Älykkäisiin sähköverkkoihin kohdistuvat kyberuhat ja niiden torjuminen

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Toukokuu 2025
Micke Sarro

TURUN YLIOPISTO
Tietotekniikan laitos

MICKE SARRO: Älykkäisiin sähköverkkoihin kohdistuvat kyberuhat ja niiden torjuminen

TkK-tutkielma, 23 s.
Tietotekniikka
Toukokuu 2025

Älykkäät sähköverkot ovat moderni infrastruktuuriratkaisu, jossa sähkön tuotannon, jakelun ja kulutuksen hallitsemiseksi hyödynnetään kaksisuuntaisia digi- ja viestintäteknologioita. Näiden järjestelmien keskeisiä etuja ovat energian tehokkaampi käyttö, verkon parempi toimintavarmuus sekä mahdollisuus integroida uusiutuvia energianlähteitä osaksi sähköntuotantoa. Samalla näiden järjestelmien vahva riippuvuus tieto- ja viestintäverkoista altistaa ne monenlaisille kyberuhille.
Tässä tutkielmassa tarkastellaan älykkäisiin sähköverkkoihin kohdistuvia kyberuhkia ja keinoja niiden torjumiseksi. Työssä kartoitetaan keskeisimpiä hyökkäysvektoreita, kuten palvelunestohyökkäyksiä, haittaohjelmia, tiedon manipulointia ja sisäpiiririskejä, sekä analysoidaan niiden mahdollisia yhteiskunnallisia vaikutuksia. Lisäksi työssä perehdytään nykyisiin kyberturvallisuuden arviointi- ja torjuntamenetelmiin, kuten tunkeutumisen havaitsemisjärjestelmiin, tekoälypohjaisiin analyysimenetelmiin sekä turvallisuusarkkitehtuurien kehityssuuntiin.
Tutkielma korostaa, että älyverkkojen kyberturvallisuus on moniulotteinen ilmiö, joka vaatii teknisten ratkaisujen lisäksi myös organisatorista ja inhimillistä huomiota. Kattava kyberturvallisuus edellyttää riskien tunnistamista, ennakoivaa suojautumista ja jatkuvaa sopeutumiskykyä kehittyvään uhkaympäristöön. Lopuksi työ tuo esiin kyberturvallisuuden keskeisen roolin yhteiskunnan toimivuuden ja huoltovarmuuden turvaamisessa.

Asiasanat: älykkäät sähköverkot, kriittinen infrastruktuuri, kyberturvallisuus

Sisällys

1 Johdanto **1**

2 Älykkäät sähköverkot **3**

2.1 Sähköverkkojen toiminta ja rakenne 3

2.2 Älykkäiden sähköverkkojen tuomat edut 6

2.3 Hyökkäysten yhteiskunnalliset vaikutukset 7

3 Sähköverkkoihin kohdistuvat kyberuhat **9**

3.1 Keskeisimmät hyökkäysvektorit 10

3.2 Pienemmän skaalan hyökkäykset 12

3.3 Suuremman skaalan hyökkäykset 13

3.4 Koordinoidut hyökkäykset 15

4 Uhkien torjunta ja riskienhallinta **17**

4.1 Keskeiset suojatumismenetelmät 17

4.2 Tekoälypohjaiset suojautumismenetelmät 19

4.3 Pohdintaa 20

5 Yhteenveto **22**

Lähdeluettelo **24**

1 Johdanto

Älykkäillä sähköverkoilla tarkoitetaan verkkoja, joissa sähköntuotannon, -jakelun ja -kulutuksen ohjaus tapahtuu reaaliaikaisen tiedonkeruun ja -analyysin pohjalta. Älykkäät sähköverkot parantavat verkon luotettavuutta, tehostavat energiankäyttöä sekä vähentävät häiriöitä ja kustannuksia. Niiden suurin ero perinteisiin verkkoihin on kaksisuuntainen kommunikaatio, joka lisää verkon joustavuutta, tehokkuutta ja mahdollistaa muun muassa uusiutuvien energialähteiden liittämisen verkkoon. Lisäksi ne tukevat uudenlaisia palveluita, kuten dynaamista hinnoittelua sekä kuluttajien osallistumista oman energiankäytön optimointiin älymittarien avulla. [1]

Tässä tutkielmassa tarkastellaan älykkäisiin sähköverkkoihin kohdistuvia kyberuhkia ja keinoja näiden uhkien torjumiseksi. Työn tavoitteena on syvällisesti analysoida merkittävimpiä kyberuhkia, joita älykkäiden sähköverkkojen järjestelmiin kohdistuu, sekä analysoida nykyisiä ja kehittyviä torjuntamenetelmiä. Lisäksi älykkäiden sähköverkkojen kriittisen yhteiskunnallisen aseman vuoksi tutkielmassa käsitellään myös sähköverkkojen kyberturvallisuuden merkittävyyttä ja mahdollisten hyökkäysten aiheuttamia vaikutuksia. Tutkielman tutkimuskysymykset ovat:

- Tk1: Millaisia merkittäviä kyberuhkia älykkäisiin sähköverkkoihin kohdistuu?
- Tk2: Millä tavoin älykkäisiin sähköverkkoihin kohdistuvia kyberuhkia pyritään torjumaan?

Tutkielma toteutettiin analyyttisena kirjallisuuskatsauksena ja tietoa haettiin pääosin informaatioteknologian tietokannoista, kuten Web of Science, IEEE Xplore

ja ACM Digital Library. Tiedonhaku suoritettiin englanniksi ja aiheeseen liittyvien käsitteiden ja hakusanojen perusteella muodostettiin seuraava hakulause:

- ("smart grid"OR "power grid")AND infrastructure AND (cyber AND security) AND (threat* OR solution*)

Kyseisen hakulauseen tuottamien tulosten perusteella koottiin noin 10 tieteellisen vertaisarvioidun artikkelin joukko, joka perustui pääosin artikkelien sisältöön ja julkaisuvuoteen. Yksi tärkeimmistä rajaavista tekijöistä oli lähteen julkaisuvuosi, sillä älykkäiden sähköverkkojen jatkuvan kehityksen ja yleistymisen myötä vanhempien tutkimusten tieto voi olla vanhentunutta ja harjaanjohtavaa. Kokonaisuudessaan hakuprosessin toinen vaihe oli käyttää hyväksi valittujen artikkeleiden lähdeluetteloa uusien lähteiden haussa.

Tutkielmassa on kolme asialukua. Luvussa 2 pohjustetaan älykkäiden sähköverkkojen rakennetta, verkkojen hyötyjä sekä hyökkäysten vaikutuksia. Luvussa 3 käsitellään keskeisimpiä kyberuhkia ja kategorisoidaan hyökkääjiä. Luvussa 4 tarkastellaan uhkien tunnistamista, ennaltaehkäisykeinoja ja riskienhallintamenetelmiä. Lopuksi luvussa 5 esitetään johtopäätökset ja vastataan tutkimuskysymyksiin.

