Ere Auvinen

Sähköverkon turvaaminen hybridiuhilta

Tietotekniikan kandidaatintutkielma

2. toukokuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Ere Auvinen

Yhteystiedot: ere.et.auvinen@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Sähköverkon turvaaminen hybridiuhilta

Title in English: Securing the electricity grid from hybrid threats

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 25+0

Tiivistelmä: Tämä tutkielma luo katsauksen modernin sähköverkon ohjausjärjestelmän suojaukseen hybridiympäristön puitteissa. Se kuvailee sähköverkon ohjausjärjestelmää ja siihen sidottuja järjestelmiä. Tutkielmassa tarkastellaan sähköverkkoon kohdistuvia uhkatekijöitä ja mahdollisia hyökkäysten toteutuksia. Lopuksi esitellään keinoja suojata sähköverkko edellä mainituilta uhilta ja pohditaan niiden yhteisvaikutusta suojaukseen.

Avainsanat: sähköverkko, sähköasema, internet, SCADA, kyber, hybridivaikuttaminen

Abstract: This study examines the protection of a modern power grid control system in the hybrid environment. It describes the power grid control system and the systems associated with it. The study reviews threat factors and possible attack conductions. Lastly it introduces means to protect the power grid from malicious acts and examines their joint effectiveness.

Keywords: power grid, substation, internet, SCADA, cyber, hybrid attacks

Termiluettelo

Haittaohjelma	Haitallinen ohjelma tai haitallista koodia, jotka vahingoittavat tai häiritsevät tietokoneen normaalia käyttöä.
HMI	Human Machine Interface, käyttöliittymä, jolla ihminen voi seurata ja ohjata koneen toimintaa.
Injektio	Oman datan syöttäminen tietojärjestelmään vaikutuksen aikaansaamiseksi.
Keskijännite	Yli kilovoltin mutta alle 36 kilovoltin nimellisjännite. Suomessa käytetään 20 kilovoltin jännitettä.
Pienjännite	Suurimmillaan kilovoltin nimellisjännite. Suomessa sähkönsiirtoon käytetään 1000 ja 400 voltin jännitteitä.
SCADA	Supervisory Control And Data Acquisition tai valvomo-ohjelmisto, jolla automaatiojärjestelmiä voi ohjata ja valvoa tietokoneelta käsin.
Suurjännite	Yli 36 kilovoltin nimellisjännite. Suomessa käytettävät jännitteet ovat 110, 220 ja 400 kilovolttia.
VPN	Virtual Proxy Network eli virtuaalinen erillisverkko.

Kuviot

Sisällys

1 Johdanto

Nykyaikainen yhteiskunta ei selviä ilman sähkön jatkuvaa saatavuutta. Lainsäädäntö velvoittaakin sähköverkosta vastaavia yrityksiä turvaamaan sähkönsiirron siihen kohdistuvilta uhilta. Sähkön siirtoverkon nojautuessa täysin tietotekniseen valvontaan ja ohjaukseen on se myös alttiina kyberympäristön uhille. Kyberhyökkäyksen aiheuttamia sähkökatkoja on jo tapahtunut. Venäläinen toimija onnistui kyberhyökkäyksellään vuonna 2015 katkaisemaan sähköt yli 200 000 ukrainalaiselta.

Tässä tutkielmassa tutustutaan sähköverkon ohjauksen tärkeimpiin laitteisiin, uhkatekijöihin sekä hyökkäys- ja suojausmahdollisuuksiin. Kyberulottuvuuden suojausjärjestelmien kehittyessä on inhimillisten virheiden hyödyntäminen vihamieliseen toimintaan korostunut. Informaatio- ja ihmisvaikuttaminen ovat myös vakavasti otettavia uhkia kriittiselle infrastruktuurille, kuten sähköverkolle, minkä vuoksi niitä käsitellään kybervaikuttamisen rinnalla tässä tutkielmassa.

Toisessa luvussa kuvaillaan sähköverkon teknistä toteutusta ja ohjauskojeistoa pintapuolisesti, jolloin vaadittava ymmärrys hybridivaikuttamisen vaikutuksesta sähkönsiirtoon saavutetaan.

Kolmas luku esittelee mahdolliset hyökkääjät, hyökkäystavat sekä toteutustekniikat. Luvussa pohditaan erilaisten toimijoiden, kuten aktivistien tai rikollisjärjestöjen, luomaa uhkakuvaa sähköverkolle. Luku myös kuvailee tietojärjestelmän turvallisuutta ympäröivää semantiikkaa ja erilaisten hyökkäysten erityyppisiä vaikutuksia kohteeseen.

Neljännessä luvussa tarjotaan suojauskeinoja aiemmin mainittuja uhkia vastaan. Erilaiset tekniset ratkaisut ja henkilöstön toiminta voivat yhdessä suojata kriittistä infrastruktuuria, sähköverkko mukaan lukien.

2 Sähköverkko

Kotitalouksien, yritysten ja koko yhteiskunnan toiminnot ovat riippuvaisia sähköstä. Ilman sähköä ruoan säilöminen ja valmistus, yhdyskuntatekniikka, tietoliikenne, lähestulkoon kaikki yhteiskunnan toiminta, pysähtyy. Tämän vuoksi lainsäädäntö velvoittaa verkkoyhtiöitä huolehtimaan sähkön saatavuudesta ja verkon toimintavarmuuden jatkuvasta kehittämisestä. (Sähkömarkkinalaki 2013)

Tässä luvussa esitellään sähköverkon tekninen toteutus ja etenkin suomalaisten olosuhteiden vaikutus sähköverkon rakenteeseen. Lisäksi käydään läpi sähköverkon ohjauskojeistoa perusperiaatteesta yksittäisen kojeen tasolle asti. Tämän ymmärtäminen on tärkeää, jotta voimme jatkaa ohjausjärjestelmän kautta tapahtuvan hybridivaikuttamisen pariin.

