Tampereen yliopisto

Mikko Kaukonen

ESINEIDEN INTERNET JA ÄLYKAUPUNGIT

Älykaupunkien kehitys – mahdollisuudet ja uhat

Kandidaatintutkielma
Informaatioteknologian ja viestinnän tiedekunta
Tarkastaja: Petri Kannisto
Huhtikuu 2023

TIIVISTELMÄ

Mikko Kaukonen: Esineiden internet ja älykaupungit: Älykaupunkien kehitys – mahdollisuudet ja uhat
Kandidaatintutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Informaatioteknologian ja viestinnän tiedekunta
Huhtikuu 2023

Esineiden internet viittaa laajaan joukkoon erilaisia esineitä, jotka ovat yhdistettyinä verkkoon ja lähettävät sekä mahdollisesti vastaanottavat tietoa verkon avulla. Näiden esineiden määrä on kasvanut räjähdysmäisesti ja onkin jo suurempi kuin maapallon väkiluku. Nykyään tekniikka on kehittynyt jo niin pitkälle, että pystytään rakentamaan kokonaisia älykaupunkeja joidenka infrastruktuuri ja palveluiden tuottaminen perustuu esineiden internetin avulla toimivaan teknologiaan. Nopea kehitys on tuonut eteemme ennennäkemättömiä mahdollisuuksia sekä uhkia. Tämä kandidaatintutkielma on kirjallisuuskatsaus, joka perustuu pääosin verkosta löydettävissä oleviin vertaisarvioituihin tieteellisiin artikkeleihin. Tutkielman tarkoituksena on selvittää, mitä uhkia ja mahdollisuuksia aiheuttaa esineiden internetiin kytkettyjen laitteiden määrän nopea kasvu. Tätä on tarkoitus lähestyä erityisesti älykaupunkien näkökulmasta.

Tutkielmassa kerrotaan mikä on esineiden internet. Esitellään esineiden internetin kehitys nykyisen kaltaiseksi niin valtavaksi ilmiöksi, että kokonaisten kaupunkien infrastruktuuri ja informaatiovirrat voidaan rakentaa toimimaan sen avulla. Lisäksi esitellään myös älykaupungit ja käydään läpi miten ne ovat kehittyneet futuristisista visioista todellisuudeksi. Lähdeaineiston avulla pyritään selvittämään millaisia mahdollisuuksia kehitys tarjoaa. sekä arvioida miten kehitystä voitaisiin mahdollisesti parantaa. Tutkielmassa keskitytään erityisesti kahteen kysymykseen. Mitä mahdollisuuksia esineiden internetin avulla kehitetyt älykaupungit tarjoavat, ja millaisia riskejä esineiden internet ja älykaupungit aiheuttavat?

Kaupunkien väestömäärät kasvavat nopeasti ja tämän vuoksi kaupunkien kehittyminen onkin jatkuvaa kamppailua resurssien riittävyyden kanssa. Tutkielmassa selvitetään älykaupunkien tähän tarjoamia ratkaisuja erityisesti kolmen eri osatekijän näkökulmasta. Älykäs rakennettu elinympäristö auttaa tehostamaan kaupungin tarjoamia kriittisiä toimintoja sekä palveluja. Älykäs liikenne auttaa kontrolloimaan liikennevirtoja ja optimoimaan joukkoliikenteen aikatauluja sekä reittejä. Innovaatioekosysteemi puolestaan auttaa kehittämään sekä kaupungin inhimillistä pääomaa että taloutta ja on tärkeä tulevaisuuden innovaatioiden mahdollistaja.

Tutkielman perusteella tietoturvallisuudelle suurimpia haasteita tuottavat tekniset ongelmat kuten laitteiden ja ohjelmistojen yhteensopivuus. Suurimmat kehityksen tuomat uhat liittyvät laitteiden tietoturvaan, digitaaliseen eriarvoistumiseen, yksityisyyteen sekä turvallisuuteen. Nyt kun kaupunkiteknologiat ja monet palvelut tuotetaan esineiden internetiä apuna käyttäen, kaupungin infrastruktuuri sekä ihmisten fyysinen turvallisuus ovat alttiina myös etänä suoritettaville hyökkäyksille. Älykaupunkien kehittämisessä tietoturvallisuuden vaatimusten tunteminen ja päivittäminen onkin erityisen tärkeää riskien minimoimiseksi.

Avainsanat: esineiden internet, älykaupungit, tietoturvallisuus, turvallisuusuhat, yksityisyys, kehitys

SISÄLLYSLUETTELO

1. JOHDANTO 1
2. TUTKIMUSMENETELMÄ 3
3. ESINEIDEN INTERNET 5
    3.1 Mikä on esineiden internet? 5
    3.2 Historia ja kehitys 5
    3.3 Toimintaperiaate 6
    3.4 Kehitys ja sen vaikutukset 8
4. ÄLYKAUPUNKI 9
    4.1 Mikä on älykaupunki? 9
    4.2 Älykaupunkien historia ja kehitys 9
5. ÄLYKAUPUNGIT – UHAT JA MAHDOLLISUUDET 11
    5.1 Älykaupungit – mitä kehitys tuo tullessaan? 11
        5.1.1 Älykäs rakennettu elinympäristö 11
        5.1.2 Älykäs liikenne 12
        5.1.3 Innovaatioekosysteemi 13
    5.2 Tietoturvallisuus, kyberhyökkäykset ja muut kehityksen mukanaan tuomat uhat 14
        5.2.1 Älykaupungit hyökkäyksen kohteena 15
        5.2.2 Digitaalisten teknologioiden haavoittuvuudet 15
        5.2.3 Digitaalinen eriarvoistuminen 17
    5.3 Tietoturvallisuuden parantaminen 17
6. YHTEENVETO 20
LÄHTEET 22

LYHENTEET JA MERKINNÄT

ARPANET	Advanced Research Projects Agency Network
GPS	Global Positioning System, maailmanlaajuinen paikallistamisjärjestelmä
IBSG	Cisco Internet Business Solutions Group
ICT	Information and Communications Technology, Tieto- ja viestintäteknologia
IDS	Intrusion Detection System, Tunkeutumisen havaitsemisjärjestelmä
IoT	Internet of things, esineiden internet
RFID	Radio Frequency Identification, radiotaajuinen etätunnistus
VSN	Vehicular Social Networks,
WWW	World Wide Web

.

1. JOHDANTO

Internetiin liitettävien laitteiden määrä kasvaa koko ajan huimaa vauhtia, niiden määrä on kasvanut jo suuremmaksi kuin maapallolla on ihmisiä (Harwood 2019). Termi esineiden internet (internet of things, IoT) viittaakin laajaan joukkoon erilaisia esineitä ja antureita, jotka ovat yhdistettynä internetiin (Empirica n.d.). Esineiden internetin leviämisen mukana kasvaa myös esineiden internetin merkitys, esimerkiksi monissa teollisuuden prosesseissa sekä terveydenhuollossa siitä on tullut jo lähes korvaamaton apuväline. Lisäksi se on ottanut paikkansa mm. ihmisten kodeissa, autoissa ja liikennejärjestelmissä.

Esineiden internet on levinnyt niin huimaa vauhtia että kuluttaja ei välttämättä edes tiedä, mitkä laitteet ovat yhdistyneitä internetiin, mitä tietoja ne käyttäjästään keräävät ja mihin ne tietonsa lähettävät. Monia tuotteita, jotka vielä hetki sitten olivat verkosta irrallaan, kuten esimerkiksi televisiot on jo lähes mahdotonta löytää ilman internetyhteyttä. Valitettavasti tietoturvallisuus ei kehity samaan tahtiin esineiden internetin leviämisen kanssa ja tästä seuraa merkittäviä tietoturvariskejä, kun heikkotehoiset esineet eivät pysty käsittelemään samanlaisia suojausmenetelmiä kuin tehokkaammat laitteet. Myös yhtenäisten standardien puute, tuotteiden kiireellinen kehitys, tästä johtuva puutteellinen testaus sekä ihmisten huolettomampi suhtautuminen kodinkoneiden tietoturvaan verrattuna esimerkiksi tietokoneiden ja puhelinten tietoturvaan aiheuttavat ongelmia. Tämän seurauksena tietoturvariskit ovat merkittäviä ja kasvavat koko ajan verkkoon kytkettyjen laitteiden määrän lisääntyessä.

Nykyään tekniikka on kehittynyt jo niin pitkälle, että pystytään rakentamaan kokonaisia kaupunkeja, joidenka infrastruktuuri on rakennettu esineiden internetin avulla toimivaksi. Näitä kaupunkeja kutsutaan älykaupungeiksi. Tässä kandidaatintutkielmassa esittelen mitä ovat esineiden internet sekä älykaupungit, tarkastelen esineiden internetin kehityksen tarjoamia mahdollisuuksia ja tästä aiheutuvia uhkia tietoturvallisuudelle sekä yksityisyydelle älykaupunkien näkökulmasta. Tutkielmassa keskitytään erityisesti kahteen kysymykseen:

1. Mitä mahdollisuuksia esineiden internetin avulla kehitetyt älykaupungit tarjoavat?
2. Millaisia riskejä esineiden internet ja älykaupungit aiheuttavat?