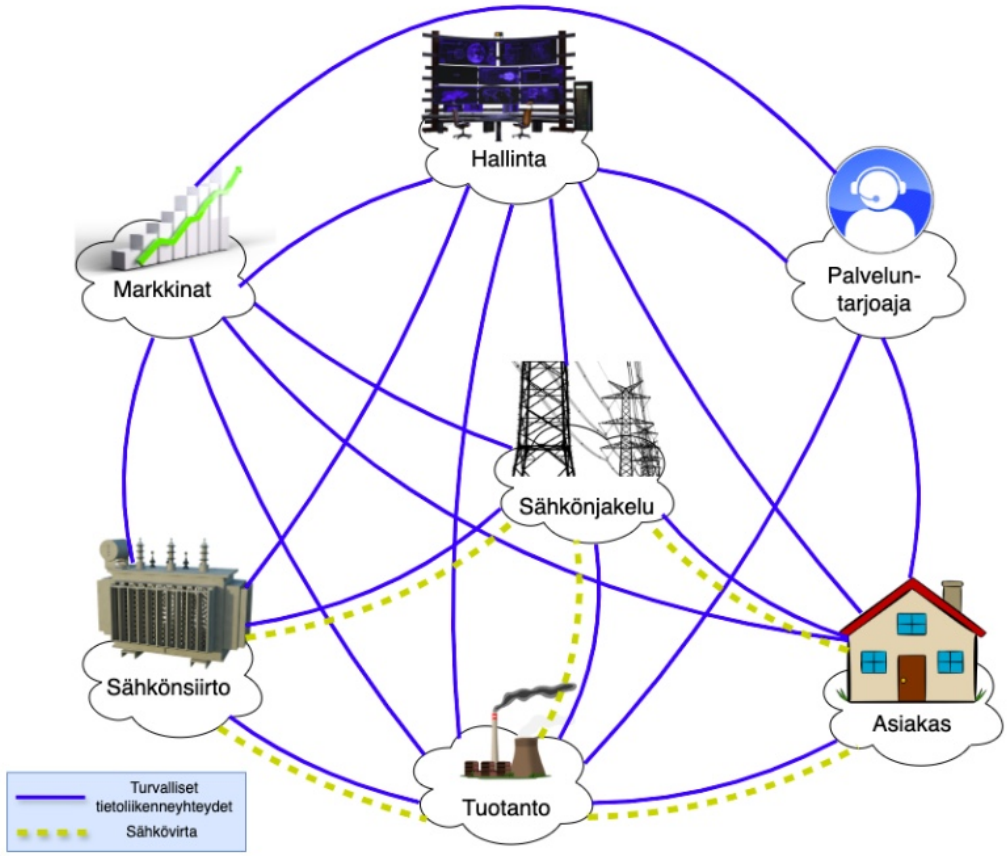
2 Älykkäät sähköverkot

Tässä luvussa esitetään älykkäiden sähköverkkojen keskeisimmät teknologiset piirteet sekä kuvaillaan tarkemmin infrastruktuurin tärkeimpien osa-alueiden toimintaa ja niiden rakennetta. Näiden osa-alueiden toiminnan ymmärtäminen on olennaista tutkielman seuraavissa luvuissa, joissa käsitellään sähköverkkoihin kohdistuvia kyberuhkia ja niiden suojautumismenetelmiä.

2.1 Sähköverkkojen toiminta ja rakenne

Modernien tieto- ja viestintäteknologioiden ansiosta älykkäiden sähköverkkojen eri osa-alueiden välinen kommunikaatio mahdollistaa laajan ja kokonaisvaltaisen sähkönsiirtojärjestelmän, jonka kaikki osat ovat älykkäästi yhteydessä toisiinsa. Tämä laaja kokonaisuus voidaan jakaa seitsemään eri luokkaan. Yhdysvaltain standardisointi- ja teknologiainstituutin (engl. National Institute of Standards and Technology, NIST) luoman sähköverkkojen kyberturvallisuuden viitekehyksen mukaan nämä seitsemän luokkaa ovat sähkönsiirto, jakelu, hallinta, tuotanto, markkinat, asiakas ja palveluntarjoaja [2]. NIST:n luoma viitekehys on hahmoteltu kuvassa 2.1.

Älykäs sähköverkko on siis kokonaisuudessaan yhdistelmä organisaatioita, rakennuksia, laitteita, systeemejä, yksilöitä ja muita toimijoita, joilla kaikilla on asema verkon ylläpitämisessä ja toiminnassa [1]. Jokaisella verkon toimijalla on myös olennainen osa tiedon siirtämisessä, tallentamisessa, muokkaamisessa ja prosessoinnissa. Verkon osapuolet usein myös kommunikoivat keskenään.



Kuva 2.1: Älykkään sähköverkon mallikonsepti (NIST) [2]

Älykkään sähköverkon eri osat koostuvat lukuisista hajautetuista järjestelmistä ja sovelluksista [3]. Monet näistä sovelluksista ovat kriittisiä verkon toiminnan kannalta, mutta ne myös sisältävät mahdollisia haavoittuvuuksia [1]. Tässä luvussa käsitellään kolmea kriittistä sovellusta sähköverkon infrastruktuurissa, jotka ovat edistynyt mittausinfrastruktuuri (engl. Advanced Metering Infrastructure, AMI) [4], automaattiset sähköasemat (engl. Automation Substation) [3] ja sähköverkkojen valvonta ja informaation hallinta (engl. Supervisory Control and Data Acquisition, SCADA) [5].

AMI-järjestelmien tehtävänä on kerätä ja analysoida tietoa kuluttajan energian- ja vedenkulutuksesta. Sähköverkkojen tapauksessa AMI mahdollistaa kaksisuuntaisen kommunikaation kuluttajan ja sähköntarjoajan välillä ja se koostuu kolmesta osasta: sähkömittarit (engl. smart meters), keskusjärjestelmä (engl. AMI headend)

ja viestintäverkko [6]. Jo yksinomaan AMI on monimutkainen ja laaja kompleksi, minkä takia siihen voi kohdistua useita kyberuhkia, kuten tietomurtoja, energiavarkauksia ja muita rikoksia. Koska AMI-järjestelmät ovat suoraan kytköksissä energiankulutukseen, rahalliseen tuottoon ja kuluttajien yksityisyyteen, infrastruktuurin kyberturvallisuuden takaaminen on erittäin tärkeää [6]. Sähköverkon eri osiin kohdistuvia hyökkäyksiä käsitellään tarkemmin seuraavissa luvuissa.

Automaattiset sähköasemat ovat avainasemassa sähkönjakelun infrastruktuurissa. Niiden tehtäviin kuuluu muun muassa sähkön vastaanottaminen tuotantolaitoksilta, sähkön jakelun sääteleminen ja virtapiikkien rajoittaminen [1] [3]. Sähköasemat koostuvat useista järjestelmistä, jotka toimivat automaattisesti ja mahdollistavat luotettavan ja tehokkaan sähköverkon. Edistyneen mittausinfrastruktuurin tapaan sähköasemat ovat myös kriittisiä ja niihin voi kohdistua useita kyberuhkia.

SCADA-järjestelmät ovat keskeisiä älykkäiden sähköverkkojen infrastruktuurissa [7]. Ne toimivat ikään kuin hermokeskuksina ympäri sähköverkkoa ja valvovat erilaisia hajautettuja järjestelmiä ja sovelluksia. SCADA-järjestelmät sijaitsevat usein sähköverkkojen hallintakeskuksissa, ja ne mahdollistavat ihmisen ja laitteiden välisen käyttöliittymän (engl. Human Machine Interface, HMI) [7] [8].

SCADA-järjestelmien yhteys ihmisten hallitsemiin laitteisiin tuo mukanaan mahdollisia haavoittuvuuksia infrastruktuuriin. Järjestelmien keskeisestä asemasta johtuen niiden kyberturvalliset seikat ovat entistäkin tärkeämpiä, ja erilaiset hyökkäykset ja haittaohjelmat voivat helposti vaarantaa verkon toimintavarmuuden. SCADA- ja muihin keskeisiin järjestelmiin kohdistuvia hyökkäyksiä käsitellään tarkemmin luvussa kolme.

2.2 Älykkäiden sähköverkkojen tuomat edut

Tieto- ja viestintäteknologioiden integraatio sähköverkkoihin on muuttanut verkkojen toimintaa ja kehitystä merkittävästi. Perinteisiin yksisuuntaisiin sähköverkkoihin verrattuna älykkäät sähköverkot ovat monin puolin tehokkaampia ja luotettavampia. Vakaa ja taloudellinen sähkönsiirto sekä sähkön säilyttäminen ovat älykkäiden sähköverkkojen merkittävimpiä etuja, jotka mahdollistavat muun muassa sähköautojen lataamisen ja uusiutuvien energianlähteiden integroinnin sähköverkkoon [9].

Ilmastonmuutoksen nopean kehityksen myötä yhä useammat valtiot ja organisaatiot ovat alkaneet siirtymään uusiutuviin energianlähteisiin [3]. Näiden lähteiden integrointi sähköverkkoon tuo kuitenkin mukanaan haasteita, kuten merkittäviä muutoksia sähkön tuotannossa sekä tarpeen pitkän matkan ja suuren kapasiteetin sähkölinjoille [10]. Fossiilisten energianlähteiden etu energiantuotannossa on se, että ne pystyvät tuottamaan energiaa jatkuvasti tasaisella syötöllä. Puolestaan uusiutuvien lähteiden, kuten tuulivoiman energiantuotto voi vaihdella jopa 100 prosenttia, ja aurinkovoiman 70 prosenttia olosuhteista riippuen [10]. Lisäksi uusiutuvat energianlähteet voivat aiheuttaa ilmiön nimeltä saariutuminen (engl. islanding), joka voi ilmetä sähkökatkon seurauksena [4]. Tavallisesti sähkökatkon aikana sähkönsiirto tietylle alueelle keskeytyy kokonaan, mutta saariutuminen voi johtaa siihen, että jokin uusiutuva energialähde tahattomasti jatkaa energiantuotantoa kyseiselle alueelle. Tämä voi aiheuttaa odottamattomia sähkövirtoja ja siten merkittäviä turvallisuusriskejä [11].