2.1 Sähköverkon toteutus

Sähköverkon muodostavat suurjännitteiset kanta- ja alueverkko ja keski- ja pienjännitteinen jakeluverkko. Kantaverkko siirtää sähköä voimalaitoksista ja ulkomailta kaikkialle maahan ja jakeluverkko jakaa sen edelleen loppukäyttäjille. Alueverkko käsittää pienempiä alueita kattavat suurjännitelinjat. Suomessa kantaverkosta vastaa valtionyhtiö Fingrid ja alue- jakeluverkosta noin 80 verkkoyhtiötä. (Energiateollisuus 2023)

Eri jännitetasojen solmukohta on sähköasema, jossa muuntaja muuntaa jännitteen kulloinkin vaaditulle tasolle. Sähköasemien ominaisuuksissa on sijainnin, omistajan ja siirrettävän jännitteen mukaisesti mittavia eroavaisuuksia. Suurimmat sähköasemat ovat kantaverkon sisäisiä 400 kilovoltin muuntoasemia, pienimmät asuinalueilta löytyviä 400 voltin muuntamoita. Sairaaloilla, tehtailla tai muilla vastaavilla keskuksilla voi olla omat, suoraan kantaverkkoon kytketyt sähköasemat suuren kulutuksen ja tärkeän yhteiskunnallisen aseman vuoksi. (Energiateollisuus 2023)

Sähkönsiirto tapahtuu joko ilmajohdoilla, maa- tai vesikaapeleilla. Langattoman sähkönsiirron kehitystyö loppui 1800-luvulla tuloksettomana.(Tesla 2020) Avojohtolinjat vaativat enemmän ylläpitoa ja ovat alttiimpia vioille, mutta ovat etenkin pitkillä etäisyyksillä huomat-

tavasti maakaapelia halvempi ratkaisu. Maakaapelilinja maksaa Suomessa noin kolme kertaa ilmajohtoa enemmän. (Kuusisto 2022) Suomessa valtaosa sähköverkosta muodostuu keski- ja suurjännitettä kantavasta, ilmassa kulkevasta alumiiniavojohdosta. Haja-asutusalueilla pienjännitejakelu toteutetaan päällystetyin alumiinijohtimin. Taajamissa koko jakeluverkko on rakennettu maakaapeleista.

2.2 Sähköverkon ohjaus

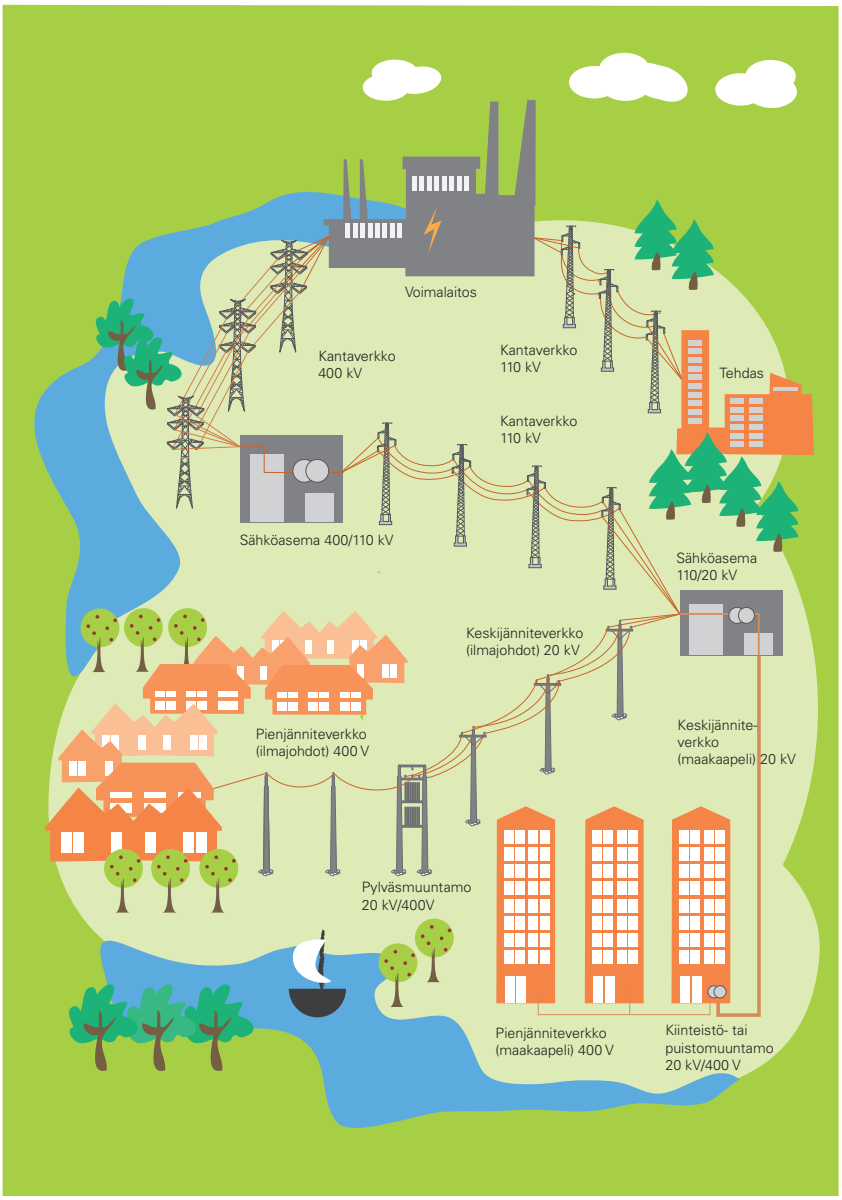
Jakeluverkon osia voidaan kytkeä verkkoon tai irti verkosta käsin kahvasulakkeilla tai käsikäyttöisillä erottimilla. Yhä suurempi osuus sähköverkon kytkennöistä tehdään kaukoohjatuilla tai automatisoiduilla järjestelmillä. Sähköisen ohjauksen etuna manuaaliseen ohjaukseen nähden ovat parempi tavoitettavuus maastossa, sekä vika-alueiden tehokkaampi rajaaminen ja katkoaikojen lyheneminen. (Petäys 2017)

Sähköverkon valvonta ja ohjaus on nykyään keskittynyt verkkoyhtiöiden käyttökeskuksiin ja sähköasemille, mutta hajautetun valvonnan mahdollisuuksia tutkitaan enenevissä määrin. Hajautetun valvonnan periaatteella suurempi osa verkon mittauksista tapahtuu linjoissa, vian rajaus tehostuu entisestään ja toimitusvarmuus paranee. (Petäys 2017)