Tutkielman avulla pyritään tutkimaan esineiden internetin roolia älykaupunkien kehityksessä, älykaupunkien tarjoamia mahdollisuuksia ja uhkia, sekä arvioida miten kehitystä voitaisiin mahdollisesti parantaa. Tutkielma toteutetaan kirjallisuuskatsauksena, jossa hyväksikäytetään sekä tieteellisiä lähteitä että populaarilähteitä.

2. TUTKIMUSMENETELMÄ

Tässä luvussa käyn läpi aineiston haussa käytetyt palvelut, hakukoneet, tietokannat sekä hakusanat. Kandidaatintutkielma on toteutettu kirjallisuuskatsauksena käyttäen hyväksi pääasiassa tieteellisiä mutta myös joitakin populaarilähteitä. Lähteitä olen etsinyt Tampereen yliopiston kirjaston Andor, Google sekä Google Scholar hakupalveluiden avulla sekä tietokannoista (ACM Digital Library, Computer Science Database (ProQuest), IEEE Xplore - IEEE Electronic Library (IEL), ScienceDirect (Elsevier)).

Hakusanoina olen käyttänyt aiheeseen liittyviä käsitteitä (”smart city", "Internet of things", IoT, "IOT architecture layer", privacy, security, ”security challenges”, legislation, "Data protection", "Information security”, "Security threats", "Risk management", architecture, ”Digital divide”, ” Intrusion Detection System”, tietoturvallisuus, tietoturva, tietoturvauhka, ”esineiden internet”, ”tietoturvallisuuden hallinta”, riskienhallinta, yksityisyys, älykaupunki). Hakusanoja yhdistelemällä on tullut paikoitellen runsaastikin hakutuloksia, näitä olen karsinut tilanteen mukaan. Esineiden internetin esittelyyn olen hakenut lähteitä hakusanoilla (”internet of things”, IoT, history, ”history of IoT”, architecture, ”esineiden internet” ja määrittely). Tieteellisiä lähteitä hakiessani olen rajannut hakua vaatimalla että tulokset ovat sekä vertaisarvioituja että saatavilla verkossa.

Kandidaatintyön ja tähän liittyvän koulutuksen edetessä lähdehakutekniikkani ovat parantuneet tutkielmaa kirjoittaessa. Aloittaessani työn kirjoittamisen esineiden internetin esittelyllä kirjoitin vain erilaisia yhdistelmiä hakusanoista ja valitsin isosta joukosta nimen perusteella ne, joita lähdin lukemaan tarkemmin. IoT-arkkitehtuureista löysin lähteet tutkimalla ensimmäisten löytämieni kiinnostavien aiheeseen liittyvien artikkeleiden avainsanoja ja löytämällä sieltä hakusanaksi "IOT architecture layer".

Älykaupungeista taustatietoa etsin järjestelmällisemmin ja hyödynsin jo löytämiäni lähteitä hakuprosessissa kuten alla olevassa esimerkkiketjussa. Taustatietoa etsiessäni aloitin etsimällä Andor-palvelusta artikkeleita hakulauseella "history of smart city". Tällä haulla löysin Margarita Angelidoun 2015 kirjoittaman artikkelin *Smart cities: A conjuncture of four forces, Cities.* Artikkeli oli mielenkiintoinen joten päätin tutkia mihin artikkeleihin tätä kyseistä artikkelia oli käytetty viitteenä. Artikkeleihin viitanneiden joukosta löysin artikkelin, *Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges* (Appio et al. 2019). Artikkelissa oli viittaus myös toiseen aihettani käsittelevään artikkeliin. Tämä ei valitettavasti ollut saatavilla verkossa mutta katsoin tekijän nimen ja suoritin Andorissa haun tekijän nimellä Dustdar ja tällä

haulla löysin lähteen *Smart cities - enabling services and applications. Journal of Internet Services and Applications* (Curry et al. 2016). Artikkeleiden etsinnässä käytin siis hyödykseni jo olemassa olevia lähteitä sekä mainitsemiani hakusanoja yhdisteltyinä.

3. ESINEIDEN INTERNET

Tässä luvussa on selitetään lukijalle mikä on esineiden internet. Käydään läpi esineiden internetin kehityshistoria joidenkin sen kehitykseen johtaneiden tapahtumien avulla. Esitellään esineiden internetin toimintaperiaatteita sen arkkitehtuurin kautta. Lopuksi tarkastellaan vielä kehityksen mukanaan tuomia vaikutuksia.

3.1 Mikä on esineiden internet?

Kuten Mouha (2021) artikkelissaan toteaa, käsitettä ”esineiden internet” ei ole tarkoin rajattu tai määritelty yleisesti hyväksyttyjen tai globaalien käyttäjäyhteisöjen hyväksymien määritelmien mukaan, vaan se jatkaa kehitystään teknologian kehityksen mukana. Esineiden internet viittaakin laajaan joukkoon erilaisia laitteita ja antureita, jotka ovat yhdistettynä internetiin ja voivat internetin välityksellä jakaa sekä mahdollisesti vastaanottaa tietoa. (Empirica n.d.). Esineiden internet on siis eräänlainen runko, jossa kaikki laitteet ovat yhdistettynä internetiin, koneiden keskinäisten yhteyksien muodostaen viestinnän perustan. Se pyrkii tarjoamaan uusia palveluita ja ohjelmia, jotka yhdistävät fyysisen ja virtuaalisen maailman. Mahdollistaen kommunikaation esineiden ja niiden lähettämää tietoa vastaanottavan tahon välillä. (Mouha 2021)

Ennen esineiden internetin syntymistä, tallennettu data oli pääasiassa ihmisen kirjoittamaa, mutta nykyään suuri osa datasta muodostuu internetiin yhdistetyiden laitteiden keräämänä. Esineiden internet on levinnyt huimaa vauhtia, ja esimerkiksi teollisuuden prosesseissa sekä terveydenhuollossa siitä on tullut jo lähes korvaamaton apuväline. Lisäksi se on ottanut paikkansa muun muassa ihmisten kodeissa, liikennejärjestelmissä ja jopa kokonaisia älykaupunkeja voidaan rakentaa esineiden internetin avulla. Esineiden internetin ydinajatus on parantaa käyttäjän käyttökokemusta, helpottaa elämää ja mahdollistaa siirtyminen tietoyhteiskunnasta yhteiskuntaan, jossa ihmiset, esineet ja asiat ovat yhteydessä toisiinsa teknologian avulla (Penttinen 2016, s 112).

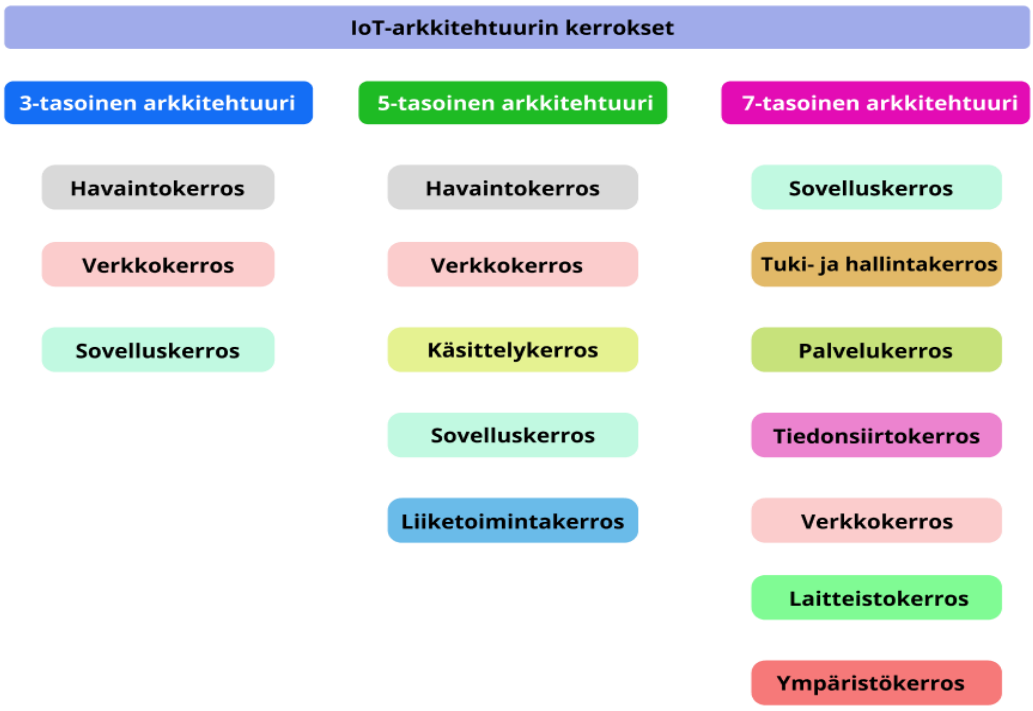
3.2 Historia ja kehitys

Vuonna 1982 Carnegie Mellon yliopiston opiskelija David Nichols opiskelutovereidensa avustuksella muodosti yhteyden kampuksella sijaitsevaan limonadiautomaattiin. Heidän päämääränään oli nähdä työhuoneestaan, onko automaatissa virvoitusjuomapulloja ja ovatko ne kylmiä. Yhteyden muodostamiseen käytettiin ARPANET (Advanced Research Projects Agency Network) -verkkoa, josta kaupallisten palveluntarjoajien tuella nykyinen

