Sähköisen äänestämisen tietoturva

Oulun yliopisto
Tieto- ja sähkötekniikan tiedekunta
Tietojenkäsittelytieteiden
koulutusohjelma
LuK-tutkielma
Tomi Jolkkonen
5.6.2019

Tiivistelmä

Sähköistä äänestämistä on kokeiltu parin vuosikymmenen ajan eri puolilla maailmaa Suomesta Yhdysvaltoihin muutamassa kymmenessä maassa. Sähköisiä äänestyksiä on toteutettu valtakunnallisista vaaleista yritysten pienäänestyksiin. Tutkimusmenetelmänä käytetään kuvailevaa kirjallisuuskatsausta, jossa tutkittavaa ilmiötä kuvataan laaja-alaisesti mutta, josta luokitellaan eri kriteerein sähköisten äänestysjärjestelmien ominaisuuksia tietoturvan näkökulmasta eri ympäristöissä. Tutkielmassa kartoitetaan erilaisia ympäristöjä, joissa sähköisiä äänestysjärjestelmiä on hyödynnetty lähtien maailman ensimmäisestä valtakunnallisesta äänestyksestä Virossa, aina viimeaikaisiin kokeiluihin. Tutkielmassa käydään läpi myös uudempia tutkimuksia tekniikoista, joilla havaittuja ongelmia yritetään ratkaista. Kirjallisuuskatsaus keskittyy siihen, millaisia tietoturvaan liittyviä haasteita sähköisessä äänestämisessä on ja miltä äänestämisen tulevaisuus näyttää.

Sähköisten äänestysjärjestelmien käyttöönottoon liittyy useita haasteita ohjelmisto- ja laitesuunnittelusta internetin turvallisuuteen sekä äänestyskäytäntöihin. Kirjallisuuskatsaus käy läpi eri tutkimuksissa toistuvat sekä yleisimmät huomioitavat asiat, joita ovat täydellisen tietoturvallisuuden saavuttamisen vaikeus sekä tietoturvahaasteet, ei pelkästään laitteissa tai ohjelmissa vaan myös ihmisten käyttäytymisessä. Lopuksi luodaan katse tulevaisuuden näkymiin ja annetaan jatkotutkimusehdotuksia siitä, miten rakennetaan tietoturvallinen äänestysjärjestelmä, jota kaikki osaavat käyttää.

Tutkimusmenetelmänä käytetään kuvailevaa kirjallisuuskatsausta, jossa tutkittavaa ilmiötä kuvataan laaja-alaisesti mutta josta luokitellaan eri kriteerein sähköisten äänestysjärjestelmien ominaisuuksia tietoturvan näkökulmasta eri ympäristöissä.

Avainsanat
sähköinen äänestäminen, äänestysjärjestelmät, tietoturva, tietoturvauhka, tietoturvahyökkäys, tietoturvateknologia

Ohjaaja
Tutkijatohtori Mari Karjalainen

Sisällysluettelo

1. Johdanto

Tässä tutkielmassa tarkastellaan kirjallisuuden pohjalta sähköisten äänestysjärjestelmien tietoturvaa. Sähköisellä äänestämisellä tarkoitetaan äänestämistä tietotekniikan avustuksella. Sähköinen äänestys voidaan toteuttaa esimerkiksi internetin välityksellä, matkapuhelimella tai äänestyspaikalla olevalla laitteella, jolle äänestäjä syöttää äänensä. Sähköinen äänestäminen voi olla myös perinteistä äänestämistä, jonka jotain osa-aluetta avustetaan tietotekniikan avulla. (Wikipedia, 2019.) Sähköisen äänestämisen tarkoitus on nopeuttaa ja helpottaa äänestysprosessia sekä saada prosessi läpinäkyväksi.

Uutisissa kerrotaan tasaisin väliajoin yhtäältä sähköisen äänestämisen mahdollisuuksista, toisaalta tietoturvauhkista kaikkialla sekä sovelluksissa, verkoissa että laitteissa. Vaikka sähköistä äänestämistä on kokeiltu jo kohta kahden vuosikymmenen ajan ja tutkittu vielä sitäkin kauemmin, emme ole vielä onnistuneet löytämään virheetöntä tapaa järjestää äänestämistä sähköisesti. Tässä tutkielmassa käydään läpi kirjallisuutta, jossa kuvaillaan erilaisia sähköisen äänestämisen järjestelmiä ja niiden testaamista. Viime aikoina asiaan on herätty myös tietoturva-alan konferensseissa, joista on tuotettu hyödyllisiä dokumentteja yhteistyössä poliitikkojen kanssa (mm. Blaxe et al., 2018). Tutkielma keskittyy siihen, millaisia tietoturvaan liittyviä haasteita sähköisessä äänestämisessä on ja miltä äänestämisen tulevaisuus näyttää. Tavoitteena on muodostaa kokonaiskäsitys aiheesta sekä tietojenkäsittelytieteen ammattilaiselle että aiheesta yleisesti kiinnostuneelle taholle.

1.1 Tutkimusmenetelmä

Yliopiston tehtävä on uuden tiedon tuottaminen ja siihen perustuvan korkeimman opetuksen antaminen. Opetus ja tieteellinen tutkimus nivoutuvat yliopistossa yhteen, mistä syystä yliopistossa opetellaan alusta asti kriittistä ajattelua, käsiteltävän ilmiön analysointia sekä synteesien luomista laajasta kirjallisuudesta. Kirjallisuutta analysoidaan kirjallisuuskatsauksessa ja tieteellisessä esseessä, joka palvelee yleisten ajattelutaitojen kehittämistä. (Lehto, 2019.)

Tutkimusmenetelmänä käytetään kuvailevaa kirjallisuuskatsausta, tarkemmin sanottuna integroivaa kirjallisuuskatsausta, jossa pyritään kuvaamaan sähköisten äänestysjärjestelmien tietoturvahaasteita eri ympäristöissä mahdollisimman monipuolisesti, ottaen huomioon sekä tekniset että ihmisiin liittyvät uhat (Salminen, 2011). Tämän kirjallisuuskatsauksen pohjalta voidaan sanoa, ettei täysin tietoturvallista äänestystä ole mahdollista luoda tai haaste on ainakin suuri. Äänestämisen tietoturvaan liittyy ohjelmistot, laitteet, ihmiset ja verkot, joiden tietoturvallisuutta ei olla vielä pystytty varmistamaan sataprosenttisesti muillakaan osa-alueilla. Lopuksi ehdotetaan monitieteistä lisätutkimusta siitä, miten ihminen saadaan mukaan tähän ennen tekniseen mutta nykyään koko yhteiskuntaan vaikuttavaan demokraattiseen jokamiehenoikeuteen siten, että sähköinen äänestäminen on helppoa, virheetöntä ja läpinäkyvää.

Kirjallisuuden hakuprosessissa olen käyttänyt Oulun yliopiston Oula-Finna -sivuston palveluja ja sitä kautta erityisesti tietojenkäsittelytieteen tiedonhakuopasta. Pyrin löytämään mahdollisimman monipuolisesti sekä kirjallisuutta, nettisivuja ja videoita, että tieteellisiä artikkeleita siten, että Julkaisufoorumi tai Ulrichsweb antaa näillä riittävän hyvän luokituksen, artikkeleihin on viitattu

riittävästi, tai julkaisu on yleisesti seuratun tekijän käsialaa (tai maailman suurimmista alan tapahtumista).

Työssä on käytetty eniten Scopus -tietokantaa ja erityisesti hakusanoja "emediated voting", "electronic voting". Laajensin myöhemmin hakua myös IEEE Xploreen, Web of Scienceen, ACM Digital Libraryyn ja Google Scholariin. Koska huomattiin että artikkeleita oli aika vähäinen määrä ja lisäksi niiden julkaisuluokitus ei ollut paras mahdollinen (mm. Scopus antoi electronic voting -sanayhdistelmällä 161 Open Access -viitettä), etsimistä laajennettiin kaikkiin alan merkittäviin tapahtumiin sekä puhujiin. Lisäksi etsittiin pelkästään "security", "cyber" ja "vulnerability" -sanoilla. Mitä enemmän haettiin tietoturvaongelmia, sitä enemmän huomattiin, että tietoturvaongelmat ovat itse asiassa universaleja ongelmia, jotka liittyvät internettiin, ihmisiin, laitteisiin ja ohjelmistoihin. Tämän jälkeen aloitettiin etsintä uudestaan miettimällä tietoturvaongelmia yleisesti internetissä, ihmisissä ja laitteissa, kuitenkin pitäen mielessä viiteryhmänä sähköisen äänestämisen. Lisäksi haasteena oli parhaiden julkaisuluokiteltujen julkaisujen oleminen maksumuurien takana, joten etsintätyötä laajennettiin. Kielenä käytettiin pääasiassa englantia ja etsinnän ulkopuolelle rajattiin liian yleiset tietoturva-artikkelit keskittyen sähköiseen äänestämiseen.