Älykkäiden sähköverkkojen sovellukset onnistuvat vastaamaan näihin haasteisiin. Verkkoinfrastruktuurin lukuisat sensorit, laitteet ja sähkömittarit valvovat verkkoa jatkuvasti ja ylläpitävät sähköntuotannon ja kulutuksen välistä tasapainoa. Verkon erilaiset sovellukset myös ennakoivat sähkönkulutusta vuorokauden ajasta ja muista tottumuksista riippuen ja ohjaavat sähkön tuotantoa jatkuvasti [12]. Lisäksi tärkeässä osassa uusiutuvien energianlähteiden integrointia verkkoon ovat valtavat

energiavarastot, joita hyödyntämällä pystytään tasaamaan sähköverkkoa ja samalla vähentämään sähkötappioita [13].

Ylimääräistä sähkönkulutusta voidaan vähentää kokonaisuudessaan välttämällä suuria tappioita. Älykkäiden sähkömittarien ansiosta myös kuluttajat voivat seurata ja vähentää kulutustaan. Älykäs sähköverkko myös tarjoaa kuluttajalle mahdollisuuden seurata sähkömarkkinoita ja täten alentaa kustannuksia [12].

Älykkäiden sähköverkkojen tuomia etuja on siis lukuisia. Ne mahdollistavat muun muassa uusiutuvien energianlähteiden käytön, parantavat tehokkuutta ja vähentävät tappioita. Ennusteiden mukaan energian käytön ja päästöjen vähentämisen avulla älykkäät sähköverkot aikovat saavuttaa 290 miljardin dollarin kokonaissäästöt vuoteen 2029 mennessä. Tämä on 249 % enemmän kuin vuonna 2024, jolloin säästöjä kertyi 84 miljardia dollaria [14].

2.3 Hyökkäysten yhteiskunnalliset vaikutukset

Sähköverkko on modernin yhteiskunnan yksi kriittisimmistä infrastruktuureista. Nykypäivänä lähes kaikki keskeiset järjestelmät ja palvelut ovat täysin riippuvaisia vakaasta sähköverkosta [15]. Sähköverkkoihin kohdistuvat kyberhyökkäykset voivat aiheuttaa laajamittaisia sähkökatkoja, joiden vaikutukset voivat vaihdella yksilötasolta aivan yhteiskunnan kriittisimpiin palveluihin.

Laajamittaisen sähkökatkon tapahtuessa sen vaikutukset voidaan huomata lähes välittömästi yhteiskunnan elintärkeissä palveluissa, kuten vedenjakelussa, liikenteessä ja viestintäyhteyksissä. Erilaiset jäte- ja vedenhuoltopalvelut tarvitsevat jatkuvasti sähkövirtaa toimikseen, ja sähkökatkon tapahtuessa nämä järjestelmät ovat äkkiä toimintakelvottomia. Välitön vaikutus näkyy myös liikenteenohjauksen järjestelmissä, kuten liikennevaloissa ja raideliikenteessä, mikä aiheuttaa häiriöitä ja mahdollisia onnettomuuksia. Lisäksi viestintäverkot voivat kaatua, mikä vaikeuttaa viranomaisten ja kansalaisten välistä tiedonkulkua kriisitilanteessa. [16]

Sairaalat ja muut terveydenhuollon palvelut ovat yksi tärkeimmistä osista yhteiskuntaa, ja myös ne ovat riippuvaisia sähköverkosta. Elintärkeät laitteet, kuten hengityskoneet ja leikkaussalien varusteet ovat toimintakelvottomia sähkökatkon tapahtuessa. Näiden lisäksi sairaaloissa jouduttaisiin keskeyttämään elintärkeitä toimintoja, kuten sterilointi, kuvantaminen ja laboratoriopalvelut. Yllättävien sähkökatkojen varalle useimpiin sairaaloihin on onneksi asennettu varageneraattori, joka on suunniteltu säilyttämään sairaalan kriittiset toiminnot jopa kahdeksan tunnin ajan. Kyberhyökkäyksen aiheuttaman kokonaisvaltaisen sähkökatkoksen tapauksessa katkos voi kuitenkin tilanteesta riippuen kestää huomattavasti pidempään, ja sen mahdollisesti aiheuttaman kriisitilanteen aikana polttoaine- ja muut tarviketäydennykset voivat viivästyä. [17]

Sähkökatkon ajankohdalla on myös suuri merkitys sen vakavuuteen ja vaikutuksiin. Oikein ajoitetun kyberhyökkäyksen aiheuttama sähkökatkos esimerkiksi kylmänä talvipäivänä voi aiheuttaa suurta yhteiskunnallista vahinkoa. Esimerkiksi Suomessa omakotitaloista 36 % ja kaikista taloista viidesosa lämmitetään sähköllä vuoden 2022 tilastojen mukaan [18]. Tämä vastaisi hyvin merkittävää ihmismäärää kovissa talviolosuhteissa ilman tarvittavaa lämmitystä, minkä seurauksena valtakunnallinen kriisitilanne olisi lähes väistämätön.

3 Sähköverkkoihin kohdistuvat kyberuhat

Älykkäät sähköverkot ovat monin tavoin alttiita kyberhyökkäyksille. Verkon lukuisat osa-alueet, sovellukset, fyysiset komponentit ja näiden väliset yhteydet muodostavat kaikki mahdollisia kohteita hyökkääjille. Näiden tavoitteena voi olla esimerkiksi henkilötietojen kaappaus, sähkömittarien manipulointi tai laajamittaiset palvelunestohyökkäykset sähköverkkoihin. [19]

Tässä luvussa käsitellään ensiksi keskeisimpiä hyökkäysvektoreita ja sitä, miten niiden avulla voidaan manipuloida sähköverkon eri osia. Seuraavaksi tarkastellaan sähköverkkoihin kohdistuvia uhkia ja hyökkäyksiä, jotka on jaettu pienemmän- ja suuremman skaalan hyökkäyksiin. Tässä yhteydessä perehdytään tarkemmin hyökkäysten toimintaperiaatteisiin, kohteisiin ja tavoitteisiin sekä siihen, miten edellä mainittuja hyökkäysvektoreita voidaan konkreettisesti hyödyntää.

Luvun lopussa tarkastellaan koordinoituja hyökkäyksiä, kuten vuoden 2015 hyökkäystä Ukrainan sähköverkkoon. Tämä tapaus on yksi merkittävimmistä älykkäisiin sähköverkkoihin kohdistuneista kyberhyökkäyksistä. Tässä tarkastelemme tarkemmin hyökkäyksen kulkua, hyökkäysmentelmiä ja siitä opittuja asioita, joita voidaan hyödyntää sähköverkkojen kyberturvallisuuden parantamisessa myös tulevaisuudessa.