internet on kehittynyt. Tätä voidaan pitää yhtenä varhaisimmista esimerkeistä esineiden internetistä. Seuraava tärkeä kehitysaskel tapahtui vuonna 1990, kun amerikkalainen tietotekniikan insinööri John Romkey kehitti leivänpaahtimen, joka voitiin kytkeä päälle ja pois päältä internetin avustuksella. Tämä käsitetään ensimmäiseksi internetiin kytketyksi esineeksi, ja koko esineiden internetin lähtölaukaukseksi. (Talabi 2022) Ensimmäisen kerran esineiden internet käsiteen nimesi Massachusettsin teknillisen ylipiston AutoID Labsin toiminnanjohtaja Kevin Ashton vuonna 1999. Seuraavana vuonna elektroniikkayhtiö LG julkaisi suunnitelmansa internetiin yhdistetystä jääkaapista. IBSG (Cisco Internet Business Solutions Group) arvioi esineiden internetin syntyhetken vuosien 2008–2009 väliselle ajalle. Tuolloin internetiin kytkettyjen esineiden määrä ylitti maapallon väkimäärän. (Harwood. 2019)

3.3 Toimintaperiaate

Esineiden internetin arkkitehtuurin tarkoituksena on tarjota turvallinen tapa välittää tietoa, sekä esineiden että niitä ympäröivän ”älykkään ympäristön” välillä tähän kehitetyiden antureiden avulla. Esineiden internetin arkkitehtuuri perustuu esineiden kykyyn lähettää ja vastaanottaa dataa. Nallapaneni et al. (2018) esittelee teoksessaan esineiden internet arkkitehtuurin eri malleja (kuva 1). Ensimmäisten joukossa kehitetty ja yksinkertaisin näistä on kolmikerroksinen arkkitehtuurimalli. Tekniikan kehittyessä ja tutkimuksen keskittyessä erilaisten teknologioiden integroimiseen yhteensopiviksi ja muuntautumiskykyisten sovellusten luomiseen. Kolmikerroksinen malli todettiin riittämättömäksi ja rinnalle kehitettiin viisikerroksinen arkkitehtuurimalli. Teknologian edelleen kehittyessä syntyi tarve huomioida antureiden toimintaan vaikuttavia erilaisia ulkoisia esimerkiksi käyttäjään ja ympäristöön liittyviä tekijöitä. Vastauksena tähän tarpeeseen kehitettiin seitsemänkerroksinen arkkitehtuurimalli. (Nallapaneni et al. 2018)



Kuva 1 IoT-arkkitehtuurin kerrosmallit (kuva muokattu Nallapaneni et al. 2018)

Kolmikerroksinen arkkitehtuurimalli koostuu havainto-, verkko/kuljetus-, ja sovelluskerroksista. Tässä mallissa havaintokerros kerää ja tallentaa dataa verkkoon liitettyjen laitteiden ympäristöstä, verkkokerros välittää ja prosessoi dataa laitteiden välillä ja sovelluskerroksen tehtävänä on välittää käyttäjälle sovelluksen tuottama palvelu. (Nallapaneni et al. 2018)

Viisikerroksisessa mallissa kolmikerroksiseen malliin on lisätty käsittely- ja liiketoimintakerrokset. Malli toimii muuten kuten kolmikerroksinenkin malli, mutta verkkokerros on jaettu kahteen osaan verkko- ja käsittelykerrokseen. Verkkokerroksen tehtävänä on datan siirtäminen, datan käsittelyyn, analysointiin ja varastointiin on luotu uusi käsittelykerros. Tämän lisäksi malliin on luotu vielä liiketoimintakerros, jonka avulla järjestelmää ohjataan käyttäjäystävällisempään ja tietoturvallisempaan toimintaan, liiketoiminnan näkökulmat huomioon ottaen. (Nallapaneni et al. 2018)

Seitsemänkerroksinen arkkitehtuurimalli koostuu sovellus-, sovellusten tuki ja hallinta-, palvelu-, tiedonsiirto-, verkko-, laitteisto- ja ympäristökerroksista. Tässä mallissa sovelluskerroksen tehtävänä on kerätä tietoa käyttäjälle suoritetuista tehtävistä. Sovellusten tuki- ja hallintakerros mahdollistaa järjestelmän hallinnan, ja vastaa käyttäjäturvallisuudesta. Palvelukerros vastaa käyttäjän tarvitsemien toimintojen suorittamisesta, tiedonsiirtokerroksen muodostaessa linkin kerrosten välille. Verkkokerros mahdollistaa datan siirron eri laitteiden välillä. Laitteistokerros auttaa integroimaan esineiden internet yhtey-

den mahdollistavat eri komponentit keskenään, ja ympäristökerros mahdollistaa ulkoisten tekijöiden kuten esimerkiksi ihmisten, autojen tai lämpötilan havainnoimisen. (Nallapaneni et al. 2018)

3.4 Kehitys ja sen vaikutukset

Esineiden internet on avannut uusia mahdollisuuksia, älykaupunkien kehittyminen futuristisista visioista todellisuudeksi onkin suurelta osin esineiden internetin ansiota. Arkielämän helpottamisen lisäksi, siitä toivotaan löytyvän apua myös moniin maailman laajuisiin ongelmiin kuten ylikansoitukseen, ilmastonmuutokseen ja nälänhätään. Kehitys ei kuitenkaan ole täysin ongelmatonta, mitä enemmän laitteita internetiin on yhdistettynä, sitä suurempi riski on, että suojaus on näiden kautta mahdollista murtaa. Tämän vuoksi laitteiden määrän nopea kasvu altistaa verkkoa hyökkäyksille ja luo uusia turvallisuusuhkia. (Maras 2015) Suurimmat ongelmat liittyvät käyttäjän yksityisyyden suojaan sekä turvallisuuteen. Kenellä on mahdollisuus päästä laitteiden välittämään dataan käsiksi ja miten ehkäistä kolmannen osapuolen pääsy laitteiden käyttäjäksi, eli estää laitteen kaappaus?

Myös tuotteiden kehityksessä on useita tietoturvaa heikentäviä ongelmia. Valmistajien on niin kiire saada tuotteensa markkinoille, ettei tietoturvallisuuteen ehditä panostaa tarpeeksi. Lisäksi monissa tuotteissa on valmistajan tarkoituksella luoma takaovi tai salasana, jolla suojauksen voi ohittaa. Valmistajia on monia ja lainsäädäntö niin pahasti jäljessä kehityksestä, ettei laitteiden suojaukselle ole olemassa yhteisiä standardeja. Tämä heikentää tietoturvaa entisestään. (Maras 2015) Käyttäjät saattavat joko tietämättömyytensä tai laiskuuden ja mukavuudenhalujensa vuoksi, aiheuttaa tietoturvauhkia esimerkiksi helppojen tai vuotaneiden salasanojen, verkon huonon suojauksen tai vaikkapa laitteiden puutteellisen identifioinnin vuoksi. Käyttäjät ovat myös alttiita perinteisille huijauskeinoille, joissa käyttäjään otetaan yhteyttä, ja hän joko antaa hyökkääjälle pääsyn verkkoonsa, tai paljastaa salasanansa. Kaksi suurinta tietoturvauhkaa muodostavatkin laitteiden puutteellinen turvallisuus sekä käyttäjät itse.

Esineiden internetin yleistyessä ja laajentuessa lähes kaikkialle, näihin tietoturvaongelmiin olisikin pyrittävä löytämään pikaisesti ratkaisuja. Maras (2015) tarjoaa yhtenä ratkaisuna ongelmiin päivitettyä kansainvälistä lainsäädäntöä, asetuksia joilla määrätään käyttötarkoituksen mukaan laitteen vähimmäissuojaustaso, sekä yleismaailmallisia standardeja, joiden avulla tietoturvaohjelmistot saataisiin yhtenäisemmiksi.