Moderni, automatisoitu verkon valvonta toteutetaan niin kutsutun ohjauskehän arkkitehtuurin mukaan. Tällöin verkon mittauslaitteet seuraavat reaaliajassa erilaisia määreitä, kuten virtaa ja jännitettä, ohjauslaitteet seuraavat saamiaan mittausarvoja ja tilanteen mukaan joko suorittavat itse kytkentöjä tai antavat hälytyksen ihmisoperaattorille. Jatkuva valvonta, arvojen analysointi ja automaattiset korjaustoimenpiteet luovat sähkönsiirron turvaavan kehän. (Campbell 2015)

2.3 Ohjauskojeet

Sähköasemalla on useita kojeita, jotka suojaavat sähköverkkoa, -asemaa, lähiympäristöä ja toimitusvarmuutta. Näistä moni toimii suurelta osin sähkömekaanisesti, eivätkä tietotekniset ratkaisut vaikuta niiden omaan toimintaan. (Frilander 2021)



Kuvio 1. Havainnekuva sähköverkosta

(Säteilyturvakeskus 2021)

2.3.1 Releet

Sähköverkon releet voidaan jakaa karkeasti kahteen joukkoon: suojareleisiin ja suojareleiden apureleisiin.

Suojarele vastaanottaa apureleiltään mittaustietoja ja ohjaa hallinnoimiansa laitteita, yleensä katkaisijaa, konfiguraationsa mukaan, esimerkiksi virran noustessa yli turva-arvon. Suojarele on myös rajapinta mittauslaitteistona toimivien apureleiden ja käyttökeskuksen välillä. Se lähettää saamansa mittaustiedot sähköverkon valvontaohjelmistolle internet-yhteydellä, jolloin verkkoyhtiö voi seurata verkon toimintaa ja havaita indikaattoreita vikatilanteista. Käyttökeskuksen operaattori ohjaa sähköverkkoa suojareleen avulla. Jokaisella aseman johtolähdöllä on oma suojareleensä.(Korpinen 1998)

2.3.2 Katkaisijat ja erottimet

Erottimet avaavat virtapiirin pienillä kuormilla tai ilman kuormia, ja katkaisijat kykenevät avaamaan virtapiirin myös kuormitettuna. Modernit katkaisijat toimivat myös erottavina, eli niiden koskettimien jälleenkytkentä on fyysisesti estettävissä. Katkaisijoista ja erottimista on erilaisia sovelluksia sähköasemalla, sähköasemien ja muun verkon välissä toimivalla alaasemalla sekä muualla sähköverkossa. (Korpinen 1998)

2.3.3 SCADA-järjestelmä

Mittausreleet informoivat suojarelettä, joka kommunikoi internet-yhteydellä SCADA-ohjelmiston kanssa. SCADA-ohjelmiston avulla käyttökeskuksen käyttöliittymä saa dataa verkon toiminnasta, voi asettaa hälytyksiä epätavanomaisuuksien varalta ja ohjata suojareleen kautta sähköverkkoa. Eri valmistajien laitteistot ja ohjelmistot ovat nykypäivänä yhteensopivia keskenään alan standardisoinnin ansiosta. Tällöin sähköverkon ohjaus voidaan toteuttaa usean eri valmistajan kojeilla, tyyppivioista tai haavoittuvuuksista johtuvien vikojen välttämiseksi. (Frilander 2021) Mittausautomaation, etävalvonnan ja etäohjauksen ansiosta sähköasemat ovat miehittämättömiä ja verkkoa on kokonaisuudessaan mahdollista operoida hallintajärjestelmästä käsin. (Zhang ym. 2015)

SCADA-järjestelmän perusosat ovat fyysisiä toimintoja ohjaavat releet, kuten sähköaseman tapauksessa suojarele, sekä sen operointiin ja seurantaan käytettävä HMI-ohjelmisto. HMI-asemien ja muun ohjausohjelmiston lisäksi käyttökeskuksen tietojärjestelmät pitävät yllä verkon tietokantaa. Sähköaseman ohjausreleet ovat yhdistettynä keskenään paikallisverkossa, samoin käyttökeskuksen tietokoneet. Käyttökeskus on yhteydessä sähköasemien suojareleisiin laajaverkon kautta. Laajaverkko on voitu toteuttaa valokuitu- tai radioyhteydellä, tai internet-yhteyttä käyttäen. (Janicke 2012)

3 Ohjausjärjestelmään kohdistuvat uhat

Tietotekniikan sisällyttäminen sähkönsiirtojärjestelmään tekee sähkönsiirron alttiiksi kybervaikuttamiselle. Vihamieliset toimijat voivat ohjausjärjestelmään vaikuttamalla pysäyttää sähkönsiirron, tai mittausautomaatiota manipuloimalla vaikuttaa verkon ohjaamiseen. Muita tietoteknisiä uhkia sähköverkolle ovat laitteistoviat ja käyttäjän virheet, kuten konfiguraatioongelmat ja väärät analyysit.

Hallintajärjestelmän tietoturvallisuutta voidaan tarkastella samalla tavoin kuin minkä tahansa informaation. Informaatioturvallisuudelle on lukuisia eri määritelmiä. Se voidaan tiivistää muun muassa CIA-kolminaisuuteen. (Laari 2019) C, Confidentiality, eli luottamuksellisuus tarkoittaa sitä, että tietoon pääsevät käsiksi vain ne, joilla on oikeus siihen. I, Integrity, eli yhteneväisyys kuvaa tiedon eheyden turvaamista, ja A, Availability tai saatavuus kuvaa tiedon saatavuuden turvaamista sitä tarvitseville. Näillä kolmella mittarilla voidaan kyberturvallisuuden tilaa voidaan arvioida ja kehittää. Vastaavasti kyberhyökkäyksien voidaan katsoa kohdistuvan yhteen tai useampaan CIA-mallin osa-alueeseen. Tässä tutkielmassa kyberturvallisuutta tarkastellaan käytännön esimerkkien lisäksi CIA-mallin mukaisesti, sillä se on yleisesti käytetty ja myös SCADA:an sovellettavissa oleva malli.