Taulukko 3.1: Hyökkääjäprofiilit ja niiden tavoitteet [8]

Rooli	**Motivaatio**	**Tavoite**	**Pääsy**	**Osaaminen**
Pienemmän skaalan hyökkäykset				
Yksityinen kuluttaja	Rahallinen tuotto	Sähkönkulutuksen muuntelu	Fyysinen	Julkinen tieto
Script-kiddie	Julkisuus	Kaikki	Etä	Julkinen tieto
Kyberrikollinen	Rahallinen tuotto	Tietovarkaus, Markkinoiden manipulointi	Etä	Julkinen tieto
Suuremman skaalan hyökkäykset				
Kyberterroristit	Toimialan häiritseminen	Verkon häiritseminen	Etä, Fyysinen	Alan osaaminen
Valtioterrorismi	Geopolitiikka	Häiritseminen, Vakoilu, Tietovarkaus, Markkinoiden manipulointi	Etä, Fyysinen	Sisäpiiritieto
Sabotoiva sisäpiiriläinen	Toimialan häiritseminen	Verkon häiritseminen	Etä, Fyysinen	Sisäpiiritieto

Taulukossa 3.1 kuvaillaan sähköverkkoihin kohdistuvien hyökkäysten motivaatiota, tavoitteita ja hyökkääjien roolia. Hyökkäykset on jaettu pienemmän ja suuremman skaalan hyökkäyksiin. Aliluvussa 3.2 käsitellään tarkemmin pienemmän skaalan hyökkäyksiä ja niiden tavoitteita ja toimintamenetelmiä. Aliluvussa 3.3 puolestaan käsitellään suuremman skaalan hyökkäyksiä näistä näkökulmista. Pienemmän skaalan hyökkäyksiä ja niiden seurauksia käsitellään tiivistetysti, mutta suuremman skaalan hyökkäyksiä käsitellään syvällisemmin niiden yhteiskunnallisen merkittävyyden vuoksi.

3.1 Keskeisimmät hyökkäysvektorit

Älykkäisiin sähköverkkoihin kohdistuvat kriittisimmät hyökkäysvektorit ovat sellaisia, jotka muuttavat tai häiritsevät verkon toimintaa. Hyökkäysten aiheuttamat vaikutukset eivät kuitenkaan välttämättä ole suoraan huomattavissa, kuten esimerkiksi taustalla pyörivä haittaohjelma. Nämä keskeisimmät hyökkäysvektorit ovat palvelu-

nestohyökkäykset (engl. Denial of Service, DoS), väärän datan injektio (engl. False Data Injection, FDI), väliintulohyökkäykset (engl. Man-in-the-middle, MITM), haittaohjelmat (engl. Malware) [20].

Palvelunestohyökkäysten eri menetelmiä on useita, kuten SYN-hyökkäykset, puskurin ylivuotovirheet (engl. buffer overflow) ja Smurf-hyökkäykset. Erilaiset palvelunestohyökkäykset toimivat eri menetelmillä ja kohdistuvat eri osiin kohdejärjestelmää, mutta niiden kaikkien tavoitteena on yksinkertaisesti kohdistaa mahdollisimman paljon verkkoliikennettä samanaikaisesti yhteen kohteeseen. Tällä tavoin hyökkääjät pyrkivät hidastamaan tai pahimassa tapauksessa estämään järjestelmän toiminnan täysin. [1]

Väärän datan injektiolla (engl. FDI) tarkoitetaan menetelmää jossa sähköverkon eri järjestelmiin syötetään väärennettyä tietoa tai komentoja. FDI-hyökkäyksen menetelmiä ovat muun muassa väärentäminen ja SQL-injektio. Tyyppillisesti FDI-hyökkäys voi kohdistua AMI-järjestelmiin, missä hyökkääjä voi peukaloida tai jopa poistaa sähkömittarien keräämää dataa tavoitteena muunnella kuluttajan sähkönkulutustietoja. [20] [21]

Väliintulohyökkäyksessä hyökkääjä asettaa itsensä kahden luotetun osapuolen väliin, josta se voi kuunnella, muokata ja manipuloida osapuolten välistä tiedonsiirtoa. Onnistuneessa väliintulohyökkäyksessä kummatkin osapuolet ovat täysin tietämättömiä siitä, että heidän välinen tiedonsiirto on kompromisoitu. Hyökkääjä voi esimerkiksi siepata TCP/IP-yhteyden sähköaseman ja SCADA-hallintakeskuksen välillä, jonka seurauksena arkaluonteista tietoa voidaan lukea ja muokata täysin huomaamatta. [1] [12] [20]

Haittaohjelmat tunkeutuvat kohdejärjestelmään tavoitteena ohjata ja päästä luvattomasti käsiksi arkaluonteisiin tietoihin. Erilaisia haittaohjelmia ovat muun muassa troijalaiset hevoset, kiristyshaittaohjelmat ja madot. Haittaohjelmat ovat suuri riski etenkin hallintajärjestelmissä, jotka ovat yhteydessä HMI-järjestelmiin niiden

inhimillisen aspektin seurauksena. Haittaohjelmat leviävät usein esimerkiksi sähköpostien, tekstidokumenttien, nettisivujen ja USB-tikkujen välityksellä kohdejärjestelmään, josta haittaohjelma pystyy etenemään laitteesta toiseen. Kuten väliintulohyökkäykset, myös haittaohjelmat voivat toimia huomaamattomasti järjestelmän taustalla, keräten kriittistä dataa tai odottaen sopivaa hetkeä iskeä. [20] [22]

Muita kriittisiä sähköverkkoihin kohdistuvia hyökkäytekniikoita ovat muun muassa kalastelu (engl. Phishing), kuorman muuntelu (engl. Load altering) ja väärentäminen (engl. Spoofing). Kalastelu on merkittävä tekniikka, jonka avulla hyökkääjät pyrkivät huijaamaan käyttäjiä luovuttamaan arkaluontoisia tietoja tai asentamaan haittaohjelmia esimerkiksi sähköpostin välityksellä. Kuorman muuntelu hyödyntää edellä mainittuja hyökkäytekniikoita päästäkseen käsiksi hallintajärjestelmiin, joiden avulla hyökkääjät voivat manipuloida sähköverkon kuormaa [20]. Väärentämisellä puolestaan tarkoitetaan tekniikkaa, jossa hyökkääjä esiintyy luotettavana osapuolena järjestelmässä saadakseen pääsyn arkaluontoisiin tietoihin [19].

3.2 Pienemmän skaalan hyökkäykset

Pienemmän ja suuremman skaalan kyberhyökkäysten suurin ero on niiden aiheuttamat seuraamukset. Pienemmän skaalan hyökkäysten tavoitteena voi olla esimerkiksi rahallinen tuotto tai tietovarkaus, mutta niiden seuraukset eivät fyysisesti vaikuta osallisiin. Yksi yleisimmistä tämänkaltaisista hyökkäyksistä on AMI-järjestelmän tai tarkemmin älykkäiden sähkömittarien manipulointi. Sähkömittareiden peukalointiin voidaan käyttää erilaisia FDI-menetelmiä, kuten SQL-injektiota [12]. Koska sähkömittarit ovat osa sähköverkon fyysistä infrastruktuuria ja sijaitsevat usein asiakkaiden kodeissa, ne ovat erityisen alttiita hyökkäyksille [8]. Yksityisen kuluttajan motiivina voi olla esimerkiksi energiavarkaus, jonka tavoitteena on säästää rahaa vähentämällä omaa sähkönkulutusta valheellisesti [5].

Myös kyberrikollisten toteuttamat hyökkäykset voidaan lukea pienemmän skaalan hyökkäyksiin. Toisin kuin yksityinen kuluttaja, kyberrikolliset toteuttavat hyökkäyksiä yleensä etänä ja tavoittelevat rahallista tuottoa hyödyntämällä erilaisia hyökkäysmenetelmiä. Rahallisen hyödyn lisäksi kyberrikolliset voivat varastaa kuluttajien yksityisiä tietoja ja käyttää niitä kiristääkseen sekä yksityishenkilöitä että suurempia toimijoita. [8]

Kyberrikolliset hyödyntävät aiemmin mainittuja hyökkäysvektoreita, kuten FDI- ja DoS-hyökkäyksiä [8]. Hyökkäykset kohdistuvat usein infrastruktuurin hallinta ja palveluntarjoajan osa-alueisiin. Hyökkääjät voivat muun muassa kohdistaa DoS-hyökkäyksen palveluntarjoajan järjestelmiin ja aiheuttaa täten merkittäviä tappioita [23].

Kyberrikollista yksinkertaisempi toimija on niin sanottu harrastelijahakkeri (engl. Script-kiddie). Harrastelijahakkerilla ei yleensä ole yhtä paljon teknistä osaamista kuin kyberrikollisella, eikä hänen tavoitteensa välttämättä ole saavuttaa mitään konkreettista. Harrastelija pyrkii käyttämään kaikkia osaamiaan keinoja saadakseen edes rajoitetun pääsyn sähköverkon järjestelmiin. Harrastelijaa voi motivoida halu saada mainetta ja tunnustusta, sekä kehittyä kohti vaativampia hyökkäyksiä. [24] Kaiken kaikkiaan harrastelijahakkerit eivät muodosta merkittävää uhkaa älykkäiden sähköverkkojen kyberturvallisuudelle.