4. ÄLYKAUPUNKI

Tässä luvussa esitellään yleisellä tasolla älykaupungit ja niiden toimintaperiaatteet, käydään läpi kaupunkisuunnittelun historiaa syntymästä nykyhetkeen ja selitetään miten teknologian kehittyessä älykaupungit ovat nousseet keskeiseksi tekijäksi kaupunkisuunnittelussa.

4.1 Mikä on älykaupunki?

Kaupunkien nopea kasvu, sekä tieto- ja viestintäteknologioiden (ICT, Information and Communications Technology) kehitys, ovat kasvattaneet älykaupunkien suosiota. Älykaupunkien määritelmä onkin hyvin laaja-alainen. Perusajatuksena on, että älykaupunkien hallinta, infrastruktuuri ja erilaiset toiminnot, kuten esimerkiksi terveydenhuolto, koulutus sekä ympäristönsuojelu, toteutettaisiin mahdollisimman kattavasti kaupungin sisään integroidun ICT-teknologian avulla. (Ijaz et al. 2016)

Älykaupungeissa esineiden internet muodostaa fyysisten esineiden verkoston, jonka integroimiseen käytettäviä ICT-teknologioita ovat esimerkiksi älypuhelimet, RFID-tunnisteet (Radio Frequency Identification, radiotaajuinen etätunnistus), älymittarit, semanttinen web, linkitetty data, ontologiat, tekoäly, pilvipalvelut, kollektiivinen älykkyys, ohjelmistot, älysovellukset ja biometriset tunnisteet. Esineiden internetillä, älykäillä teknologioilla ja sulautetuilla järjestelmillä onkin elintärkeä rooli luotaessa ihanteellista ja turvallista älykaupunkia. (Ijaz et al. 2016) Älykaupunkien kehitykseen vaikuttavat useat eri tieteenalat ja kehitys muotoutuu jatkuvasti teknologian ja kaupunkien suunnittelun kehittyessä. (Angelidou 2015) Curry et al. (2016) määrittelee artikkelissaan älykaupungin kaupungiksi, jonka tavoitteena on hyödyntää fyysisiä ja sosiaalisia rakenteita, ICT-teknologioita sekä tietoresursseja, taloudellisen kehityksen sekä asukkaiden elämänlaadun parantamiseen. Asukkaiden hyvinvointi onkin yksi keskeinen piirre älykaupunkien suunnittelussa.

4.2 Älykaupunkien historia ja kehitys

Teknologia on ollut osana kaupunkien suunnittelua jo 1700- ja 1800-lukujen vaihteen teollisesta vallankumouksesta lähtien. Ensimmäisiä suunnitelmia tulevaisuuden älykkäistä kaupungeista onkin löydettävissä jo 1800-luvulta, mutta suurempaa suosiota ajatukset alkoivat kerätä vasta 1900-luvulla. Toisen maailmansodan ajaksi kaupunkien kehittäminen jäi taka-alalle, mutta sodan jälkeen kaupunkien väestömäärän kasvu sekä

tarve paremmille elin- ja asuinolosuhteille johtivat kaupunkisuunnittelun kehittymiseen. 1960-luvulla teknologian kehittyminen sai kaupunkisuunnittelijat kiinnittämään huomioita tietovirtojen liikenteeseen ja tämän tarjoamiin mahdollisuuksiin kaupunkien suunnittelussa. (Angelidou 2015)

Ajatukset kaupunkien yhdistämisestä erilaisin verkostoin alkoivat yleistyä 1980-luvulla. Tämä johti käsitteiden kuten "kyberkaupungit", "älykkäät kaupungit" ja "virtuaaliset kaupungit" yleistymiseen. Monet näistä suunnitelmista olivat kuitenkin mahdotonta toteuttaa, ja olivatkin ennemmin oletuksia siitä, mitä tulevaisuudessa voitaisiin mahdollisesti rakentaa. Pian aikakauden teknologian kiihtyvä kehitys mahdollisti ensimmäistä kertaa laajamittaisen tiedon- ja viestintäteknologioiden leviämisen ja yleistymisen osaksi jokapäiväistä elämää. WWW (World Wide Web) helpotti verkostoitumista ja tiedonsiirtoa. Ensimmäiset internetselaimet toivat verkon kaikkien ulottuville. 1990-luvun puolivälistä eteenpäin ICT alkoikin olla yhä keskeisempi tekijä tulevaisuuden kaupunkien suunnittelussa. Tämän seurauksena alkoi syntyä teorioita siitä, että tulevaisuudessa kaikki toiminnot siirtyisivät digitaaliseen maailmaan. Internetin mahdollistaessa tavaroiden ja palveluiden saavutettavuuden kaikkialta maailmasta, ihmisen fyysisestä olinpaikasta riippumatta. (Angelidou 2015)

Voidaan siis sanoa että kiitos ICT-teknologian vauhdikkaan kehittymisen ja tämän myötä syntyneen esineiden internetin, myös älykaupunkien suosio, mahdollisuudet ja suunnitelmat ovat kehittyneet nopeasti. Älykaupunkien suunnittelun ja tutkimuksen jatkaessa kehityskulkuaan ICT-teknologioiden kehityksen tahdissa. Älykaupunkien kehitykseltä toivotaankin tulevaisuudessa apua monien ihmiskunnan ongelmien ratkaisemiseen, aina ilmastonmuutoksesta ylikansoittumiseen. Joidenkin tutkijoiden mukaan älykaupunkien suunnittelussa onkin enemmän kyse strategisesta tulevaisuuden suunnittelusta nykypäivän sijaan (Angelidou 2015).

5. ÄLYKAUPUNGIT – UHAT JA MAHDOLLISUUDET

Tässä luvussa selvitetään tutkimuskysymyksen mukaisesti minkälaisia mahdollisuuksia älykaupunkien kehitys tuo tullessaan, sekä minkälaisia uhkia tämä kehitys aiheuttaa. Lisäksi pohditaan miten uhkiin voisi varautua ja miten niitä voisi torjua.

5.1 Älykaupungit – mitä kehitys tuo tullessaan?

Joidenkin arvioiden mukaan 180 000 ihmistä muuttaa maailmanlaajuisesti kaupunkeihin joka päivä, tämä tarkoittaa yli 65 miljoonaa uutta kaupunkilaista vuodessa (Appio et al. 2019 mukaan Suzuki 2017). Kaupunkien väestömäärän räjähdysmäisen kasvu aiheuttaa ongelmia, esimerkiksi kasvavien saastemäärien sekä liikenteenohjauksen, julkisen liikenteen järjestelyjen ja asuininfrastruktuurin rakentamisen kanssa. Näihin ongelmiin yhä useammin ratkaisua yritetään löytää älykaupungeista. Vuonna 2012 pidetyssä Rio+20-konferenssissa tunnistettiin kestävän kaupunkisuunnittelun johtavan taloudellisesti sosiaalisesti ja ekologisesti kestävään yhteiskuntaan. (Balova et al. 2021) Ekologinen, taloudellinen ja sosiaalinen kestävyys onkin erittäin tärkeää tasapainon ylläpitämiseksi nopeasti kasvavan kaupungistumisen ja kaupunkien resurssien välillä (Ahmad et al. 2022).

Tutkimusten perusteella kestävän kaupunkisuunnittelun neljä tärkeintä vaatimusta ovat: saasteettomuus, ekologinen ja toimiva jätehuolto, ilmastonmuutoksen ehkäisy sekä toimivat ja kestävällä pohjalla olevat liikennejärjestelyt (Balova et al. 2021). Älykaupunkien tavoitteena onkin parantaa asukkaiden elämänlaatua, tarjoamalla paremmin organosoituja julkisia palveluita sekä puhtaamman ympäristön. Tässä esineiden internet on yksi tärkeimpiä osatekijöitä, mahdollistamalla älykkäät energiaverkot, älykkään vesihuollon, älykkään liikenteenohjauksen ja joukkoliikenteen suunnittelun sekä älykkäät rakennukset. Esineiden internetin avulla on myös mahdollista oppia reaaliajassa muun muassa miten, parantaa liikenteenohjausta, ohjailla julkista liikennettä optimaalisemmaksi, säästää energiaa, parantaa turvallisuutta, vähentää hävikkiä, parantaa kierrätystä sekä vähentää saastuttavuutta. (Appio et al. 2019)

5.1.1 Älykäs rakennettu elinympäristö

Älykäs rakennettu elinympäristö tarkoittaa teknologian käyttöä kaupungin kriittisten toimintojen, kuten esimerkiksi jätehuollon, elintarviketuotannon, ympäristön saastumisen

valvonnan, älykkäiden sähköverkkojen, asuinolosuhteiden ja kiinteistöjen huollon parantamiseen. Esineiden internetiä ja älykaupunkeja voidaan hyödyntää elinympäristön parantamisessa monella tavalla, esimerkiksi estämään metsäpaloja, tarkkailemalla ilmansaasteiden tasoa ja parantamalla niiden ennustettavuutta, asentamalla langattoman järjestelmän sekä julkisiin kulkuvälineisiin että yksityisautoihin, joka valvoisi päästöjen tasoa ja parantaisi tehokkuutta. (Appio et al. 2019)