Jotta sähköverkolle voi aiheuttaa suoraa haittaa hallintajärjestelmän kautta, on vihamielisen toimijan joko estettävä järjestelmän käyttö tai ohjattava itse hallintajärjestelmää omiin tavoitteisiinsa. CIA-mallin mukaisesti se tarkoittaisi järjestelmän saatavuuden ja yhtenäisyyden vaarantumista. Pelkkä pääsy tarkastelemaan ohjausverkkoa ja -laitteita antaa uhkatekijöille tietoa iskujensa tueksi, sekä rikkoisi järjestelmän luottamuksellisuuden. Siksi myös tiedustelu voidaan luokitella hyökkäykseksi järjestelmää vastaan. (Andress 2014)

3.1 Kyberuhkatoimijat

Kyberhyökkäyksiä toteuttavat tahot voidaan jaotella eri uhkatyyppeihin niiden saatavilla olevien resurssien mukaan. Tätä kautta työkalujen laatua ja määrää sekä toiminnan vakavuutta voidaan arvioida. Jaottelun ulkopuolelle jäävät verkon sisäpiiristä tehdyt iskut sekä onnettomuudet, jotka yhdessä muodostavat kaksi kolmasosaa kaikista SCADA:n kyberuhista. (Ja-

nicke 2012)

Kybervandaalit ovat verrattain löyhästi järjestäytyneissä ryhmissä tai itsenäisinä toimivia hyökkääjiä. Resurssit ovat muita uhkatyyppejä pienemmät ja hyökkäystyökalut ovat tyypillisesti julkisia ohjelmistoja tai valmiita algoritmeja, niin kutsuttua hyllytavaraa. Motiivina kybervandaalien toiminnalle on yleensä ideologiansa tai osaamisensa esittely tai tuhon ja häiriön aiheuttaminen. (Laari 2019) Muita kybervandaaleihin rinnastettavia toimijoita ovat huomion herättämiseen pyrkivät haktivistit sekä hakkerointia kokeilevat "koodikakarat"(Script Kiddies).

Kyberrikolliset harjoittavat laitonta toimintaa kyberympäristössä taloudellisen hyödyn vuoksi. Kyberrikolliset voivat varastaa rahanarvoista tietoa, kiristää uhriaan tai toimia kolmannen tahon, kuten valtiollisen toimijan, alihankkijana, tarjoten kyberrikosta palveluna (Cybercrime as a service). (Janicke 2012)

Kyberterrorismi tarkoittaa terroristisen toiminnan ulottamista kyberympäristöön. Terroristit voivat pyrkiä iskemään yhteiskunnallisesti merkittäviin kohteisiin edistääkseen toimiaan tai kineettisen iskun tueksi. Tämä määritelmä on kiistanalainen, sillä joitakin rikollisorganisaatioita ja valtionvirastoja on luokiteltu terroristijärjestöiksi ja näiden operaatioita on tulkittu terrori-iskuiksi. (Laari 2019)

Valtiolliset toimijat ovat virastoja, asevoimia tai muita valtiollisesti tuettuja ryhmittymiä. Valtiolliset toimijat eroavat muista kybertoimijoista hienostuneemmalla toiminnallaan ja miljardibudjettien mahdollistamilla, usein itse kehitetyillä työkaluillaan. Eri maiden asevoimat ja tiedustelupalvelut toimivat kyberympäristössä jatkuvasti kybersodankäynnin keinoin. (Laari 2019) Tiedustelu, häirintä ja tuhoamisoperaatiot kyberhyökkäysten avulla ovat kineettisiä iskuja halvempia suorittaa ja helpompia kiistää. Lisäksi kyberhyökkäyksillä voidaan tukea kineettisiä iskuja, kuten Israelin hyökkäyksessä Syyrian ydintutkimuslaitokseen. (Laari 2019) Tunnetuimmat sähköverkkoon kohdistuvat kyberhyökkäykset ovat olleet valtiollisen toimijan suorittamia.

3.2 Hyökkäyskuormat, eli mitä hyökkäyksessä toimitetaan

Kyberhyökkäysten luokittelulle on useita tapoja, eivätkä luokittelun rajat ole aina kiistattomia. (Andress 2014) Tässä tutkielmassa hyökkäyksiä tarkastellaan jakamalla ne ensin kuormaan ja toimitukseen, jotka voidaan vielä jaotella useilla eri tavoilla.

Andress (2014) luokittelee kyberhyökkäysten hyötykuormat neljään osa-alueeseen: kaappaus, keskeytys, muuntelu ja väärennys. Näillä eri osa-alueilla kuvataan hyökkäyksen vaikutusta kohteeseen. Kohteen toiminta voidaan estää tai se voidaan kaapata, jolloin sitä voidaan käyttää hyökkääjän omana toimijana. Kohteen toimintaa tai tietoja voidaan muunnella, tai kokonaan uusia rakenteita voidaan väärentää omien tarkoitusperien tukemiseksi. Nämä eri hyötykuormat vaikuttavat CIA-mallin eri osiin häilyvin rajoin.

Morris (2013) luokittelee SCADA:an kohdistuvat kyberhyökkäykset tiedustelu-, vasteinjektio-, komentoinjektio- ja palvelunestohyökkäyksiin. Tämänkaltainen luokittelu ei ole yhtä yleispätevä kuin edellä mainittu, mutta se kuvaa paremmin kyberfyysisiin järjestelmiin kohdistuvien iskujen hyötykuormia. Hyökkäyskuormille on myös tarkempia määritelmiä, mutta tässä tutkielmassa noudatetaan nelikohtaista määritelmää selkeyden vuoksi.

3.2.1 Tiedusteluhyökkäys

SCADA-järjestelmiin kohdistuvat kyberhyökkäykset eroavat esimerkiksi toimistotietokonetta vastaan tehtävästä kyberhyökkäyksestä merkittävästi ohjausjärjestelmien moninaisuuden vuoksi. (Clarke, Reynders 2004) Ohjausjärjestelmän arkkitehtuuri riippuu paikallisesta lainsäädännöstä, verkkoyhtiöstä, käyttöjännitteestä, ympäristöstä ja laitetoimittajista. Suojareleiden valmistajakohtaiset erot ohjauksessa, valvonnassa ja yhteyksissä ovat olleet suuria, mutta eri valmistajien releistä on tullut yhä laajemmin yhteensopivia erilaisten laitteiden kanssa standardisoinnin vuoksi. (Clarke, Reynders 2004) Vaikka kaikkia suojareleitä ja HMI-ohjelmia ohjattaisiin samalla tavalla, on silti tiedustelu kriittisen tärkeää hyökkääjän valmistellessa iskuaan. Kaikkia kyberhyökkäyksiä edeltää tiedustelutoiminta ja tiedusteluisku. (Andrey 2018)

Tiedusteluhyökkäyksen tavoite on kerätä kohteesta tarvittava tieto. Tiedusteluhyökkäys voi tukea jatkoiskujen toteutusta, tai se voi olla itse päähyökkäys. SCADA-järjestelmää tiedus-

tellessa tärkeitä tietoja ovat ohjausverkon rakenne, järjestelmän laitteet, näiden mallit ja protokollat, sekä muut verkon tai verkkoyhtiön tiedot, joihin hyökkäys voi tarjota pääsyn.