1.2 Käytetyt termit ja lyhenteet

Taulukko 1 sisältää sähköiseen äänestämiseen liittyviä termejä, joita käytetään lähdekirjallisuudessa. Taulukkoon on otettu yleisimpiä kirjallisuuskatsaukseen liittyviä termejä selityksineen eikä ole lähdetty avaamaan kaikkia tietoturvaan liittyviä termejä, joiden oletetaan olevan lukijoille tuttuja.

Taulukko 1. Sähköisen äänestämisen termistöä.

Englanniksi	**Suomeksi**	**Selitys**
EVM electronic voting machine	Sähköinen äänestyslaite	Mikä tahansa sähköiseen äänestämiseen käytettävä laite
DRE direct-recording electronic voting system	Itsenäinen äänestyslaite	Erillinen irrallinen laite äänestämistä varten
Cryptography	Salakirjoitus, salaus	Informaatio prosessoidaan muotoon, jossa se ei ole ymmärrettävä kolmannelle osapuolelle.
E2E verifiability	end to end varmistus	Äänestäjä voi varmistaa äänestyksen jälkeen, että ääni meni perille, paljastamatta ketä äänesti.
RFVV receipt-free voter-verifiable system	Reseptitön äänestysvarmistaminen	Äänestys, jossa äänestäjä ei saa kuittia varmistukseksi äänestämisen suorittamisesta.
BEV blockchain-enabled	Lohkoketjuäänestäminen	Lohkoketju- ja bitcoin-teknologian

voting		hyödyntäminen äänestämisessä

Tutkielman alussa käydään läpi lyhyesti mitä on tietoturva, turvallisuus ja tieto sekä mitä tietoturvauhkia on olemassa. Luvussa 2 määritellään lisäksi kirjallisuuden avulla, mitä on sähköinen äänestäminen sekä sähköisen äänestämisen eri järjestelmiä, kokemuksia ja niistä opittuja asioita. Luvussa 3 pohditaan suurimpia tietoturvahaasteita, joita sähköiseen äänestämiseen liittyy. Lopuksi luvuissa 4 ja 5 yhteenvedetään työn tulokset, pohditaan sähköisen äänestämisen tietoturvan luotettavuutta tulevaisuudessa ja annetaan suosituksia jatkotutkimukselle liittyen tietoturvallisen äänestämisympäristön rakentamiseen siten, että se on myös riittävän yksinkertainen käyttää.

2. Sähköinen äänestäminen ja tietoturvan määritelmä

Sähköisen äänestäminen määritellään äänestämisenä, joka käyttää elektronisia keinoja joko äänestämisessä auttamiseen tai hoitaakseen koko äänestyksen (Wikipedia, 2019). Sähköistä äänestämistä voidaan ajatella toisaalta keinona, jolla uusi teknologia tekee äänestämisestä kustannustehokkaampaa sekä käytännöllisempää äänestäjälle sitä kautta nostaen äänestysprosenttia. Toisaalta, sähköinen äänestäminen tuo tullessaan tietoturvariskejä ja vaikuttaa äänestämisen arvostukseen, koska äänestyspaikka ei ole aina valvottu. (Svensson & Leenes, 2003.)

Ajan saatossa sähköisiä apukeinoja on esitelty äänestämisen yhteydessä jo 1960-luvulta asti. Ensimmäiset äänestykset, joissa sähköiset apukeinot olivat mukana, olivat normaaleja paperiäänestyksiä korteille, mutta äänten laskenta hoidettiin elektronisesti (paper-based voting system). Tämän jälkeen on kehitetty erilaisia tapoja, joissa elektroniset laitteet avustavat normaalia äänestämistä (Arzt-Mergemeier et al., 2008) tai hoitavat äänestämistilanteen kokonaan. Äänestystapoja kehitetään jatkuvasti, vaikka niiden käytössä on havaittu paljon ongelmia.

Tietoturva sekä myös sähköinen äänestäminen ovat laajoja kokonaisuuksia, joista tässä tutkielmassa käsitellään tietojenkäsittelytieteen alueelta sekä äänestämiseen liittyvien laitteiden ja ohjelmien näkökulmasta. Sähköisen äänestämisen laitteet ja ohjelmistot tehdään samoista osista ja samoilla ohjelmointikielillä kuin muutkin laitteet ja ohjelmat, joten on syytä määritellä tietoturva yleisellä tasolla.

Sähköistä äänestämistä on kokeiltu Wikipedian mukaan ainakin 25 maassa runsaine ongelmineen, joita on listattu yli sadan eri lähteen kautta Wikipedian koostesivulla. Esimerkiksi Australiassa 2015 lähes 66 000 ääntä vaarantui tietomurron vuoksi. Kanadassa 2012 ihmiset kenen ei pitänyt voida äänestää, pystyivät äänestämään ja DDoS-hyökkäys hidasti äänestystä. Myös 2018 löydettiin teknisiä vikoja, kuten kaistan riittämättömyys kriittisellä hetkellä. Intiassa sekä 2009 että 2017 jopa 18 sähköistä äänestyslaitetta rekisteröi väärien ihmisten ääniä väärille puolueille. Laitteita oli myös peukaloitu. Suomessa 2009 korkeimman hallinto-oikeuden kuntaäänestyksessä rekisteröitiin vääriä tuloksia, löydettiin käytettävyysongelmia, saatiin monitulkintaisia viestejä siitä, onko ääni annettu vai ei ja havaittiin, että ääniä oli annettu mutta käyttäjä ei kirjautunut ulos, jolloin ääntä ei laskettu. Suomessa ei enää tehdä sähköistä äänestämistä vaan seurataan sen kehittymistä maailmalla. Hollannissa 2006 yli 1180 äänestyslaitteita vedettiin pois äänestyksestä, koska niitä voitiin "salakuunnella".

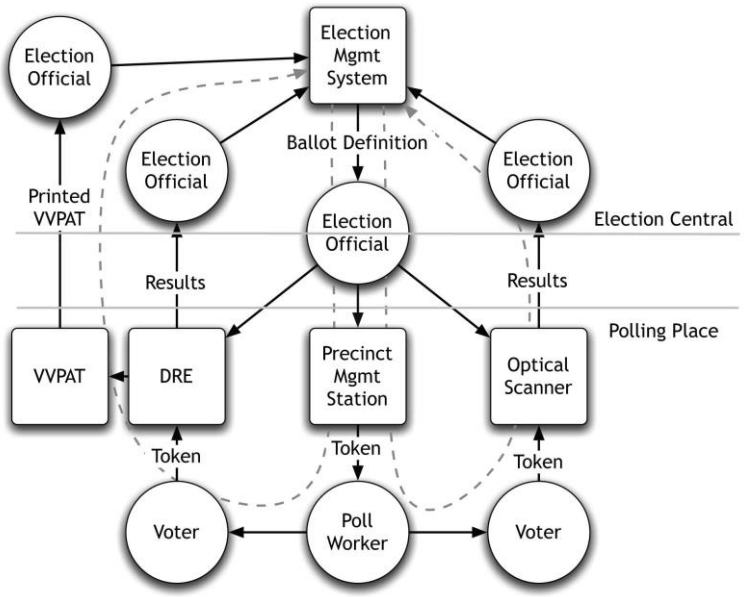
Sähköisiä äänestysjärjestelmiä on runsaasti eri yrityksillä (Blaze et al., 2018). Lisäksi yliopistomaailmassa on sekä tutkittu että kehitetty uusia järjestelmiä tietoturvaongelmien löytämiseksi (mm. Kshetri, N., Voas, J., 2018). Voidaan siis todeta, että yritys löytää uusia keinoja sähköiselle äänestämiselle on kova ja sitä on yritetty jo viisi vuosikymmentä, joista 15 viimeistä vuotta erityisen ahkerasti. Silti tietoturvaongelmia on edelleen runsaasti.

2.1 Tietoturva, turvallisuus ja tieto

Tietoturva on laaja käsite, joka voidaan määritellä monilla eri tavoilla. Yksi tapa tietoturvan määrittelyyn yrityksen näkökulmasta on nähdä se tietoisuutena ja ymmärryksenä siitä, että informaation riskit ja kontrollit ovat tasapainossa (Whitman & Mattord, 2012). Yrityksen näkökulmasta tärkeintä on se, että tiedon turvaamisen tarpeet ja liiketoiminnan tavoitteet ovat

linjassa keskenään ja kumpikaan ei ole toisen yläpuolella. Turvallisuuteen voidaan liittää seuraavat alueet: fyysinen turvallisuus, henkilöstön turvallisuus, operaatioiden turvallisuus, kommunikaation turvallisuus ja tiedon turvallisuus eli tietoturva. Toisaalta tietoturvaa voidaan analysoida monin eri tavoin kuten esimerkiksi CIA-mallin avulla, jossa lähdetään siitä, mikä on tiedon luottamuksellisuus eli Confidentiality, eheys eli Integrity ja saatavuus eli Availability. (Radl & Chen, 2005.)