Jätehuoltoa, lajittelua ja kierrätystä voidaan tehostaa asentamalla roskapönttöihin anturit, jotka jakaisivat tietoa jätteiden laadusta ja määrästä. Tätä tietoa voitaisiin käyttää hyväksi sekä logistiikkaa että valistuskampanjoita suunnitellessa. Nykyteknologialla on myös mahdollista rakentaa ”älykäs” sähköverkko, joka suosii uusiutuvia energianlähteitä reaaliaikaisen tiedon perusteella. Sähköverkot voivat myös ostaa ja varastoida ylimääräistä energiaa, jota asukkaat tuottaisivat yksityisillä aurinkopaneeleillaan. (Appio et al. 2019) Sähköverkkojen ja muun tärkeän infrastruktuurin täydellinen ohjailtavuus verkonkautta tuo mukanaan suuria riskejä verkkohyökkäysten ja kyberterrorismin muodossa. On myös pidettävä huoli siitä, että olisi olemassa joku mahdollisuus käyttää laitteita hätätilanteessa, mikäli verkkoyhteydet kaatuvat tai niitä häiritään. Myös muiden kriittisten alojen kuten kaupungin taloudellisen kehityksen ja terveydenhuollon toimintavarmuuden kannalta, kunnossa oleva tietoturva on erittäin tärkeää (Ijaz et al. 2016).

Älytalot mahdollistavat paremman infrastruktuurin rakentamisen. Asukkaiden koteihin voidaan rakentaa itse oppiva järjestelmä, joka oppisi asukkaan tapoja tarkkailemalle esimerkiksi säätämään valaistusta sekä lämmitystä. Turvallisuutta voidaan lisätä verkkoon yhdistettyjen kameroiden sekä hälytinjärjestelmien avulla ja älykkäiden verkkoon yhteydessä olevien jääkaappien avulla voidaan auttaa sekä asukkaita että kauppoja ja tuottajia vähentämään hävikkiä. (Appio et al. 2019) Älytalot keräävät ja lähettävät käyttäjästään paljon tietoa, ja aina kun tietoa verkon kautta lähetetään, on mahdollista että se päätyy vääriin käsiin. Vääriin käsiin joutuessaan nämä tiedot voivat paljastaa käyttäjästään muun muassa hänen kulutustottumuksensa ja kotonaolorutiininsa. Suurimmat riskit ovat henkilön altistuminen rikollisten uhriksi, sekä yksityisyyden menetys. Rikollisten lisäksi esimerkiksi totalitääriset valtiot voivat käyttää näitä tietoja kansalaistensa valvontaan.

5.1.2 Älykäs liikenne

Yksi yleisimmistä älykaupunkeihin liitetyistä tehtävistä on liikenteenohjaaminen, sekä joukkoliikenteen reittien ja aikataulujen suunnittelu. Appio et al. 2019 nimeääkin suurkaupunkien ruuhkatilanteiden parantamisen yhdeksi älykaupunkihankkeiden keskeisimmistä motiiveista. Liikenteen sujuvoittamiseksi on monia ratkaisuja. Liikennevirtoja on

mahdollista seurata kaupungin infrastruktuuriin asennettavilla antureilla, jotka mahdollistavat liikennevirtojen tarkkailun reaaliajassa. Tämän datan avulla voidaan laskea onnettomuusriskiä parantaa julkista liikennettä sekä helpottaa pysäköintiongelmia. Liikennevirtoja seuraamalla on myös mahdollista optimoida kaupungin liikenteenohjausta esimerkiksi liikennevalojen algoritmien avulla. (Appio et al. 2019)

VSN (Vehicular Social Networks) ajoneuvoverkoston avulla voidaan integroida GPS-tiedot (Global Positioning System, maailmanlaajuinen paikallistamisjärjestelmä) tuhansista kuljettajista ja heidän älypuhelimistaan toisiinsa. Tämän avulla ajoneuvot voivat lähitulevaisuudessa olla yhteydessä sekä keskenään että ympäröivän infrastruktuurin kanssa, mahdollistaen paitsi paremman tiedon saannin, autojen yhteiskäytön ja tarkemmat turvallisuus varoitukset. Tulevaisuudessa myös yhteiskäytössä olevat itseohjautuvat autot ovat yksi keino yksityisautoilun tarpeen vähentämiseksi. (Appio et al. 2019)

Liikenteen olosuhteiden parantaminen ei koske pelkästään autoja vaan myös kävelyä ja muita liikuntamuotoja. Kävely- ja pyöräilyolosuhteiden parantamiseksi voidaan muuttaa osa kaduista kevyen liikenteen väyliksi. Tätä muutosta helpottaa antureiden avulla saatu tieto, jonka perusteella voidaan suunnitella vaihtoehtoisia reittejä, sekä mukauttaa julkista liikennettä muutoksiin. Useilla kaupungeilla on tarjolla myös liikkumista helpottamaan kehitetty palvelu, johon on integroitu julkisen liikenteen aikataulut ja reitit. (Appio et al. 2019) Kehitys tuo mukanaan myös lukuisia turvallisuusriskejä. Tietomurto esimerkiksi itseohjautuvien autojen tai liikenteenohjauksen järjestelmiin, voi aiheuttaa vakavia uhkia sekä ihmisille että infrastruktuurille (Ahmad et al. 2022).

5.1.3 Innovaatioekosysteemi

Innovaatioekosysteemi ei nojaudu yhtä paljon esineiden internetin tarjoamaan tekniikkaan kuin älykäs rakennettu elinympäristö sekä älykäs liikenne, mutta on silti tärkeä osa älykaupunkien kehitystä. Innovaatioekosysteemin muodostavat älykäs talous (smart economy) ja älykkäät ihmiset (smart people). Yhdysvaltalainen ekonomisti Robert Solow osoitti jo 1950-luvulla, että suurin osa tuottavuuden kasvusta johtuu tekniikan ja pääoman sijaan ihmisten tietotaidosta ja luovuudesta, näiden ollessa kaksi tärkeää tekijää innovaatioiden muodostumisessa. Erityisesti yliopistot ja muut korkeakoulut ovatkin tärkeässä osassa älykaupunkien innovaatioekosysteemin luomisessa. Ne auttavat kehittämään inhimillistä pääomaa, jolla on korkea vaikutus kaupunkien taloudelliseen kasvuun. Pelkkä koulutusmahdollisuuksien tarjonta ei yksin riitä, vaan kaupungin hallinnon tulisi pyrkiä houkuttelemaan lahjakkuuksia ja investointeja, tarjoamalla korkeat elintason standardit turvallisuuden, terveydenhuollon ja vapaa-ajan infrastruktuurin suhteen. Avoimet

ja suvaitsevaiset yhteisöt houkuttelevat puoleensa monimuotoista joukkoa luovia työntekijöitä, jotka ovat perusta sosiaalisen pääoman kehittämiselle innovaatioekosysteemeissä. Taloudellisen vaikutuksen kannalta on tärkeää että innovatiiviset ihmiset ovat yhteydessä toisiinsa, kaupungin tulisikin olla luonteva ympäristö luoville mielille kokoontua, jakaa ajatuksia ja ideoita sekä oppia lisää taitoja. Tiedon jakamista helpottaakseen älykkäät kaupungit luovatkin usein teknologiakeskuksia, tutkimuskeskusten, yrityskehityskeskusten sekä innovaatiopuistojen muodossa. (Appio et al. 2019)

Älykäs talous on yksi älykaupungin tunnusmerkeistä. Se tarkoittaa taloutta, jonka perustana ovat teknologiset innovaatiot, resurssitehokkuus, kestävyys ja korkea sosiaalinen hyvinvointi. Älykään talouden tavoitteena on kannustaa luovuuteen, lisätä tuottavuutta ja kilpailukykyä, sekä parantaa asukkaiden elämänlaatua. (Sofyaningrat 2022) Innovatiiviset ihmiset yhdessä älykkään elinympäristön ja älykkäiden liikennejärjestelyjen kanssa, luovat perustan älykkäälle taloudelle (Appio et al. 2019). Innovaatioekosysteemi onkin tärkeä tekijä sekä kaupungin taloudellisen kehityksen että erityisesti tulevaisuuden innovaatioiden kannalta.