Tyypillisiä tiedusteluiskuja ovat erilaiset skannaukset, joilla datan määrää, laatua ja liikennettä pyritään selvittämään. (Morris 2013) Kommunikoimalla kohdeverkon kanssa Verkkoja skannailemalla hyökkääjä voi selvittää ohjausjärjestelmän palvelimen osoitteen, verkon avoimet portit ja jopa verkossa olevien laitteiden tyypit. (Andrey 2018) Kuormitusiskuilla ja salasanamurtoyrityksillä voidaan etsiä heikkoja kohtia ohjausverkosta, samalla hahmottaen verkon rakennetta ja osoitteita. (Andrey 2018)

Tiedustelutoiminnassa hybrilditoiminta on tehokkaimmillaan, sillä tiedonkeräys ihmisiltä on toteutettavissa ilman väkivaltaa tai jopa kohteen huomaamatta. Tietojenkalastelu on erittäin monipuolinen ja kustannustehokas keino päästä käsiksi tietojärjestelmiin. (Mityukov 2019) Kaikki skannattavissa oleva tieto voidaan selvittää myös asian tietäviltä henkilöiltä kysymällä, mikä onnistuessaan säästää aikaa ja vaivaa. Lisäksi tietojenkalastelulla voi saada suoran, sallitulta näyttävän pääsyn hallitsemaan esimerkiksi sähköverkon ohjausjärjestelmää. (Mityukov 2019)

Tietojenkalastelu voidaan toteuttaa aidon näköisillä, tutuilla sähköpostiviesteillä, mainoksilla tai nettisivuilla, jonne käyttäjä syöttää hyökkääjän tarvitsemat tiedot vapaaehtoisesti. Valtiollinen toimija voi selvittää kriittistä informaatiota myös väliintulohyökkäyksellä (Man-in-the-middle attack), jossa kohteen tiedonsiirto tapahtuu hyökkääjän hallitseman osapuolen läpi. Tällainen suodatin voi olla kohteen luotettu henkilö, tai hyökkääjän verkon väliin asentama laite tai ohjelmisto, joka käy läpi välittämänsä tietoliikenteen. (MITRE ATT&CK 2023)

3.2.2 Mittaus- ja vasteinjektiot

Onnistunut mittaus- tai vasteinjektio pystyy manipuloimaan verkon operaattorin ja aseman laitteiston välistä tietoliikennettä siten, että mittaustiedot tai järjestelmän reaktiokyky vääristyvät kohteen sitä huomaamatta. (Morris 2013)Erityisesti sähköverkossa tällaiset iskut voivat aiheuttaa peruuttamatonta tuhoa. Kun suojareleen vasteaika vikatilanteessa lasketaan millisekunneissa, voi huomaamatonkin vasteinjektio saada aikaan tuhoa verkolle ja sen ympärille. Mittaus- ja vasteinjektiot voivat saada aikaan myös vääriä hälytyksiä ja niistä seuraavia

katkotilanteita.

3.2.3 Komentoinjektio

Komentoinjektio merkitsee ulkopuolisen ohjausjärjestelmässä ajamaa käskyä. (Morris 2013) Tällainen toiminta voi olla muita iskuja helpommin havaittavissa, mutta kaikkia muita tuhoisampi. Jos hyökkääjä esimerkiksi pääsisi pyyhkimään koko sähköaseman suojareleiden asetukset pois ja kytkisi verkon irti, olisi vaikutus hyvin pitkäaikainen ja tuhoisa.

3.2.4 Palvelunestohyökkäys

Palvelunestohyökkäys on tunnettu tapa vaikuttaa tietojärjestelmiin. (Laari 2019) Sen vaikutuksesta kohde ei pysty suorittamaan sille määritettyä tehtävää. Palvelunestohyökkäys voi sähköverkon ohjausjärjestelmässä kohdistua ohjauskojeiden ja käyttäjien lisäksi verkkolaitteisiin, jolloin ohjausjärjestelmän sisäiset yhteydet voivat katketa. (Morris 2013) Tavallinen tapa suorittaa palvelunestohyökkäys on kuormittaa kohdetta niin suurella määrällä liikennettä, että se menee vikatilaan. Suuren liikenteen aikaansaamiseksi hyökkääjä käyttää yleensä haittaohjelmia, joilla useita verkkoon kytkettyjä laitteita voidaan saada kohdistamaan tehonsa kohdelaitteen liikenteen kuormittamiseen.

3.3 Hyökkäystavat, eli kuinka hyökkäys suoritetaan

Hyökkäyskuorman saattaminen kohteeseen voidaan toteuttaa mitä mielikuvituksellisimmin keinoin. Vaikka tietojärjestelmät toimivatkin kyberympäristössä, eivät ne ole riippumattomia fyysisen maailman toiminnasta. (Laari 2019) Tietojärjestelmien tullessa yhä murtovarmemmiksi on etenkin valtiollinen kybersota painottunut myös fyysisen maailman vaikuttamiseen, kuten järjestelmiin sidoksissa oleviin ihmisiin vaikuttamiseen. (Laari 2019) Tällaista kyber-, informaatio-, kineettis- ja ihmiseen vaikuttamisen järjestelmällistä sekoittamista kutsutaan hybridivaikuttamiseksi. Tässä luvussa huomioidaan myös hybridivaikuttaminen kyberhyökkäyksen työkaluna, sillä se on historiallisten tapausten osoittamana oleellinen osa myös sähköjärjestelmän turvallisuutta.

Seuraavaksi lueteltuja hyökkäystapoja voidaan yhdistellä ja suorittaa rinnakkain. Luokittelu ei ole kaikenkattava tai pitkäikäinen, ja sitä tulee soveltaa. Lisäksi uusia hyökkäysratkaisuja kehitellään tälläkin hetkellä ympäri maailmaa.