On mahdollista argumentoida, että tällä hetkellä jokin näennäisen "arvoton" tieto voi olla kiusallista tai vaarallista jatkossa. Tietokantoja yhdistelemällä on mahdollista saada kokonaiskuva henkilön käyttäytymisestä, sijainnista, tuttavapiiristä tai henkilökohtaisista asioista. Whitman ja Mattord (2012) määrittelevät, että käsiteltävänä olevan tiedon arvo määrittää tietoturvan tarpeellisuuden. Tietoon liittyy myös ominaisuuksia, joista jokainen liittyy omalla tavalla tietoturvaan. Tiedon ominaisuuksia ovat myös osittain edellä mainitut saatavuus, tarkkuus, oikeellisuus, luotettavuus, eheys, hyöty ja omistajuus (Whitman & Mattord, 2012). Whitman ja Mattord nostavat myös esiin oman määritelmänsä tietojärjestelmän osa-alueista, joihin kuuluvat ohjelmat, laitteisto, tieto, ihmiset, toimintatavat sekä verkot eli kommunikaatio. Lisäksi tieto liikkuu sähköisessä äänestysjärjestelmässä eri tavoin riippuen järjestelmästä. Kuvassa 1 on esimerkki siitä, miten monia asioita tulisi huomioida, kun luodaan äänestysjärjestelmä. Äänestäjä jättää äänensä, jonka jälkeen ääni menee viranomaisen kautta äänestyksen hallintajärjestelmään. Tilanteesta lähtee tieto toiselle viranomaiselle, joka vie tiedon kolmeen eri tietokantaan, joista äänestystieto kulkee edelleen sekä äänestäjälle, uusiin tietokantoihin että kolmannelle viranomaiselle. Jokaisessa osa-alueessa on potentiaaliset tietoturvariskinsä teknisesti, jonka lisäksi eri määrä ihmisiä osallistuu prosessiin eri kohdissa. Nämä kaikki yhdessä - mihin ja millaista tietoa käytetään, mitä tietojärjestelmän osa-alueita prosessissa on, mitä miten tieto liikkuu - muodostavat laajan ja kompleksisen verkon, jossa jokainen solmukohta on mahdollinen tietoturvariski.



Kuva 1. Tiedon liikkuminen äänestysjärjestelmässä eri komponenttien välillä kuvattuna graafisesti. (Balzarotti et al., 2010)

2.2 Tietoturvauhat, -hyökkäykset sekä puolustautuminen

Whitman ja Mattord (2012) esittelevät useita tietoturvauhkia ja -hyökkäyksiä, jotka ovat jo uutisista tuttuja monelle meistä vaikkakin ovat teknisiä termejä. Eri tyyppisiä hyökkäyksiä ja tietoturvauhkia

ovat mm. virukset, madot ja troijalaiset, tekniset ongelmat, vakoilu sekä ns. social engineering, jossa yritetään vaikuttaa ihmisen käyttäytymiseen.

Tietoturva-alalla käytetään yleisesti John Viegan määrittelyä tietoturvan kuolemansynneistä, jotka toteutuessaan sovellusten kehitystyössä tekevät tietoturvan pitämisen kunnossa lähes mahdottomaksi (Whitman & Mattord, 2012). Kuolemansyntejä ovat mm. epäonnistuminen virheiden hallitsemisessa, datan tallentamiseen liittyvät vaikeuden tai tiedon vuotaminen ulkopuolisille. Huomioitavaa on, että tämä lista on julkaistu John Viegan kirjassa jo vuonna 2009 eli asiat on havaittu tätä ennen jo 2000-luvun alussa. Silti useat tietoturvaongelmat ovat edelleen olemassa.

Tietoturvaan on olemassa myös useita torjuntateknologioita, joista Whitman ja Mattord (2012) nostavat esiin palomuurit, VPN (Virtual Private Network), kulunvalvonta, virustorjunta, varmuuskopiointi, biometriset laitteet sekä kryptografia. Jokaisesta uhasta ja tietoturvateknologiasta on runsaasti tietoa tarjolla internetissä. Tässä tutkielmassa asiat esitellään otsikkotasolla, jotta lukija ymmärtää kuinka suuri määrä erilaisia uhkia on olemassa myös sähköisten äänestysjärjestelmien käyttöönotossa ohjelma-, laite- ja ihmistasolla.

Yksi tärkeimmistä keinoista puolustautumisessa tietoturvaongelmia vastaan on teknologian lisäksi ihmisten kouluttaminen sekä yhteiskunnan tasolla poliittiset päätökset ja käytännöt. Onkin todettu, että yksi suurimmista uhistamme on se, ettei valtion tasolla ole määritelty tietoturvakäytäntöjä, vaikka hienostuneiden hyökkäysten määrä kasvaa jatkuvasti. Erityisesti kriittiset järjestelmät tulisikin rakentaa tietoturvalliselle pohjalle eikä halvimmille yleiskäyttöisille pohjille. Tarvittaisiin käytännöt ja ohjeistukset, jossa yhdistyy ihmisten kouluttaminen, lainsäätäjien lisätyt resurssit, järjestelmien tietoturvallisempi kehittäminen, tietoturvan tutkiminen monitieteellisesti sekä luotettavuuden lisääminen palveluille yleisesti. (Spafford, 2009.)

3. Sähköisen äänestämisen tietoturvahaasteita

Sähköisessä äänestämisessä erityishaaste tulee siitä, että virheitä ei saisi tulla, sillä demokratiassa jokaisella on perustuslain mukaan äänioikeus. Äänestämisen tulisi siis olla valvottua, läpinäkyvää sekä käytännössä virheetöntä. Tämä luo haasteita sähköisen äänestämisen järjestämiselle.

Yksi uusia tietoturvahaasteita on skaalautuvuus. Äänestysjärjestelmä, joka on kehitetty toimivaksi pienessä ryhmässä, tuo uusia ongelmia, kun sitä kokeillaan suurten ryhmien äänestystilanteissa (Cubric & Jefferies, 2015). Cubricin ja Jeffersiesin mukaan elektronisen äänestämisen hyödyistä on tehty lukuisia tutkimuksia, mutta ne ovat nimenomaan keskittyneet pieniin ryhmiin, minkä vuoksi he keskittyivät tutkimuksessaan siihen, miten samat toimintatavat toimivat, kun siirrytään suurempiin ryhmiin. Suurissa ryhmissä kaikki opettajat tai äänestäjät eivät hallitse teknologiaa yhtä hyvin eikä teknologia tällöin aina säästä aikaa. Yllättävä havainto Cubricin ja Jefferiesin tutkielmassa oli myös se, että vaikka äänestysjärjestelmä olisi yksinkertainen, käytettävyysongelmia esiintyi silti aina myös opiskelijoiden kesken. Kaikki ihmiset eivät ole yhtä näppäriä, heillä voi olla fyysisiä rajoitteita, joita kaikkia ei ole huomioitu. Cubric ja Jefferies myös nostavat aiheellisesti esiin äänestäjien motivaation; Äänestäjillä ei välttämättä riitä motivaatiota varmistaa äänestyksen oikeellisuutta, jolloin vastuu esimerkiksi ääntenlaskun oikeellisuudesta ei aina soisi siirtyvän äänestäjälle itselleen. Tarvittaisiin lisätutkimusta myös ryhmien koosta sekä siitä, kuinka paljon tarvitaan pedagogisia taitoja tai miten vaikkapa äänestyksen kysymykset tai ehdokkaat kirjoitetaan oikeaan muotoon (mm. Cubric & Jefferies, 2015).

Simpson ja Storer (2018) puhuvat tutkielmassaan tämän hetken "kultastandardista" tutkijoiden keskuudessa, joita ovat äänestysjärjestelmät, joissa äänestäjä itse voi varmistaa, että hänen äänensä on laskettu. Tämä tarkoittaa sitä, että kun tällä hetkellä äänestämisestä voi jäädä esimerkiksi kuitti tai jokin muu todiste, jonka laite antaa äänestäjälle, kun ääni on annettu todisteeksi mitä hän äänesti, jatkossa vastaavan kuitin tai muun todisteen saaminen jäisi äänestäjän itsensä vastuulle. Tällainen järjestelmä asettaa korkeita vaatimuksia äänestäjille, joilta yhtäkkiä vaaditaan osaamista ja ymmärtämistä. Tästä seuraa aivan uudenlaisia tietoturva- ja käytettävyysongelmia. Kuitenkin lukuisat uudet järjestelmät ovat esitelleet tällaista äänestystapaa, jossa äänestäjä itse voi ilman kolmatta osapuolta varmistaa äänestämisen turvallisuuden erilaisin keinoin (esimerkiksi esitäytetyt äänestyskupongit, tai äänen varmistaminen kolmannen osapuolen avulla). Tavoite on ylevä; saadaan tehokas, tarkka ja läpinäkyvä äänestysmalli, turvallinen erillinen äänestysympäristö sekä äänen varmistamiseen että äänestämiseen käyttäen kryptografisia keinoja. Äänestäjä voi tarkistaa, että hänen äänensä on mennyt laskentaan tietoturvallisesti ja anonyymisti myöhemmin erillisellä salausavaimella vaikka kotoa käsin. Tämä on tuonut uusia edellä mainittuja tietoturvaongelmia äänestämiseen sekä kohtuuttomia vaatimuksia yksittäiselle tietotekniikkaa osaamattomalle henkilölle oman äänestämisensä varmistamiseen. (Simpson & Storer, 2018.)