5.2 Tietoturvallisuus, kyberhyökkäykset ja muut kehityksen mukanaan tuomat uhat

Kuten aiemmin tässä luvussa olen tuonut ilmi, älykaupunkien kehitys ei ole täysin ongelmatonta. Vaikkakin älykaupunkeja parantuneen tehokkuuden ja suorituskykynsä ansiosta mainostetaan tehokkaana ratkaisuna väestönkasvun mukanaan tuomiin ongelmiin, luovat ne myös paradoksaalisen tilanteen, jossa saavutettavat edut, kuten mukavuus, taloudellinen vauraus, turvallisuus ja kestävä kehitys, tuovat mukanaan myös ei toivottuja seurauksia sekä uusia variaatioita jo olemassa olevista ongelmista. Näitä ovat esimerkiksi eriarvoistumisen kasvu, negatiiviset ympäristövaikutukset ja kaupungin altistaminen uudenlaisille turvallisuuden sekä verkkorikollisuuden riskeille (Kitchin et al. 2019). Suurimmat haasteet älykaupungeille muodostavat tekniset ongelmat, kuten esimerkiksi esineiden ja ohjelmistojen yhteensopivuus, kustannustehokkuus sekä tärkeimpänä turvallisuuteen ja yksityisyyteen liittyvät uhat. Älykaupungit ovat koko ajan alttiina erilaisille hyökkäyksille, jotka voivat vahingoittaa kaupungin infrastruktuuria ja viestintäjärjestelmiä. Älykaupunkeja tutkiessa onkin erityisen tärkeä selvittää, mitä saavutuksia ja puutteita tietoturvallisuuden näkökulmasta kehityksessä on ilmennyt. Tietoturvallisuuden perusvaatimusten tunteminen ja päivittäminen onkin erittäin tärkeää älykaupunkien kehityksen edetessä. (Ijaz et al. 2016)

5.2.1 Älykaupungit hyökkäyksen kohteena

Niin kauan kun on ollut kaupunkiyhteiskuntia, on ollut myös rikollista toimintaa ja yrityksiä tunkeutua ja hyökätä kaupungin infrastruktuuria ja julkisia palveluita vastaan. Näitä uhkia vastaan yritetään puolustautua sekä arkkitehtuurisin keinoin (esimerkiksi ovet, lukot, muurit ja aidat) että teknologian avulla (valvontakamerat ja hälytinjärjestelmät). Kaikilla turvatoimilla on kuitenkin omat heikkoutensa, ja ajan kuluessa ne tullaan murtamaan. Turvajärjestelmien kehityksessä onkin siis jatkuva tasapainoilu, jotta järjestelmät tarjoaisivat riittävän suojan, mutta eivät olisi liian rajoittavia käyttäjilleen. Tässä suhteessa älykaupungit eivät poikkea mitenkään edeltäjistään, ja kyberturvallisuusalan sekä rikollisten välillä onkin käynnissä jatkuva kamppailu. (Kitchin et al. 2019)

Koska älykkäät kaupunkiteknologiat toimivat verkon välityksellä, niiden haavoittuvuuksien hyväksikäyttö voidaan toteuttaa etäältä ja hyökkäykset voidaan naamioida. Tämä taitavasti toteutettuna vähentää kiinnijäämisen riskiä. Hyökkäyksiä helpottavat verkkoon kytkettyjen laitteiden määrän kasvaessa hyökkäyksille alttiina olevan rajapinnan moninkertaistuminen, sekä hakkeroinnissa apuna käytettävien haittaohjelmien kehittyminen. (Kitchin et al. 2019) Esineiden internet ja sen myötä myös älykaupunkien järjestelmät tuottavat käyttäjistään suuret määrät henkilökohtaisia, taloudellisia, kaupallisia ja luottamuksellisia tietoja, joita täytyy kerätä, siirtää, käsitellä sekä varastoida. Näitä tietoja on pystyttävä suojelemaan järjestelmiä vastaan kohdistuvilta hyökkäyksiltä (Khan et al. 2023).

5.2.2 Digitaalisten teknologioiden haavoittuvuudet

Älykaupunkien järjestelmiin integroitujen antureiden keräämä tieto on yksi tärkeimmistä kyberhyökkäyksien kohteista. Hyökkääjät etsivätkin älykaupunkien kohdejärjestelmistä haavoittuvuuksia tai puutteita, joita vastaan hyökätä erilaisin tekniikoin. (Siham et al. 2019) Järjestelmiä vastaan suoritettavat hyökkäykset voidaan jakaa kolmeen eri muotoon. Käytettävyyshyökkäykset (availability attacks), pyrkivät joko sulkemaan järjestelmän tai estämään sen käytön. Luottamuksellisuushyökkäykset (confidentiality attacks), pyrkivät keräämään tietoa sekä valvomaan toimintaa ja eheyshyökkäykset (integrity attacks), pyrkivät pääsemään järjestelmään sisään muuttaakseen järjestelmän tietoja ja asetuksia. (Kitchin et al. 2019)

Kyberhyökkäykset pyrkivät hyödyntämään viittä suurta digitaalisten teknologioiden haavoittuvuutta, jotka ovat keskeisiä älykaupunkijärjestelmille. Näistä ensimmäinen on heikko ohjelmistoturvallisuus ja datan salaus. Carnegie Mellon -yliopiston tiimin vuonna 2004 tekemän tutkimuksen mukaan jokaista 1000 koodiriviä kohden on keskimäärin 30

virhettä tai mahdollisesti hyödynnettävissä olevaa vikaa. Tyypillisissä kaupungeissa käytössä olevissa suurissa järjestelmissä on miljoonia rivejä koodia, lisäksi kaupunkien hallinto ja älykaupunkiteknologioiden toimittajat ottavat ohjelmistoja usein käyttöön ilman kunnollista tietoturvatestausta. Ongelmia aiheuttaa myös markkinoilla olevien antureiden ja laitteiden tehottomuus, jonka vuoksi ne eivät pysty tukemaan salattuja verkkolinkkejä. (Kitchin et al. 2019)

Toinen haavoittuvuusalue liittyy epävarmojen vanhojen järjestelmien käyttöön ja puutteelliseen ylläpitoon. Monet älykaupunkiteknologiat on rakennettu vanhan teknologian ja ohjelmistojen päälle, jonka vuoksi siirtyminen uudempiin ja turvallisempiin järjestelmiin on hankalaa, ellei jopa mahdotonta. Nämä teknologiat voivat luoda sisäänrakennettuja haavoittuvuuksia uudempiin järjestelmiin vanhempien ohjelmistojen kautta, joita valmistaja ei enää tue, eikä niitä näin ollen enää päivitetä tai huolleta. Jopa uudempien teknologioiden tapauksessa voi olla vaikeaa testata suorittaa korjauksia kriittisille toiminnallisille järjestelmille, jotka on pidettävä jatkuvasti käynnissä. (Kitchin et al. 2019)

Kolmannen haavoittuvuusalueen aiheuttavat suuret ja monimutkaiset älykaupunkijärjestelmät, joilla on keskenään monia riippuvuuksia ja monimutkaisia rajapintoja alttiina hyökkäyksille. Tällaisten monimutkaisten järjestelmien tietoturvallisuuden varmistaminen on hankalaa. Vaikka yksittäinen järjestelmä olisikin turvallinen, yhdistäminen muihin järjestelmiin altistaa sen tietoturvahyökkäyksille. Tällaisten monimutkaisten järjestelmien tietoturvan taso määräytyy järjestelmän heikoimman lenkin mukaan. Järjestelmien monimutkaisuus altistaa ne myös muille kuten esimerkiksi ohjelmointi tai muille käyttäjästä johtuville virheille. (Kitchin et al. 2019)

Neljäs haavoittuvuuden muoto on dominoefekti, jossa hyökkäys yhteen tosiinsa sidotuista järjestelmistä leviää myös kaupunkijärjestelmän muihin järjestelmiin. Käyttöjärjestelmä missä useita järjestelmiä on linkitetty toisiinsa, aiheuttaakin yhden älykaupunkijärjestelmien suurimmista turvallisuusriskeistä. Esimerkiksi onnistuneella hyökkäyksellä sähköverkkoon on valtavia kerrannaisvaikutuksia sähköverkon tukiessa niin monia muita toimintoja. (Kitchin et al. 2019)

Viides ja yleisin haavoittuvuus ovat inhimilliset virheet sekä tahalliset väärinkäytökset. Näitä ovat esimerkiksi vahingossa tai tarkoituksella asennetut virukset, tietoturvallisuusohjelmien virheelliset asennukset tai puutteelliset päivitykset, ja kriittisen informaation kuten käyttäjätunnusten tai salasanojen kalastelu käyttäjiltä valheellisilla tietojenkalasteluviesteillä. (Kitchin et al. 2019)