3.3 Suuremman skaalan hyökkäykset

Suuremman skaalan hyökkäykset eroavat pienemmän skaalan hyökkäyksistä ensisijaisesti niiden vakavuuden ja laajuuden osalta. Hyökkäysten tavoitteena voi olla muun muassa kriittisen infrastruktuurin häiritseminen, tietovarkaus, sähkömarkkinoiden manipulointi, vakoilu tai jopa geopoliittisten tavoitteiden edistäminen. Pienemmän skaalan hyökkäyksiin verrattuna suuremman skaalan hyökkäykset voivat aiheuttaa laajamittaisia taloudellisia, poliittisia tai yhteiskunnallisia vahinkoja.

Älykkään sähköverkkoinfrastruktuurin kriittiset osat, kuten SCADA-hallintajärjestelmät, sähköasemat ja älykkäät sähkömittarit ovat usein hyökkäysten kohteena. Nämä merkittävät järjestelmät ovat tyypillisesti hyvin suojattuja, jonka seurauksena myös hyökkääjät ovat hyvin valmistautuneita. Hyökkääjillä on enemmän resursseja, osaamista ja päätösvaltaa kuin pienemmän skaalan hyökkäyksissä, jonka ansiosta heillä on myös useimmiten fyysinen pääsy moniin järjestelmiin. Fyysisen tason hyökkäykset ovat monesti tehokkaampia etä-hyökkäyksiin verrattuna, mutta ne ovat myös huomaatavasti helpompi havaita [21]. Sekä etä- että fyysisen tason pääsyn yhdistelmä sähköverkon eri järjestelmiin tekee suuremman skaalan hyökkäyksistä erityisen tehokkaita. Kun tähän lisätään hyökkääjien osaaminen ja mahdollinen sisäpiiritieto järjestelmien toiminnasta, hyökkäysten vaikutukset voivat olla merkittäviä [8] [25].

Kyberterroristi on hyvä esimerkki suuremman skaalan hyökkääjästä. Kyberterroristiksi voidaan luokitella tekijä, jonka tavoitteena on sähköverkon häiritseminen ja sitä kautta yhteiskunnan vahingoittaminen. Kyberterroristi voi esimerkiksi manipuloida katkaisijoita (engl. circuit breakers) eri osissa verkkoa, mikä voi johtaa sähkökatkoihin. Hyökkääjä voi muun muassa päästä käsiksi piirien väliseen kommunikaatioverkkoon ja muunnella viestejä (väliintulohyökkäys), kohdistaa palvelunestohyökkäyksen katkaisijoita ohjaaviin järjestelmiin tai tunkeutua suoraan SCADA-järjestelmään. [25].

Suuremman skaalan hyökkäysten taustalla voi olla myös niin sanottu sabotoiva sisäpiiriläinen. Tällainen toimija on esimerkiksi palveluntarjoajan tai sähköverkon hallintaan erikoistuvan yrityksen työntekijä, jolla on työtehtävästä ja oikeuksista riippuen suora pääsy kriittisiin hallintajärjestelmiin [26]. Työntekijän pääsy ja tekninen osaaminen tekevät sisäpiiriläisestä merkittävän riskin sähköverkon kyberturvallisuudelle, ja hänen motiivinaan on usein verkon häiritseminen. Hyökkäykset ovat erityisen vaarallisia silloin, kun sisäpiiriläisen taitoja ja järjestelmäoikeuksia

hyödynnetään organisoidusti esimerkiksi kyber- tai valtioterroristien toimesta [8].

Merkittävin uhka älykkäille sähköverkoille on valtioterrorismi. Näiden toimijoiden aiheuttamat hyökkäykset ovat usein hyvin rahoitettuja, suunniteltuja ja niitä varten on varattu suuri määrä resursseja [22]. Hyökkäysten tavoitteena voi pahimmillaan olla sähköverkon ja sähköntuotanto-operaatioiden laajamittainen häirintä, mutta niihin voi kuulua myös esimerkiksi vakoilu, tietovarkaus tai markkinoiden manipulointi. [8].

3.4 Koordinoidut hyökkäykset

Valtioterroristien aiheuttamat hyökkäykset ovat hyvä esimerkki koordinoidusta hyökkäyksestä, sillä ne ovat usein hartaasti valmisteltu ja suunniteltu. Tällaiset hyökkäykset tavallisesti koostuvat neljästä vaiheesta, jotka ovat tiedustelu, kartoitus, hyväksikäyttö ja pääsyn ylläpitäminen [27]. Ensimmäinen vaihe eli tiedustelu koostuu muun muassa verkkoliikenteen tiedostelusta ja sosiaalisesta manipuloinnista. Kalastelu on hyvä esimerkki sosiaalisesta manipuloinnista [20]. Toisen vaiheen eli kohdeverkon ja järjestelmien kartoituksen tavoitteena on skannata verkosta löytyviä haavoittuvuuksia, kuten avoimia portteja, IP-osoitteita ja verkkoon yhdistettyjä laitteita. Muun muassa Modbus ja DNP3 ovat kaksi älykkäiden sähköverkkojen järjestelmissä käytettyä protokollaa, jotka ovat myös haavoittuvaisia skannaushyökkäyksille [1]. Kolmas vaihe on hyväksikäyttö tai niin sanottu hyökkäysvaihe, jossa hyökkääjä pyrkii pääsemään käsiksi sähköverkon hallinta- ja muihin kriittisiin järjestelmiin. Tässä vaiheessa hyökkääjä voi käyttää hyväkseen mitä tahansa aliluvussa 3.1 mainittuja hyökkäysvektoreita saadakseen järjestelmän hallinnan [1]. Hyökkäyksen viimeinen vaihe on pääsyn ylläpitäminen. Tässä vaiheessa hyökkääjä käyttää keinoja kuten takaovia ja haittaohjelmia mahdollistaakseen itselleen huomaamattoman pääsyn järjestelmään myös hyökkäyksen jälkeen [26].

Hyvä esimerkki huomaamattomasta pääsyn ylläpitämisestä on haittaohjelma nimeltä Stuxnet, joka havaittiin ensimmäisen kerran kesäkuussa 2010 ja onnistuttiin asentamaan Iranin ydinlaitokseen muistitikun välityksellä. Stuxnet oli mato, joka hyödynsi Windows-käyttöjärjestelmän haavoittuvuuksia levitäkseen huomaamattomasti laitteesta toiseen. Haittaohjelman avulla hyökkääjät pystyivät myös valvomaan ja hallitsemaan järjestelmiä sekä lopulta sabotoimaan laitteistot toimintakelvottomiksi. [28]

Yksi merkittävimmistä älykkäisiin sähköverkkoihin kohdistuneista hyökkäyksistä on vuonna 2015 Ukrainan sähköverkkoon kohdistunut hyökkäys, joka vaikutti noin 225 tuhanteen ihmiseen [29]. Hyökkäys on mainio esimerkki kokonaisvaltaisesta koordinoidusta hyökkäyksestä, sekä osoitus valtioterrorismin vahvuudesta kyberhyökkäyksissä sähköverkkoja kohtaan. [22]. Myöhemmin vuonna 2021 Yhdysvaltojen hallitus kertoi hyökkäyksen takana olevan joukko venäläisten kansallisvaltioiden kybertoimijoita, joiden tavoitteena oli häiritä Ukrainan kriittistä infrastruktuuria [29] [30].

Ukrainan sähköverkkoon kohdistunut hyökkäys seurasi aikasemmin mainittua mallia, jossa venäläisten hyökkääjien ensimmäinen vaihe oli tiedustelu [8]. Tiedustelun jälkeen hyökkääjät pystyivät kehittämään jo ennestään löytyvää haittaohjelmaa ja räätälöimään sen kyseistä hyökkäystä varten [22]. Tiedustelu ja kartoitusvaiheen jälkeen hyökkääjät iskivät koordinoidusti useaan osaan järjestelmää, kuten SCADA-hallintajärjestelmiin ja sähköasemiin. Hyökkäyksessä käytettiin lukuisia eri tekniikoita, kuten palvelunestoa, haittaohjelmia, FDI-hyökkäyksiä ja kalastelua [5] [8]. Kaiken kaikkiaan hyökkäys oli malliesimerkki onnistuneesta kyberhyökkäyksestä älykkääseen sähköverkkoon, mutta sen ansiosta kyberturvallisuuden seikkoihin kiinnitetään entistä enemmän huomiota ja elintärkeitä edistyksiä on saatu aikaan.