Vuonna 2004 yhtenä tietoturvaa parantavana vaihtoehtona pidettiin erillisiä äänestyslaitteitta (direct recording electronic voting systems DRE). Mutta vaikka laite rakennettiin varta vasten äänestämistä varten, niitä tutkittaessa on huomattu, että niihinkin on eksynyt sekä bugeja että tietoturvaongelmia (Bannet et al., 2004). Näissäkin laitteissa on painotettu käytettävyyttä kenties muiden seikkojen kustannuksella. Jo vuonna 2004 on ehdotettu, että sähköinen äänestäminen ei korvaa paperiäänestämistä, vaan sen sijaan se voi tuoda siihen joko laajennuksia tai apukeinoja, sillä esimerkiksi paperiset kuitit ovat edelleen tehokas tapa varmentaa ääni jälkeenpäin. Bannetin ja kumppaneiden tutkielmassa mielenkiintoista on se, että heidän Hack-a-vote -järjestelmä oli tutkijoiden itse rakentama järjestelmä, joka tehtiin tietoturvaa silmälläpitäen. Silti siinäkin huomattiin tietoturvaongelmia, koska se sekä ohjelmat että laitteet ovat edelleen universaaleja

ongelmineen. Bannet kumppaneineen toteaakin, että ongelmien riski vain kasvaa, jos sähköinen äänestäminen yleistyy.

Culnane kumppaineen (2015) kehitti Pret-a-voter -äänestysympäristöstä oman itsenäisen äänestysjärjestelmän nimeltään vVote (Kuva 2). vVote-järjestelmässä äänestäjä käyttää äänestyslaitetta ja äänestämisestä tulee sekä tieto yksityiselle verkkosivulle (WBB, Web Bulletin Board) että kuitti äänestäjälle. Äänestyskuitti viedään edellään sekä elektroniseen äänen merkitsijään että tietokantaan josta tarvittaessa äänen voi varmistaa. Äänen merkitsemisen jälkeen äänestä kulkeutuu sekä yksityiseen tietokantaan että kuitiksi äänestäjälle. Äänen voi myös perua. vVotea käytettiin oikeassa äänestystilanteessa Australiassa, ja heti kun tutkimusympäristössä tehty äänestysjärjestelmä vietiin käytäntöön, seurasi lukuisia ongelmia. Tutkielma käy läpi useita käyttäjäkokemuksia, joiden pääviestinä voidaan pitää sitä, että moni teoriassa hyvä asia osoittautuu käytännössä paljon vaikeammaksi. Lisäksi monia asioita ei edes ole osattu raportoida tieteellisesti etukäteen ennen kuin asiat käytännössä nähdään, mikä yllättää tutkijoita toistuvasti. Tämä tuo uudenlaisen ongelman sähköisen äänestyslaitteen kehitystyöhön; pitäisi olla tapa testata järjestelmää suuressa mittaluokassa, koska valtakunnallinen äänestys tehdään jopa satojen miljoonien - jopa miljardien - ihmisten välillä. Sellainen testiympäristö ei ole missään olemassa, mikä tuo esiin kysymyksen siitä, pitäisikö sähköistä äänestämistä esitellä kansalle pieni pala kerrallaan. Kun yhtäkkiä muutetaan satoja vuosia vanha äänestysjärjestelmä toisenlaiseksi, tulisi ottaa huomioon, että ihmiset tarvitsevat erilaisia "sisäänajoaikoja" helppokäyttöiselle paperiäänestämiselle. Sähköistä äänestämistä voisi siis esitellä siten että se hoitaa jonkin osan äänestämisestä - vaikka kuitin tulostamisen todisteena äänestämisestä - eikä koko äänestämistä kerralla.

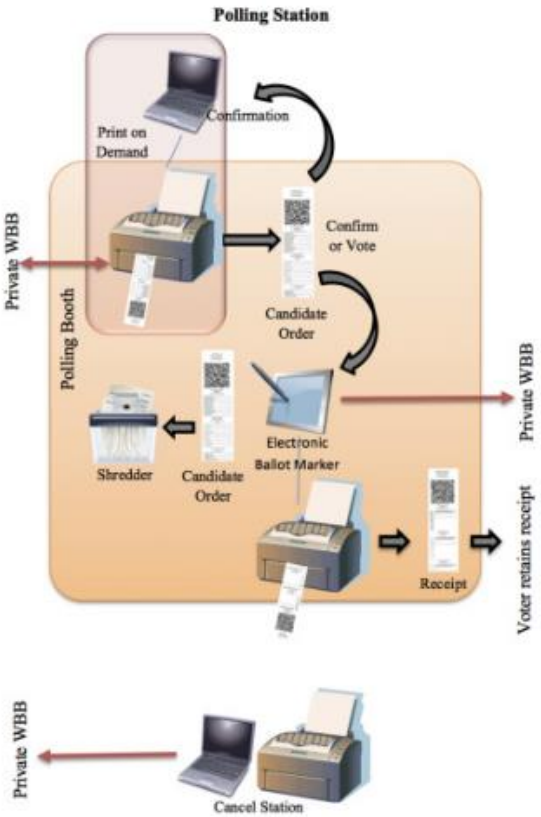


Fig. 2. Station process.

Kuva 2. vVoten sähköinen äänestysjärjestelmä kuvattuna graafisesti (Culnane et al., 2015)

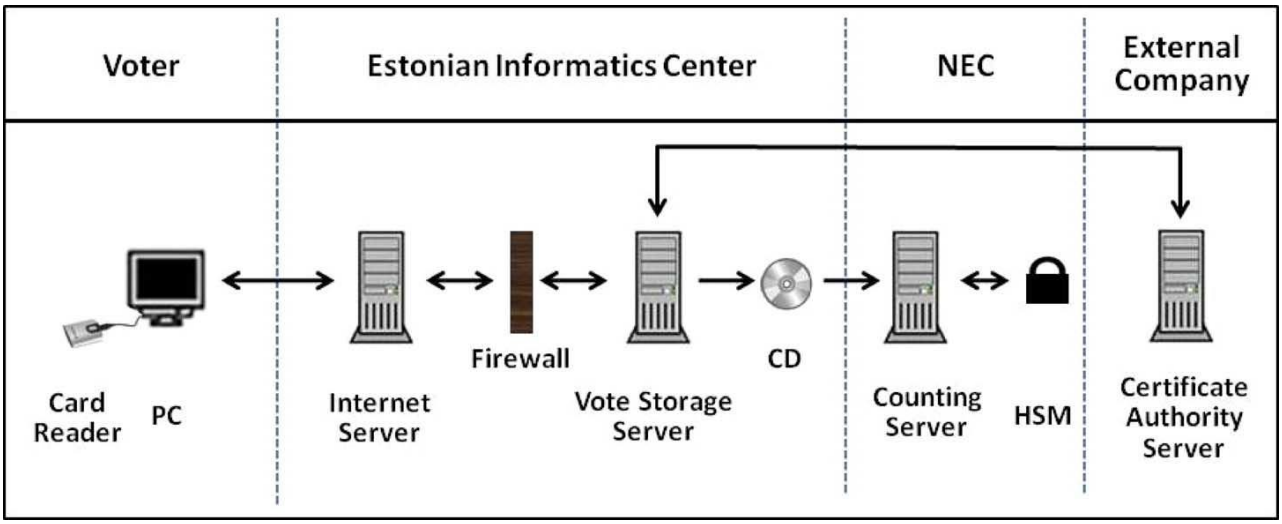
Japanissa vuonna 2008 käytiin läpi kaikki markkinoilla olevat elektroniset äänestysjärjestelmät ja tehtiin niistä tietoturva-analyysi (Hisamitsu & Takeda, 2008). Teknisesti edistyksellisessä maassa huomattiin, että tietyn käyttöjärjestelmän, ohjelmiston tai laitteen tietoturvan rinnalla on myös suurempi ongelma: operationaalisen prosessin tietoturva (vaikkakin järjestelmienkin tietoturvaa tulisi kehittää paljon). Pääriskinä nähtiin mm. se, että kaikkien järjestelmien ja koneiden kaikkia ohjelmia ei voida tarkistaa, äänestystyöntekijät voivat päästä järjestelmiin käsiksi ja äänen oikeellisuuden varmistus puuttuu (Hisamitsu & Takeda, 2008). On siis kokonaan oma tietoturvalukunsa, miten ihmiset käyttävät tietojärjestelmiä; jos sähköinen äänestäminen halutaan järjestää, laitteiden ja ohjelmistojen tietoturvan lisäksi niitä käyttää useita eri sidosryhmiä: äänestäjät, viranomaiset, äänten laskijat, äänten raportoijat mediassa, poliitikot, IT-osapuolet ja niin edelleen. Jokaisen ihmisryhmän pitää itse omata riittävät tiedot ja taidot oman osuutensa hoitamiseen. Lisäksi ihmisryhmien välisen kommunikaation tulee toimia moitteettomasti. Tämä kaikki tulisi myös jollain tavalla varmistaa, siitä pitää jäädä lokitiedot ja kaikki tulee salata. Äänestysprosessi on oma suuri osa-alueensa, johon liittyy useampi tieteenala tietojenkäsittelytieteen lisäksi.