5.2.3 Digitaalinen eriarvoistuminen

Eräs älykaupunkien kehitykseen liittyvä enemmänkin eettinen tai sosioekonominen kuin tekninen ongelma on digitaalinen eriarvoistuminen. Yksi älykkään kaupungin tavoitteista on että kaikki asukkaat osallistuisivat aktiivisesti kaupungin toimintoihin, jakaen tietoa uusinta ICT-teknologiaa hyödyntäen. Todellisuudessa osalta asukkaista puuttuvat joko tarvittavat taidot, tarvittava teknologia tai molemmat. Uhkana onkin että monet älykkään kaupungin tarjoamat palvelut jäävät näiden heikommassa asemassa olevien kansalaisten ulottumattomiin. Ollakseen eettisesti ja lainsäädännöllisesti kestävällä pohjalla älykkään kaupungin tarjoamien palveluiden tulisi kuitenkin olla tasapuolisesti kaikkien saatavilla. Merkittävin selittävä tekijä digitaaliselle eriarvoistumiselle on ikä, muita selittäviä tekijöitä ovat esimerkiksi sosioekonominen asema, koulutusaste ja asuinalue. Joidenkin viimeaikaisten väitteiden mukaan internet yhteyksien saatavuuden helpottuminen ja älypuhelinten hintojen lasku, olisivat laskemassa sosioekonomisen aseman merkitystä digitaalisessa eriarvoistumisessa, helpottaen omalta osaltaan pyrkimyksiä digitaalisen eriarvoistumisen estämiseen. (Seung-Yoon et al. 2021)

Tärkein tekijä mihin on mahdollista vaikuttaa digitaalisen eriarvoistumisen ehkäisyssä, on digitaalinen lukutaito. Tutkimusten mukaan paras tapa ehkäistä digitaalista eriarvoistumista onkin digitaalisen lukutaidon ja erityisesti mobiilikäyttötaitojen opetus. Tämän vuoksi olisikin tärkeää että kaupungit tarjoaisivat yksilöllisiä koulutusmahdollisuuksia vanhuksille ja pienituloisille digitaalisen lukutaidon parantamiseksi ja ylläpitämiseksi. Toinen tutkimuksissa esille tullut digitaalisten palvelujen käyttöön rohkaiseva tekijä on palvelujen tarpeellisuuden tunne. Kaupungin tulisikin pyrkiä jakamaan tietoa tarjoamistaan digitaalisista palveluista niin, että asukkaat kokisivat palvelut itselleen tarpeelliseksi ja innostuisivat niitä kokeilemaan, sillä ensimmäinen käyttökerta vähentää tutkitusti kynnystä seuraavalle käyttökerralle. (Seung-Yoon et al. 2021) Yksi merkittävä asia, jota Seung-Yoon et al. 2021 tutkimuksessa jätettiin vähälle huomiolle, on laitteiden fyysinen omistaminen. Olisikin syytä miettiä, olisiko vähävaraisia mahdollisuus tukea älylaitteiden hankinnassa syrjäytymisen ehkäisemiseksi.

5.3 Tietoturvallisuuden parantaminen

Älykaupunkien ominaisuuksiin kuuluvat muun muassa tehokkuus sekä älykäs infrastruktuuri, mutta tärkein ominaisuus on turvallisuus. Voidaksemme turvata älykaupunkien tarjoamat palvelut, meidän on kehitettävä älykkäät puolustautumiskeinot hyökkääjiä vastaan. (Siham et al. 2019) Älykaupunkijärjestelmien tietoturvallisuus koostuu joukosta sekä teknillisiä ratkaisuja että tietoturvakeinoja, joidenka tavoitteena on estää järjestelmää vastaan kohdistuneet hyökkäykset, ja mahdollistaa järjestelmän palautus, mikäli

hyökkäystä ei kyetä torjumaan. Esimerkkeinä näistä voidaan mainita erilaiset kulunvalvontakäytännöt, asianmukaisesti ylläpidetyt palomuurit, virustentorjunta, päästä päähän -salaus, säännölliset ohjelmistopäivitykset, sekä varmuuskopiosuunnitelmat. Lisäksi on hyvä olla valppaana oleva ja ammattitaitoinen IT-henkilöstö, sekä kattavaa tietoturvakoulutusta muulle henkilöstölle ja asukkaille. (Kitchin et al. 2019)

Älykkäiden kaupunkiteknologioiden muuttuessa yhä keskeisemmäksi tekijäksi kaupunkisuunnittelussa, vanhat tietoturvaratkaisut ovat käymässä riittämättömiksi. Niiden sijaan tarvitaan systemaattisempaa lähestymistapaa teknisen suunnittelun ja koulutuksen suhteen. Erityisen tärkeää on ennaltaehkäisevä ja ennakoiva turvallisuussuunnittelu (security-by-design). Ennakoivassa turvallisuussuunnittelussa pyritään rakentamaan vahvat turvatoimet järjestelmiin heti alusta lähtien, sen sijaan että niitä yritettäisiin lisätä käytössä oleviin järjestelmiin kehityksen jälkeen. Tämä tarkoittaa tarkkaa turvallisuusriskien arviointia suunnitteluprosessin aikana, järjestelmän perusteellista testausta ennen käyttöönottoa sekä sitoutumista järjestelmän valvontaan ja huoltoon koko sen elinkaaren ajaksi. Turvallisuutta parantaakseen kaupunginhallinnon tulisi muodostaa normaalin IT-henkilöstön lisäksi erillinen tietoturvallisuustiimi, joka ottaisi vastuuta tietojärjestelmien turvallisuudesta, sekä kaikesta muusta älykaupungin tietojärjestelmiin kuuluvista asioista. Tiimin toimenkuvaan kuuluisi esimerkiksi laaja-alaisen uhka- ja riskimallinnuksen toteuttaminen, älykkäiden järjestelmien turvallisuuden aktiivinen testaaminen, jatkuva tietoturvallisuuden arviointi, yksityiskohtaisten toimintasuunnitelmien laatiminen erilaisille mahdollisille uhille ja häiriöille, yhteydenpito kaupunginhallinnon ja älykaupunkien hankkeita hallinnoivien yritysten välillä sekä erillisen tiimin muodostaminen kyberturvallisuuteen liittyvien hätätilanteiden varalle. (Kitchin et al. 2019)

Eräs tärkeä suojautumismekanismi älykaupunkien ja organisaatioiden taistelussa kyberhyökkäyksiä vastaan on tunkeutumisen havaitsemisjärjestelmä (Intrusion Detection System, IDS) (Siham et al. 2019). IDS havaitsee järjestelmään kohdistuneet hyökkäykset tavoitteenaan tunnistaa vihamielinen verkkoliikenne ja laitteiden käyttö, jota perinteinen palomuuri ei havaitse (Khraisat et al. 2019). Kuten aiemmin digitaalisia tekniikoita käsittelevässä luvussa 5.2.2 mainittiin, hyökkääjät etsivät älykaupunkien järjestelmistä puutteita ja haavoittuvuuksia, joiden avulla tunkeutua järjestelmään. IDS:ää tarvitaankin vihamielisten hyökkäysten havaitsemiseksi, sekä tietoturvallisuuden tavoitteiden kuten luottamuksellisuuden ja eheyden saavuttamiseksi (Siham et al. 2019). Tämän lisäksi erityisesti niille, jotka osallistuvat älykkäiden kaupunkitekniikoiden hankintaan, käyttöönottoon ja päivittäiseen käyttöön, olisi kehitettävä ja tarjottava erityistä ja jatkuvaa tietoturvallisuuteen liittyvää koulutusta. Mikäli käyttäjät eivät ole turvallisuusvaatimusten tasolla hyvätkin tietoturvallisuusratkaisut voivat mitätöityä inhimillisten virheiden vuoksi. Myös

markkinoita voisi ohjata ja sitouttaa tietoturvallisuuden parantamiseen sekä kannustamalla että lainsäädännön ja muiden määräysten avulla. Vaikka älykaupungeilla on kiistatta etunsa, voisi olla myös hyvä rakentaa hätätilanteiden varalle tarkoituksella joitakin infrastruktuurin järjestelmiä, jotka ovat irrallaan verkosta. Näin voitaisiin taata niiden toimivuus kyberhyökkäyksistä riippumatta. (Kitchin et al. 2019)

6. YHTEENVETO

Tutkielmassa esiteltiin esineiden internet sekä älykaupungit, käsiteltiin esineiden internetin vaikutusta älykaupunkien kehitykseen ja selvitettiin mitä mahdollisuuksia ja uhkia tämä kehitys tuo tullessaan sekä pohdittiin miten löytyneitä uhkia voisi ehkäistä. Tutkielma toteutettiin kirjallisuuskatsauksena, jossa käytettiin hyväksi sekä akateemisia että populaarilähteitä. Tutkimuksessa oli kaksi tutkimuskysymystä.