4 Uhkien torjunta ja riskienhallinta

Yleisesti älykkäät sähköverkot ovat hyvin suojattuja yksinkertaisilta kyberhyökkäyksiltä. Laajamittaisilta ja hyvin suunnitelluilta hyökkäyksiltä suojautuminen on kuitenkin haastavaa, kuten aliluvussa 3.3 todettiin. Tässä luvussa käsitellään tarkemmin sähköverkkojen keskeisiä suojautumismenetelmiä, niihin liittyviä haasteita sekä muita tärkeimpiä toimintaperiaatteita. Lopuksi tarkastellaan tekoälypohjaisia suojautumismenetelmiä ja pohditaan älykkäiden sähköverkkojen kyberturvallisuuden tulevaisuutta.

4.1 Keskeiset suojatumismenetelmät

Älykkäillä sähköverkoilla on muutamia merkittäviä suojatumismekanismeja, jotka ovat yleisessä käytössä usessa osassa järjestelmää. Näistä yksi hyvin keskeinen on tunkeilijan havaitsemisjärjestelmä (engl. Intrusion Detection System, IDS), jonka keskeinen toimintaperiaate on valvoa laitteita ja niiden välistä verkkoliikennettä [31]. IDS-järjestelmät voidaan jakaa verkko-pohjaisiin (engl. Network-based IDS) ja isäntä-pohjaisiin (engl. Host-based IDS), mikä määrittelee valvooko järjestelmä kokonaisia verkkovirtoja vai ainoastaan isäntäjärjestelmän toimintaa [5]. Näiden järjestelmien kaksi yleisintä toimintatapaa on tietoon- tai allekirjoitukseen perustuva havaitseminen, sekä poikkeavuuksiin perustuva havaitseminen [31]. Allekirjoitukseen perustuva menetelmä valvoo verkkoliikennettä ja etsii jo ennestään tunnettuja jälkiä ja merkkejä, jotka voisivat osoittaa yleisimpiin kyberhyökkäyksiin. Poikkea-

vuuksiin perustuva menetelmä yksinkertaisesti etsii poikkeuksia verkkoliikenteestä [32]. Kumpikaan näistä järjestelmistä ei kuitenkaan ole täydellinen. Allekirjoitukseen perustuva menetelmä perustuu tarkkaan joukkoon sääntöjä, joten hälyytyksen aikaansaamiseksi vaaditaan jo ennestään tunnettu uhka. Poikkeavuuksiin perustuva menetelmä puolestaan aktivoituu hyvin helposti, sekä aiheuttaa usein myös vääriä hälyytyksiä [5].

Älykäs sähköverkko muodostaa laajan ja kriittisen kokonaisuuden, joka koostuu sekä fyysisistä että digitaalisista järjestelmistä (engl cyber physical system, CPS) [5]. Sähköverkon suojautumisjärjestelmiä kehittäessä niiden testaaminen on myös hyvin tärkeää, mutta näiden järjestelmien testaus aktiivisessa sähköverkossa on hyvin riskialtista. Tämän seurauksena on kehitetty erilaisia kyberfyysisten järjestelmien testialustoja sähköverkon simuloimiseksi (engl. CPS testbed) [33]. Nämä testialustat mahdollistavat etenkin verkon haavoittuvuuksien ja suojatumismenetelmien tarkemman tutkimuksen [5]. Täysin digitaalisiin simulaatioihin verrattuna kyberfyysiset alustat tarjoavat tarkemman mallin todellisen maailman järjestelmistä, jonka seurauksena ne mahdollistavat tehokkaan ja luotettavan kehityksen [33].

Kaikki edellä mainitut suojatumismenetelmät perustuvat laitteisiin ja järjestelmien suojaamiseen. Siitä huolimatta yksi suurimmista sähköverkkojen turvallisuusongelmista on inhimillinen tekijä [34]. Aliluvussa 3.1 mainitut hyökkäysvektorit, kuten haittaohjelmat, leviävät usein työntekijöiden heikkojen tietoturva-käytänteiden seurauksena, esimerkiksi kalasteluhyökkäysten avulla [35]. Tämän vuoksi älykkäiden sähköverkkojen yksi keskeisimmistä suojatumismenetelmistä on työntekijöiden koulutus hyviin tietoturvakäytänteisiin sekä tilannetietoisuuden kehittäminen mahdollisten hyökkäysten tapahtuessa [22].

4.2 Tekoälypohjaiset suojautumismenetelmät

Viimeisen vuosikymmenen aikana kone- ja syväoppimisen menetelmien soveltaminen älykkäiden sähköverkkojen kyberturvallisuudessa on lisääntynyt merkittävästi. Muun muassa kasvanut laskentateho, laajentunut anturidata ja kehittyneet neuroverkkoarkkitehtuurit mahdollistavat reaaliaikaisen tiedon käsittelyn ja poikkeavuuksien tunnistamisen perinteisiä IDS-järjestelmiä tehokkaammin. Tämän tehokkuuden avulla tekoälyjärjestelmät pystyvät siis tunnistamaan hyökkäyksiä todennäköisemmin ilman, että jokaista hyökkäyskuviota tarvitsee etukäteen määritellä. [35] Tekoälymallit oppivat erottamaan poikkeavat ilmiöt analysoimalla muun muassa tietovirtojen jännite- ja virtasignaaleja sekä verkon viive- ja pakettidataa [20].

Uhkien torjumiseen käytettyjen tekoälymallien koulutukseen käytetään useita tekniikoita, mutta yleisemmin tekoälymallit koulutetaan joko valvotusti (engl. supervised) tai valvomattomasti (engl. unsupervised). Valvotussa koulutuksessa opetusdata sisältää tarkasti merkityt verkon hyökkäys- ja normaaliolosuhteet, kun taas valvomattomassa koulutuksessa malli opetetaan automaattisesti tunnistamaan muutokset verkon toiminnassa ilman ylimääräistä tietoa [35]. Näitä koulutusmenetelmiä käyttämällä voidaan luoda erilaisia havaitsemisjärjestelmiä eri käyttötarkoituksiin, kuten esimerkiksi reaaliaikaiseen valvontaan. Siinä saapuva data skalataan ja syötetään opetetetulle neuroverkolle, joka tuottaa hälyytyksen aina kun järjestelmän tila poikkeaa opitusta normaalista tasosta [22]. Joissakin ratkaisuissa hyödynnetään myös vahvistusoppimista (engl. reinforcement learning), jossa kyseinen tekoälymalli eli agentti opetetaan etsimään ja paikkaamaan verkon haavoittuvuuksia olemalla suorassa vuorovaikutuksessa sähköverkon järjestelmien kanssa [20]. Luvussa 4.1 mainitut kyberfyysisten järjestelmien testialustat ovat lähes välttämättömiä näiden tekoälymallien kehittämiseen, sillä interaktiivisen tekoälyagentin kouluttaminen aktiivisessa verkossa olisi erittäin riskialtista.

Tekoälypohjaisten menetelmien suurimpia etuja ovat siis niiden kyky havaita ennestään tuntemattomia uhkia, sopeutua muuttuviin olosuhteisiin ja analysoida suuria määriä tietoa perinteisiä IDS-järjestelmiä nopeammin [22]. Näihin menetelmiin liittyy kuitenkin myös haasteita, kuten laadukkaan ja tarpeeksi laajan harjoitusdatan puute. Lisäksi laskentateho ja muut resurssiperäiset vaatimukset rajoittavat tekoälymallien integroimista useisiin kenttälaitteisiin, sekä runsas tiedonsiirto laitteiden ja keskusyksikön välillä on raskasta ja riskialtista [20].

Osittainen ratkaisu näihin ongelmiin on Googlen vuonna 2016 ehdottama konsepti yhdistetystä oppimisesta (engl. Federated Learning), joka perustuu tekoälymallien kouluttamiseen ilman, että arkaluontoista dataa siirretään keskuspalvelimelle [36]. Tämän oppimismallin etuna on myös niiden suuri tarkkuus uhkien tunnistamiseksi sekä matalat laskentakustannukset [22].