3.3.1 Verkkoon murtautuminen

Tehokkain keino vaikuttaa SCADA-järjestelmään on päästä itse operoimaan järjestelmää suoraan. Verkon kautta tapahtuvaan ohjaukseen voi päästä käsiksi hyökkääjän omalta päätteeltä, kunhan pääsy verkkoon on turvattu.

Verkkoon murtautuminen voi tapahtua skannauksella selvitettyjen väylien läpi kulkemalla, tarvittavat salasanat joko murrettuna tai tietojenkalastelulla hankittuna. (MITRE ATT&CK 2023) Salasanan murtaminen vaatii valtavasti laskentatehoa ja on helposti havaittavissa, (MITRE ATT&CK 2023) joten siihen ryhdytään käytännössä vain, jos on tarkoitus aiheuttaa nopeasti laajaa tuhoa, eikä kiinni jääminen ole uhka toiminnalle. Hienovaraisempi keino tunkeutua ohjausverkkoon on hallintatunnusten hankkiminen ja mahdollisesti ohjauksen HMI-ohjelmiston käyttäminen julkisen verkon kautta. Tämä on mahdollista, jos käyttökeskus toimii suoraan internetissä tai käyttää VPN-yhteyttä, jolloin oikeilla tunnuksilla hyökkääjä voi tunnistautua yhdeksi käyttökeskuksen koneeksi ja toimia vapaasti. (MITRE ATT&CK 2023)

3.3.2 Haittaohjelmat

Haittaohjelmat ovat sovellettavissa kaikenlaiseen haitalliseen toimintaan. Erityisen vaarallisia haittaohjelmista tekee niiden mahdollisuus toimia itsenäisesti ja monistaa itseään, jolloin pahimmillaan koko ohjausjärjestelmän voi altistaa haittaohjelmalle yhden laitteen kautta. (Laari 2019) Riittävällä osaamisella ja tiedolla kohteesta haittaohjelmilla voi tehdä lähes mitä tahansa. Haittaohjelma voi lukita SCADA-ohjelmiston käytön, ohjata itse suojareleitä, tuhota loki- ja asetustiedot, vain mielikuvitus ja suojatoimenpiteet ovat rajana. (E-ISAC 2016)

3.3.3 Väliintuloiskut

Väliintuloiskussa hyökkääjä ujuttautuu kohteen tietoliikenteeseen ja vaikuttaa lävitsensä kulkevaan dataan. (Goulart 2021) Huomaamattomammasta väliintuloiskusta esimerkkinä on tapaus, jossa hyökkääjä saa sähköaseman tietoliikenteen kulkemaan päätteensä kautta käyttökeskukseen ja väärentää mittaustietoja. Väliintuloiskuja hyödynnetään etenkin tiedusteluun ja mittaus- ja vasteinjektioihin. (MITRE ATT&CK 2023)

3.3.4 Henkilöiden hyödyntäminen

Järjestelmien tullessa yhä murtovarmemmiksi, on ihmisten hyväksikäyttö korostunut. (Laari 2019) Tietojenkalastelu, mikä mainittiin jo tiedusteluhyökkäyksistä puhuttaessa, voi tarjota hyökkääjällä suoran pääsyn minne tahansa järjestelmään. (MITRE ATT&CK 2023) Hienostunut tiedonkalastelu luo tarkan kopion kohteen työympäristön käyttöliittymästä, saaden näin käyttäjän syöttämään tarvittavat tunnukset. Internet-sivujen tai sähköpostin liitetiedostojen kautta on mahdollista ajaa haittaohjelmia kohteessa. Tässäkin kehitys on jatkuvaa ja vain mielikuvitus on rajana.

Tuotantoketjuisku vaikuttaa kohteen käyttämään palveluun, täten häiriten tai estäen kohteen toiminnan. (Buchicchio ym. 2022) Tietotekniset ratkaisut, varsinkin ohjelmistot, voivat olla riippuvaisia useasta eri tahosta, eikä kaikkia keskinäisiä riippuvuuksia välttämättä edes tiedetä. Vihamielinen toimija voi käyttää tätä hyväkseen ja etsiä tuotantoketjusta haavoittuvuuksia, jotka vaikuttavat loppukäyttäjään. (Buchicchio ym. 2022) Esimerkiksi käyttökeskuksen suojausohjelman saattaa hyödyntää avoimen lähdekoodin kirjastoa, jota hyökkääjä voi vapaasti muokata ja näin sisällyttää haavoittuvuuksia ohjelman seuraavaan päivitykseen.

Pitkäjänteisesti ja suurilla resursseilla toimivalla toimijalla voi myös olla omia asiamiehiään kohteessa, jolloin esimerkiksi haittaohjelman päästäminen järjestelmään on vaivatonta ja huomaamatonta. (E-ISAC 2016) Hyökkääjä voi päästä kohdejärjestelmään fyysisesti myös ujuttamalla muistilaitteen päätteeseen asiamiehensä tai tietämättömän kohdehenkilön avulla. Näin on käynyt ainakin Iranissa. (Laari 2019)

4 Vastakeinot

Tässä luvussa käsitellään keinoja, joilla verkkoyhtiö voi estää tai minimoida edellä mainittujen hyökkäysten aiheuttamia vahinkoja. Kuten hyökkäyskeinoja luetellessa, myös vastakeinot toimivat yhdessä ja kehittyvät jatkuvasti.

4.1 Tietoverkkojen suojaus

Sähköasema ja käyttökeskus toimivat omissa paikallisverkoissaan. Nämä paikallisverkot yhdistyvät toisiinsa laajaverkkojen, joskus myös internetin, kautta. (Zhang ym. 2015) Ulkopuolisten tietoverkkojen hyödyntäminen kyberhyökkäyksessä mahdollistaa toiminnan lähes mistä tahansa ja on lisäksi helposti kiistettävissä. (Laari 2019) Siksi tietoverkkoihin hyökkääminen ja vastaavasti niiden suojaaminen on sähköverkon ohjausjärjestelmässä keskeistä.