Tietoturvaongelmat johtuvat usein myös internetin ja ihmisten luonteesta, PC:n arkkitehtuurista ja sovellusten rakenteesta eikä niitä voida sivuuttaa yksittäisellä tietoturvallisella laitteella tai sovelluksella (Weldemariam et al., 2007). Lisäksi on olemassa useita proseduraalisia riskejä ja uhkia itse sähköisessä äänestämisessä, ei niinkään järjestelmissä tai teknologiassa vaan ihmisissä ja organisaatioissa. Weldemariam et al. (2007) toteavatkin, että tietoturvan kehittäminen on jatkuva prosessi, jota pitää kehittää ja kehitetään alituiseen. Tässä tarkoitetaan nimenomaan prosessia, johon yhtenä osana kuuluvat myös laitteet ja ohjelmat. Äänestysprosessi sisältää jopa useita laitteita, verkostoja ja järjestelmiä, joita hallitsee suuri joukko eri organisaatioita, ihmisiä ja kansalaisia. Tämä luo toisenlaisen tietoturvahaasteen, joka vielä moninkertaistuu, jos siirrytään itsenäisistä äänestyslaitteista online-äänestämiseen, koska kotikoneet ovat paljon heterogeenisempi ryhmä laitteita eri ohjelmistoineen ja tietoturvaversioineen.

Jefferson kumppaineen (2004) kuvaa kattavasti, kuinka jättikonsulttiyhtiö Accenture ja Yhdysvaltain puolustusministeriö tekivät yhteishankkeen nimeltään SERVE (The secure electronic registration and voting experiment). Hankkeessa tutkittiin internettiin ja etä-äänestämiseen liittyviä riskejä. Oleellisia löydettyjä asioita olivat se, että äänestämisen muuttaminen perinteisestä sähköiseen sisältää haasteita sosiaalisesti, teknologisesti, proseduaalisesti ja riskisesti. Ihmiset ovat tottuneet tietynlaiseen käyttäytymiseen ja toimintamalleihin äänestyspäivänä, jotka nyt muuttuisivat. Ihmisten teknologinen osaaminen ei myöskään ole samalla tasolla, eikä voida olettaa, että kaikki erityisryhmät omaksuvat proseduurit sataprosenttisella varmuudella. Tämä kaikki luo siis riskejä uudessa äänestystilanteessa. Lisäksi tällä hetkellä ei ole näköpiirissä, että internet-äänestäminen voisi olla tietoturvallista, koska hyökkäys voi tulla mistä päin maailmaa tahansa eikä sitä välttämättä edes havaita. Huomioitavaa on myös löydös, jossa tietoturvaongelmia ei voitu korjata päivityksinä itse SERVE-järjestelmään, vaan ne ovat fundamentaalisia ongelmia itse internetin arkkitehtuurissa sekä tietokoneen laitteiden ja sovellusten rakenteissa kaikkialla läsnäolevana (Jefferson et al., 2004). Vaikka SERVE oli itsessään kohtuullisen turvallinen laite, näkyvimpiä ongelmia siinä itsessään oli silti äänestäjän varmistus oman äänen jättämisestä, sisäiset hyökkäykset, yksityisyys, äänien ostaminen tai myyminen sekä lukuisat tekniset haavoittuvuudet.

Yhtenä päähaasteena tutkimus tuo esiin internet-äänestyksessä hyvän näkökulman; äänestysviranomaisilla ei ole kontrollia äänestäjien käyttämiin laitteisiin tai ohjelmiin. Jefferson et al. (2004) mainitsevat, että kirjoitelmassa ei ollut edes tilaa kaikille ongelmille, joita löydettiin, joten esiin nostettiin vain muutama mahdollinen hyökkäys, joita voidaan tehdä kaikkialta maailmasta ja jotka voivat usein jäädä selvittämättä, kuka hyökkäsi ja mistä. Lopputuloksena sekä internet-äänestys että SERVE-järjestelmä eivät ole turvallisia tapoja järjestää äänestyksiä (Jefferson et al., 2004).

Samanlaisia esimerkkejä äänestysjärjestelmien heikkouksista on ympäri maailmaa. Viro oli maailman ensimmäinen maa, joka piti valtakunnanlaajuisen äänestyksen ja tänä päivänä kolmasosa äänestyksistä on sähköisiä. Kuvassa 3 esitellään Viron äänestysjärjestelmä. Siinä äänestäjä käyttää äänioikeuttaan tietokoneellaan, tunnistautuu koneelle omalla kortillaan, minkä jälkeen ääni rekisteröityy internet-palvelimille. Tämän jälkeen ääni varmennetaan palomuurien kautta viralliselle äänestyspalvelimelle, joka kommunikoi kolmannen osapuolen varmennuspalvelimen kanssa. Lisäksi äänistä otetaan varmenne CD:lle, joka kuljetetaan erikseen vielä yhdelle palvelimelle, jossa äänet lasketaan ja äänestystulos "lukitaan". Springall et al. (2014) analysoivat tutkimuksessaan tuota äänestystä tietoturvan kannalta.



Kuva 3. Viron äänestysjärjestelmä (Schryen & Rich, 2009)

Raportissa käytiin läpi tietoturvaa tarkkailijoiden, koodin tarkistuksen ja eri testien yhdistelmänä. Lopputuloksena huomattiin, että sähköisen äänestämisen arkkitehtuurissa on vakavia rajoitteita ja epäyhtenäisiä toimintatapoja, jotka vaarantavat järjestelmän laillisuuden. Verrattuna muihin online-palveluihin kuten kauppaan tai pankkiyhteyksiin, äänestämisessä ei saa tulla ongelmia, tarkkuus on oltava moitteetonta ja anonymiteetin pitää säilyä (Springall et al., 2014). Sähköisen äänestämisen suunnitteluvaiheessa oli tehty muutamia kompromisseja, kuten keskusservereiden käyttö, joita ei edelleenkään ole muutettu, vaikka se on selkeä riski. Tänä päivänä hyökkäysten määrä ja tavat ovat moninkertaistuneet myös tuota rakennetta kohtaan. Lisäksi löytyi useita tapoja rikkoa sekä teknologiaa että menettelytapoja ja täten manipuloida äänestyksen lopputulosta. Huomioitavaa on, että nykyisen geopoliittisen tilanteen lisäriskit yhdistettynä teknisiin tietoturvaongelmiin, raportti ehdottaa lopuksi, että Viro luopuu sähköisestä äänestysjärjestelmästään. Vaikka tietoisesti vastattaisiin jokaiseen tietoturvauhkaan, sellaisen järjestelmän monimutkaisuus ei ole kenenkään hallittavissa; raportin tekijät eivät usko, että tänä päivänä voidaan vielä tehdä täysin turvallista sähköistä äänestysjärjestelmää. (Springall et al., 2014.)

Tiedemaailma on myös esittänyt yleisen tason kysymyksen siitä, onko internet-äänestäminen uhka vai mahdollisuus demokratialle. Luottamus demokratiaan saattaa vähentyä, koska ihmisillä ei ole samalla tavalla pääsyä "järjestelmään" kuin perinteisessä äänestämisessä, kun kaikki katoaa koodien ja servereiden taakse. Tämän lisäksi perinteisellä äänestämisellä on satojen vuosien historia, jolloin luottamuksen saaminen saattaa kestää uudelle äänestystavalle. (Springall et al., 2014.) Lisäkysymyksiä on myös se, kuinka estää "perheäänestäminen" kotoa käsin tai äänien ostaminen. Kuten edelläkin mainittiin, kotikoneilla voi myös olla viruksia tai troijalaisia johtuen

päivittämättömistä virustorjuntaohjelmistoista ja monista muista uhkista, joihin henkilö saattaa törmätä surffatessaan internetissä, saadessaan sähköpostia ja niin edelleen. Samassa artikkelissa mietitään myös sähköiseen äänestämiseen liittyviä usein mainostettuja hyötyjä; Springall kumppaneineen ei usko, että äänestysprosentti nousisi sähköisen äänestämisen myötä.