4.3 Pohdintaa

Älykkäiden sähköverkkojen kyberturvallisuus kehittyy jatkuvasti, sillä teknologisen kehityksen myötä myös verkkoihin kohdistuvat hyökkäykset muuttuvat. Eräs merkittävä kehityskohde kyberturvallisuuden maailmassa on Zero Trust-arkkitehtuuri, joka voisi paremmin mahdollistaa jatkuvasti laajenevan sähköverkon turvallisuuden. Zero trust tarkoittaa menetelmää, jossa verkon jokainen käyttäjä, laite ja sovellus validoidaan jatkuvasti [37]. Tämä estää luvattoman pääsyn verkkoon paremmin kuin perinteiset menetelmät, jotka olettavat järjestelmän sisäisen verkkoliikenteen olevan luonnollisesti turvallista. Myös NIST tarjoaa ohjeet Zero Trust-arkkitehtuurin soveltamiseksi teollisuusympäristöissä kuten älykkäissä sähköverkoissa, ja korostaa etenkin jatkuvan valvonnan merkitystä [38].

Tärkeisiin kehityskohteisiin kuulu myös jo aikasemmin mainittu ihmisten tekemien virheiden vähentäminen. Tilannetietoisuuden lisääminen sekä hyvien tietoturvakäytänteiden opettaminen työntekijöille ovat tärkeitä askelia kohti parempaa ky-

berturvallisuutta. Lisäksi selkeästi määritelty suunnitelma hyökkäyksen tapahtuessa voi olla ratkaiseva tekijä negatiivisten vaikutusten minimoimisessa.

Luvussa 2.3 käsiteltiin sähköverkkoihin kohdistuvien hyökkäysten yhteiskunnallisia vaikutuksia, sekä todettiin kuinka sähköstä riippuvainen nyky-yhteiskuntamme on. Vaikka hyökkäysten torjuminen on ensisijaisesti aina paras vaihtoehto, se ei kuitenkaan aina ole mahdollista laajamittaisen hyökkäyksen tapahtuessa. Tämän seurauksena on myös tärkeä olla varautunut hyökkäyksiin monin eri keinoin. 28. päivä huhtikuuta 2025 Espanjan ja Portugalin välisessä sähköverkossa ilmeni laajamittainen sähkökatko, joka raporttien mukaan vaikutti noin 6.4 miljoonaan ihmiseen [39]. Katko kesti noin 10 tuntia, jonka aikana muun muassa puhelinyhteydet, kauppojen maksupäätteet ja liikennevalot lakkasivat toimimasta. Lisäksi julkisen liikenteen katkokset jättivat yli 35 tuhatta ihmistä jumiin, sekä hätäpalvelut toimivat puutteellisesti [39] [40]. Vaikka raporttien mukaan katkossa ei ollut kyse kyberhyökkäyksestä, sen aiheuttamat vaikutukset ovat erinomainen esimerkki laajamittaisten sähkökatkojen aiheuttamasta kaaoksesta. Varautuminen sähkökatkoihin esimerkiksi varageneraattoreilla, toimivilla viestintävälineillä ja tarkoin suunnitelluilla hätäpalvelujärjestelyillä ovat hyviä varautumiskeinoja, joiden avulla kriisitilanteesta voidaan selvitytyä tehokkaammin.

5 Yhteenveto

Älykkäät sähköverkot tuovat sähköntuotantoon ja -jakeluun merkittäviä teknologisia ja merkittäviä etuja. Ne mahdollistavat muun muassa tehokkaan energianhallinnan, paremman toimintavarmuuden ja mahdollisuuden uusiutuvien energianlähteiden hyödyntämiseen. Kaksisuuntaisen tiedonsiirron ja automatisaation avulla sähköverkot voivat reagoida nopeasti muuttuviin energiatarpeisiin ja täten paremmin optiomoida energian käyttöä. Näiden hyötyjen rinnalla verkon riippuuus tietojärjestelmistä ja kommunikaatioyhteyksistä kuitenkin kasvaa, mikä altistaa järjestelmät kyberuhille.

Tutkielmassa tarkasteltiin älykkäisiin sähköverkkoihin kohdistuvia merkittävimpiä kyberuhkia ja niiden torjuntamenetelmiä. Tk1 selvitti millaisia uhkia sähköverkkoihin voi kohdistua, ja Tk2 käsitteli ratkaisuja näiden uhkien torjumiseksi. Tarkastelun kohteena oli yleisemmät tekniset ja inhimilliset uhat, kuten palvelunestohyökkäykset, haittaohjelmat ja datan manipulointi. Tutkielmassa havainnoitiin myös verkkoon kohdistuvan kyberhyökkäyksen reaalimaailman vaikutuksia ja vakavuutta käsittelemällä Ukrainan vuoden 2015 kyberhyökkäystä.

Tutkielmassa todettiin, että älykkäät sähköverkot muodostavat kyberfyysisen kokonaisuuden, johon hyökkääjät voivat aiheuttaa niin tietovuotoja kuin myös fyysisiä häiriöitä infrastruktuurille. Verkkoon kohdistuvia uhkia ei voida tarkastella ainoastaan teknisenä uhkana, sillä ne ovat hyvin laajasti kytköksissä yhteiskunnan turvallisuuteen ja toiminnallisuuteen. Todettiin myös, että järjestelmäperäisten haavoittu-

vuuksien lisäksi inhimillisillä virheillä on merkittävä rooli verkon haavoittuvuudessa.

Hyökkäysten torjuntaan tarkoitettuja teknologioita ja menetelmiä esiteltiin useita, kuten IDS-järjestelmät, tekoälypohjaistet havaitsemisjärjestelmät sekä simulaatiotestialustat. Lisäksi tutkielmassa mainittiin joitakin uusia lähestymistapoja, kuten Zero Trust-arkkitehtuuri ja erilaiset hajautetut tekoälyn oppimismenetelmät.

Mahdollisia jatkotutkimuksia voisi kohdistaa tarkempaan analyysiin sähköverkkoihin kohdistuvien riskien aiheuttamista syistä. Tarkempi tieto siitä miten tekniset haavoittuvuudet, organisaatioiden kyberturvalliset puutteet tai inhmilliset tekijät kukin vaikuttavat kyberhyökkäysten mahdollisuuteen olisi todella tärkeää kehityksen kannalta. Syvällisempi ymmärrys näistä tekijöistä voisi parantaa sekä uhkien ennakointia että suojatumismenetelmien kehitystä.

Kaiken kaikkiaan älykkäiden sähköverkkojen turvallisuus edellyttää moniulotteista lähestymistapaa, joka yhdistää verkon kaikki osapuolet ja järjestelmät turvalliseksi kokonaisuudeksi. Uhkien torjunta on pääosin tekninen haaste, mutta se edellyttää myös jatkuvaa valmiutta, tilannetietoisuutta ja sopeutumista muuttuvaan uhkaympäristöön.

Lähdeluettelo

[1] Z. E. Mrabet, H. E. Ghazi, N. Kaabouch ja H. E. Ghazi, "Cyber-Security in Smart Grid", *Computers & Electrical Engineering*, vol. 67, s. 469–482, 2018. DOI: 10.1016/j.compeleceng.2018.01.015.

[2] T. S. G. I. P.-S. G. C. Committee, "Guidelines for smart grid cybersecurity", tekninen raportti, 2014, NIST IR 7628r1. DOI: 10.6028/NIST.IR.7628r1.

[3] V. C. Gungor, D. Sahin, T. Kocak et al., "A Survey on Smart Grid Potential Applications and Communication Requirements", *IEEE Transactions on Industrial Informatics*, vol. 9, s. 28–42, 2013. DOI: 10.1109/TII.2012.2218253.

[4] A. Usman ja S. H. Shami, "Evolution of Communication Technologies for Smart Grid applications", *Renewable and Sustainable Energy Reviews*, vol. 19, s. 191–199, 2013. DOI: 10.1016/j.rser.2012.11.002.