4.1.1 Verkkojen erottelu

Olennainen osa tietoverkon suunnittelua ja suojausta on erotella aliverkot toisistaan. Tällä tavoin tietoverkkoon muodostuu enemmän läpäisyn vaativia pintoja yksilöllisine pintajännitteineen, mikä tekee verkon läpi murtautumisesta haastavampaa, hitaampaa ja kalliimpaa. Tietoverkot voidaan erotella virtuaalisesti tai fyysisesti.

Tietoverkkojen virtualisointi mahdollistaa yhden laitteen suorituskyvyn jakamisen useaan erilliseen verkkoon. Vastaavasti virtualisoinneilla voidaan yhdistää fyysisesti eri verkoissa toimivat laitteet yhteiseen virtuaaliverkkoon. Tämä mahdollistaa vanhojen laitteiden ja ohjelmistojen käyttöiän pidentämisen, kun vanhat, fyysiset verkot voidaan suunnitella abstrakteina rakenteina.(Dimitrios, Sarigiannidis 2020) Virtualisointi myös laskee tietoverkkojen rakentamisen ja testaamisen kustannuksia, kun yhdellä laitteella voidaan toteuttaa useiden verkkojen toiminta. (Dimitrios, Sarigiannidis 2020) Verkkojen fyysinen erottelu tarkoittaa verkkojen pitämistä fyysisesti erillään, eri laitteissa ja parhaimmillaan eri tiloissa. Vaikka fyysinen erottelu on virtuaalista erottelua työläämpää, hyödynnetään sitä edelleen etenkin kriittisen infrastruktuurin tietoverkoissa. Tällöin verkon toimintaa voidaan suojata riskitekijöiltä, kuten kytkimien hajoamiselta ja sähkökatkoksilta. Myös kyberhyökkäyksen kohteeksi

joutuneen laitteen eristäminen muista on fyysisesti erotetussa verkossa mahdollista. (Neerja, Alabbad, Khedri 2021)

Eri lähiverkot erotetaan toisistaan demilitarisoiduilla alueilla (DMZ), jotka toimivat ikäänkuin ilmalukkoina lähiverkon ja muun maailman rajalla. Demilitarisoitu verkko mahdollistaa pääsyn lähiverkkoon muista verkoista, mutta pyrkii estämään luvattoman kulun verkkoon salasanasuojauksin, sekä palomuurein, joita käytetään sekä lähi-, että ulkoverkon rajoilla. Sähkönsiirron verkkoratkaisuissa demilitarisoidut verkot sijoitetaan tavallisesti itsenäisiin laitteisiin lisäturvan vuoksi. (Zhang ym. 2015)

4.1.2 Palomuurit

Palomuurit suodattavat verkon liikennettä molempiin suuntiin, sallien läpikulun vain erikseen määritetyille, luvallisille toimijoille ja toiminnoille. Palomuureja tuotetaan ohjelmistoina sekä itsenäisinä ja integroituina laitteina. Palomuurit kehittyvät jatkuvasti ja ovat peruskomponenttina lähestulkoon kaikissa maailman tietoverkoissa tuomansa suojan vuoksi. (He 2021) Sähkönsiirron tietoverkoissa palomuurit sijoitetaan tavallisesti verkkojen kytkimien tai reitittimien yhteyteen. (Zhang ym. 2015)

4.1.3 Tiedon salaus

Tiedon salaus on ikiaikainen, ja tehokkain, keino turvata sen luottamuksellisuus. (Hur 2011) Erilaisten salakielien ja tiedon piilottamisen tärkeys on korostunut kriittisen infrastruktuurin siirryttyä hyödyntämään tietojärjestelmiä. Sähköverkkoon liittyviä salattavia tietoja ovat muun muassa kojeiden mallit, lokitiedot, konfiguraatiot, mittausdata ja liikenne eri yksiköiden välillä. (Hur 2011) Nykyaikainen salaus nojaa ainutlaatuisiin avaimiin, joita ei voi murtaa tai kopioida. Avaimia voi olla yksi tai useampi, riippuen salausprotokollasta. (Hur 2011) Eri tavoille käsitellä tai säilöä tietoa on erilaisia salausprotokollia, esimerkiksi internetliikenteelle HTTPS. (Stouffer ym. 2015) Salaus ehkäisee väliintuloiskuja ja tiedon vuotamista, kuten verkon kautta tapahtuvaa salakuuntelua. (Stouffer ym. 2015)

4.1.4 VPN

VPN eli virtuaalinen erillisverkko mahdollistaa tiedon salauksen ja verkkojen erottelun julkisessa verkossa. (Stouffer ym. 2015) Virtuaalisesti luotu verkko eristää tietoliikenteen muusta julkisesta verkosta, sekä mahdollistaa pääsyn verkkoon fyysisesti erotetusta laitteesta. (Stouffer ym. 2015) VPN-yhteyden riskinä on sen tunnusten päätyminen vääriin käsiin, jolloin vihamielinen toimija voi päästä sisälle ohjausverkkoon omalta päätteeltään. (MITRE ATT&CK 2023)

4.2 Murtohälytinjärjestelmät

Olennainen osa suojausjärjestelmiä on murtohälytinjärjestelmä, joka tunnistaa, ilmoittaa ja estää havaitsemansa vihamielisen toiminnan. (Yang ym, 2014) Murtohälytin, tai IDS (Intrusion Detection System), seuraa palomuurin tavoin verkon liikennettä ja iskee havaitsemiinsa sääntörikkomuksiin tai tuntemiinsa poikkeustilanteisiin. (MITRE ATT&CK 2023) IDS seuraa myös tietokoneiden sisäistä toimintaa. Hälytinratkaisut ovat yleensä kaupallisesti tuotettuja tuotteita, joita yritykset päivittävät jatkuvasti yhteistyössä asiakkaidensa ja viranomaisten kanssa.