Edellä mainittu E2E -äänestäminen, jossa äänestäjä itse voi ilman kolmatta osapuolta varmistaa äänestämisen turvallisuuden erilaisin keinoin, on yksi uusia teorioita. Eräs tällainen järjestelmä on esitelty Kiayiasin et al. artikkelissa (2017). E2E-järjestelmässä äänestäjä antaessaan äänen saa siitä kuitin tietyllä autentikointikoodilla ja hän voi käyttää tätä kuittia ja autentikointikoodiaan myöhemmin äänensä varmistamiseen missä tahansa tilanteessa. Kiayuis et al. (2017) esittelevät tavan varmistua oman äänen oikeellisuudesta ilman, että äänestäjän tietokonetta tarvitsee salata. Äänestäjä saa äänestään "kuitin", jolla ääni voidaan varmistaa myöhemmin. Kiayuisin et al. (2017) mukaan myös tämä äänestystapa on saanut kritiikkiä osakseen, mutta sitä voidaan pitää tämän hetken "turvallisimpana" ja suosituimpana sähköisen äänestämisen mallina. Kysymys lienee, riittääkö tämä vai olemmeko vasta matkalla kohti turvallista sähköistä äänestämistä, kuten ylivoimaisesti suurin osa artikkeleista pohtii. Uusia järjestelmiä siis kehitetään ja asiat paranevat hitaasti.

Vaikka haavoittuvuuksia on löydetty runsain mitoin, tiede on yrittänyt kehittää uusia järjestelmiä ja myös esitellyt useita tietoturvallisempia äänestysprotokollia viimeisen kymmenen vuoden aikana. Moran kumppaineen (2016) kertoo, että kaikista järjestelmistä on löydettävissä heikkouksia usein jo siksi, että järjestelmät ovat monimutkaisia ja kattavaa analyysia on tällöin vaikea tehdä. Moran et al. on keskittynyt kahteen äänestysjärjestelmään, jotka lupaavat turvallisuutta ilman salausta ja silti täyttä anonymiteettia. Järjestelmät ovat nimeltään ThreeBallot ja VAV. Tutkimuksessa huomattiin, että yksi tärkeistä oletuksista näissä järjestelmissä - nimeltään short ballot assumption (SBA) - on hyvin epämääräisesti määritelty kirjallisuudessa. Yksinkertaistettuna SBA tarkoittaa sitä, että tiedon määrä tulisi olla äänestyksissä olla minimissään. Mitä enemmän ihminen joutuu "täyttämään kuponkia", sitä enemmän hänen käyttäytymistään tai ryhmien käyttäytymistä voidaan analysoida. Sosiaalisesta mediasta tuttua käyttäjien analysointia voidaan siis harjoittaa myös äänestystilanteissa, joka on ristiriidassa anonymiteetin kanssa. Äänestäjistä voidaan siis päätellä asioita perustuen hänen käyttäytymiseensä. Tämä luo aivan uuden tietoturvariskien kentän, johon liittyy käyttöliittymäsuunnittelu, ihmisten käyttäytymiseen liittyvät tieteet ja big data -analyysi.

Yhtenä tietoturvallisempana äänestystapana voidaan pitää perinteisen äänestämisen ja sähköisen äänestämisen yhdistelmää. Saksassa kokeiltiin vuoden 2008 äänestämisessä ns. sähköistä kynää. (Arzt-Mergemeier et al., 2008.) Digitaalinen äänestyskynä on mahdollisimman lähellä perinteistä äänestämistä, jossa sähköinen kynä tallentaa äänestystuloksen. Sähkökynää kokeiltiin 667 äänestäjän kanssa Hampurin vaaleissa ja sitä käytettäessä kuitenkin huomattiin, että vaikka järjestelmä olisi yksinkertainen ja hyvin lähellä perinteistä äänestystä, tekninen tuki on silti välttämätöntä. Yhtään teknistä ongelmaa ei saa tulla, sillä jokainen äänestys on tärkeä. Konferenssijulkaisu toi silti mielenkiintoisen uuden näkökulman, jossa voitiin pohtia, voisiko elektroninen äänestäminen toimia jonkin osa-alueen hoitajana, joka vaatii asioita, jossa tietokone on hyvä, esimerkiksi laskemisessa, eikä silti muuta koko järjestelmää toisenlaiseksi, mikä on kansalaisille suurempi kynnys. Jatkotutkimusajatuksena esitettiin, että äänestyksen seurauksia pitäisi tutkia lisää nimenomaan teknologian ulkopuolella; miten ihmiset ja yhteiskunta asian ottaa vastaan. (Arzt-Mergemeier et al., 2008.)

Rivest ja Stark (2017) pohtivat artikkelissaan aiheellisesti sitä, voiko mihinkään äänestyksiin luottaa. Tärkein kysymys heidän mukaansa on se, mitä todisteita äänestysjärjestelmä tuottaa siitä, menikö äänestys oikein ja miksi meidän pitäisi uskoa sitä. On hienoa nähdä, että paljon tutkimusta tehdään turvallisen sähköisen äänestämisen puolesta ja monia lupaavia avauksia on tehty (mm. STAR-Vote System Travis Countyssa, End-to-End Verifiability useammassa uudessa järjestelmässä), mutta silti internet-äänestys on vasta kaukainen haave, koska itse internet on

haavoittuvainen. Äänestämisellä on rajuja vaatimuksia luotettavuudelle, samaan aikaan äänestämisen pitäisi kuitenkin olla yksinkertaista, joten aina kun uusi järjestelmä esitellään, tulee kysymys äänestyksen luotettavuudesta esittää. (Rivest & Stark, 2017.) Perinteinen satavuotinen äänestystapakin aiheuttaa aika ajoin ongelmia luotettavuuden puolesta johtuen yhteiskunnan rakenteista ja valtasuhteista. Monissa maissa ei edes olla demokraattisesti valmiita täysin läpinäkyvään äänestämiseen. Jos siirryttäisiin sähköiseen äänestämiseen, idea on kannatettava helppouden ja läpinäkyvyyden osalta, mutta ongelmaksi tulee edellä mainitut jatkuvat haasteet yleisesti ohjelmistojen ja laitteiden sekä internetin turvallisuuden puolella. Äänestysjärjestelmät eivät ole erillinen saareke, vaan ne rakentuvat samoilla tietokoneen osilla ja ohjelmointikielillä sekä tietoliikenteen rakenteilla kuin muutkin. Äänestysprosessi on myös oma lukunsa.

Tulevaisuutta on aina ollut vaikea ennustaa erityisesti suurten massojen kohdalla. Muutamia seikkoja voidaan kuitenkin huomioida lähteiden ja tutkimuksen kautta. DEF CON konferenssi vuonna 2018 esitteli toisen kerran ns. "Voting Villagen". Joka vuosi tämä alan jättimäinen tietoturvakonferenssi kutsuu koolle tuhansia valkohattuhakkereita, jotka yrittävät murtaa tärkeiden teknologioiden tietoturvaa, ja kahden vuoden ajan yhtenä huoneista on ollut pyhitetty pelkästään äänestysjärjestelmille. Vielä hetki sitten viranomaisten pääfokus elektronisessa äänestämisessä oli turvata erilliset äänestyslaitteet. Tänä päivänä hyökkäykset tulevat laajemmalla rintamalla, jolloin pitää turvata äänestäjien rekisteröitymistietokanta, valtioiden äänestysjärjestelmien hallintatietokanta, äänestysillan raportoinnin tietokannat, valtion hallitusten ja paikallispoliitikkojen sosiaalinen media ja väärän levitetyn tiedon estäminen äänestäjille muutamia mainitaksemme. (Blaze et al., 2018.) Alex Pardilla, Californian valtiosihteeri, avasi viime vuoden DEF CONin, jossa äänestysjärjestelmiin todella panostettiin suuremmin kuin koskaan. DEF CON Voting Villagen raportissa (Blaze et al., 2018) tilannetta kuvataan siten, että äänestämisympäristöön liittyy paljon äänestäjän rekisteröitymisestä äänestysillan äänten laskentaan, eli paljon ihmisiä ja laitteita välissä. DEF CONinlla oli iso määrä äänestyslaitteita, viranomaisia, laitteistoja, prosesseja ja raportteja käytössään Voting Villagessa, jonka jäseniin kuuluu hakkereita, tietoturva-ammattilaisia, journalisteja, lakimiehiä, tiedemiehiä ja paikallisia viranomaisia.

Lopputuloksena saatiin hämmästyttävä määrä tietoturvaongelmia, jotka edelleen ovat olemassa kaikissa äänestysjärjestelmissä, jotka ovat käytössä Yhdysvalloissa tänä päivänä. Osa ongelmista on löydetty jo aiemmin, osa löydetyistä olivat uusia. Kysymyksiä herättää, miksi vanhoja ongelmia ei ole korjattu. Tietoturvattomia äänestyslaitteita löytyi kymmenistä osavaltioista, hakkerointia pystyi tekemään nopeimmillaan 2 minuutissa suoraan äänestyskopista käsin ja myös etänä. Raportissa käydään läpi useita sivuja laite- ja ongelmakohtaisia tietoturvahäiriöitä ja lisäksi annetaan kriisiviestintäneuvoja.

Vaikka haavoittuvuuksia oli kymmeniä, raportti nostaa esiin neljä pääongelmaa: logistiikkaketju, etäyhteydet, hakkeroinnin nopeus ja se, että löydettyjä tietoturva-aukkoja ei korjata. Lopuksi annetaan neljä ehdotusta: kongressin tulee huolehtia siitä, että löydetyt tietoturva-aukot korjataan, äänestysturvallisuuteen pitää investoida, kriisiviestintäsuunnitelma tehtävä ja kongressin pitää ymmärtää asian vaarallisuus. (Blaze et al., 2018.)

