac.uk/download/pdf/220153793.pdf

Soesanto, S. (2017). EUROPE'S DIGITAL POWER: FROM GEO-ECONOMICS TO CYBERSECURITY. European Council on Foreign Relations. http://www.jstor.org/stable/resrep21528

The Guardian (2018) Facebook says nearly 50m users compromised in huge security breach. [online] Saatavilla: https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

Turvallisuuskomitea (2021) Kokonaisturvallisuutta yhdessä #2: Kyberturvallisuus pandemiassa [online] Saatavilla: https://turvallisuuskomitea.fi/kokonaisturvallisuutta-yhdessa-2-kyberturvallisuus-pandemiassa/

Vuorinen, S. (2019) Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille [online] Saatavilla: http://urn.fi/URN:ISBN:978-952-00-4085-7

World Economic Forum (2013) Global Risks 2013 [online] Saatavilla: https://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

World Economic Forum (2020) The Global Risks Report 2020 [online] Saatavilla: https://www.weforum.org/publications/the-global-risks-report-2020/

Yle (2014) Supo: Ulkoministeriö joutui kaksi kertaa vakoilun kohteeksi [online] Saatavilla: https://yle.fi/a/3-7332824