4.3 Suunnittelu, seuranta, koulutus ja käyttöoikeudet

Kuten todettua, ihminen on tietojärjestelmän turvallisuuden heikoin lenkki. Oikean henkilön tietojen selvittäminen antaa vapaan pääsyn ohjausjärjestelmään. Siksi halvin ja paras keino turvata tietojärjestelmä on henkilöiden koulutus ja käyttöoikeuksien hallinta. (Laari 2019)

Asianomaisia kouluttamalla voidaan estää tietojenkalastelu, injektiot, väliintuloiskut sekä asiaton pääsy järjestelmien lähelle. Koska vahinkoja voi sattua missä vain, tulee niiden mahdollisuuteen varautua etenkin sähköverkossa, jossa virheet voivat aiheuttaa valtavia tuhoja. Siksi pelkän koulutuksen varaan ei pidä laskea, vaan myös käyttäjien käyttöoikeudet tulee rajata vain tarpeellisiin oikeuksiin. (Stouffer ym. 2015) Tietovuotojen varalta järjestelmien hallinnassa tulee myös hyödyntää käyttöoikeuksien hallintajärjestelmää, jolla vuotaneet avaimet saadaan korvattua nopeasti uusilla. Tällöin mahdollisten tietovuotojen aiheuttamat vahingot

voidaan rajata edelleen. (Stouffer ym. 2015)

Jatkuva toiminnan seuranta ja suunnittelu luovat edellytykset turvallisuuden ja toimitusvarmuuden jatkuvalle kehitykselle, mikä on välttämätöntä kriittisen infrastruktuurin toiminnan kannalta. (Stouffer ym. 2015)

5 Yhteenveto

Sähköverkon toiminta on elintärkeää koko yhteiskunnalle. Sähkön toimitusvarmuus on lailla turvattu ja verkkoyhtiöt ovat siitä vastuussa.

Sähköverkko on maantieteellisesti laajalle ulottuva järjestelmä, joten sen ohjausta ja valvontaa tehostaa huomattavasti tietotekniikan käyttöönotto. Verkkoa ohjaavat ja seuraavat suojareleet ovat yhteydessä käyttökeskusten tietokoneisiin verkkoyhteydellä.

Tietotekniikka tuo mukanaan uusia uhkia sähkön toimitusvarmuudelle, joita tässä tutkielmassa tarkasteltiin. Erilaisia uhkatekijöitä ovat vandaalit, rikolliset ja vihamieliset valtiot. Näiden toimijoiden toimintamahdollisuuksissa on suuria eroja, suurin vaikuttaja siihen on toimijan käytettävissä oleva raha.

Vihamieliseen toimintaan käytettäviä työkaluja voidaan käyttää tiedusteluun, tiedon väärentämiseen, kohteen ohjaamiseen tai pysäyttämiseen. Näitä mahdollistavia ratkaisuja on valtava määrä, niitä käytetään yhdessä ja erikseen ja niitä kehitetään jatkuvasti lisää. Hyökkääjät voivat hyödyntää tietoverkkoja, haittaohjelmia, laitteistoja ja henkilöitä, rajana vain raha, osaaminen ja mielikuvitus.

Ohjausjärjestelmän suojaus kehittyy myös jatkuvasti. Kehitystyöhön osallistuvat niin yritykset kuin viranomaisetkin. Vahva suojaus rakentuu teknisten suojaratkaisujen, kuten palomuurien, hälytinohjelmistojen ja erillisverkkojen, yhtäaikaisesta toiminnasta.

Lähteet

Andress, Jason. 2014. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Vol. Second edition.*

Andrey, Marcio. 2018. “SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach”, https://www.mdpi.com/1999-5903/10/8/76.

Campbell, Richard J. 2015. *Cybersecurity issues for the bulk power system.*

Clarke, Reynders. 2004. *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems.*

Dimitrios, Sarigiannidis. 2020. *A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics.* https://doi.org/10.1109/COMST.2020.2987688.

E-ISAC. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case.* https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6a77276749b76a40/607f235992f0063e5c070fff/E-ISAC_SANS_Ukraine_DUC_5%5b73%5d.pdf.

Frilander, Miika. 2021. *Sähköverkon suojausratkaisut Suomessa.* Opinnäytetyö, Kaakkois-Suomen ammattikorkeakoulu. https://www.theseus.fi/bitstream/handle/10024/512902/frilander_miika.pdf?sequence=2.

Goulart, Ana. 2021. *Man-in-the-middle Attacks and Defence in a Power System Cyber-physical Testbed.* https://doi.org/10.1049/cps2.12014.

He, Xinzhou. 2021. *Research on Computer Network Security Based on Firewall Technology.* https://doi.org/10.1088/1742-6596/1744/4/042037.

Hur, D. 2011. *Proposal Strategies of Key Management for Data Encryption in SCADA Network of Electric Power Systems.* https://doi.org/10.1016/j.ijepes.2009.03.004.

Janicke, H. 2012. *SCADA security in the light of Cyber-Warfare.* https://www.sciencedirect.com/science/article/abs/pii/S0167404812000429.

Korpinen, Leena. 1998. *Sähköverkon automaatio ja suojaus.* http://leenakorpinen.com/archive/svt_op/5sahkoverkon_auto%02maatio_ja_suojaus.pdf.

Kuusisto, Janne. 2022. *Sähkökatkojen välttäminen.* Kandidaatintutkielma, Tampereen yliopisto. https://trepo.tuni.fi/bitstream/handle/10024/145133/KuusistoJanne.pdf?sequence=2.

Laari, Tommi. 2019. *#kyberpuolustus, Kyberkäsikirja Puolustusvoimien henkilöstölle.* https://urn.fi/URN:ISBN:978-951-25-3120-2.

MITRE ATT&CK. 2023. *ICS tactics.* https://attack.mitre.org/tactics/TA0108/.

Mityukov, E A. 2019. *Phishing Detection Model Using the Hybrid Approach to Data Protection in Industrial Control System.* https://doi.org/10.1088/1757-899X/537/5/052014.

Morris, Thomas H. 2013. *Industrial Control System Cyber Attacks.*

Neerja, Alabbad, Khedri. 2021. *A Formal Approach to Network Segmentation.* https://doi.org/10.1016/j.cose.2020.102162.

Petäys, Antti. 2017. *Älykkään sähköverkon valvontaratkaisut, vikojen havaitseminen maakaapeliverkossa.* Opinnäytetyö, Tampereen ammattikorkeakoulu. https://www.theseus.fi/handle/10024/130626.

Sähkömarkkinalaki. 2013. *Työ- ja elinkeinoministeriö.*

Säteilyturvakeskus. 2021. *Sähkönsiirto piirros.* https://www.stuk.fi/documents/12547/103407/Sahkonsiirto_piirros.pdf/1216a642-2cba-4543-9aa4-838871405c87.

Tesla, Science Center. 2020. *Tesla's Wireless Power.* https://teslasciencecenter.org/teslas-wireless-power/.