Toinen löytö viime ajoilta on laitteiden (erityisesti prosessorien) tietoturva. Kaikkien valmistajien prosessoreissa on tietoturva-aukkoja sekä toiminnallisuuksia, joita ei selitetä arkkitehtuurimanuaaleissa. (Domas, 2017.) Yritykset haluavat pitää tietoja itsellään, joten emme tiedä käytetäänkö laitteiden aukkoja hyödyksi valtiotasolla, yritystasolla vai käytetäänkö mihinkään, koska ne ovat suljettuja ohjelmistoja.

On myös olemassa kattava määrä jo dokumentoituja tietoturvaongelmia, joita ei edelleenkään ole korjattu kaikkialla kuten edellä mainittiin, koska ei ole kaiken kattavaa standardia vaikkapa nettisivuille. Yksi haavoittuvuuksista, joka löydettiin jo 2000-luvun alussa on ns. SQL-injektio. Se on edelleen yksi kaikkein vaarallisimmista uhista; joka päivä tuhannet verkkosivut ovat

hyökkäyksen alla, koska sivut suunnitellaan tietoturvattomasti. Suunnittelijoiden olisi hyvä saada edes jonkinlainen peruskoulutus tietoturvalliseen koodaukseen eikä keskityttäisi kiireessä vain näyttävyyteen tai käytettävyyteen. (Gudipati et al., 2016.) Näemme uutisissa jatkuvasti, miten myös Suomeen koulutetaan 12-viikkoisella ohjelmalla internet-koodareita tekemään Javascriptillä sivuja mainostajille. Gudipatin et al. (2016) artikkelin myötä herää kysymys, onko 12 viikkoa riittävä aika oppia tietoturvallisen koodauksen alkeet. Laajemmin kysyttynä, riittääkö tietoturva-aukkojen etsiminen turvalliseen sähköiseen äänestämiseen, vai tarvitsemmeko myös rakenteellisia ja asenteellisia muutoksia ylätasolla laite- ja ohjelmakantaan sekä ihmisten käyttäytymiseen.

4. Pohdinta

Tutkielmassa on käyty läpi sähköisen äänestämisen tietoturvaongelmia tutkimusten ja dokumentoitujen käytännön kokeilujen kautta. Taulukossa 2 on koottu oleellisimmat tietoturvahaasteet, joita kirjallisuuskatsauksessa löydettiin.

Taulukko 2. Sähköisen äänestämien tietoturvahaasteita.

Haasteet	**Lähteet**
Skaalautuvuus	Cubric & Jefferies, 2015; Culnane et al. 2015
Äänestäjän tietotaidot, ohjelmistot ja laitteet	Simpson & Storer, 2018; Cubric & Jefferies, 2015; Jefferson et al., 2004; Springall et al., 2014
Itsenäiset äänestyslaitteet, kotikoneet ja tietokannat	Bannet et al., 2004; Jefferson et al., 2004; Blaze et al. 2018; Arzt-Mergemeier et al., 2008; Domas, 2017
Äänen varmistaminen	Kiayias et al., 2017
Äänestysjärjestelmän luotettavuus	Rovest & Stark, 2017; Springall et al., 2014
Yksityisyys, tiedon tarkkuus ja tekniset ongelmat	Jefferson et al., 2004; Springall et al., 2019; Moran et al., 2016
Eettisyys	Blaze et al., 2018; Springall et al., 2014
Tietoturvaosaamisen puute ja yhteiskunnalliset haasteet	Blaze et al., 2018; Gudipati et al., 2016

Kuvaavaa aiheen ongelmallisuudelle on se, että lähes kaikissa lähteissä joko pohdintana tai jatkotutkimusehdotuksena tuotiin esille, että turvallista tapaa äänestää sähköisesti ei ole. Ongelma näyttäisi olevan se, että sähköisen äänestämisen järjestelmät sisältävät samoja laitteita ja ohjelmistoja, joita tehdään samalla tavalla kuin kaikkia muitakin elektronisia komponentteja tai ohjelmoidaan ohjelmia. Lisäksi online-äänestämiseen liittyvät ongelmat ovat samoja kuin internetin ongelmat yleisesti. Jotta voitaisiin tehdä turvallinen äänestäminen kaikille, meillä pitäisi olla mahdollisuus tarkistaa jokaisen henkilön henkilökohtaisten laitteiden tietoturvallisuus, mikä on tehtävänä haasteellinen. Äänestämiseen liittyy myös suuri määrä järjestävää tahoa, joiden koulutus ja käytännön äänestystilanteen osaaminen olisi pystyttävä tarkistamaan. Jokaisen äänestäjän olisi myös osattava käyttää laitetta eli sen tulee olla käytettävyydeltään yksinkertainen. Kuitenkin tietoturvallisen laitteen tai ohjelmiston rakentaminen vaatii hyvinkin monimutkaisia järjestelmiä ja

ohjelmistoja, jotka eivät anna 100-prosenttista tietoturvaa tänä päivänä. Emme voi myöskään olettaa, että jokainen kansalainen osaa käyttää näitä laitteita tai ohjelmistoja.

Huomioitavaa lähdekirjallisuudessa on myös se, että jo 2000-luvun alussa löydettyjä tietoturvaongelmia ei ole edelleenkään korjattu kaikissa tapauksissa. Tämä osaltaan kertoo siitä, kuinka monisyisestä ongelmasta on kyse jo yhteiskunnallisella ja taloudellisella tasolla. Eri lähteissä on tutkittu aihetta monesta eri kulmasta laadullisesta haastattelututkimuksesta määrällisiin kyselyihin (Cubric & Jefferies, 2015) sekä konstruktiivista tutkimusta, jossa rakennetaan uusi järjestelmä ja testataan sen toimivuutta (Jefferson et al., 2014). Lähes kaikkien tutkimusten lopputulema on se, että turvallista sähköistä äänestysjärjestelmää ei tällä hetkellä ole.

Kirjallisuudesta löytyy useita tietoturvahaasteita, jotka on koottu Taulukossa 2. *Skaalautuvuudella* tarkoitetaan äänestysjärjestelmän kasvattamista pienestä ympäristöstä suurempaan. Kun sähköinen äänestysjärjestelmä viedään pienestä testiympäristöstä suurten massojen käyttöön, tulee useita aiemmin näkemättömiä ongelmia, koska suuri massa ihmisiä ei käyttäydy samoin kuin pienempi massa.

Äänestäjien tietotaidot, ohjelmistot ja laitteet viittaa siihen, että äänestäjällä on oltava tietyt tietotekniset ja tietoturvaan liittyvät perustaidot sekä tekniset valmiudet, jotta sähköinen äänestäminen olisi turvallista. On aina huomioitava, että kaikki tavalliset ihmiset eivät ole jatkossakaan tietoteknisesti eteviä vaikka tekniikka edistyykin yhteiskunnassa. Tämä tuo uuden kentän tietoturvaongelmia, joita kaikkia ei osata vielä ennakoida.

Sähköistä äänestämistä voidaan tehdä myös *itsenäisillä äänestyslaitteilla*, jotka on tehty ja joita käytetään vain sähköiseen äänestämiseen. Näillä laitteilla (ja niiden tietokannoilla) on samat tietoturvahaasteet kuin kaikilla muillakin standardoimattomilla sulautetuilla järjestelmillä kuten lääketieteenkin puolella; olisi löydettävä yksi yhdessä sovittu tapa ja järjestelmä, joilla äänestäminen suoritetaan tietoturvallisesti. Äänestyksen voi myös tehdä kotikoneiden avulla.

Kriittisissä järjestelmissä kuten sähköisessä äänestämisessä, *äänen varmistaminen* on tärkeää. Itse äänestämisen tulee olla läpinäkyvää ja virheprosentti tulee olla nolla, koska demokratiassa kaikilla on oikeus äänestää. Olisi siis luotava äänestysjärjestelmä, jossa äänestäjä voi itse varmistaa äänensä menemisen läpi järjestelmään missä tahansa vaiheessa. *Äänestysjärjestelmään tulee pystyä myös luottamaan.* Sen tulee olla läpinäkyvä ja valvottu kaikissa tilanteissa.

Yksityisyys, tiedon tarkkuus ja tekniset ongelmat tarkoittaa sitä, että jokaisella äänestäjällä on oikeus anonymiteettiin äänestystilanteessa. Hänen on myös pystyttävä äänestämään helposti eli äänestystiedon tulee olla tarkkaa valintatilanteessa. Lisäksi äänestämisestä mentävä tieto tulee mennä tarkasti sille tarkoitettuun paikkaan. Äänestystilanne sisältää monia kohtia, joissa tekniset ongelmat voivat tuoda haasteita yksityisyydelle ja tiedon tarkkuudelle.