Ensimmäinen tutkimuskysymys oli: Mitä mahdollisuuksia esineiden internetin avulla kehitetyt älykaupungit tarjoavat? Tämän avulla kartoitettiin älykaupunkien kehityksen tuomia etuja sekä ongelmia, joita kehityksen avulla olisi mahdollista ehkäistä. Tutkielman perusteella älykaupunkien kehityksen toivotaan tuovan apua kaupunkien räjähdysmäisen väestönkasvun aiheuttamiin ongelmiin. Älykaupungeista erottuivat kolme tärkeää osatekijää, älykäs rakennettu elinympäristö, älykäs liikenne sekä älykään talouden ja älykkäiden ihmisten muodostama innovaatioekosysteemi Älykäs rakennettu elinympäristö mahdollistaa kaupungin tärkeiden toimintojen tuottamisen ympäristöystävällisemmin, energia tehokkaammin sekä edullisemmin. Älykäs liikenne auttaa vähentämään ruuhkia, optimoimaan joukkoliikenteen aikataulut ja reitit, vähentämään tarvetta yksityisautoiluun, ja parantamaan pyöräilijöiden sekä jalankulkijoiden liikkumismahdollisuuksia. Innovaatioekosysteemin avulla kaupunkiin pyritään houkuttelemaan osaajia sekä investointeja luomalla ihmisille hyvät olosuhteet verkostoitua ja jakaa ideoitaan. Älykkään talouden tavoitteena on kannustaa luovuuteen sekä parantaa tuottavuutta ja elämänlaatua. Innovaatioekosysteemillä onkin tärkeä rooli, sekä älykaupunkien talouden parantajana että erityisesti älykaupunkien kehityksen näkökulmasta, tulevaisuuden innovaatioiden mahdollistajana. Älykaupunkien suunnittelu jatkaa kehittymistään ICT-teknologioiden rinnalla, kuten Angelidou (2015) asian ilmaisi, älykaupunkien suunnittelussa onkin enemmän kyse strategisesta tulevaisuuden suunnittelusta nykypäivän sijaan.

Toinen tutkimuskysymys oli: Millaisia riskejä esineiden internet ja älykaupungit aiheuttavat? Tämän avulla kartoitettiin älykaupunkien kehityksen mukanaan tuomia riskejä sekä yritettiin etsiä löydetyille uhille mahdollisia ratkaisuja. Tutkimuksen perusteella inhimilliset tekijät sekä tekniset ongelmat, kuten esimerkiksi vanhojen laitteiden ja ohjelmistojen yhteensopivuus aiheuttavat suurimmat haasteet älykaupunkien kehitykselle. Ijaz et al. (2016) listaa artikkelissaan älykaupunkien viisi keskeisintä haavoittuvuutta:

1. heikko ohjelmistoturvallisuus ja datan salaus
2. epävarmojen vanhojen järjestelmien käyttö ja puutteellinen ylläpito

3. suuret ja monimutkaiset yhteen linkitetyt älykaupunkijärjestelmät, joilla on keskenään monia riippuvuuksia ja monimutkaisia rajapintoja alttiina hyökkäyksille
4. dominoefekti, jossa hyökkäys yhteen toisiinsa sidotuista järjestelmistä leviää myös kaupunkijärjestelmän muihin osiin
5. ihmisten suorittamat inhimilliset virheet ja tahalliset väärinkäytökset.

Älykaupunkien tietoturvallisuusriskit johtuvat siis tyypillisesti suurista hyökkäyksille alttiina olevista rajapinnoista, heikosta tai puutteellisesti ylläpidetystä tietoturvasta sekä inhimillisistä tekijöistä. Löytyneitä uhkia voi ehkäistä pitämällä tietoturva sekä ohjelmistot ja niiden päivitykset ajan tasalla. Tämän lisäksi suositellaan tunkeutumisen havaitsemisjärjestelmän käyttöä (Siham et al. 2019) sekä ennaltaehkäisevää ja ennakoivaa turvallisuussuunnittelua (security-by-design) (Ijaz et al. 2016). Henkilöstön ja asukkaiden kunnollinen tietoturvakoulutus on myös erittäin tärkeässä asemassa, sillä inhimillisten virheiden vuoksi hyväkin tietoturvallisuus voi vaarantua.

Tietoturvallisuutta koskevien riskien lisäksi yksi älykaupunkien rinnalla kehittyvä uhka on digitaalinen eriarvoistuminen. Älykaupungin tavoitteena on että sen asukkaat osallistuisivat tiedon jakamiseen, mutta valitettavasti kaikilla ei ole tähän tarvittavia taitoja tai digitaalisia laitteita. Ongelmaa voitaisiin helpottaa tarjoamalla yksilöllisiä koulutusmahdollisuuksia niitä tarvitseville sekä miettiä, olisiko vähävaraisia mahdollisuus tukea älylaitteiden hankinnassa syrjäytymisen ehkäisemiseksi.

Tutkielman aihe oli kiinnostava mutta laaja, ja valitettavasti kandidaatintutkielman laajuuden puitteissa tarkastelu kovin syvällisesti ei ollut mahdollista. Tutkielmassa löytyi kyllä joitakin selkeitä tuloksia, mutta lähdeaineiston vähäisyys sekä se että tuoreita lähteitä ei löytynyt aivan niin paljon kun olisin toivonut, vaikuttavat siihen että lisätutkimukset aiheesta olisivat vielä tarpeen.

LÄHTEET

Ahmad k., Maabreh M., Ghaly M., Khan K., Qadir J., Al-Fuqaha A., (2022), Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges, Computer Science Review 43, 100452, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2021.100452

Angelidou, M., (2015), Smart cities: A conjuncture of four forces, Cities, 47, 95-106, ISSN 0264-2751, https://doi.org/10.1016/j.cities.2015.05.004

Appio, F., Lima, M., Paroutis, S., (2019), Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges, Technological Forecasting and Social Change, 142, 1-14, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2018.12.018

Balova, S. L., Velazco, J., Polozhentseva, I. V., Chernavsky, M. Y., & Shubtsova, L. V., (2021), The formation of the concept of smart sustainable city with the purpose of environmental protection. Journal of Environmental Management & Tourism, 12(5), 1269-1275. doi:https://doi.org/10.14505/jemt.12.5(53).12

Curry, E., Dustdar, S., Sheng, Q. Z., & Sheth, A., (2016), Smart cities - enabling services and applications. Journal of Internet Services and Applications, 7(1), 1-3. doi:https://doi.org/10.1186/s13174-016-0048-6

Empirica Finland Oy (N.d.), Mikä on IoT? Esineiden internet yksinkertaisesti selitettynä, Empirica Finland Oy, Haettu 11.02.2023 osoitteesta https://www.empirica.fi/iot/

Harwood, T., (December 2019), Internet of Things (IoT) History, Postscapes, Haettu 11.02.2023 osoitteesta https://www.postscapes.com/iot-history/

Ijaz, S., Munam, A. S., Khan, A., & Ahmed, M., (2016), Smart cities: A survey on security concerns. International Journal of Advanced Computer Science and Applications, 7(2) doi:https://doi.org/10.14569/IJACSA.2016.070277

Khan, Y., Mohd Su'ud M. B., Muhammad, M. A., Sayed, F. A., Nur, A. S., & Khan, N., (2023), Architectural threats to security and privacy: A challenge for internet of things (IoT) applications. Electronics, 12(1), 88. doi:https://doi.org/10.3390/electronics12010088

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., (2019), Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 . https://doi.org/10.1186/s42400-019-0038-7

Kitchin R., Dodge M., (2019), The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention, Journal of Urban Technology, 26:2, 47-65, doi: 10.1080/10630732.2017.1408002

Maras, M.-H., (2015), Internet of things: Security and privacy implications, International Data Privacy Law, 5(2), 99—104, doi:https://doi.org/10.1093/idpl/ipv004

Mouha, R., (2021), Internet of Things (IoT), Journal of Data Analysis and Information Processing, 9, 77-101. doi: 10.4236/jdaip.2021.92006.

Nallapaneni M., Pradeep K., (2018), The Internet of Things: Insights into the building blocks, component interactions, and architecture layers, Procedia Computer Science, 132, 109-117, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.05.170.

Penttinen, J., (2016), Wireless Communications Security : Solutions for the Internet of Things, John Wiley & Sons, Incorporated, ProQuest Ebook Central

Seung-Yoon, S., Kim, D., & Chun, S. A., (2021), Digital divide in advanced smart city innovations. Sustainability, 13(7), 4076. doi:https://doi.org/10.3390/su13074076

Siham, T., Tomader, M., (2019), Security in a smart city: challenges and solutions, In Proceedings of the 4th International Conference on Smart City Applications (SCA '19). Association for Computing Machinery, New York, NY, USA, Article 89, 1–7. https://doi.org/10.1145/3368756.3369076

Sofyaningrat S., (2022), What is a Smart Economy and What Its Benefits?, Jakarta smart city, haettu 16.04.2023 osoitteesta https://smartcity.jakarta.go.id/en/blog/membedah-smart-economy-dan-manfaatnya-buat-jakarta/

Talabi, D., (April 11, 2022), Internet of Things (IoT), Assurecondo, Haettu 11.02.2023 osoitteesta https://assurecondo.com/internet-of-things-iot/