[5] C.-C. Sun, A. Hahn ja C.-C. Liu, "Cyber security of a power grid: State of the art", *International Journal of Electrical Power & Energy Systems*, vol. 99, s. 45–56, 2018. DOI: 10.1016/j.ijepes.2017.12.020.

[6] M. A. Faisal, Z. Aung, J. R. Williams ja A. Sanchez, "Data-Stream-Based Intrusion Detection", *IEEE Systems Journal*, vol. 9, s. 31–44, 2015. DOI: 10.1109/JSYST.2013.2294120.

[7] K. Sayed ja H. A. Gabbar, "Chapter 18 - SCADA and smart energy grid control automation", teoksessa *Smart Energy Grid Engineering*, 2017, s. 481–514. DOI: 10.1016/B978-0-12-805343-0.00018-8.

[8] J. S. Ríos, J. C. Sánchez, C. M. Hernandez ja S. Pastrana, "Threat analysis and adversarial model for Smart Grids", *WACCO*, 2024. DOI: 10.48550/arXiv.2406.11716.

[9] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni ja N. Gudi, "Smart meters for power grid — Challenges", teoksessa *2011 IEEE/PES Power Systems Conference and Exposition*, 2011, s. 1–7. DOI: 10.1109/PSCE.2011.5772451.

[10] G. Crabtree, J. Misewich, R. Ambrosio et al., "Integrating Renewable Electricity on the Grid", *AIP Conference Proceedings*, vol. 1401, s. 387–405, 2011. DOI: 10.1063/1.3653865.

[11] Umbrex, *Islanding*. url: https://umbrex.com/resources/energy-industry-glossary/energy-storage-glossary/islanding (viitattu 05. 03. 2025).

[12] M. Z. Gunduz ja R. Das, "Cyber-security on smart grid: Threats and potential solutions", *Computer Networks*, vol. 169, s. 107 094, 2020. DOI: 10.1016/j.comnet.2019.107094.

[13] M. L. Tuballa ja M. L. Abundo, "A review of the development of Smart Grid technologies", *Renewable and Sustainable Energy Reviews*, vol. 59, s. 710–725, 2016. DOI: 10.1016/j.rser.2016.01.011.

[14] M. Purnell, *Smart Grids to Save Over $290 Billion in Global Energy Costs by 2029*, Juniper Research. url: https://www.juniperresearch.com/press/pressreleasessmart-grids-to-save-over-290bn-in-global-energy-costs/ (viitattu 05. 03. 2025).

[15] D. of Health, *Health Building Note 00-07: Planning for a resilient healthcare estate*. url: https://www.england.nhs.uk/publication/resilience-planning-for-nhs-facilities-hbn-00-07/ (viitattu 07. 03. 2025).

[16] F. Mahdavian, S. Platt, M. Wiens, M. Klein ja F. Schultmann, "Communication blackouts in power outages", *International Journal of Disaster Risk Reduction*, vol. 46, 2020. DOI: https://doi.org/10.1016/j.ijdrr.2020.101628.

[17] C. Klinger, O. Landeg ja V. Murray, "Power Outages, Extreme Events and Health: a Systematic Review of the Literature from 2011-2012", *PLoS Currents*, vol. 6, 2014. DOI: 10.1371/currents.dis.04eb1dc5e73dd1377e\-05a10e9edde673.

[18] Tilastokeskus, *Maalämpö yleistynyt pääasiallisena lämmitystapana*. url: https://stat.fi/julkaisu/cktwror9c4ee10b618t3njtsh (viitattu 07. 03. 2025).

[19] J. Lázaro, A. Astarloa, M. Rodríguez, U. Bidarte ja J. Jiménez, "A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid", *Electronics*, vol. 10, s. 1881, 2021. DOI: 10.3390/electronics10161881.

[20] M. K. Hasan, R. A. Abdulkadir, S. Islam, T. R. Gadekallu ja N. Safie, "A review on machine learning techniques for secured cyber-physical systems in smart grid networks", *Energy Reports*, vol. 11, s. 1268–1290, 2024. DOI: 10.1016/j.egyr.2023.12.040.

[21] X. Liu, P. Zhu, Y. Zhang ja K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", *IEEE Transactions on Smart Grid*, vol. 6, s. 2435–2443, 2015. DOI: 10.1109/TSG.2015.2418280.

[22] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva ja P. Burnap, "Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology

Attacks", *ACM Computing Surveys*, vol. 55, s. 1–36, 2023. DOI: 10.1145/3565570.

[23] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari ja P. Dehghanian, "Electric Power Grid Resilience to Cyber Adversaries", *IEEE Access*, vol. 8, s. 87 592–87 608, 2020. DOI: 10.1109/ACCESS.2020.2993233.

[24] S. Pastrana, A. Hutchings, A. Caines ja P. Buttery, "Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum", teoksessa *Research in Attacks, Intrusions, and Defenses*, RAID, 2018, s. 207–227. DOI: 10.1007/978-3-030-00470-5_10.

[25] S. Adepu, N. K. Kandasamy, J. Zhou ja A. Mathur, "Attacks on smart grid: power supply interruption and malicious power generation", *International Journal of Information Security*, vol. 19, s. 189–211, 2020. DOI: 10.1007/s10207-019-00452-z.

[26] A.-A. Bouramdane, "Cyberattacks in Smart Grids", *Journal of Cybersecurity and Privacy*, vol. 3, s. 662–705, 2023. DOI: 10.3390/jcp3040031.

[27] P. Engebretson, *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Syngress, 2013, s. 1–14. DOI: 10.1016/B978-1-59749-655-1.00001-5.

[28] D. Kushner, "The real story of stuxnet", *IEEE Spectrum*, vol. 50, s. 48–53, 2013. DOI: 10.1109/MSPEC.2013.6471059.

[29] A. C. D. Agency, *Cyber-Attack Against Ukrainian Critical Infrastructure*, 2021. url: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (viitattu 06. 04. 2025).

[30] R. Anderson, *Security Engineering*. Wiley, 2020, s. 17–61, ISBN: 978-1-119-64278-7.

[31] IBM, *What is an Intrusion*, 2023. url: https://www.ibm.com/think/topics/intrusion-detection-system (viitattu 11. 04. 2025).

[32] R. Mitchell ja I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems", *ACM Comput. Surv.*, vol. 46, 55:1–55:29, 2014. DOI: 10.1145/2542049.

[33] S. Adepu, N. K. Kandasamy ja A. Mathur, "EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security", teoksessa *Computer Security*, 2019, s. 37–52. DOI: 10.1007/978-3-030-12786-2_3.

[34] Y. Bao, C. Guo, J. Zhang, J. Wu, S. Pang ja Z. Zhang, "Impact analysis of human factors on power system operation reliability", *Journal of Modern Power Systems and Clean Energy*, vol. 6, s. 27–39, 2018. DOI: 10.1007/s40565-016-0231-6.

[35] T. Berghout, M. Benbouzid ja S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A", *International Journal of Critical Infrastructure Protection*, vol. 38, s. 100 547, 2022. DOI: 10.1016/j.ijcip.2022.100547.

[36] Q. Yang, Y. Liu, T. Chen ja Y. Tong, "Federated Machine Learning: Concept and Applications", *ACM Trans. Intell. Syst. Technol.*, vol. 10, nro 2, 2019. DOI: 10.1145/3298981.

[37] J. Hertz, *Zero-Trust: Preventing Grid Cyber Attacks - Tech Insights*, EEPower. url: https://eepower.com/tech-insights/zero-trust-preventing-grid-cyber-attacks/ (viitattu 09. 05. 2025).

[38] S. Rose, O. Borchert, S. Mitchell ja S. Connelly, "Zero Trust Architecture", National Institute of Standards ja Technology, tekninen raportti, 2020. DOI: 10.6028/NIST.SP.800-207.

[39] France24, *Power restored in Spain and Portugal after massive blackout left millions stranded*, 2025. url: https://www.france24.com/en/europe/20250429-power-restored-spain-after-massive-blackout-leaves-millions-stranded (viitattu 10. 05. 2025).

[40] J. G. S. León, *Spain-Portugal blackouts: what actually happened, and what can Iberia and Europe learn from it?*, The Conversation, 2025. url: https://theconversation.com/spain-portugal-blackouts-what-actually-happened-and-what-can-iberia-and-europe-learn-from-it-255666 (viitattu 13. 05. 2025).