Tulevaisuutta pohtiessa nousee kysymys, onko olemassa luotettavaa äänestysjärjestelmää tai voiko sellaisen kehittäminen olla mahdollista. *Äänestämisen eettisyys, tietoturvaosaamisen puute sekä yhteiskunnalliset haasteet* kuten SOME-käyttäytyminen ovat asioita, joihin meidän on hyvä kiinnittää huomiota tulevaisuudessa, kun mietimme sähköistä äänestämistä. Emme ole vielä tehneet internetistä tai kaikista teknisistä laitteistamme sataprosenttisen tietoturvallisia, myöskään ihmiset eivät ole täysin virheettömiä. Joten jos tehtävänä on luoda sähköinen äänestämistilanne, jossa jokainen ääni lasketaan virheettömästi, se on tehtävä, joka sisältää runsaasti haasteita.

5. Johtopäätökset

Tietoturvallisen sähköisen äänestämisen haaste on mittava. Äänestämiseen liittyy useita sidosryhmiä, kuten äänestyksen rakentajat (laitteet ja ohjelmat), äänestyksen järjestäjät (poliitikot, viranomaiset, vapaaehtoiset) ja äänestäjät. Äänestämisen pitäisi olla helppoa ja intuitiivista, jotta äänestysprosentti ei romahda ja kaikki osaavat tehdä kansalaisvelvollisuutensa helposti. Toisaalta tietoturvan pitäisi olla kunnossa, jotta saavutetaan 100-prosenttinen luotettavuus. Erilaisia pullonkauloja on runsaasti aina kouluttamisesta tietoliikenteeseen, prosessien osaamisesta ohjelmien käytettävyyteen. Johtopäätöksenä tutkimusten perusteella voidaan sanoa, että emme ole vielä siellä asti, jossa yksikään maa voisi siirtyä täysin sähköisen äänestämisen pariin. Se voiko sähköisen äänestämisen jokin osa-alue olla mukana äänestyksessä–kuten vaikkapa sähköinen äänestyskynä (Arzt-Mergemeier, 2018)– on varmasti mahdollista. Lisätutkimusta kuitenkin tarvitaan sekä ohjelmisto- että laitepuolella siitä, miten voidaan rakentaa sellainen tietoturvallinen ympäristö, joka on riittävän yksinkertainen käytettäväksi. Lisäksi muilta tieteenaloilta tarvittaisiin avauksia sille, miten suurten massojen opettaminen uusien järjestelmien käyttämiseen voitaisiin järjestää järkevästi. Olisi myös huomioitava erityisryhmät, kuten liikuntarajoitteiset ja monet muut, koska äänestäminen on jokaisen kansalaisvelvollisuus.

Tätä kirjallisuuskatsausta voi käyttää kokonaiskuvan saamiseen aiheen tämänhetkisestä tutkimuksesta. Se käsittelee parikymmentä tutkimusta viimeisen kahdenkymmenen vuoden ajalta ja pureutuu sekä olemassa oleviin että uusiin uhkiin ja mahdollisuuksiin. Uusina tutkimusimplikaatioina voisi olla miten tavallinen ihminen otetaan mukaan sähköisen äänestämisen suunnittelemiseen. Voidaan pohtia liittyvätkö sähköisen äänestämisen ongelmat siihen, että meiltä puuttuvat standardit ja hyvät käytännöt vai onko tavallinen ihminen vielä liian kaukana teknisesti sähköisestä äänestämisestä. Äänestäminen on demokratian ydin ja sen pitäisi olla helppoa, virheetöntä ja läpinäkyvää. On kysyttävä, onko meillä kaikki tieto ja taito teknisen osaamisen lisäksi kasvatustieteellisessä mielessä ja onko yhteiskuntamme valmis siirtymään äänestyskopeista tietokoneelle. Jatkotutkimus vaatii monitieteellistä lähestymistä ennen hyvin tekniseen toimintoon; tänä päivänä tekniikka on vain väline normaaliin yhteiskunnalliseen ja ihmisen sosiaaliseen toimintaan. Ei voida olettaa, että erityisryhmät tai ei-tekniset ihmiset oppivat sähköisen äänestämisen, joten jatkotutkimuskohteena voisi olla miten luodaan tietoturvallinen riittävän yksinkertainen äänestysjärjestelmä, jota kaikki ihmiset osaavat käyttää, esimerkiksi integroiden pieniä osa-alueita perinteiseen äänestämiseen ilman että korvataan koko äänestäminen kerralla sähköisesti.

Lähdeluettelo

Arzt-Mergemeier, J., Beiss, W., & Steffens, T. (2008). The Digital Voting Pen at the Hamburg Elections 2008: Electronic Voting Closest to Conventional Voting. *Lecture Notes in Computer Science* 4896, 88-98.

Balzarotti, D., Banks, G., Cova, M., Felmetsger, V., Kemmerer, R.A., Robertson,W., Valeur, F., & Vigna, G. (2010). An Experience in Testing the Security of Real-World Electronic Voting Systems. *IEEE Transactions on Software Engineering* 36(4), 453 – 473.

Bannet, J., Price, D.W., Rudys, A., Singer, J., Wallach, D.S. (2004). Hack-a-vote: Security issues with electronic voting systems. *IEEE Security &* Privacy January/February 2004, 32-37.

Benoist, E., Anrig, B., Jaquet-Chiffelle, D-O. (2008). Internet-Voting: Opportunity or Threat for Democracy? *Lecture Notes in Computer Science* 4896, *29-37*.

Blaze, M., Braun, J., Hursti, H., Jefferson, D., MacAlpine, M., Moss, J. (2018). Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure. *DEF CON 26 Voting Village,* September 2018.

Cubric, M., Jefferies, A. (2015). The benefits and challenges of large-scale deployment of electronic voting systems: University student views from across different subject groups. *Computers & Education* 87, 98-111.

Culnane, C.B., Ryan, P.Y.A., Schneider, S.B., Teague, V.C. (2015). vVote: A verifiable voting system. *ACM Transactions on Information and System Security* 18(1), 1-30.

Domas, C. (2017). Breaking the x86 ISA.

Gudipati, V. K., Venna, T., Subburaj, S., Abuzaghleh, O. (2016). Advanced Automated SQL Injection Attacks and Defensive Mechanisms. *2016 Annual Connecticut Conference on Industrial Electronics, Technology and Automation, CT-IETA 2016,* Article number 7868248

Lehto, J.E. (2019). Tieteellisen kirjoittamisen ohjeista: Essee, proseminaari, kandidaatintutkielma ja Pro Gradu-tutkielma. Haettu 15.4.2019, saatavilla: https://www.avoin.helsinki.fi/oppimateriaalit/tieteellisen-kirjoittamisen-ohjeet-APA.htm#1

Hisamitsu, H. & Takeda, K. (2008). The Security Analysis of e-Voting in Japan. *Lecture Notes in Computer Science* 4896, *99*-110.

Jefferson, D., Rubin, A.D., Simmons, B., Wagner, D. (2004). Analyzing internet voting security. *Communications of the ACM* 47(10), 59-64.

Kiayias, A., Zacharias, T., Zhang, B. (2017). An Efficient E2E Verifiable E-voting System without Setup Assumptions. *IEEE Security & Privacy* 16, 1-9.

Kshetri, N., Voas, J. (2018). Blockchain-Enabled E-Voting. *IEEE Software* July/August, 95-99

Moran, M., Heather, J., Schneider, S. (2013). Automated anonymity verification of the ThreeBallot and VAV voting systems. *Software & Systems Modeling* 15, 1049-1062.

Radl, A., Chen, Y.-C. (2005). Computer Security in Electronic Government: A State-Local Ecucation Information System. *International Journal of Electronic Government Research* 1(1), 78-99.

Rivest, R.L., Stark, P.B. (2017). When Is an Election Verifiable? IEEE Computer and Reliability *Societies,* May/June, 48-50.

Salminen, A. (2011). Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. *Vaasan yliopiston julkaisuja.* Vaasa.

Schryen, G., Rich, E. (2009). Security in large-scale internet elections: A retrospective analysis of elections in Estonia, the Netherlands, and Switzerland. *IEEE Transactions on Information Forensics and* Security, 4, 729-744.

Simpson, R., Storer, T. (2018). Third-party verifiable voting systems: Addressing motivation and incentives in e-voting. *Journal of Information Security and Applications* 38, 132-138.

Spafford, E.H. (2009). Cyber Security: Assessing our vulnerabilities and developing an effective defence. *Annual Workshop on Information Privacy and National* Security, 20-33.

Springall, D., Finkenauer, T., Durumenic, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, J.A. (2014). Security analysis of the Estonian internet voting system. *Proceedings of the ACM Conference on Computer and Communications Security 2014,* 703-715.

Weldemariam, K., Villafiorita, A., Mattioli, A. (2007). Assessing procedural risks and threats in e-voting: Challenges and an approach. *Lecture Notes in Computer Science* 4896, *37-48*.

Whitman, M.E., Mattord, H.J. (2012). *Principles of Information Security*. Boston: Thomson Course Technology.

Wikipedia. (2019). "Electronic voting". Haettu 15.1.2019, saatavilla: https://en.wikipedia.org/wiki/Electronic_voting .